Virtual Private Network Technology

Liyi Zhao
Naeem Haris
Gohar Saeed

1. History of the Virtual Private Network

The term VPN(Virtual Private Networks) is first introduced in telephone company. The purpose is to dial private-patterned (usually short)phone numbers through a public telephone network. Nowadays, the term VPN is mainly used in data transmission context. It introduces a concept of establishing private network access without requiring owned or leased private network lines. Concretely, it is a communication network tunneled through another network for communication. You have different ways to perform a tunneling.

One way is called encrypted VPN. It uses user data encryption protocol to provide a more secure environment than the standard internet.

The alternative is to use tunneling protocol for encapsulation, namely tunneled VPN. However it do not enforce encryption.

You might use non-tunneled VPN also, policy-based VPN is of this kind. They use access control lists within the router to change the normal routing behavior. Thus one site can only make their connection to a site which within the same virtual private network.

2. The definition of tunnel

A tunnel is a network build within another network. This isolation made the VPNs could have:
------improved data security. the intruder have to figure out the tunnel within the public network.
------make the intruder of the public network unable to direct traffic to the VPN sites. the provider control the whole connection.
------potentially improved performance due to QoS methods

3. The definition of VPN

VPN is a network that imitate(or reproduce) the actual private network using a shared public networking infrastructure.

4. The Property of a Private Network
------Private Network ensure the bandwidth of a physical network.
------Private Network is isolated from the public network.

5. The benefits of VPN
The introduce of private network helps to produce the following benefits:
A. Improved security. Because of isolation, the private network have a much less possibility of an attack from the outside world. (However, you must trust the leasing line provider which might eavesdrop your connection)
B. Predictable performance. The private network ensures the bandwidth. So it makes the network more predictable.

The introduce of tunnel-based network helps to produce the following benefits:
C. Independent choice of network infrastructure. You can choose whatever network infrastructure can use according to the vendor and manufacture of the network.
D. Independent IP address space. You can choose whatever address you can that is compatible to the internal packet type.

The insecure and unpredictable nature of public IP network makes A and B rather important. C is suppressed because of the dominance usage of TCP/IP protocol. D is suppressed because of the boost of address space due to IPv6. However the independence has no doubt improved the network security.

6. Consideration before construction
Currently, there is no single VPN technology that fulfills all the private network properties. VPN is usually created on different technologies.(Encryption, Tunneling, QoS, MPLS). So what should you choose?

The actual question is: What should be concerned to the VPN services?
1. From the user's point of view.
   Protect unauthorized access? Confidentiality? Non-VPN users? Performance?
2. From the provider' s point of view.
   How many sites I should support? (Scalability)
   How much effort I should spend on maintaining the network?(Manageability)

7. The construction of VPN

7.1 Protocol used for tunneling

Most VPNs rely on tunneling to create a private network that reaches across the Internet. As mentioned above, essentially,

tunneling is the process of placing an entire packet within another packet and sending it over a network. Tunneling is not a myth. It uses existing protocols.
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

Important: The VPN security mechanism lay in the encapsulating protocol. Passenger protocol use encapsulating protocol to perform security concern.

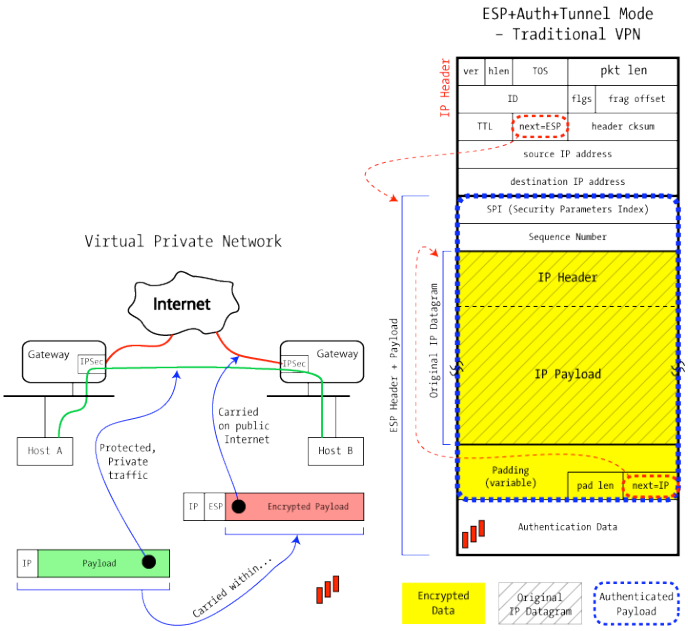
Tunneling has amazing implications for VPNs. For example, you can place a packet that uses a protocol not supported on the Internet (such as NetBeui) inside an IP packet and send it safely over the Internet. Or you could put a packet that uses a private (non-routable) IP address inside a packet that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

7.2 Before connecting to the VPN server:
When you try to log into a VPN server, VPN server first do authentication for you. Typically, you need to enter your VPN username and password, like what chapter 3 tells you to do. This is the first level security protection you may always find first.
Authentication method include but not limited to:
------Passwords(use strong passwords)
------Biometrics(fingerprints, face, iris signature or even DNA)
------Cryptographic functions(SHA or MAC etc.) and
------Firewalls(Some VPN products, such as Cisco's 1700 routers, can be upgraded to include firewall capabilities by running the appropriate Cisco IOS on them)

7.3 After authentication :

There are many kinds of VPN:
------Encrypted VPNs(IPsec, SSL/TLS...) 44%
------tunnel-based VPNs(L2TP, MPLS, PPTP...) 31%
------optical private networks(SDH, DWDM) 7%
------policy-based VPNs...

7.3.1 IPsec VPN:
Encrypted VPNs encrypts user data to make sure the data can not be eavesdropped during transmission. The secure data exchange through a public network provided by encrypted VPNs usually complements an organizations' firewall services.



IPsec and SSL are the most popular protocols used nowadays for establishing secure channels. PPTP by Microsoft is another example.

IPSec VPN uses the encapsulating security payload and authentication data to ensure security. Encapsulating security payload

ensures the confidentiality and the authentication data ensures the origin of data. We cannot use AH here, because this make the network unavailable to the NAT-enabled situation. AH cannot do address translation.

Because of emulation of private network, the Secured VPN gives you predictable performance. Because of isolation from the public network, it gives you the improved security. But IPsec and SSL can only encapsulate IP packets, It do not support the various kinds of network. PPTP can carry PPP packet, PPP can carry any traffic, It can. However they all support the address space independence.

The scalability of a encrypted VPN depends on its topology. The mesh topology require the N * N secure channel for N sites, it is a bad scalability. The central-based or hub topology require the N secure channel for a better scalability.

The management of encrypted VPN is hard because you need to control the distribution, configuration and storage of authentication and encryption information(ID, Password, digital certificate, secure keys).

7.3.2 L2TP/IPsec VPN
Different technologies can be used to implement tunnel-based VPNs, the more sophisticated the technology is, the more functionality it can provide. The current tunneling technology is L2TP and MPLS. L2TP and MPLS do not enforce security concerns.(ATM and frame-relay has been replaced by MPLS for the reason of the meet of future demand. However, MPLS has not disappeared.)

L2TP can encapsulate PPP packet inside a IP packet. PPP packet can encapsulate any kinds of packet. So the freedom of choosing network infrastructure is ensured.
Tunnel-based VPN using L2TP can take advantage of IPsec to implement its security mechanism.
Let's take a look at the IPsec version of the L2TP VPN.

IPsec version of VPN connection protocol is called L2TP(Layer 2 Tunneling Protocol)/IPsec. It allows L2TP/PPP packets to be transported over IP. It uses LAC as the client and LNS as the server to communicate. It lay in layer 5, but works like layer 2. Like MPLS, it has a packet header to encapsulate the payload data. It builds a tunnel between LAC and LNS to sent data. It does not provide confidentiality and integrity within the protocol, but it can take advantage of IPsec to establish a secure connection.

The Procedure is like the following:
1.LAC and LNS make a IPsec security association(SA) using Internet Key Exchange protocol, carried out over UDP port 500, using the shared-keys, public keys or X.509 certificates on both ends.
2.Negotiation and establish a Encapsulating Security Payload(ESP) communication in transport mode using SA. According to the current Passenger protocol you use. ESP for IP is 50, TCP is 6 and UDP is 17, etc. Here is just the IP.
3.Negotiation and establish a L2TP tunnel between LAC and LNS with the SA's secure channel, using the IPsec encrytion.
Now the L2TP packet between the endpoints are encapsulated by IPSec. Data confidentiality and integrity is ensured.

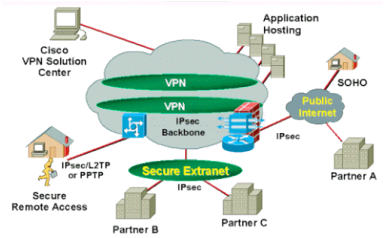


Photo courtesy Cisco Systems, Inc.
A remote-access VPN utilizing IPSec

7.4 Security differences
The difference between 'originally' encrypted VPN and tunnel-based encrypted VPN is:
The tunnel-based encrypted VPN do not enforce encryption and authentication. And the security mechanism is not provisioned by provider. The security mechanism can be insecure inside the network. Thus the security level of the tunnel-based VPN can never be considered high.

7.5 The scalability and management of encrypted VPN and tunnel-based VPN

The tunnel-based VPN ensures A,D like the encrypted VPN.
The scalability is like the encrypted VPN. It use point-to-point topology. This means it must establish secure channel between all the sites. Usually N * N for a mesh VPN, or N for a hub VPN.
The management of tunnel-based VPN is easier because you do not have to maintain the authentication and encryption information.

Reference:

http://www.microsoft.com/technet/isa/2004/help/fw_VPNIntro.mspx?mfr=true
http://www.techworld.com/networking/features/index.cfm?featureid=2763
http://openvpn.net/articles.html
http://computer.howstuffworks.com/vpn6.htm
http://en.wikipedia.org/wiki/Point-to-point_tunneling_protocol
http://en.wikipedia.org/wiki/VPN
http://www.ja.net/development/vpn/different-flavours-of-vpn-web.pdf
http://www.unixwiz.net/techtips/iguide-ipsec.html#esp