VIRTUAL PRIVATE NETWORK (VPN) AND IPSEC

The Internet is a worldwide, publicly accessible IP network. Due to its vast global proliferation, it has become a viable method of interconnecting remote sites. However, the fact that it is a public infrastructure has deterred most enterprises from adopting it as a viable remote access method for branch and SOHO sites.

A virtual private network (VPN) is a concept that describes how to create a private network over a public network infrastructure while maintaining confidentiality and security. VPNs use cryptographic tunneling protocols to provide sender authentication, message integrity, and confidentiality by protecting against packet sniffing. VPNs can be implemented at Layers 2, 3, and 4 of the Open Systems Interconnection (OSI) model.

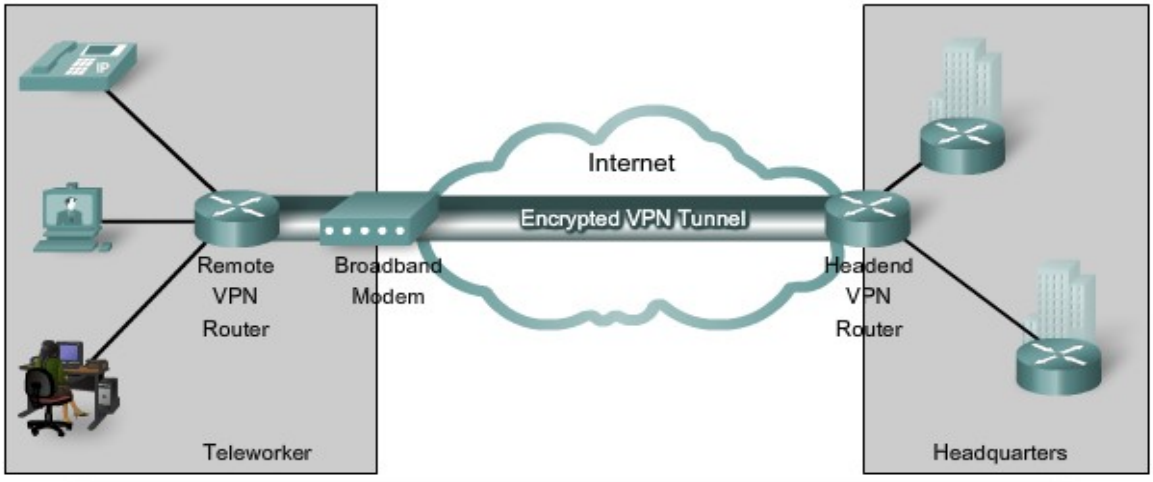
Figure illustrates a typical VPN topology. Components required to establish a VPN include:

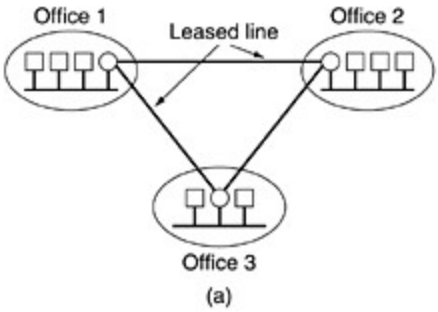
- An existing network with servers and workstations
- Connection to the Internet
- VPN gateways (i.e., routers, PIX, ASA, VPN concentrators) that act as endpoints to establish, manage, and control VPN connections
- Software to create and manage tunnels

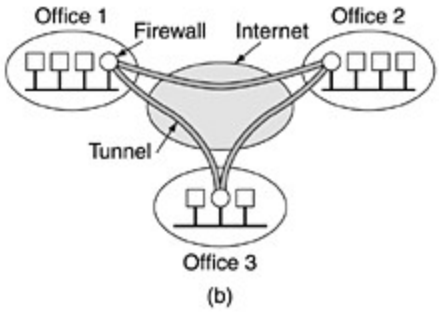
The key to VPN technology is security. VPNs secure data by encapsulating the data, encrypting the data, or both encapsulating the data and then encrypting it:

Fig:(a) A leased-line private network. (b) A virtual private network

- Encapsulation is also referred to as tunneling because encapsulation transmits data transparently from network to network through a shared network infrastructure.
- Encryption codes data into a different format. Decryption decodes encrypted data into the data's original unencrypted format.







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.
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

IPSEC

IPsec provides a mechanism for secure data transmission over IP networks, ensuring confidentiality, integrity, and authenticity of data communications over unprotected networks such as the Internet . IPsec encompasses a suite of protocols and is not bound to any specific encryption or authentication algorithms, key generation technique, or security association (SA). IPsec provides the rules while existing algorithms provide the encryption, authentication, key management, and so on. IPsec acts at the network layer, protecting and authenticating IP packets between IPsec devices (peers), such as Cisco PIX Firewalls, Adaptive Security Apliances (ASA), Cisco routers, the Cisco Secure VPN Client, and other IPsec-compliant products.

IPsec is an Internet Engineering Task Force (IETF) standard (RFC 2401-2412) that defines how a VPN can be created over IP networks.

IPsec provides the following essential security functions:

Data confidentiality: IPsec ensures confidentiality by using encryption. Data encryption prevents third parties from reading the data, especially data that is transmitted over public networks or wireless networks. The IPsec sender can encrypt packets before transmitting the packets across a network and prevent anyone from hearing or viewing the communication (eavesdropping).

Data integrity: IPsec ensures that data arrives unchanged at the destination; that is, that the data is not manipulated at any point along the communication path. IPsec ensures data integrity by using hashes.

Data origin authentication: The IPsec receiver can authenticate the source of the IPsec packets. Authentication ensures that the connection is actually made with the desired communication partner.

Source : http://dayaramb.files.wordpress.com/2011/03/computer-network-notes-pu.pdf