Cisco − How Virtual Private Networks Work

Table of Contents

How Virtual Private Networks Work

Related Topics
Additional Documentation

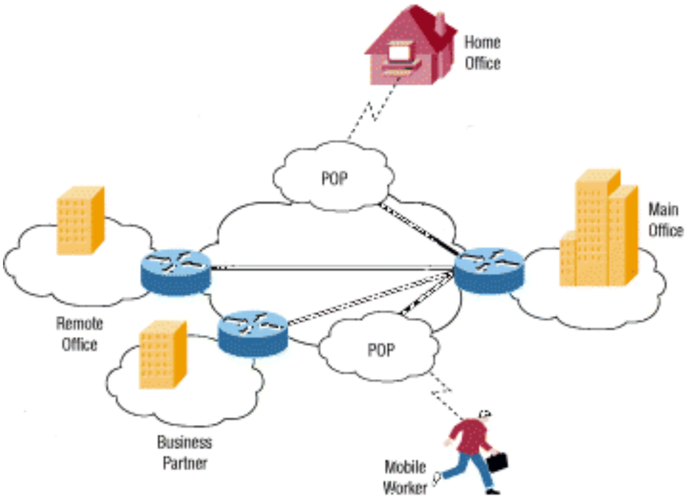
Introduction

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

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).

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 are creating 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 connecting from out in the field.

Basically 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 built between offices of the same company, or, for example, to an external supplier to share a database for product ordering.

A well−designed VPN can greatly benefit a company. For example, it can do the following:

- Extend geographic connectivity
- Improve security
- 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 the following:

- 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. Of course, traveling on a ferry means that you have almost no privacy. Anything you do can be seen by someone else.

Let's say that each island represents a private LAN and the ocean is the Internet. Traveling by ferry is like connecting to a Web server or to another other 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 are trying to connect between two private networks using a public resource.

Continuing with our analogy, 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 the cost are simply too much to bear.

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 the following amazing properties:

- It's fast.

- It's easy to take with you wherever you go.

- It's able to completely hide you from any other boats or submarines.

- It's 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's 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 for keeping your connection and data secure:

- **Data Encryption** − Since your private data is traveling over a public network, data encryption is vital. It 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 the following 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 Authentication** − While it is important that your data is encrypted over a public network, it is just as important to verify that it hasn't been changed while in transit also. IPSec for example, can authenticate the encrypted portion of the packet, or the entire header and data portion of the packet to verify its integrity.

- **Data Tunneling** − Tunneling is the process of encapsulating an entire packet within another packet and sending it over a network. All the encryption protocols listed above 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, but it is still visible with a packet capture device. 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) being 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. As you can see, 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 sitting 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 will also have 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 the following:

    - 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.

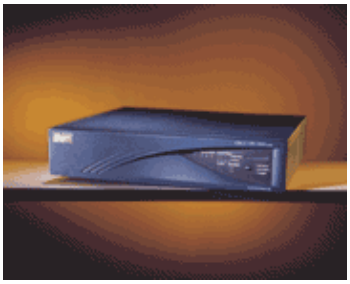
VPN Products

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

- 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 including the following:

- **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. They 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−optimized router** − Cisco's VPN−optimized routers provide scalability, routing, security, and Quality of Service (QoS). Based on the Cisco Internetwork Operating System (IOS)® software, there is a router suitable for every situation, from small−office/home−office (SOHO) access through central−site VPN aggregation, to large−scale enterprise needs.

- **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 OS that trades the ability to handle a variety of protocols for extreme robustness and performance by focusing on IP.

Tools Information

For additional troubleshooting resources, refer to Cisco TAC Tools for VPN Technologies.

Related Information

- **VPN Top Issues**
- **Cisco VPN 3000 Concentrator and Client Technical Tips**
- **Cisco VPN 3000 Concentrator Support Pages**
- **Cisco VPN 3000 Client Support Pages**
- **IP Security (IPSec) Product Support Pages**
- **Virtual Private Networks (VPNs)**

Related Topics

- **Understanding VPDN**
- **A Primer for Implementing a Cisco Virtual Private Network**
- **Cisco Secure PIX Firewall Series**
- **RFC 1661: The Point−to−Point Protocol (PPP)**
- **RFC 2661: Layer Two Tunneling Protocol "L2TP"**

Additional Documentation

- **How Stuff Works: How Virtual Private Networks Work**
- **Overview of VPNs**
- **Tom Dunigan's VPN Page**
- **Virtual Private Network Consortium**