

Secure Business Communications over Public Networks

A Cisco Small Business Guide to Virtual Private Networks

To the long list of things being transformed by networking technology and the Internet you can now add the corporate wide area network (WAN). For a variety of reasons—cost, flexibility, simplicity, and ease of management—businesses are increasingly using public data networks to connect remote workers, branch offices, customers, partners, and suppliers. The key to doing so securely and privately is the virtual private network (VPN). This paper provides a basic introduction to VPNs for the small business that needs quick, secure, and prioritized connections for mobile users, teleworkers or remote locations, with a minimum of new investment and management overhead.

What Is a VPN?

Put as simply as possible, a VPN is a private network deployed over public facilities that provides similar levels of privacy, security, quality of service, and manageability to networks built entirely on dedicated, privately owned or leased facilities. The term originated in the circuit-switched environment of the telephone industry, where it referred to dynamically allocated, “on demand” connections used to replace dedicated, leased line connections in private networks at a substantial cost savings.

Today, the VPN is an increasingly popular means of using public IP networks to simply and cost-effectively extend corporate data networks to remote operations and mobile users. With the right software and access systems, secure communication becomes possible even over the notoriously wide-open Internet. Correctly implemented VPNs are indistinguishable to users from the corporate LAN environment. They can also be simpler to set up, less costly to operate, and easier to administer than leased line networks.

To better understand the VPN, it may help to consider it in relation to the technology it most often augments or replaces, the private line WAN. A private WAN uses dedicated bandwidth leased from a telephone company to connect distant locations. Because these interoffice lines are private, they provide a high level of inherent security and transmission quality, but the company pays for the allocated bandwidth whether or not it's used, so operating costs tend to be high.

Because high lease rates are an incentive for underdesign, the available bandwidth is sometimes insufficient for peak transmission loads, resulting in bottlenecks and blockages. In addition, the owner of a private WAN must buy, configure, and maintain the terminal equipment required to connect the leased lines to the LAN, and the access modems necessary for dial-up remote access support. All this makes private line networks expensive to build, labor-intensive to maintain, and difficult to reconfigure for rapidly changing business needs.

In contrast, a VPN uses the public data network infrastructure to connect distant locations and remote users, and the owner pays only for the bandwidth actually consumed. Because most bandwidth is idle most of the time, transmission costs are much lower than for dedicated private lines. In addition, transmission rates over virtual networks are not constrained by the capacity of fixed connections, making them much better adapted to the bursty nature of data transmission. Finally, because VPNs are a natural extension of the services offered by Internet service providers (ISPs) and alternative network service providers (NSPs), most companies will have the option of outsourcing all or part of a VPN implementation, eliminating most of the engineering and administrative load on internal IT staff.

Where Are VPNs Used?

Virtual private networks are the technology of choice wherever secure data links are required between a business and its smaller branch operations and mobile personnel, or when network infrastructure must respond quickly to changes in the business environment. The three primary types of VPNs are identified with their most common applications.

Remote Access VPNs use dial-up or broadband (DSL or cable) access to a service provider network to connect remote or mobile users to the company network. By outsourcing access connectivity to a provider with widely distributed local points of presence (POPs), companies can eliminate the cost of long distance access calls and the internal modem banks necessary to receive them. The savings can be very significant.

Intranet VPNs connect main and branch office locations using persistent (always on) connections to a third-party network or the Internet. Because this type of connection is fast and easy to establish, Intranet VPNs make it easy and affordable to provide all employees with full access to the company network, regardless of the size, number, or location of its remote operations.

Extranet VPNs connect a company with its customers, suppliers, and other business partners, providing them with limited access to specific portions of the company network for purposes of collaboration and coordination. Access methods may include both dial up and persistent connections, but all access is subject to rigorous user identification and authorization controls. A major appeal of extranet VPNs is the ease and speed with which secure communications can be extended to new partners, even for temporary, per-project alliances.

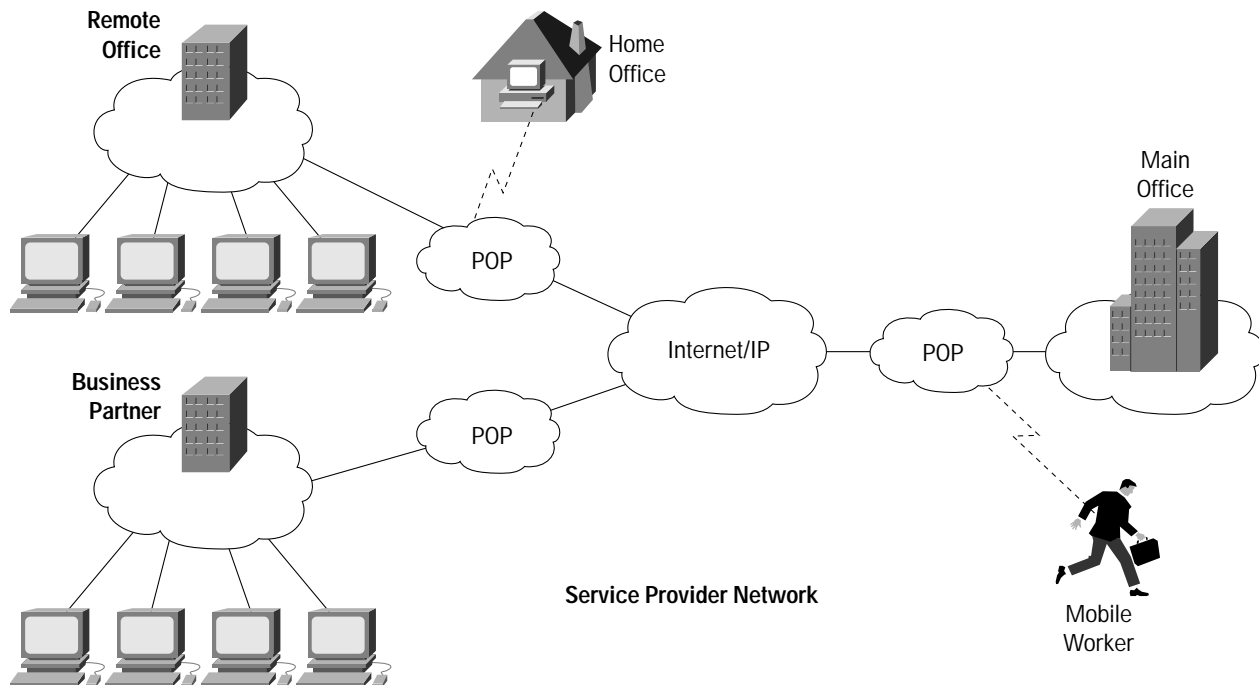
How Does a VPN Work?

In a VPN, a company uses the bandwidth of a public packet-routed network (typically the Internet) or a service provider's backbone network, to establish private, secure connections between its remote offices and employees. Figure 1 shows a typical example, with a company headquarters, remote offices, mobile workers, and partners all connecting to a network service provider's local points of presence (POPs). The company's LANs and remote users are connected to the provider network with the same types of access methods used for Internet access: dial-up, DSL, cable, ISDN, T1, and wireless. The key to this type of internetworking lies in a class of technologies called "tunneling."

Tunneling is the practice of repackaging data from one network in the transmission protocol, or native language, of another. At the originating end of a tunneled transmission, a data packet from the LAN is wrapped, or encapsulated, with new header information that allows an intermediary network to recognize and deliver it. At the terminating end of the transmission, the tunneling protocol "wrapper" is stripped off, and the original packet is transferred to the destination LAN for delivery.

While tunneling allows data to be carried over third party networks, tunneling alone does not ensure privacy. To secure a tunneled transmission against interception and tampering, all traffic over a VPN is typically encrypted for safety. In addition to tunneling and encryption, VPNs typically include additional features to enhance transmission security, ensure quality of service (QoS), and defend the private network perimeter with a firewall. Setting up a VPN requires routing equipment with software-defined VPN capabilities (tunneling, encryption, security, QoS) at each participating location, or at the ISPs nearest point of presence.

Figure 1 A Typical VPN



What Are the Benefits of a VPN?

VPNs offer distinct advantages over traditional leased line networks. Among the most compelling are:

Lower capital and operating costs—The lower cost of transport bandwidth and backbone equipment, plus a reduced need for in-house terminal equipment and access modems all contribute to substantially lower cost of ownership and operation. According to Infonetix, a network management consulting firm, LAN-to-LAN connectivity costs are typically reduced by 20 to 40 percent over private line networks, with cost reduction for remote access in the 60 to 80 percent range.

More agile networks—Because VPN links are easy and relatively inexpensive to set up, add, and remove, communications infrastructure can more easily and responsively support changing business demands. Extending the corporate network to the offices of a new acquisition, or adding new vendors to a supply chain extranet become simple tasks, that are quickly accomplished. By using the Internet as the medium for their internal networks, companies make it possible to extend corporate systems anywhere the Internet is accessible.

Management outsourcing opportunities—With many ISPs lower management and support costs, much of the engineering, management, and administrative workload required to set up and operate a VPN can often be outsourced to a network service provider. VPNs let companies concentrate on core business and reduce the overall resources they devote to IT and communications infrastructure.

Anywhere, anytime access—VPN subscribers across the extended network have the same access and logical view of central services such as e-mail, directory, internal, and external Web sites, security, and other shared applications. Although they may reach these resources over very different paths, the underlying network is transparent to the user.

Features of a VPN: A Checklist for Successful Networking

Three characteristics distinguish a VPN from normal IP data transmissions: security, the ability to manage different types of traffic for optimum quality, and the availability of management tools to configure, monitor, and control network devices. The degree to which any particular network exhibits these characteristics, as well as its ultimate scalability, depend largely on the access systems selected for the network periphery. Several different feature sets should be carefully compared.

- *Security features* include all the capabilities that contribute to keeping VPN traffic private and secure. These include tunneling, encryption, packet authentication, firewalls, and user identification, to name just a few.
- *Tunneling capability*, which was discussed earlier, is the feature that allows all other security and transmission quality measures to be imposed on the Internet environment. Important tunneling protocols supported by all Cisco VPN systems include:

IPSec	IP Security Protocol
L2TP	Layer 2 Tunneling Protocol
GRE	Generic Route Encapsulation

- *Encryption* puts the privacy in a virtual network, and is essential for secure communications. In a VPN, encryption is applied to a tunneled connection to scramble the data, making it indecipherable to unauthorized viewers. Important standards for encryption include:
 - IPSec: An IETF standard in development for multilevel encryption, including Public Key Infrastructure (PKI) for user authentication
 - DES: Data Encryption Standard. A 56 bit, secret key encryption system
 - 3DES: Triple DES. DES applied three times for effective 168 bit secret key security
- *Packet integrity* features protect against data tampering by applying a header to each packet that reveals any attempt to modify the contents.
- *Firewalls* protect the private network from unauthorized entry by examining each packet at the network perimeter and allowing or prohibiting passage based on user-defined rules restricting origin, destination, or application.
- *User and device authentication*, authorization, and accounting provides reliable identification of all users and identity-based access control to sensitive network resources.


Quality of service (QoS) and bandwidth management features are what allow a VPN to deliver high transmission quality for time-sensitive applications such as voice and video. Each packet is tagged to identify the priority and time sensitivity of its payload, and traffic is sorted and routed based on its delivery priority. Cisco VPN solutions support a wide range of QoS features, including:

- Committed Access Rate (CAR)
- Policy Routing
- Weighted Fair Queuing (WFQ)
- Generic Traffic Shaping (GTS)
- Resource Reservation Protocol (RSVP)

It is important to understand that quality of service cannot be completely controlled independently of the underlying network. Users must confirm with a potential service provider that its network can support priority services over a VPN.

Network management features simplify the addition or deletion of users, software upgrades, and policy management for security and QoS assurance. They are essential tools in controlling the management costs of VPN infrastructure, and important factors in its scalability. An additional consideration unique to VPNs is that a network owner may choose to outsource some amount of network management responsibility to its service provider, making interoperability between corporate and vendor management tools a critical issue.

Cisco VPN solutions support a comprehensive suite of management tools designed to provide simple, secure, cost-effective device configuration, policy management, and monitoring for any size VPN. These tools employ the same features used in the management of large Cisco Powered service provider networks, and interoperate smoothly with those systems, giving owner and provider a consistent view of network operation and a platform for collaborative management.



Working with Service Providers and VARs

Establishing a VPN requires, at minimum, access to the Internet or an alternative, private IP network arranged through an ISP or network service provider (NSP). Many of these firms also offer design and management services specifically aimed at VPN implementation, ranging in breadth from simple connectivity to total outsource solutions. It should be understood that a VPN service provider becomes a long-term partner in a basic element of business infrastructure, and the selection should be made carefully and on the basis of well-defined expectations. A list of Cisco Powered Network providers can be found on the Web at <http://www.cisco.com/warp/customer/779/servpro/cpn/>.

For smaller networks a value-added reseller (VAR) can often be very helpful. These are typically systems and network engineering specialists who provide Cisco VPN access hardware and control software as part of a design solution. They may or may not also provide network access.

Cisco VPN Solutions for Small and Medium Sized Networks

VPN solutions can be built on integrated router platforms or multi-device systems using separate routers, firewalls, and bandwidth managers. In the broadest view, integrated solutions offer the simplest and most cost-effective solution, while multi-device systems using specialized appliances can provide greater performance and more rigorous security. Cisco provides an open implementation architecture that includes VPN optimized routers with software defined firewall and bandwidth management capabilities as well as high performance VPN and firewall appliances. Cisco IOS software ensures interoperability between devices and across the Internet.

Cisco 800 series routers provide secure ISDN, Serial, and DSL access to the Internet and the corporate LAN. By incorporating Cisco IOS VPN Software feature set that include tunneling, encryption, QoS, and dynamic firewall protection, Cisco 800 routers extend VPN applications to telecommuters and small offices. The 800 series includes nine router models in various WAN flavors and a choice of software feature sets.

Cisco 1700 modular access routers provide all the necessary components required to build an integrated VPN solution on one platform. The Cisco 1700 is optimized to support VPN applications with full IOS software support for encryption, tunneling (L2TP, IPSec, and GRE), quality of service management, and dynamic firewall protection. 1700 series routers also offer optional hardware-assisted encryption for 3DES encryption at full-duplex T1/E1 speeds without compression. This all-in-one VPN solution minimizes setup costs and simplifies deployment and management of VPNs in small branch offices and small to medium sized businesses.

Cisco 2600 series modular access routers accommodate a wide range of serial, channelized, ISDN, and modem interfaces, allowing them to support robust intranet, extranet, and remote access VPNs. Built on a powerful RISC processor, 2600 series routers provide ample speed and throughput for CPU-intensive tunneling, encryption, and QoS management features. Like all IOS powered Cisco routers, the 2600 series provides secure stateful firewall protection for the internal network. Cisco 2600 routers are sized for medium sized branch offices and businesses of around 100 employees.

Cisco PIX firewalls are dedicated firewall appliances that offer an unprecedented level of network security in multi-device VPN implementations. PIX firewalls provide stateful inspection access control based on Adaptive Security Algorithm (ASA), an exclusive session state monitoring technology. When deployed as part of a VPN, PIX firewalls provide data encryption and firewall protection, while routing, tunneling, and QoS functions are handled by the access router.

Cisco Secure VPN Client

The Cisco Secure VPN Client enables secure connectivity for remote access VPNs, including e-commerce, mobile user, and telecommuting applications. The Cisco Secure VPN Client provides Microsoft Windows 95/98 and NT 4.0 users with a complete implementation of IPSec standards.

Cisco VPN 3000 Concentrator

The Cisco VPN 3000 Concentrator Series is a family of purpose-built, remote access VPN platforms and client software that incorporates high availability, high performance, and scalability with the most advanced encryption and authentication techniques available today. With the Cisco VPN 3000 Concentrator Series, customers can take advantage of the latest VPN technology to vastly reduce their communications expenditures. Unique to the industry, it is the only scalable platform to offer field-swappable and customer-upgradable components.

Cisco IOS Software

Cisco IOS software provides the intelligence behind the Internet, and is the operating system on all Cisco access routers. It provides reliable routing and protocol management across the widest range of media, with security features that include access control lists; user authentication, authorization, and accounting; and data encryption.

Cisco Secure Integrated Software, an optional software firewall solution for Cisco routers, enriches the existing security capabilities of IOS software with robust stateful firewall, intrusion detection (not supported on 800 series routers), DES and 3DES encryption, and secure administration capabilities. This integrated security solution enables sophisticated policy enforcement throughout the network and leverages an organization's investment in Cisco infrastructure.

Call On Cisco for a Better VPN Connection

Cisco VPN solutions offer small businesses a perfectly integrated set of hardware and software tools for building secure private networks over cost-effective public IP infrastructure. Cisco VPN solutions provide the most rigorous security protections, quality of service features, and network management support available. They ensure scalability and offer a defined migration path for fast growing businesses, giving them the flexibility they need to prosper in a dynamic commercial environment. For more information on Cisco solutions for virtual private networks, visit Cisco Systems online at <http://www.cisco.com>.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000, Cisco Systems, Inc. All rights reserved. Printed in the USA. Access Registrar, AccessPath, Any to Any, Are You Ready, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMux, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0007R) 9/00 LW