VPN

Virtual Private Networks (VPNs) were designed to provide a defined link across a network. The original data is encapsulated within a securitized packet and carried across a network such as the public Internet. This process is called "tunneling", as it sets up a virtual tunnel between the source and destination, ignoring the original addressing and other protocol information. Combined with an encryption method this has proved to be invaluable to companies who want to transfer traffic in a reasonably secure fashion across public networks like the Internet.

VPN has nothing to do with data rates or the underlying networking protocols. It is simply a way to encapsulate securitized data within public address space for transmission across a public network.

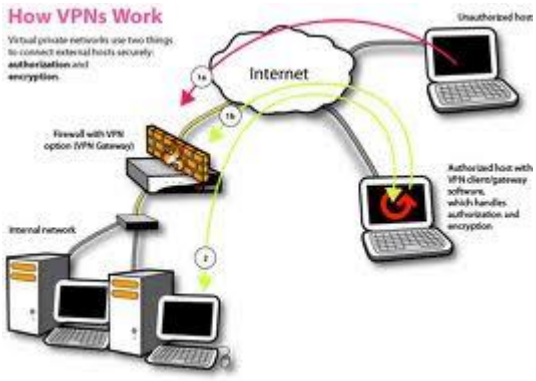
How does it work?

VPNs in business

Whenever data crosses the Internet there is risk. Latency is uncontrolled, and data can be captured and decoded, regardless of the encryption method used. If your company values the data and their network, they will use VPNs judiciously. Dedicated links and private networks are vastly more secure over these types of networks.

There are some cases where VPNs are the only convenient alternative. VPN clients installed in remote employees' laptop computers and VPN capable gateways installed at a company's server locations have proven to be effective and convenient. This enables traveled employees full access to company network resources at the full data rate available from whatever network they connect to. However, the network manager must always be aware and must always implement remote access technologies that are in the best interest of protecting the company's data resources, yet deliver a reasonable access for those who are also trying to make the company successful.

VPNs can be setup in very short order when compared to ordering, installing supporting hardware, and testing dedicated circuits. VPNs are virtually free. A company must, of course, have already installed the infrastructure to access the Internet and a gateway device to interface between the local network and the Internet.



VPN clients can be configured to be able to access only a single server, like an internal mail server, rather than the entire network. Often companies will require their remote VPN users to carry a random number generating device that regenerates a random number every few seconds and is synchronized

with the same random number generated at the server. The remote VPN user must enter the current random number, and that number must compare equally with the server's random number.

Uses of VPNs, other than for remote VPN client accesses which the author calls "access VPNs", include extending a company's network to what the author call an extranet. Some business want their suppliers and customers to access the company's private network across a pre-configured static VPN to perform functions like accounts payable and accounts receivable, or inventory replenishment, etc. Due to the business necessity to have the Internet available from nearly all of its offices, and the relative inexpensive creation of a VPN across the Internet, businesses more and more are devising ways to further securitize VPNs and using VPNs for a bigger and bigger part of their private internet, or what the author calls "intranet VPNs".

Remember that a VPN tunnel just defines the end of the link. Encryption must be added in order to provide any measure of security. Some common VPN encryption methodologies include:

Layer 2 Tunnel Protocol - L2TP
Point-to-Point Tunnel Protocol – PPTP
IP Security - IPSec

L2TP
L2TP operates just as the name implies, at the data link layer-2. Remember that layer-2 protocols operate on a device-to-device basis, so too does L2TP. This may be an advantage or a disadvantage depending on the business environment where it is installed. If device-to-device is not also end-point-to-end-point, then multiple intermittent devices may have a need to understand the particular L2TP implementation. Layer-2 uses MAC addresses for source and destination, so using L2TP across networks may be unmanageable in an environment where MAC addresses are not published.

PPTP
PPTP, for the most part, is a Microsoft developed vendor standard and not an IETF sanctioned industry standard. PPTP does operate at the transport layer using TCP as the underlying transport protocol. PPTP is a tunnel protocol which first requires the use of PPP (point-to-point protocol), which originally was a protocol developed for dial-up access to an IP network. PPTP uses single DES encryption and in recent years has lengthened the key to gain a higher degree of security, but is still regarded as a weak securitized tunneling protocol.

IPsec
IPsec is the most popular VPN methodology in use today. Notice that IPsec is not called a protocol like the previous two VPN types, rather it is called a VPN security methodology. IPsec was around before being used to securitize VPNs, and uses two separate transport layer protocols called Authentication Headers (AH) and Encapsulated Security Protocol (ESP). A third protocol also used by IPsec is the encapsulated IPv4 protocol which is really a pseudo transport layer protocol used to force the demultiplexing of an Ethernet frame down the reference model back to the network layer where an IP header is processed.

Since IPsec is a transport layer security methodology, and since the transport layer is the first layer when working up the reference model that is end-point-to-end-point, IPsec is in a very strong position to

perform security on an end-point-to-end point basis. Devices in the lower layers such as switches and routers will be passive to IPSec's security methodologies. When the end-to-end connection is secured at the transport layer, then the upper application layer is also secured as a result. In reference to the TCP/IP protocol suite (aka. the Internet Model) the upper layer is the application layer, but may also include an imbedded presentation layer and/or session layer as well. IPsec does not restrict itself to only one security algorithm, but allows many different algorithms many of which are much stronger than single DES as used in PPTP. IPsec uses both asymmetric encryption to authenticate sender and receiver private IPs, and symmetric encryption to securitize the payload of the encapsulated TCP segment.

VPN services are provided via a gateway device. A gateway device is defined as a device that interfaces between two separate networks. In a VPN environment, the two separate networks are a company's private network and the public Internet. The gateway function may be included in a general purpose computer or through special software available on some commercial routers. In either case, data must be fully decoded, and this takes considerable processing.