VPN Presentation Report

Kerry Nice
Matthew Reimer
Michael Semenchuk
Jeff Green

In today's global market, the need for efficient, secure and affordable means of information sharing is essential in a company's success. While companies continue to grow and span the global market, there will be a need to maintain efficient levels of communication. This communication can involve voice, video and data. There are many technologies available to handle this. One such solution is Virtual Private Networks (VPNs). VPNs offer users to stay connected to networks that normally would not be accessible or feasible. The following diagram represents this basic idea at a conceptual level:

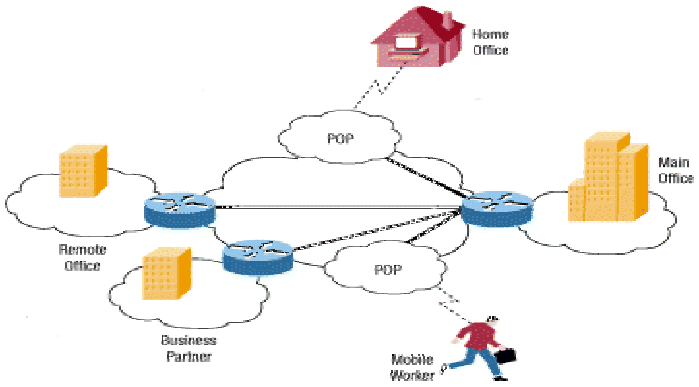

Image courtesy of Cisco Systems, Inc.

VPNs became popular because of its security, affordability and efficiency. Before VPNs were widely accepted, a common option that connected two remote offices was through the use of leased lines. These lines of communication provided a very secure option to transmit data between networks. The only invasion of privacy would involve someone physically wire-taping into the lines. Therefore these lines are still used today by some companies; however there is a significant drawback to this setup. Financially this option can be very expensive. The costs tend to increase with distance while setup and maintenance fees can involve a large overhead. As well, the monthly lease payment can be in the $1000s for a T1 communication line and even more for T3 lines. Naturally, with the introduction of the internet new forms of communication evolved. Organizations recognized the savings of exploiting the current infrastructure but were weary of losing their privacy. Thus, VPNs were a desirable choice. The basic idea of VPNs involves the secure packaging of packets, transmission through virtual tunnels and the emulation of being connected locally to a network. Along with savings, security and efficiency, this provided support for the telecommuter, the simplification of network topology and most importantly from a business perspective, a faster return on investment as compared to the traditional WANs. VPNs are most commonly classified into three functionalities:

- support for remote access to an intranet

- support for connections between multiple intranets within the same organization
- Support for the joining of networks between two organizations, forming an extranet.

In all three scenarios, the characteristics of a well designed VPN are security, reliability, scalability, network management, and policy management.

Types of VPNs

Remote Access VPN

A remote access VPN or virtual private dial-up network (VPDN) is a user to LAN connection used by companies that need a private network linking more than just static offices. The VPDN allows employees of the company out in the field to securely access a company LAN in one of its offices. So, a remote access VPN is a many to one connection where we have many users all connecting to the company LAN. This works as follows:

Each employee out in the field has some client software on their machine that allows them to dial up a toll free number and gain access to the company servers through the software. This allows the employee to gain secure access to the company LAN from an insecure remote location, using the various VPN encryption techniques. Upon connection the client receives an IP address from the server and appears as a member on the company LAN. So for all intents and purposes, the employee is now a member of the local company LAN. The obvious advantage of this lies in the fact that the employee can initiate a secure remote connection while still working through a public, non secure network (the internet). So the speed and power of the internet is still available to the remote user without sacrificing any security.

Site-to-Site VPN

Site to site VPNs are fixed VPNs that link a company's various office locations together. This is accomplished by using some dedicated equipment and again VPN's encryption techniques. This setup is a one to one VPN tunnel between two locations. These two servers have then setup an encrypted IP tunnel through which they can pass packets over the internet. There are two types of site to site VPNs.

Intranet based VPNs: Are used when a company needs to set up a dedicated connection between two or more fixed office locations. These VPNs connect the office LANs together in a secure transparent fashion.

Extranet based VPNs: Are used to connect the offices of two closely linked but different **companies** together so they can easily and securely share information over a shared LAN. For instance, in the case of a wholesale company and all it's clients this would be a useful way to share information without specialized software.

The main gains of these site to site VPNs are in cost (as they are cheaper than leased lines) while still maintaining comparable security.

Tunneling

What is tunneling?

Handling the general case of making two different networks interrelate is exceedingly difficult. However, there is a common special case that is manageable. This case is where the source and destination hosts are on the same type of network, but there is a different network in between. As an example, think of an international bank with a TCP/IP-based Ethernet in Paris, a TCP/IP-based Ethernet in London, and a non-IP wide area network (e.g. ATM) in between.

The solution to this problem is a technique called tunneling. To send an IP packet to London, Paris constructs the packet containing the IP address of London, inserts it into an Ethernet frame addressed to the London multiprotocol router, and puts it on the Ethernet. When the multiprotocol router gets the frame, it removes the IP packet, inserts it in the payload field of the WAN network layer packet, and addresses the latter to the WAN address of the London multiprotocol router. When it gets there, the London router removes the IP packet and sends it to the intended host inside an Ethernet frame. (Tanenbaum, 2003)

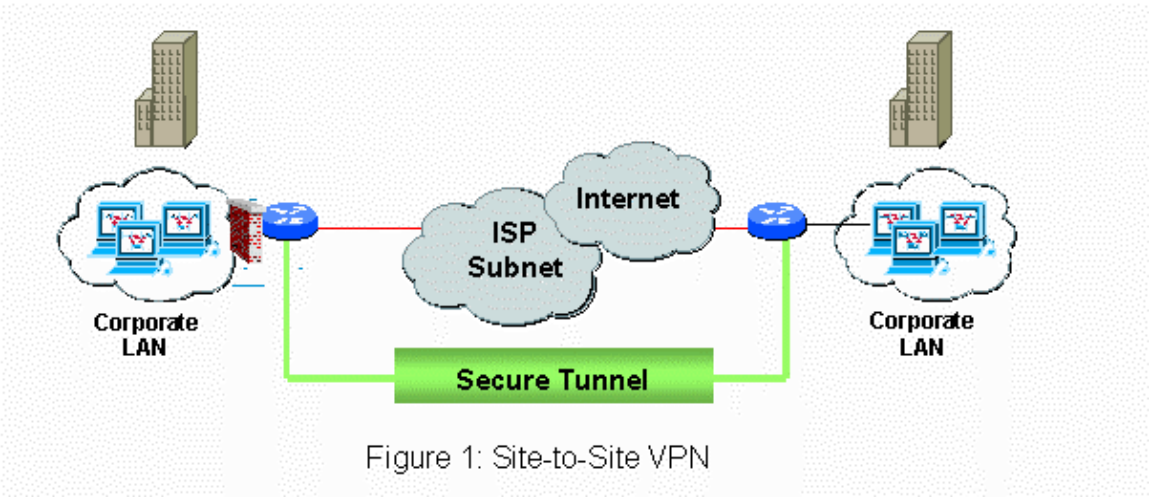

Figure 1: Site-to-Site VPN

Another example that is useful to understand tunneling is that of having a gift delivered to. The vendor packs the gift (passenger protocol) into a box (encapsulating protocol) which is then put on a truck (carrier protocol) at the vendor's warehouse. The truck (carrier protocol) travels over various highways and roads (Internet) to your home and delivers the gift. You open the box (encapsulating protocol) and remove the gift (passenger protocol).

Tunneling provides a mechanism for the transport of network specific packets over

foreign networks.

Virtual private networks

Virtual private networks rely on tunneling to transport packets over one of the most foreign networks -- the internet. (Howstuffworks, 2004).

Tunneling requires three different protocols:

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

Tunneling with vpns

As you'll recall, there are two types of virtual private networks: site-to-site and remote-access

Tunneling: site-to-site

In a site-to-site- VPN, Generic Routing Encapsulation (GRE) is normally the encapsulating protocol used to provide the framework for how to package the passenger protocol for transport via the carrier protocol. This packet includes information as to the type of encapsulated packet, as well as information about the connection between client and server. IPSec in tunnel mode, another protocol, is sometimes used as an encapsulating protocol instead of GRE. IPSec works well with both site-to-site and remote-access VPNs, but it must be supported at both tunnel ends to be effective.

Tunneling: remote-access

In a remote-access VPN, PPP is the protocol normally used by tunneling. Part of the TCP/IP stack, PPP is used as a carrier for other IP protocols when communicating between host computer and remote system. Of course, standardized use of the PPP protocol for tunneling would be too simple, so several derivative protocols have been developed. All the following protocols are based on PPP:

- 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.

Protocols

While certainly not the only protocols, Point-to-Point Tunneling Protocol (PPTP) and Generic Routing Encapsulation (GRE) are the major control and encapsulation protocols used within site-to-site and remote-access VPNs.

Point-to-Point Tunneling Protocol (PPTP)

When communicating information over a VPN tunnel, PPTP packages data within PPP packets then encapsulates the PPP packets within IP packets (datagrams) and transmits them over the tunnel. (Microsoft, 2003)

Once the VPN tunnel is established, PPTP supports two types of information flow:

- Control messages for managing and eventually tearing down the VPN connection. Control messages pass directly between VPN client and server.
- Data packets that pass through the tunnel, to or from the VPN client

Control message are as follows:

1. StartControlConnectionRequest
2. StartControlConnectionReply
3. StopControlConnectionRequest
4. StopControlConnectionReply
5. EchoRequest
6. EchoReply
7. OutgoingCallRequest
8. OutgoingCallReply
9. IncomingCallRequest
10. IncomingCallReply
11. IncomingCallConnected
12. CallClearRequest
13. CallDisconnectNotify
14. WANErrorNotify
15. SetLinkInfo

PPTP has numerous security filtered built-in, such as authentication, encryption and packet filtering. In general PPTP relies on the functionality of its underlying protocol, PPP, for its authentication and encapsulation/encryption but it also supports some additional security features for VPN data beyond what PPP provides.

Generic Routing Encapsulation (GRE)

After the PPTP control session has been established, GRE is used to encapsulate the data or payload in a secure manner. (Microsoft, 2003)

The GRE packet format that Microsoft uses for encapsulating data has the following general form:

Data Link (D/L) Header
IP Header
GRE Header
PPP Header
Encrypted PPP Payload
Data Link Trailer

The data or payload that is going to pass through the tunnel is given a Point-to-Point Protocol (PPP) header and then placed inside a GRE packet. The GRE packet carries the data between the two tunnel endpoints. After the GRE packet has arrived at the final destination (the endpoint of the tunnel), it is discarded and the encapsulated packet is then transmitted to its final destination.

Tunneling allows packets (even non-routable ones) to be transported across foreign networks in a secure and encrypted fashion

VPN Security

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

- Firewalls
- Encryption
- IPSec
- AAA Server

VPN Security: Firewalls

A firewall allows for protection of private networks from the Internet. It is simply a program or hardware device that filters incoming/outgoing packets of information to determine whether or not it should enter/leave a private network. Firewall technology both hardware and software, have been around much longer than virtual private networks. Almost every company worldwide uses the internet for its powerful methods of instant communication. The fundamental security that firewalls provide act as the basis to any properly designed VPN.

Think of a company with 200+ employees. Every employee has a computer and each computer has internet access. Without a firewall, each one of those computers will be directly accessible to anyone on the internet. If one employee accidentally (or maybe purposely) leaves a computer volatile, hackers will be able to gain access and cause harm. Simply placing a firewall in front of the connection to the internet provides the company with much more control of their network. Now they are in a position to only open

specific ports, decide on how employees will connect to Web sites, which files are allowed to leave the private network, etc.

VPN Security: Encryption/IPSec

VPN commonly uses a protocol known as IPSec, or Internet Protocol Security. This protocol has two modes, tunnel and transport. Both encrypt the payload of the packet (the information being sent) but tunneling also encrypts the header, which includes the size, type, source and destination.

VPN uses key based encryption. Encryption is "the process of encoding information in such a way that only the person (or computer) with the key can decode it" (How Encryption Works http://computer.howstuffworks.com/encryption.htm).
There are two methods which can be used, symmetric-key encryption and public key encryption.

Symmetric-key Encryption is relatively uncommon. It requires that each computer has the same private key that is used for encryption and decryption. The problem with it is how to send the private key without allowing others to potentially "steal" or copy the key while it is being transported over a network.

Public-key Encryption is more commonly used, especially over the internet. It was invented in 1976 by Whitfield Diffie and Martin Hellman, which is why it is sometimes called Diffie-Hellman encryption.
Its usage is best illustrated by a short story about Alice and Bob (from RSA Encryption - Tutorial http://www.woodmann.com/crackz/Tutorials/Rsa.htm):

Note: a common public-key cryptosystem is RSA, which will be discussed later. As a very simple example, a cryptosystem could reverse the order of each word. It would look incomprehensible to others (at least at first), but another person who knows to change the words could read it easily.

1. Alice and Bob agree on a public-key cryptosystem.
2. Bob generates a pair of mathematically linked keys: one public, one private.
3. Bob transmits his public key to Alice over any insecure medium.
4. Bob keeps the private key a secret.
5. Alice uses Bob's public key and the encryption algorithm to encrypt her message, creating a ciphertext.
6. Alice transmits the ciphertext to Bob.
7. Bob decrypts the ciphertext using the same algorithm and his private key.

Keys in public-key cryptography must have a "trapdoor function" which allows computation in one direction to be relatively easy (i.e. the encryption), and decryption (at least without the proper key) to be relatively impossible.

Keys are commonly made using RSA (defined by Rivest, Shamir, and Adleman). This algorithm generates keys as follows (from RSA Encryption - Tutorial http://www.woodmann.com/crackz/Tutorials/Rsa.htm):

1. Take two large primes, p and q
2. Compute their product n = pq; n is called the modulus
3. Choose a number, e , less than n and relatively prime to (p-1)(q-1), which means e and (p-1)(q-1) have no common factors except 1
4. Find another number d such that (ed - 1) is divisible by (p-1)(q-1). The values e and d are called the public and private exponents, respectively
5. The public key is the pair (n, e); the private key is (n, d)
6. The factors p and q may be kept with the private key, or destroyed.

Notes: p & q are large primes, with ~200 digits each

Notes about current Encryption Methods

It is not known if RSA is secure. It isn't known how to prove if an algorithm is inherently "slow". The best/fastest way to crack such encryption is using factorization, finding the two large prime numbers used to create the key. Such algorithms can take a long time to find the answers, for example factoring a 512 bit number, as part of a security challenge from RSA labs, took 292 CPU years (about 3.7 months in calendar time) in 1999 (http://www.rsasecurity.com/). The latest challenge factorization solved was a 578 bit number in 2003, which took less time than the 512 bit one because of improved algorithms and faster hardware.

Factorization techniques are improving as hardware gets faster. It's probable in the future that current encryption techniques will be solvable (i.e. crackable) in a short amount of time, rendering them useless. It's believed, however, that "If no new methods are developed, then 2048-bit RSA keys will always be safe from factorization, but one can't predict the future." (Cryptography FAQ (06/10: Public Key Cryptography) http://www.faqs.org/faqs/cryptography-faq/part06/)

VPN Security: AAA (authentication, authorization and accounting) Servers

AAA Servers (Authentication, Authorization, and Accounting Servers) can be added to the network to provide even further security beyond firewalls, encryption, etc. They are used in remote-access VPNs where the user dials into the network. Once they dial in, the AAA Server verifies:

- Who you are (authentication)
- What you are allowed to do (authorization)
- What you actually do (accounting)

Firstly, authentication allows for user identification. This is typically achieved by having users enter valid user name and password.

User credentials a stored in a database. Each user has a unique set of criteria for gaining access. If there is any inconsistency in the authentication credentials and the database stored credentials, then network access is refused. Else the user is granted access.

Next, a user must gain authorization in order to perform any tasks. This allows system administrators to enforce policies based on authenticated users. Authenticated users can thus have different privileges related to system resource access.

The final step, accounting, acts as a logger. It logs data, sessions, usage information etc. for security auditing, billing or reporting purposes.

Authentication, authorization, and accounting services are often provided by a dedicated AAA server, a program that performs these functions. A current standard by which network access servers interface with the AAA server is the Remote Authentication Dial-In User Service (RADIUS).

Future of VPNs

"The success of VPNs in the future depends mainly on industry dynamics. Most of the value in VPNs lies in the potential for businesses to save money. Should the cost of long-distance telephone calls and leased lines continue to drop, fewer companies may feel the need to switch to VPNs for remote access. Conversely, if VPN standards solidify and vendor products interoperate fully with other, the appeal of VPNs should increase.
The success of VPNs also depends on the ability of intranets and extranets to deliver on their promises. Companies have had difficulty measuring the cost savings of their private networks, but if it can be demonstrated that these provide significant value, the use of VPN technology internally may also increase."

References:

HowStuffWorks, Inc. http://www.howstuffworks.com/vpn.htm, © 1998 - 2004
Tanenbaum, Andrew S. Computer Networks 4th Ed. , Prentice Hall PTR, Upper Saddle River, NJ. 2003 pg772-790.
Bradley Mitchell, About, Inc. http://compnetworking.about.com/od/vpn/g/bldef_vpn.htm
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci514544,00.html
Cryptography FAQ (06/10: Public Key Cryptography
http://www.faqs.org/faqs/cryptography-faq/part06/
http://www.rsasecurity.com/
RSA Encryption - Tutorial http://www.woodmann.com/crackz/Tutorials/Rsa.htm
How Encryption Works http://computer.howstuffworks.com/encryption.htm
VPN Tunnels - PPTP Protocol Packet Description and Use.
http://support.microsoft.com/kb/241252/EN-US/ . Microsoft. May 14, 2003

VPN Tunnels - GRE Protocol 47 Packet Description and Use.
http://support.microsoft.com/?kbid=241251 . Microsoft. June 24, 2004
VPNs: Virtually Anything? http://www.corecom.com/html/vpn.html . Lisa A. Phifer. April 2001.

http://www.more.net/technical/netserv/tcpip/vpn.html
http://www.iquest.net/images/vpn/vpn.gif