Virtual Private Networks
Chapter 1: What is a VPN?

VPN stands for Virtual Private Network and is a way of making a secure remote connection to a private network using the public Internet. For example, if I am in New York City and would like to access a confidential company database in San Francisco, I would need a secure connection between the company network and my computer. This secure connection could be established with a physical wire traversing the entire nation or with a dedicated leased line. Since this is virtually impossible or too expensive, a better way to establish the secure connection is needed. This is why VPN technology is used. VPN establishes a secure connection between the client and host by encapsulating data with encryption (Tunneling).

Imagine that you live in a village in the Serengeti plains of Africa. There are hundreds of villages all around you, some close and others miles away. The normal way to travel is to walk from village to village. Traveling by foot is dangerous because you may encounter wild animals and hostile villages.

Each village represents a private Local Area Network (LAN) and the Serengeti Plain is the Internet. Traveling by foot is like connecting to a server through the Internet. One has no control over the physical data connections and routers that make up the Internet, just like one has no control over the perils of traveling by foot between villages. This leaves users susceptible to security issues if users are trying to connect between two private networks using a public resource.

Your village decides to build a fenced pathway to a nearby village so that there is an easier, more secure and direct way for people to travel. This solution however, is very expensive and provides little flexibility or scalability. In addition, your village would like to connect to a second village that is much farther away but the costs are too high.

This is very much like having a physical wire or a leased line. The fence (leased lines) are separate from the Plain (Internet), yet are able to connect the villages (LANs). Companies have invested in leased lines because of the need for reliable and secure connections between their remote offices and users. However, if the distance of the connection is too great, the costs are proportionally high, just like trying to build fenced pathways that span great distances.

We could give each inhabitant of our village a small vehicle. The advantages of a vehicle include versatility, security, cost savings, and scalability (adding an additional vehicle is inexpensive and easy). These are the same advantages of a VPN.
1.1 VPN Advantages: Cost savings, scalability, global reach

Because of the versatility of the technology, VPN can grow to accommodate more users and greater distances between offices much easier than a leased line because with leased lines, cost increases in proportion to the distance. VPN offers cost savings by eliminating the need for expensive long-distance leased lines on the server-side and eliminating long-distance telephone charges for remote access on the client-side. By utilizing a VPN, a company and its remote users only need internet access.

Scalability is a major advantage that VPNs have over leased lines. As a company grows, more nodes must be added to the network and the number and complexity of dedicated lines needed for full connectivity increases illustrated in Figure 1.

![Figure 1: Complexity growing exponentially as more nodes are added to network](image-url)
As Figure 2 depicts, the cost to a company for dedicated leased lines may be reasonable at first but can increase exponentially as the organization grows at a rate of:

\[ \left(\frac{n(n+1)}{2}\right) - n. \]

Mathematicians call this phenomenon a "combinatorial explosion" and in wide area networks (WAN) this explosion limits the flexibility for growth. VPNs that utilize the Internet avoid this problem by simply tapping into public networks.¹

While locations and distances between offices are significant limiting factors for leased lines, VPNs offer greater **global reach**, because Internet access is ubiquitous while dedicated leased lines are only available in certain locations. This global attribute of VPN technology facilitates companies to expand into global markets.

---

¹ [http://compnetworking.about.com/library/weekly/aa010701c.htm](http://compnetworking.about.com/library/weekly/aa010701c.htm)
1.2 VPN Disadvantages: Availability, public network security, undeveloped standards, legacy protocols

There are four commonly raised concerns with VPN. First, VPN relies on an internet connection that is susceptible to connection outages. This affects availability both at the client as well as the server end. Second, VPNs require an in-depth understanding of public network security issues. The security vulnerabilities on a public network are greater than those of a private network, as public networks are more exposed to attacks and hackers. Third, VPN technologies from different vendors may not work well together due to undeveloped standards. This means that the software running on the client must be compatible (from the same vendor) as the hardware or software running on the VPN server. Since there is no definitive industry standard for VPN, once choosing and investing in a particular manufacturer, one can become dependant on that particular manufacturer and must continue using their products to avoid compatibility issues. Starting over with a new product line with a new manufacturer would entail a penalty in costs. Lastly, VPNs need to accommodate legacy protocols other than IP. Many companies still use older proprietary protocols or alternate network protocols such as IPX, SPX, NetBIOS, AppleTalk, and NetBEUI.

2 http://compnetworking.about.com/library/weekly/aa010701c.htm
Chapter 2: Configurations and Categories

2.1 VPN Configurations: Remote Access and Site-to-Site

VPN technology is awesome because it allows you to accommodate VPN to suit your company’s needs instead of your company suiting the VPNs needs. VPNs can exist in two different configurations: Remote Access or Site-to-Site. Remote Access is when the VPN is established between an individual PC and a private LAN. This includes mobile employees and home offices. Remote access, depicted in Figure 3, to the company’s private LAN is achieved with a desktop software client. In this configuration the tunnel (discussed in detail in chapter 3) is between a user’s PC and the VPN router at the company’s private LAN.

![Remote Access VPN](image)

Figure 3: A remote access VPN is a tunnel between a single user and a company private LAN.

When VPN exists between a remote LAN and a private LAN it is in Site-to-Site configuration as depicted in Figure 4. In this configuration the tunnel is between two routers. Site-to-site configuration is further broken down into two different sub-configurations: Intranet and Extranet.
**Intranet Site-to-Site** is the most typical and occurs when a company has one or more remote locations that they wish to join through the VPN in a single private network as if it were one LAN.

**Extranet Site-to-Site** is when a company has a close relationship with a partner such as a supplier, vendor, client, or other business and they want to share a subset of the private company LAN resources (an Extranet) with the partner over the extranet. The VPN would allow the partner to access the Extranet.
Figure 4: A Site-to-Site VPN is a tunnel joining two company private LANs.
2.2 VPN Categories: Hardware and Software

There are two broad categories: hardware VPN systems and software VPN systems. Most hardware VPN systems like the one in Figure 5 are encrypting routers that are secure and easy to use. Since they provide the nearest thing to "plug and play" encryption equipment available, it is the popular choice. Since the encryption and decryption for tunneling is performed at the router and not at the server, CPU cycles are not wasted at the server nor wasted at the router in running the server operating system or applications. As a result, hardware VPN systems provide the highest network throughput of all VPN systems. However, they may not be as flexible as software based systems.

![Figure 5: EtherFast Cable/DSL VPN Router with 4-Port 10/100 Switch (www.linksys.com)](image)

Software VPNs offer flexibility that hardware VPNs cannot. They are ideal in situations where both endpoints of the VPN are not controlled by the same organization as is the case in extranets. Software VPNs offers the most flexibility in how network traffic is managed. Many software products allow traffic to be tunneled based on address or protocol, unlike hardware products, which generally tunnel all traffic they handle, regardless of protocol. In situations where users are connecting over dial-up links, software VPNs may be the best choice because dialup does not require high performance and data throughput. Software systems are generally harder to manage than encrypting routers. They require knowledge of the VPN host operating system, the VPN software itself, and the security mechanisms of the organization.3

---

3 [http://vpn.shmoo.com/vpn/FAQ.html#Q4](http://vpn.shmoo.com/vpn/FAQ.html#Q4)
Chapter 3: Security

Nearly all VPNs share three fundamental security features:

1. Authentication
2. Encryption
3. Tunneling

As we mentioned earlier, traveling from village to village in the Serengeti Plain could be dangerous without the protection of a vehicle. The internet is similar in that private data sent through the public networks without protection of tunneling could be stolen, intercepted, and corrupted.

3.1 Authentication

Before establishing a secure channel for data transmission (encryption and tunneling), one must first authenticate both endpoints of the tunnel. This means proving the identity of both the client and the server. Imagine a scenario where a client begins to send private company data to a hacker that has taken the identity of the VPN server. Likewise, imagine the opposite scenario where the VPN server sends data to a hacker who has taken the identity of a VPN remote client. To ensure these breaches of security do not occur, a strong authentication method must be used. Applications that send unencrypted passwords over networks are extremely vulnerable to these types of security breaches. Packet sniffers used by security experts and hackers, are tools that "sniff" or reveal unencrypted passwords off of a network.

Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. For more information about Kerberos authentication, visit: http://web.mit.edu/kerberos/www/.

To ensure that a VPN is secure, limiting user access is only one piece of the puzzle; once the user is authenticated the data must also be protected.

---

4 http://web.mit.edu/kerberos/www/
3.2 Encryption

Without a mechanism to keep data private, information flowing through the public networks will be transmitted in clear text, which is highly vulnerable to hackers. All modern VPNs use encryption to scramble data into cipher-text before sending the packets of data through the Internet. When the data packets arrive at their destination, they are decrypted into readable text by the recipient.

There are two basic types of cryptography: 1) symmetric and 2) asymmetric. Asymmetric cryptography is more complex than symmetric and utilizes mathematically related public and private key pairs. This method is often used for smaller, more sensitive packets of data such as during authentication.

Symmetric cryptography has performance edge over asymmetric cryptography. Thus, it is commonly used in the tunneling process to exchange larger packets of data between two parties who have already authenticated each other using asymmetric cryptography.5

VPN commonly uses asymmetric encryption to exchange keys and symmetric encryption to exchange data. Asymmetric systems are more secure, but symmetric systems have better performance. Both the client and server use asymmetric key exchange to generate a private key. Then they derive a symmetric public key from the private one to send the public key to each other. Each VPN endpoint now has its own private key as well as the other endpoint’s public key.6

An example of the cryptography used in VPN is the Triple Data Encryption Standard (3DES) which is an extension of the DES algorithm illustrated in Figure 6. 3DES encryption is defined as follows:

- Cipher Text = EK₃(DK₂(EK¹(Plain Text)))

Where EK¹ denotes DES encryption operation using key K1, and DK¹ denotes DES decryption operation using key K1. 3DES decryption is defined as:

- Plain Text = DK¹(EK²(EK³(Cipher Text)))

---

5 http://findvnp.com/articles/encryption.php
6 Meredith, Gail, Cisco System User Magazine, Q2 2002, p.2
There are other encryption options available for VPN such as AES and RSA. The encryption used for authentication does not necessarily have to match the encryption used for tunneling. This allows VPN developers to make trade-offs between performance and strength of encryption to suite their security needs.

---

7 http://ratchkov.com/vpn/des/
3.3 Tunneling

VPN technology is based on the idea of tunneling. In brief, tunneling is the process of placing an entire packet within another packet and sending it over a network. Tunneling is comprised of three parts:

1. **The Passenger**
2. **The Capsule**
3. **The Carrier**

The Passenger is the actual data being transmitted. The Capsule is the encrypting protocol being used such as PPTP, IPSec or L2TP. The Carrier is the transport protocol such as TCP/IP, NetBEUI, NetBIOS, or IPX over which the data is sent.

Think of it like a letter. The letter is the data. The envelope is the capsule protecting the data and the postal service is the carrier. The focus of the paper is not the letter nor the carrier but the envelope, in other words, the tunnel. The Passenger, capsule and carrier are illustrated in Figure 7.

VPN supports two types of tunneling: voluntary and compulsory tunneling. In **voluntary tunneling**, the VPN client manages connection setup. The client makes a connection to the VPN server over an Internet connection. Then, the VPN client application creates the tunnel to a VPN server over this connection. In voluntary tunneling there are no intermediaries between the two endpoints of the tunnel.

In **compulsory tunneling**, the remote user’s Internet Service Provider (ISP) manages VPN connection setup. When the client first makes a connection to the ISP, the ISP in turn immediately negotiates a VPN connection between that client and a VPN server. This creates an intermediary but from the VPN client’s point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels. Compulsory VPN tunneling authenticates clients and associates them with specific VPN servers using a Network Access Server (NAS). In return, service providers must take on the additional burden of installing and maintaining the NAS.8

---

8 [http://compnetworking.about.com/library/weekly/aa010701d.htm](http://compnetworking.about.com/library/weekly/aa010701d.htm)
3.3.1 Tunneling Protocols

There are currently three major tunneling protocols for VPNs. They include the Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSec), and Layer 2 Tunneling Protocol (L2TP). These three protocols are incompatible with each other.

**Point-to-Point Tunneling Protocol (PPTP)** is based on the Point-to-Point-Protocol (PPP) which supports non-IP protocols such as NetBEUI, Appletalk, and IPX/SPX. PPTP exists at the Data Link layer of the OSI model as seen in Figure 7. PPTP supports 128-bit encryption and will use any authentication scheme supported by PPP.

**Internet Protocol Security (IPsec)** is the second most popular VPN protocol. It supports stronger encryption than PPTP. IPsec exists at the Network Layer of the OSI model as seen in Figure 7. IPSec has two encryption modes: **tunnel** and **transport**. Tunnel encrypts the header and the payload of each packet while transport only encrypts the payload. IPSec can encrypt data between routers, between clients and routers, between routers and firewalls, and between clients and servers.

**Layer Two Tunneling Protocol (L2TP)** is a protocol implemented primarily in Cisco products. Like PPTP, L2TP exists at the Data Link layer of the OSI model as seen in Figure 7. L2TP can be used as a tunneling protocol for site-to-site and remote access VPNs. L2TP can create a tunnel between routers, between a NAS and a router, and between a client and a router.

---

**Figure 7: The Passenger, Capsule, and Carrier in the 7 Layer OSI model**

---

10 [http://compnetworking.about.com/library/weekly/aa010701d.htm](http://compnetworking.about.com/library/weekly/aa010701d.htm)
Chapter 4: How does a VPN work?

To make use of the VPN, the remote computer must have the VPN client software pre-installed. A connection to the internet must then be made through the local ISP. This connection may be made by any medium such as dialup, DSL, cable, T1 or wireless. Using this type of connection, a company no longer needs to lease its own lines for wide-area communication. Instead, enterprises can securely use the public networks because the communication packets are encrypted before they are sent through the Internet "tunnel". The VPN client software connects to the VPN server using a tunneling protocol such as PPTP. After the remote computer has been successfully authenticated by the VPN server, the server establishes a tunnel between the remote computer and the company private LAN. Data being exchanged through this tunnel in either direction will be encrypted at the sending end and decrypted at the receiving end. The remote computer will be assigned an IP address in the company’s IP space and can now be trusted by computers on the company private LAN. Computers on the real company network can communicate with computers on the VPN via the VPN server which provides automatic IP address translation between the Internet service provider’s IP address space and the company’s private IP address space.

Chapter 5: Conclusion

We believe VPN is a powerful tool that increases company and individual productivity. It increases productivity because employees are no longer restricted to the company campus. This allows the company to expand its reach and project itself into global markets. However, Network Administrators should grant VPN access to users with a certain level of discretion. Companies should develop and enforce security policies that list requirements that must be met by employees to qualify for remote VPN access.

As illustrated in the appendix tutorial “Step by Step Tutorial: ‘How to’ Setup a VPN”, it is relatively easy to setup up a VPN server with simple programs that already come pre-packaged with Microsoft Windows operating systems. For example, a workstation from within the company network can be setup to accept VPN connections and be connected to from the outside, creating a security hole if you have a disgruntled employee. Network Administrators should take security measures to ensure that these types of activities are blocked at the firewall.
Appendix: Step by Step Tutorial: “How to” Setup a VPN

To configure a Windows XP VPN server:
http://www.techrepublic.com/printerfriendly.jhtml?id=r00320020408shi01.htm&rcode=
Or
http://asia.cnet.com/itmanager/netadmin/printfriendly.htm?AT=39050037-39006400t-39000223c

To configure a Windows XP VPN client:
Works Cited

1) Bradley Mitchell, Introduction to VPN, 
   http://compnetworking.about.com/library/weekly/aa010701c.htm
2) Ibid
5) TheWhirs: findVPN, What is VPN encryption
6) Meredith, Gail, Cisco System User Magazine, Q2 2002, p.2
8) Ibid
10) Ibid
11) Sciodata Corportation, VPN Monitoring, 
   http://www.sciodata.com/vpn/vpnmonitoring.htm