**What is VPN**

A private network that communicates through open communication channels like the Internet rather than leased lines.

Internet-based remote network communication.

Used by businesses or organizations wanting quiet communication.

• Two parts:

Protected or "inside" network

"Outside" network or segment (less trustworthy)

**The User’s Perspective**

It appears to the user as a network made up of specialized network links.

It appears that these links are exclusive to VPN users.

* It seems to be a private connection as a result.

The data looks to be private due to encryption.

**How VPN works**

Two connections - Two calls are placed, one to the Internet and the other to the VPN.

Datagrams - include information about the source, destination, and data.

Firewalls - VPNs open up the firewalls to authorized users and data.

Protocols - The VPN tunnels that enable a private connection across a public network are created by protocols.

**Key Functions Key Funct**

**Key Functions**

Authentication - validates that the sender of the data sent it.

Access Control - preventing unauthorized users off the network.

Confidentiality - preventing the data while it is being transported from being read or copied.

Data Integrity - ensuring that no changes have been made to the data.

**Encryption and Tunneling**

Encryption - public key encryption techniques are used.

Authentication - digital signatures.

A virtual connection is made through the Internet.

Datagrams are sent along the virtual connection.

The outer part of the datagram contains a header and may or may not be encrypted.

The inner part is encrypted.

**Protocols**

There are three main protocols used:

IP Security (IPsec)

Point-to-Point Tunneling Protocol (PPTP)

Layer 2 Tunneling Protocol (L2TP)

**IPsec**

An open standard protocol suite.

Provides privacy and authentication services.

Has two modes of operation.

Transport Mode encrypts data but not the header.

Tunnel Mode encrypts both data and header.

Each connection is a security association (SA).

• Has one security identifier for each direction.

• Each security identifier is carried in packets and used to look up keys, etc.

**IPsec Transport Mode**

IPsec header is inserted just after the IP header.

Protocol field of IP header is modified to indicate that the IPsec header follows.

IPsec header contains security information:

* SA identifier
* Sequence number
* Possibly an integrity check on the payload

**IPsec Tunnel Mode**

Whole IP packet including header is encapsulated in a new IP packet with an IPsec header.

Useful when the tunnel end is not the final destination.

• E.g., tunnel ends at company firewall.

• Firewall deals with encapsulating IP packets into IPsec packets and decapsulating.

• Machines on internal network do not have to be aware of IPsec as they receive and send IP packets.

**PPTP (Point-to-Point Tunneling Protocol)**

A data link protocol.

Used to establish a direct connection between two networking nodes.

Creates the virtual connection across the Internet.

Can provide:

• Connection authentication

• Transmission encryption

• Compression

**L2TP**

A tunneling protocol.

Does not provide encryption or confidentiality but relies on an encryption protocol that it passes within the tunnel.

The entire L2P packet, including payload and header, is sent within a UDP datagram.

**Protocols Working Together**

PPTP sessions are frequently carried out over L2TP tunnels.

By itself, LTP cannot offer strong authentication or confidentiality.

Because IPsec provides confidentiality, authentication, and integrity, it is frequently used to secure L2P packets.

The L2TP/IPsec combination of these two protocols is widely recognized.

**Advantages**

• Cost effective

• Greater scalability

• Easy to add/remove users

• Mobility

• Security

**Disadvantage**

Understanding of security issues

Unpredictable Internet traffic

Difficult to accommodate products from different vendors

**VPN Connections**

A virtual private network, or VPN, is a safe way for two or more devices to communicate privately over an open network. (e.g., the Internet)

VPN devices can be:

a computer running VPN software

a special device like a VPN enabled router

An office network can be accessed by a remote computer.

Through the Internet, two computers located in distant places can connect.

**VPN Categories**

There are several types of VPN

There are different ways of classifying VPNs

We use two broad categories based upon architecture:

* Client-initiated VPNs
* Network access server (NAS)-initiated VPNs

**Client Initiated VPNs**

In order to access the customer network from the shared ISP network, users create a tunnel.

The client program that starts the tunnel is controlled by the customer.

One advantage is that they protect the client-ISP connection.

A disadvantage is that their complexity and scalability are higher than those of VPNs started by NAS.

**NAS initiated VPNs**

By connecting to the ISP NAS, users create a tunnel to access the private network.

stronger than VPNs initiated by clients.

Don't have the client maintain the program that creates the tunnel.

The client-ISP connection should not be encrypted because the Public Switched Telephone Network (PSTN) is far more secure than the Internet, most customers won't be concerned.

**VPNs and the Workplace**

VPNs can be used to connect to one or more corporate gateway routers (remote access) from a remote client PC or remote office router via the Internet or an IP service provider network.

An intranet of a firm is a VPN connecting its offices.

Extranets are VPN connections to outside business partners.

**Extranet**

An extranet is a network used to connect to business partners through the Internet or one or more service providers.

• Extends network connectivity to:

• Customers

• Business partners

• Suppliers

Due to the possibility that the VPN would be utilized for significant orders or contracts, security policies are important.

**Intranet**

Other business offices can access a basic remote access VPN through intranet VPNs.

There is connectivity through the IP backbone of the service provider or over the Internet.

It is probable that a single service provider will maintain and enforce service levels.

There are no performance guarantees for VPNs that operate across the Internet (multiple service providers).

* no one is in charge of the Internet!

**Remote Access VPN**

Encrypted connections between users' business networks and mobile devices or faraway locations.

Instead of making a long-distance call to the corporate remote access server, a distant user can make a local call to an ISP.

Perfect for mobile sales representatives or telecommuters.

Telecommuters and mobile workers can benefit from broadband with VPN.

Makes utilizes access technologies to enable distant users to join a business VPN.

Usually entails using tunnels to extend the Point-to-Point Protocol (PPP) connection from the access server to the corporate network.

The tunnel is also extended from the access server to the end-user PC using Microsoft's Point-to-Point Tunneling Protocol (PPTP).

**Virtual Private Dial-Up Networking**

With virtual private dial-up networking (VPDN), users can set up safe networks that rely on Internet service providers (ISPs) to tunnel traffic for remote access.

Local dial-up can be used by remote users to connect.

Providers of dial-up services forward traffic.

Client control over network security and configuration is maintained.

Between the sites, the dial-up service provider offers a virtual pipe.

**VPN in Industry**

Healthcare: transferring confidential patient data between healthcare providers.

Manufacturing: Suppliers are able to see stocks and enable clients to make secure online purchases.

Retail: Transferring customer or sales data securely between retail locations and corporate offices.

Banking: permits the safe transfer of account information across departments and branches.

**VPN in Small Business**

Operating systems often have built-in VPN protocols.

These often rely on usernames and passwords.

* Not very secure or private.

Standard VPNs require the deployment of software and clients.

* Costs money and time.

SSL VPNs are easy to install and use ports already available for secure traffic over the Internet.

**SSL VPNs**

Connect securely via a standard Web browser

No special software required on client computers

Traffic between Web browser and the SSL VPN device is encrypted with the SSL protocol

Support access control by:

User

Device

Location

**SSL & Data Protection**

SSL encrypts data.

Each SSL certificate uses public key encryption techniques.

The SSL handshake either authenticates the server and client or blocks unauthorized users.

Keeps data confidential and protected.

**SSL Portal VPN**

Allows a single SSL connection to a website.

User securely accesses multiple network services from the website.

Can use any modern browser.

User is authenticated via method supported by the portal.

User then has access to a web page that acts as the portal to other services.

**SSL Tunnel VPN**

Allows the safe use of a tunnel operating over SSL to access various Network services via a web browser.

* Comprises non-web-based apps and protocols.

Needs a web browser capable of displaying current content.

Can offer features that SSL portal VPNs are unable to access.

**SSL Costs**

Initial costs are higher.

* Requires purchase of SSL Certificate.

Can save money in the long run.

* Reduced management/administration costs.
* Plus, the savings from having secure communications.