

How Virtual Private Networks Work

Introduction

This document covers the fundamentals of VPNs, such as basic VPN components, technologies, tunneling, and VPN security.

Background Information

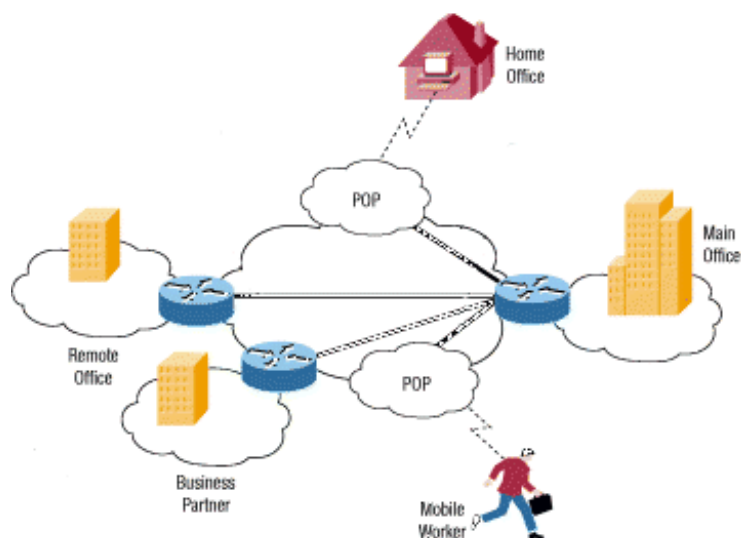
The world has changed a lot in the last couple of decades. Instead of simply dealing with local or regional concerns, many businesses now have to think about global markets and logistics. Many companies have facilities spread out across the country, or even around the world. But there is one thing that all companies need: a way to maintain fast, secure, and reliable communications wherever their offices are located.

Until recently, reliable communication has meant the use of leased lines to maintain a wide-area network (WAN). Leased lines, ranging from Integrated Services Digital Network (ISDN, which runs at 144 Kbps) to Optical Carrier-3 (OC3, which runs at 155 Mbps) fiber, provide a company with a way to expand their private network beyond their immediate geographic area. A WAN has obvious advantages over a public network like the Internet when it comes to reliability, performance, and security; but maintaining a WAN, particularly when using leased lines, can become quite expensive (it often rises in cost as the distance between the offices increases). Additionally, leased lines are not a viable solution for organizations where part of the work force is highly mobile (as is the case with the marketing staff) and might frequently need to connect to the corporate network remotely and access sensitive data.

As the popularity of the Internet has grown, businesses have turned to it as a means of extending their own networks. First came intranets, which are sites designed for use only by company employees. Now, many companies create their own Virtual Private Networks (VPNs) to accommodate the needs of remote employees and distant offices.

A typical VPN might have a main local-area network (LAN) at the corporate headquarters of a company, other LANs at remote offices or facilities, and individual users that connect from out in the field.

A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection, such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.



What Makes a VPN?

There are two common types of VPNs.

- **Remote-Access**—Also called a Virtual Private Dial-up Network (VPDN), this is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN provides some form of Internet dial-up account to their users using an Internet service provider (ISP). The telecommuters can then dial a 1-800 number to reach the Internet and use their VPN client software to access the corporate network. A good example of a

company that needs a remote-access VPN would be a large firm with hundreds of sales people in the field. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.

- **Site-to-Site**—Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Each site needs only a local connection to the same public network, thereby saving money on long private leased-lines. Site-to-site VPNs can be further categorized into intranets or extranets. A site-to-site VPN built between offices of the same company is said to be an intranet VPN, while a VPN built to connect the company to its partner or customer is referred to as an extranet VPN.

A well-designed VPN can greatly benefit a company. For example, it can:

- Extend geographic connectivity
- Reduce operational costs versus traditional WANs
- Reduce transit times and traveling costs for remote users
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support
- Provide faster Return On Investment (ROI) than traditional WAN

What features are needed in a well-designed VPN? It should incorporate these items:

- Security
- Reliability
- Scalability
- Network Management
- Policy Management

Analogy: Each LAN Is an IsLAND

Imagine that you live on an island in a huge ocean. There are thousands of other islands all around you, some very close and others farther away. The normal way to travel is to take a ferry from your island to whichever island you wish to visit. Traveling on a ferry means that you have almost no privacy. Anything you do can be seen by someone else.

Assume that each island represents a private LAN and the ocean is the Internet. When you travel by ferry, it is similar to when you connect to a web server or to another device through the Internet. You have no control over the wires and routers that make up the Internet, just like you have no control over the other people on the ferry. This leaves you susceptible to security issues if you try to connect between two private networks using a public resource.

Your island decides to build a bridge to another island so that there is an easier, more secure and direct way for people to travel between the two. It is expensive to build and maintain the bridge, even though the island you are connecting with is very close. But the need for a reliable, secure path is so great that you do it anyway. Your island would like to connect to a second island that is much farther away, but you decide that it is too expensive.

This situation is very much like having a leased line. The bridges (leased lines) are separate from the ocean (Internet), yet they are able to connect the islands (LANs). Many companies have chosen this route because of the need for security and reliability in connecting their remote offices. However, if the offices are very far apart, the cost can be prohibitively high - just like trying to build a bridge that spans a great distance.

So how does VPN fit in to this analogy? We could give each inhabitant of our islands their own small submarine with these properties.

- It is fast.
- It is easy to take with you wherever you go.
- It is able to completely hide you from any other boats or submarines.
- It is dependable.
- It costs little to add additional submarines to your fleet once the first is purchased.

Although they are traveling in the ocean along with other traffic, the inhabitants of our two islands could travel back and forth whenever they wanted to with privacy and security. That is essentially how a VPN works. Each remote member of your network can communicate in a secure and reliable manner using the Internet as the medium to connect to the private LAN. A VPN can grow to accommodate more users and different locations much easier than a leased line. In fact, scalability is a major advantage that VPNs have over typical leased lines. Unlike leased lines where the cost increases in proportion to the distances involved, the geographic locations of each office matter little in the creation of a VPN.

VPN Technologies

A well-designed VPN uses several methods in order to keep your connection and data secure.

- **Data Confidentiality**—This is perhaps the most important service provided by any VPN implementation. Since your private data travels over a public network, data confidentiality is vital and can be attained by encrypting the data. This is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.


Most VPNs use one of these protocols to provide encryption.

- **IPsec**—Internet Protocol Security Protocol (IPsec) provides enhanced security features such as stronger encryption algorithms and more comprehensive authentication. IPsec has two encryption modes: tunnel and transport. Tunnel mode encrypts the header and the payload of each packet while transport mode only encrypts the payload. Only systems that are IPsec-compliant can take advantage of this protocol. Also, all devices must use a common key or certificate and must have very similar security policies set up.

For remote-access VPN users, some form of third-party software package provides the connection and encryption on the users PC. IPsec supports either 56-bit (single DES) or 168-bit (triple-DES) encryption.

- **PPTP/MPPE**—PPTP was created by the PPTP Forum, a consortium which includes US Robotics, Microsoft, 3COM, Ascend, and ECI Telematics. PPTP supports multi-protocol VPNs, with 40-bit and 128-bit encryption using a protocol called Microsoft Point-to-Point Encryption (MPPE). It is important to note that PPTP by itself does not provide data encryption.
 - **L2TP/IPsec**—Commonly called L2TP over IPsec, this provides the security of the IPsec protocol over the tunneling of Layer 2 Tunneling Protocol (L2TP). L2TP is the product of a partnership between the members of the PPTP forum, Cisco, and the Internet Engineering Task Force (IETF). Primarily used for remote-access VPNs with Windows 2000 operating systems, since Windows 2000 provides a native IPsec and L2TP client. Internet Service Providers can also provide L2TP connections for dial-in users, and then encrypt that traffic with IPsec between their access-point and the remote office network server.
- **Data Integrity**—While it is important that your data is encrypted over a public network, it is just as important to verify that it has not been changed while in transit. For example, IPsec has a mechanism to ensure that the encrypted portion of the packet, or the entire header and data portion of the packet, has not been tampered with. If tampering is detected, the packet is dropped. Data integrity can also involve authenticating the remote peer.
 - **Data Origin Authentication**—It is extremely important to verify the identity of the source of the

data that is sent. This is necessary to guard against a number of attacks that depend on spoofing the identity of the sender.

- **Anti Replay**—This is the ability to detect and reject replayed packets and helps prevent spoofing.
- **Data Tunneling/Traffic Flow Confidentiality**—Tunneling is the process of encapsulating an entire packet within another packet and sending it over a network. Data tunneling is helpful in cases where it is desirable to hide the identity of the device originating the traffic. For example, a single device that uses IPsec encapsulates traffic that belongs to a number of hosts behind it and adds its own header on top of the existing packets. By encrypting the original packet and header (and routing the packet based on the additional layer 3 header added on top), the tunneling device effectively hides the actual source of the packet. Only the trusted peer is able to determine the true source, after it strips away the additional header and decrypts the original header. As noted in [RFC 2401](#) , "...disclosure of the external characteristics of communication also can be a concern in some circumstances. Traffic flow confidentiality is the service that addresses this latter concern by concealing source and destination addresses, message length, or frequency of communication. In the IPsec context, using ESP in tunnel mode, especially at a security gateway, can provide some level of traffic flow confidentiality."

All the encryption protocols listed here also use tunneling as a means to transfer the encrypted data across the public network. It is important to realize that tunneling, by itself, does not provide data security. The original packet is merely encapsulated inside another protocol and might still be visible with a packet-capture device if not encrypted. It is mentioned here, however, since it is an integral part of how VPNs function.

Tunneling requires three different protocols.

- **Passenger protocol**—The original data (IPX, NetBeui, IP) that is carried.
- **Encapsulating protocol**—The protocol (GRE, IPsec, L2F, PPTP, L2TP) that is wrapped around the original data.
- **Carrier protocol**—The protocol used by the network over which the information is traveling.

The original packet (Passenger protocol) is encapsulated inside the encapsulating protocol, which is then put inside the carrier protocol's header (usually IP) for transmission over the public network. Note that the encapsulating protocol also quite often carries out the encryption of the data. Protocols such as IPX and NetBeui, which would normally not be transferred across the Internet, can safely and securely be transmitted.

For site-to-site VPNs, the encapsulating protocol is usually IPsec or Generic Routing Encapsulation (GRE). GRE includes information on what type of packet you are encapsulating and information about the connection between the client and server.

For remote-access VPNs, tunneling normally takes place using Point-to-Point Protocol (PPP). Part of the TCP/IP stack, PPP is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. PPP tunneling will use one of PPTP, L2TP or Cisco's Layer 2 Forwarding (L2F).

- **AAA**—Authentication, authorization, and accounting is used for more secure access in a remote-access VPN environment. Without user authentication, anyone who sits at a laptop/PC with pre-configured VPN client software can establish a secure connection into the remote network. With user authentication however, a valid username and password also has to be entered before the connection is completed. Usernames and passwords can be stored on the VPN termination device itself, or on an external AAA server, which can provide authentication to numerous other databases such as Windows NT, Novell, LDAP, and so on.

When a request to establish a tunnel comes in from a dial-up client, the VPN device prompts for a username and password. This can then be authenticated locally or sent to the external AAA server, which checks:

- Who you are (Authentication)

- What you are allowed to do (Authorization)
- What you actually do (Accounting)

The Accounting information is especially useful for tracking client use for security auditing, billing or reporting purposes.

- **Nonrepudiation**—In certain data transfers, especially those related to financial transactions, nonrepudiation is a highly desirable feature. This is helpful in preventing situations where one end denies having taken part in a transaction. Much like a bank requires your signature before honoring your check, nonrepudiation works by attaching a digital signature to the sent message, thus precluding the possibility of sender denying participation in the transaction.

A number of protocols exist that can be used to build a VPN solution. All of these protocols provide some subset of the services listed in this document. The choice of a protocol depends on the desired set of services. For example, an organization might be comfortable with the data being transferred in clear text but extremely concerned about maintaining its integrity, while another organization might find maintaining data confidentiality absolutely essential. Their choice of protocols might thus be different. For more information on the protocols available and their relative strengths, refer to [Which VPN Solution is Right for You?](#)

VPN Products

Based on the type of VPN (remote-access or site-to-site), you need to put in place certain components to build your VPN. These might include:

- Desktop software client for each remote user
- Dedicated hardware such as a Cisco VPN Concentrator or a Cisco Secure PIX Firewall
- Dedicated VPN server for dial-up services
- Network Access Server (NAS) used by service provider for remote user VPN access
- Private network and policy management center

Because there is no widely accepted standard for implementing a VPN, many companies have developed turn-key solutions on their own. For example, Cisco offers several VPN solutions that include:

- **VPN Concentrator**—Incorporating the most advanced encryption and authentication techniques available, Cisco VPN Concentrators are built specifically for creating a remote-access or site-to-site VPN and ideally are deployed where the requirement is for a single device to handle a very large number of VPN tunnels. The VPN Concentrator was specifically developed to address the requirement for a purpose-built, remote-access VPN device. The concentrators provide high availability, high performance and scalability and include components, called Scalable Encryption Processing (SEP) modules, that enable users to easily increase capacity and throughput. The concentrators are offered in models suitable for small businesses with 100 or fewer remote-access users to large enterprise organizations with up to 10,000 simultaneous remote users.



- **VPN-Enabled Router/VPN-Optimized Router**—All Cisco routers that run Cisco IOS® software support IPsec VPNs. The only requirement is that the router must run a Cisco IOS image with the appropriate feature set. The Cisco IOS VPN solution fully supports remote access, intranet and extranet VPN requirements. This means that Cisco routers can work equally well when connected to a remote host running VPN Client software or when connected to another VPN

device such as a router, PIX Firewall or VPN Concentrator. VPN-enabled routers are appropriate for VPNs with moderate encryption and tunneling requirements and provide VPN services entirely through Cisco IOS software features. Examples of VPN-enabled routers include the Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500, and Cisco 4700 series.

Cisco's VPN-optimized routers provide scalability, routing, security, and Quality of Service (QoS). The routers are based on the Cisco IOS software, and there is a device suitable for every situation, from small-office/home-office (SOHO) access through central-site VPN aggregation to large-scale enterprise needs. VPN-optimized routers are designed to meet high encryption and tunneling requirements and often make use of additional hardware such as encryption cards to achieve high performance. Examples of VPN-optimized routers include the Cisco 800, Cisco 1700, Cisco 2600, Cisco 3600, Cisco7200, and Cisco7500 series.



- **Cisco Secure PIX Firewall**—The Private Internet eXchange (PIX) Firewall combines dynamic network address translation, proxy server, packet filtration, firewall, and VPN capabilities in a single piece of hardware. Instead of using Cisco IOS software, this device has a highly streamlined operating system that trades the ability to handle a variety of protocols for extreme robustness and performance by focusing on IP. As with Cisco routers, all PIX Firewall models support IPsec VPN. All that is required is that the licensing requirements to enable the VPN feature must be met.



- **Cisco VPN Clients**—Cisco offers both hardware and software VPN clients. The Cisco VPN Client (software) comes bundled with the Cisco VPN 3000 Series Concentrator at no additional cost. This software client can be installed on the host machine and used to connect securely to the central site concentrator (or to any other VPN device such as a router or firewall). The VPN 3002 Hardware Client is an alternative to deploying the VPN Client software on every machine and provides VPN connectivity to a number of devices.

The choice of devices that you would use to build your VPN solution is ultimately a design issue that depends on a number of factors, including the desired throughput and the number of users. For example, on a remote site with a handful of users behind a PIX 501, you could consider configuring the existing PIX as the IPsec VPN endpoint, provided that you accept the 501's 3DES throughput of roughly 3 Mbps and the limit of a maximum of 5 VPN peers. On the other hand, on a central site acting as a VPN endpoint for a large number of VPN tunnels, going in for a VPN-optimized router or a VPN concentrator would probably be a good idea. The choice now would depend on the type (LAN-to-LAN or remote access) and number of VPN tunnels being set up. The wide range of Cisco devices that support VPN provides the network designers with a high amount of flexibility and a robust solution to meet every design need.