How Virtual Private Networks Work

by Jeff Tyson

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 around the world, and there is one thing that all of them need: A way to maintain fast, secure and reliable communications wherever their offices are.

Special thanks to Cisco Systems, Inc., for its support in creating this article.

Until fairly recently, this has meant the use of **leased lines** to maintain a **wide area network** (WAN). Leased lines, ranging from ISDN (integrated services digital network, 128 Kbps) to OC3 (Optical Carrier-3, 155 Mbps) fiber, provided a company with a way to expand its private network beyond its immediate geographic area. A WAN had obvious advantages over a public network like the Internet when it came to reliability, performance and security. But maintaining a WAN, particularly when using leased lines, can become quite expensive and often rises in cost as the distance between the offices increases.

As the popularity of the Internet grew, businesses turned to it as a means of extending their own networks. First came **intranets**, which are password-protected sites designed for use only by company employees. Now, many companies are creating their own **VPN** (**virtual private network**) to accommodate the needs of remote employees and distant offices.

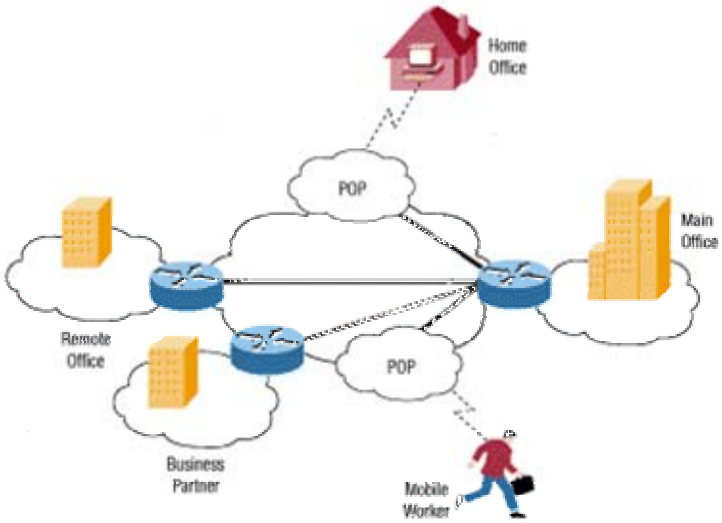


Image courtesy Cisco Systems, Inc.

A typical VPN might have a main 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. In this edition of **HowStuffWorks**, you will gain a fundamental understanding of VPNs, and learn about basic VPN components, technologies, tunneling and security.

What Makes A VPN?

There are two common VPN types:

- **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 will outsource to an **enterprise service provider** (**ESP**). The ESP sets up a **network access server** (**NAS**) and provides the remote users with desktop client software for their computers. The telecommuters can then dial a toll-free number to reach the NAS 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. Site-to-site VPNs can be either:
  - **Intranet-based** - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.
  - **Extranet-based** - When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

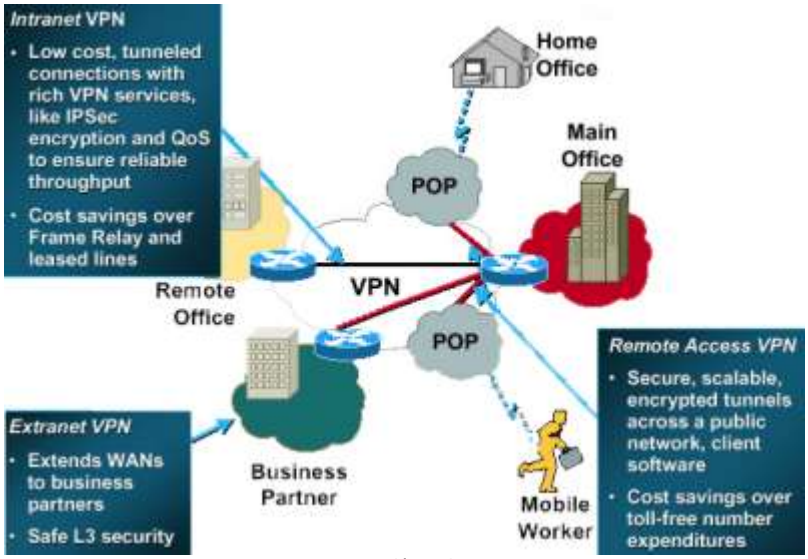


Image courtesy Cisco Systems, Inc.
Examples of the three types of VPN

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

- Extend geographic connectivity
- Improve security
- Reduce operational costs versus traditional WAN
- Reduce transit time and transportation costs for remote users

- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support
- Provide broadband networking compatibility
- Provide faster ROI (return on investment) than traditional WAN

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

- 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 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 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 decides that the cost are simply too much to bear.

This is very much like having a leased line. The bridges (leased lines) are separate from the ocean (Internet), yet 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? Using our analogy, we could give each inhabitant of our islands a small submarine. Let's assume that your submarine has some 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.

In our analogy, each person having a submarine is like a remote user having access to the company's private network.

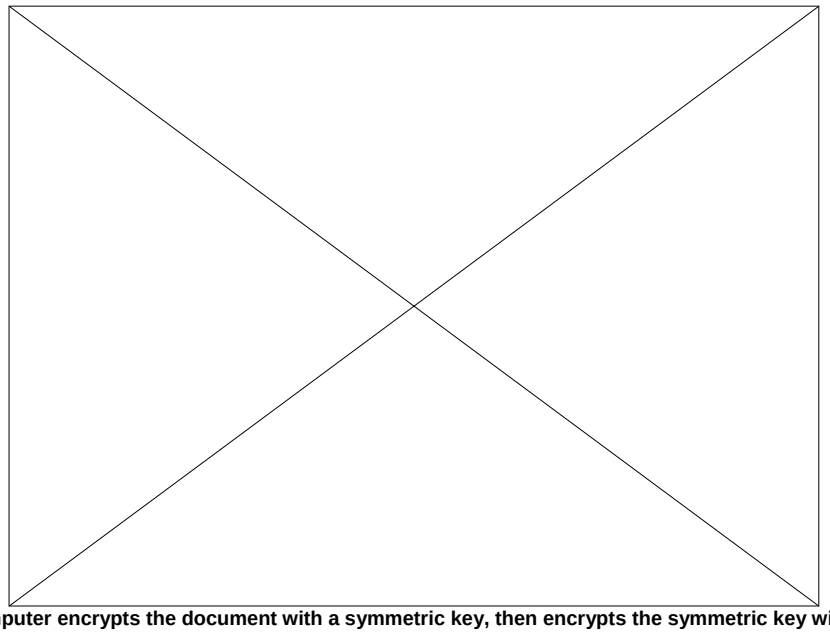
Although they are traveling in the ocean along with other traffic, the inhabitants of our two islands could travel back and forth whenever they wanted to with privacy and security. That's essentially how a VPN works. Each remote member of your network can communicate in a secure and reliable manner using 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 with 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 Security

A well-designed VPN uses several methods for keeping your connection and data secure:

- **Firewalls** - A firewall provides a strong barrier between your private network and the Internet. You can set firewalls to restrict the number of open ports, what type of packets are passed through and which protocols are allowed through. Some VPN products, such as Cisco's 1700 routers, can be upgraded to include firewall capabilities by running the appropriate Cisco IOS on them. You should already have a good firewall in place before you implement a VPN, but a firewall can also be used to terminate the VPN sessions.
- **Encryption** - 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 computer encryption systems belong in one of two categories:
    - Symmetric-key encryption
    - Public-key encryption

In **symmetric-key encryption**, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message. Think of it like this: You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So "A" becomes "C," and "B" becomes "D". You have already told a trusted friend that the code is "Shift by 2". Your friend gets the message and decodes it. Anyone else who sees the message will see only nonsense.



The sending computer encrypts the document with a symmetric key, then encrypts the symmetric key with the public key of the receiving computer. The receiving computer uses its private key to decode the symmetric key. It then uses the symmetric key to decode the document.

Public-key encryption uses a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. A very popular public-key encryption utility is called **Pretty Good Privacy** (PGP), which allows you to encrypt almost anything. You can find out more about PGP at the PGP site.

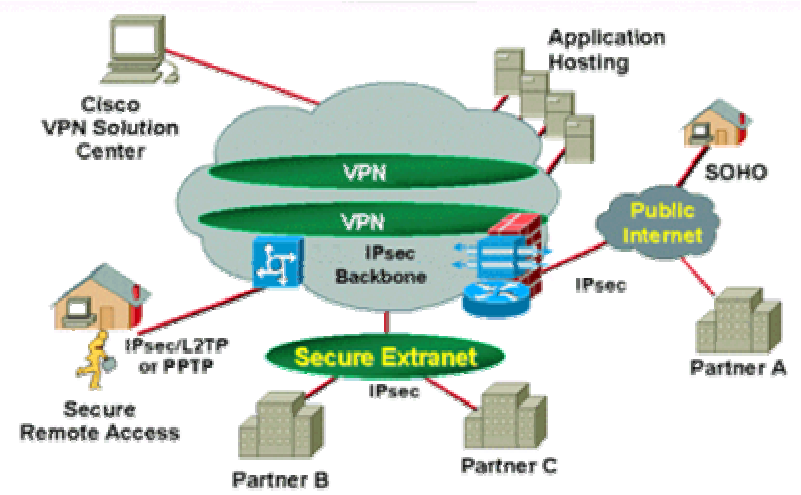


Photo courtesy Cisco Systems, Inc.
A remote-access VPN utilizing IPSec

- **IPSec** - Internet Protocol Security Protocol (IPSec) provides enhanced security features such as better encryption algorithms and more comprehensive authentication. IPSec has two encryption modes: **tunnel** and **transport**. Tunnel encrypts the header and the payload of each packet while transport only encrypts the payload. Only systems that are IPSec compliant can take advantage of this protocol. Also, all devices must use a common key and the firewalls of each network must have very similar security policies set up. IPSec can encrypt data between various devices, such as:
  - Router to router
  - Firewall to router
  - PC to router
  - PC to server
- **AAA Server** - AAA (authentication, authorization and accounting) servers are used for more secure access in a remote-access VPN environment. When a request to establish a session comes in from a dial-up client, the request is proxied to the AAA server. AAA then 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 Technologies

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:

- Desktop software client for each remote user
- Dedicated hardware such as a VPN concentrator or secure PIX firewall
- Dedicated VPN server for dial-up services
- NAS (network access server) used by service provider for remote-user VPN access
- VPN 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:

- **VPN concentrator** - Incorporating the most advanced encryption and authentication techniques available, Cisco VPN concentrators are built specifically for creating a remote-access 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 everything from small businesses with up to 100 remote-access users to large organizations with up to 10,000 simultaneous remote users.

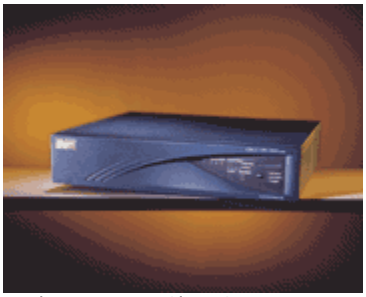


Photo courtesy Cisco Systems, Inc.
The Cisco VPN 3000 Concentrator

- **VPN-optimized router** - Cisco's VPN-optimized routers provide scalability, routing, security and QoS (quality of service). Based on the Cisco **IOS** (Internet Operating System) 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.

Photo courtesy Cisco Systems, Inc.
The Cisco 1750 Modular Access Router

- **Cisco secure PIX firewall** - An amazing piece of technology, the PIX (private Internet exchange) firewall combines dynamic network address translation, proxy server, packet filtration, firewall and VPN capabilities in a single piece of hardware.

Photo courtesy Cisco Systems, Inc.
The Cisco PIX Firewall

Instead of using Cisco IOS, 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.

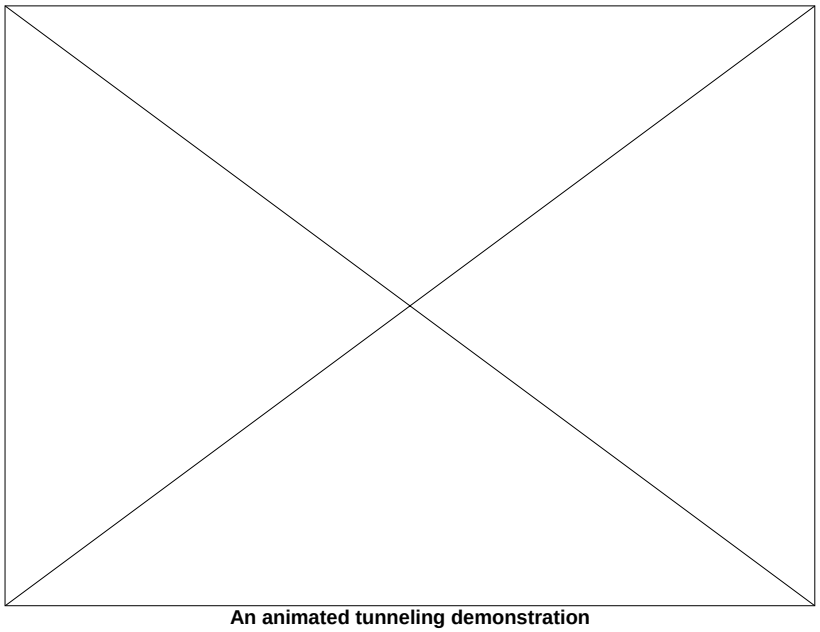
Tunneling

Most VPNs rely on **tunneling** to create a private network that reaches across the Internet. Essentially, tunneling is the process of placing an entire packet within another packet and sending it over a network. The protocol of the outer packet is understood by the network and both points, called **tunnel interfaces**, where the packet enters and exits the network.

Tunneling requires three different protocols:

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

Tunneling has amazing implications for VPNs. For example, you can place a packet that uses a protocol not supported on the Internet (such as NetBeui) inside an IP packet and send it safely over the Internet. Or you could put a packet that uses a private (non-routable) IP address inside a packet that uses a globally unique IP address to extend a private network over the Internet.



An animated tunneling demonstration

In a site-to-site VPN, **GRE** (**generic routing encapsulation**) is normally the encapsulating protocol that provides the framework for how to package the passenger protocol for transport over the carrier protocol, which is typically IP-based. This includes information on what type of packet you are encapsulating and information about the connection between the client and server. Instead of GRE, IPSec in **tunnel mode** is sometimes used as the encapsulating protocol. IPSec works well on both remote-access and site-to-site VPNs. IPSec must be supported at both tunnel interfaces to use.

In a remote-access VPN, tunneling normally takes place using 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. Remote-access VPN tunneling relies on PPP.

Each of the protocols listed below were built using the basic structure of PPP and are used by remote-access VPNs.

- **L2F** (Layer 2 Forwarding) - Developed by Cisco, L2F will use any authentication scheme supported by PPP.
- **PPTP** (Point-to-Point Tunneling Protocol) - PPTP was created by the PPTP Forum, a consortium which includes US Robotics, Microsoft, 3COM, Ascend and ECI Telematics. PPTP supports 40-bit and 128-bit encryption and will use any authentication scheme supported by PPP.
- **L2TP** (Layer 2 Tunneling Protocol) - L2TP is the product of a partnership between the members of the PPTP Forum, Cisco and the IETF (Internet Engineering Task Force). Combining features of both PPTP and L2F, L2TP also fully supports IPSec.

L2TP can be used as a tunneling protocol for site-to-site VPNs as well as remote-access VPNs. In fact, L2TP can create a tunnel between:

- Client and router
- NAS and router
- Router and router

The truck is the carrier protocol, the box is the encapsulating protocol and the computer is the passenger protocol.

Think of tunneling as having a computer delivered to you by UPS. The vendor packs the computer (passenger protocol) into a box (encapsulating protocol) which is then put on a UPS truck (carrier protocol) at the vendor's warehouse (entry tunnel interface). The truck (carrier protocol) travels over the highways (Internet) to your home (exit tunnel interface) and delivers the computer. You open the box (encapsulating protocol) and remove the computer (passenger protocol). Tunneling is just that simple!

As you can see, VPNs are a great way for a company to keep its employees and partners connected no matter where they are.