

Technical Case Study:
**Global Client Server Paradigm
For
Infrastructure Management Systems**

This is subsequent to Summary of Projects –

VMware - ESX Server to Facilitate:
IMS, Server Consolidation, Storage & Testing with Production Server

PRIMA - Panel for Remote Infrastructure Management Applications



VAssure | Virtualization Labs | trRIMS | Offshore-QA | BI | Portals

<http://www.vassure.com>

Global Client Server Paradigm over VoIP/VPN

Voice over Internet Protocol:

Voice over Internet Protocol (VoIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. VoIP supports the transmission of voice and data over the same network. VoIP results in reduced maintenance and management costs. In VoIP the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. Signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities.

VoIP Functions:

The basic functions of VoIP include:

- Signaling
- Database Services
- Call Connect and Disconnect(Bearer Control)
- CODEC operations

Signaling:

The signaling in a VoIP network activates and coordinates the various components to complete a call. Signaling in a VoIP network is accomplished by the exchange of IP datagram messages between the components. The format of these messages is covered by any number of standard protocols.

Database Services:

Database services are a way to locate an endpoint and translate the addressing that two networks use. A call control database contains these mappings and translations. VoIP employs additional logic to provide network security, such as to restricting a specific endpoint from doing certain operations. This functionality, coupled with call state control, coordinates the activities of the elements in a VoIP network. A VoIP network uses an IP address and port number to identify an endpoint.

Call Connect and Disconnect (Bearer Control):

The connection of a call is made by two endpoints opening a communication session between one another. In a VoIP implementation, this connection is a multimedia stream transported in real time. The connection is the bearer channel and represents the voice or video content being delivered. When a communication is complete, the IP sessions are released and optionally network resources are freed.

CODEC Operations:

Traditional voice communication is analog, while data networking is digital. For VoIP packetizing the voice is necessary. The process of converting analog waveforms to digital information is done with a coder-decoder (CODEC, which is also known as a voice coder-decoder [VOCODER]). There are many ways an analog voice signal can be transformed, all of which are governed by various standards. Most of these conversions are based on PCM.

In addition to performing the analog to digital conversion, CODECs compress the data stream, and provide echo cancellation. Compression/Silence Suppression results in saving the bandwidth. Silence suppression is the process of not sending voice packets between the gaps in human conversations. The output from the CODECs a data stream that is put into IP packets and transported across the network to an end point. These endpoints must use the standards, as well as a common set of CODEC parameters. The result of using different standards or parameters on both ends is unintelligible communication.

VoIP Components:

The four major components of a VoIP network are:

- Call Processing Server
- User End-Devices
- Media/VoIP Gateways
- IP network

Call Processing Server/IP PBX:

The call processing server is the heart of a VoIP phone system, managing all VoIP control connections. Call processing servers are usually software based and can be deployed as a single server, cluster of servers, or a server farm with distributed functionality. Call processors may also be based on a router platform or developed as a distributed appliance. VoIP communication requires a signaling mechanism for call establishment, known as control traffic, and actual voice stream or VoIP payload. VoIP control traffic follows the client-server model, with VoIP terminals, including messaging servers that hold voice mail messages representing the clients that communicate to the call processing servers.

User End Devices:

The user end devices consist of VoIP phones and desktop based devices. VoIP phones use the TCP/IP stack to communicate with the IP network. They have an IP address for the subnet on which they are installed. Usually, VoIP phones use DHCP to auto-configure themselves, with the DHCP server telling the phone about the location of the configuration server, which most of the time is identical to the call processing server.

VoIP phones may be software based or hardware based.

- **Software-based Phones**, or "soft" phones, use the PC's capabilities to communicate with other PC's over the Internet, by using the PC's sound card, CPU and network card as part of the phone's hardware, and thus, enable a PC to become an IP phone. They are usually targeted towards mobile users.

- **A Hardware Phone** is a physical device, similar to a common phone. The only thing that is different from the ordinary phone is that it connects to an Ethernet network rather than a telephone network. IP phones are built with all the necessary hardware (and software) to digitize voice (i.e., CODECs) as well as setup and make calls (i.e., signaling and transport).

VoIP Gateways/Gatekeepers:

A VoIP Gateway is a VoIP device that connects the VoIP network to the public telephone network (PSTN). Media gateways are responsible for call origination, call detection, analog-to-digital conversion of voice, and creation of voice packets. Traditionally gate keepers have been mainly used for Call Admission and control and bandwidth management. But in the now a days the functionality of gatekeepers also included in the gateways. In addition, media gateways have optional features, such as voice (analog and/or digital) compression, echo cancellation, silence suppression, and statistics gathering. The media gateway forms the interface that the voice content uses so that it can be transported over the IP network. Media gateways are the sources of bearer traffic. Typically, each conversation (call) is a single IP session transported by a Real-time Transport Protocol (RTP) that runs over UDP. Media gateways exist in several forms. Their features and services can include some or all of the following:

- Trunking gateways that interface between the telephone network and a VoIP network. Such gateways typically manage a large number of digital circuits.
- Residential gateways that provide a traditional analog interface to a VoIP network.
- Access media gateways that provide a traditional analog or digital PBX interface to a VoIP network.
- Business media gateways that provide a traditional digital PBX interface or an integrated soft PBX interface to a VoIP network.
- Network access servers that can attach a modem to a telephone circuit and provide data access to the Internet.

IP Network:

The VoIP network can be viewed as a logical switch. The logical switch is a distributed system, rather than that of a single switch entity; the IP backbone provides the connectivity among the distributed elements. The IP infrastructure must ensure smooth delivery of the voice and signaling packets to the VoIP elements. Due to their dissimilarities, the IP network must treat voice and data differently. If an IP network is to carry both voice and data traffic, it must be able to prioritize the different traffic types, as VoIP traffic is extremely sensitive to latency.

Voice Signaling Protocols:

There are a variety of VoIP protocols and implementations, with a wide range of features that are currently employed. Two major standards bodies govern multimedia delivery over packet based networks: International Telecommunications Union (ITU) and Internet Engineering Task Force (IETF). H.323 is the ITU's standard for establishing VoIP connections, while IETF uses Session Initiation Protocol (SIP) as its standard.

H.323:

H.323 is the primary protocol used to enable multimedia applications like voice and video to function over packet-switched networks. The main function of H.323 is not as a transport or network protocol, but rather to perform call control and management functions on a packet-switched network (H.323 is considered a session layer protocol). It is designed to operate above the transport layer of the network. Within the H.323 specification, two additional signaling methods are required for the transport of voice traffic:

- **H.225.** The H.225 specification uses the Q.931 protocol for call control signaling between two H.323 devices. This includes functions like call setup and termination.
- **H.245.** The H.245 specification creates a reliable connection between H.323 devices that is used to exchange information about the CODEC to be used, the capabilities of the devices (which allows them to determine a common level of compatibility during a session), flow control information, the port numbers to be used, and so forth.

H.323 defines four logical components: Terminals, Gateways, Gatekeepers and Multi point Control Units (MCUs). Terminals, gateways and MCUs are commonly known as endpoints. Call Processing Servers provide call routing, and communication to VoIP gateways and end devices. Gateways serve as both the H.323 termination endpoint and interface with non H.323 networks, such as the PSTN. Gatekeepers function as a central unit for call admission control, bandwidth management and call signaling. Although the gatekeeper is not a required element in H.323, it can help H.323 networks to scale to a larger size, by separating call control and management functions from the gateways.

There are five types of information exchange enabled in the H.323 architecture:

- Audio (digitized) voice
- Video (digitized)
- Data (files or image)
- Communication control (exchange of supported functions, controlling logic channels, etc.)
- Controlling connections and sessions (setup and tear down)

H.323 is dependent on TCP based signaling. There is a challenge in maintaining large numbers of TCP sessions because of the substantial overhead involved. H.323 specifications tend to be heavier and with an initial focus in LAN networking. The following features can summarize

H.323 specifications:

- * Point to Point and multi point conferencing support
- * Networking interoperability
- * Heterogeneous client capability
- * Audio and video codecs
- * Management and Accounting Support
- * Security

Real-time Transport Protocol (RTP):

RTP provides end to end network transport functions suitable for applications transmitting real time data, such as audio, video or simulation data, over multicast or unicast network services. RTP is the internet standard protocol. It does not guarantee quality of service for real time services. RTP consists of a data and a control part and the control part is called Real Time Transport Control Protocol (RTCP). For each participant, a particular pair of destination IP addresses defines the session between the two endpoints, which translate into a single RTP session for each phone in progress. RTP is an application built on UDP, so it is connectionless, with best-effort delivery.

Features of RTP:

- RTP helps in identifying payload type and maintains time stamping.
- RTP is independent of underlying protocol.
- RTP supports data transfer to multiple destinations using multicast distribution.
- RTP sequence numbers can also be used to determine the proper location of a packet.

Protocol Architecture:

RTP is a modular protocol. The base protocol is defined by RFC 1889. RFC 1889 defines basic fields for the transportation of real time data. It also defines RTCP, RTP control, whose purpose is to provide feedback on transmission quality, information about participants of RTP session, and enable minimal session control services. The RTP payload type field includes the encoding scheme that the media gateway uses to digitize the voice content. The field identifies the RTP payload format and determines its interpretation by the CODEC in the media gateway. A profile specifies a default static mapping of payload type codes to payload formats. These mappings represent the ITU G series of encoding schemes.

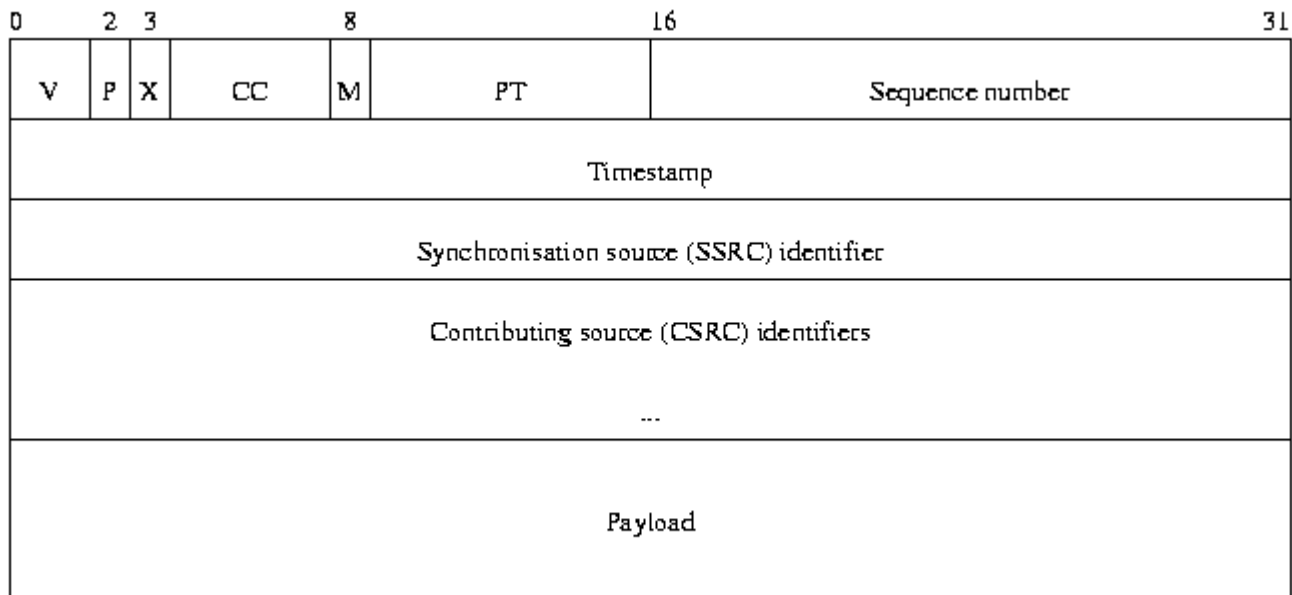


Fig: Upper Layer of RTP

- The version (V) field identifies the version of RTP (currently 2).
- If the padding (P) bit is set, the packet contains one or more padding octets at the end which are not part of the payload.
- If the extension (X) bit is set, the fixed header is followed by one header extension.
- The CSRC count (CC) field contains the number of CSRC identifiers following the fixed header.
- The interpretation of the marker (M) bit is defined by a profile.
- The payload type (PT) field identifies the format of the RTP payload and determines its interpretation by the receiving application.
- The sequence number field increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss and to restore packet sequencing. The initial value is random to make known-plain text attacks on encryption more difficult.
- The time stamp field reflects the sampling instant of the first octet in the RTP data packet. The initial value of the time stamp is random, as for the sequence number.
- The SSRC field identifies the synchronization source. This identifier is chosen randomly, with the intent that no two such identifiers within the same RTP session will have the same SSRC identifier.
- The CSRC list of fields (up to 15) identifies the contributing sources for the payload in this packet. CSRC identifiers are inserted by mixers, using the SSRC identifiers of contributing sources.

With the different types of encoding schemes and packet creation rates, RTP packets can vary in size and interval. Administrators must take RTP parameters into account when planning voice services. All the combined parameters of the RTP sessions dictate how much bandwidth is consumed by the voice bearer traffic. RTP traffic that carries voice traffic is the major contributor to the VoIP network load.

Real Time Control Protocol (RTCP):

Real Time Transport Control Protocol (RTCP) is the optional protocol to RTP. The primary function of RTCP is to provide feedback on the quality of the data distribution being accomplished by RTP. This function is an integral part of RTP's role as a transport protocol and is related to the flow and congestion control functions of the network. The reports of RTCP help in identifying problems. With the information generated from different media gateways in the network, RTCP feedback reports enable administrator to evaluate where network performance is degrading. It enables administrator to monitor the quality of a call session by tracking packet loss, latency, jitter, and other key VoIP concerns. If RTCP is implemented on a network, the organization needs to take into account bandwidth calculations for the protocol. Administrators need to limit the control traffic of RTCP to small and known fraction of the session bandwidth. RFC specifications recommend that the fraction of the session bandwidth allocated to RTCP be fixed at 5% of RTP traffic.

Media Gateway Control Protocol (MGCP):

Media Gateway Control Protocol breaks up the role of traditional voice switches into the components of media gateway, media gateway controller and signaling gateway functional units. MGCP is a control protocol, allowing a central operator to monitor and analyze events in IP phones and gateways and instruct them if necessary to send media to specific addresses. In the MGCP structure, the call control intelligence is located outside the gateways and is handled by the call control elements (the Call Agent). Also the call control elements will synchronize with each other so that they will be able to send commands to the gateways under their control. This facilitates the independent managing of each VoIP gateway as a separate entity. It is a master slave control protocol that coordinates the actions of media gateways. In most cases, the call agent informs the media gateways to start an RTP session between two endpoints.

Session Initiation Protocol (SIP):

Session Initiation Protocol (SIP) is the IETF standard for establishing a VoIP connection. It acts as an alternative protocol to H.323. SIP is an application layer control protocol for creating, modifying and terminating sessions with one or more participants. This Voice over IP standard is similar to that of HTTP (a client-server protocol). Data requests are generated by the client and sent to the server. The server processes the requests and then sends back data packets containing a response to the client. A request and response will make a complete transaction.

SIP uses invitations to create Session Description Protocol(SDP) messages to carry out capability exchange and to set up call control channel use. These invitations allow participants to agree on a set of compatible media types. SIP supports user mobility by proxying and redirecting requests to the user's current location. Users can inform the server of their current location by sending a registration message to a registrar. This function is powerful and often needed for a highly mobile voice user base. The SIP client server application has two modes of operation; SIP clients can either signal through a proxy or redirect server.

- Using proxy mode, SIP clients send requests to the proxy and the proxy either handles requests or forwards them on to other SIP servers. Proxy servers can insulate and hide SIP users by proxying the signaling messages; to the other users on the VoIP network, the signaling invitations look as if they are coming from the proxy SIP server.
- Under redirect operation, the signaling request is sent to a SIP server, which then looks up the destination address. The SIP server returns the destination address to the originator of the call, who then signals the SIP client.

Features of SIP:

- Multi cast conference and media integration
- SIP supports personal mobility

VoIP Service Considerations:

The important service considerations while working on VoIP are as follows:

- Latency
- Jitter
- Bandwidth
- Packet Loss
- Reliability
- Security
- Interoperability

Virtual Private Networks (VPN):

For transmission of data over the Internet security is one of the most important concerns. Though network firewalls prevent most attacks from outsiders entering into the network using the Internet, they also prevent remote users to access essential data. VPN is a mechanism, that establishes a secured connection between the client and server. VPN stands for Virtual Private Network. A VPN uses the Internet as it's transport mechanism, while maintaining the security of the data on the VPN. It's the concurrent use of tunneling, encryption, authentication, and access control over a public network that basically characterizes a VPN. 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. The most common configuration is to have a single main internal network with remote nodes using VPN to gain full access to the central net. The remote nodes are commonly remote offices or employees working from home.

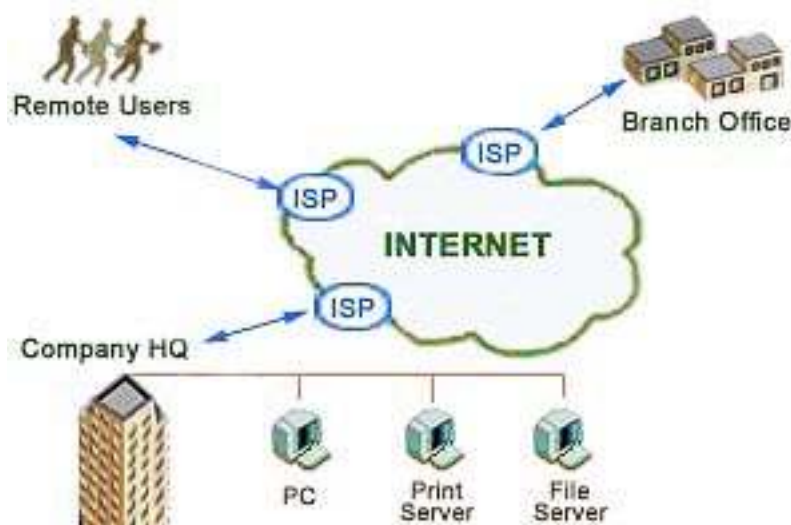


Fig: Architecture of VPN

Types of VPN:

The Virtual Private Networks can be categorized mainly into 3 categories. They are

- Intranet VPN
- Extranet VPN
- Remote Access VPN

Intranet VPN:

This type of VPN is client transparent. Intranet VPN is usually implemented for networks within a common network infrastructure but across various physical locations. For instance several buildings may be connected to a data center, or a common mainframe application that they can access securely through private lines. Intranet VPNs need to be especially secure with strong encryption and meet strict performance and bandwidth requirements. They must remain easily upgradeable since many vpn clients or users may be added (additional locations or applications).

Extranet VPN:

In this case VPN uses the Internet as main backbone. Extranet VPN usually addresses a wider scale of users and locations, enabling customers, suppliers and branch offices to access corporate resources across various network architectures. They rely on VPN standards such as IPsec to ensure maximum compatibility while trying not to overly compromise security

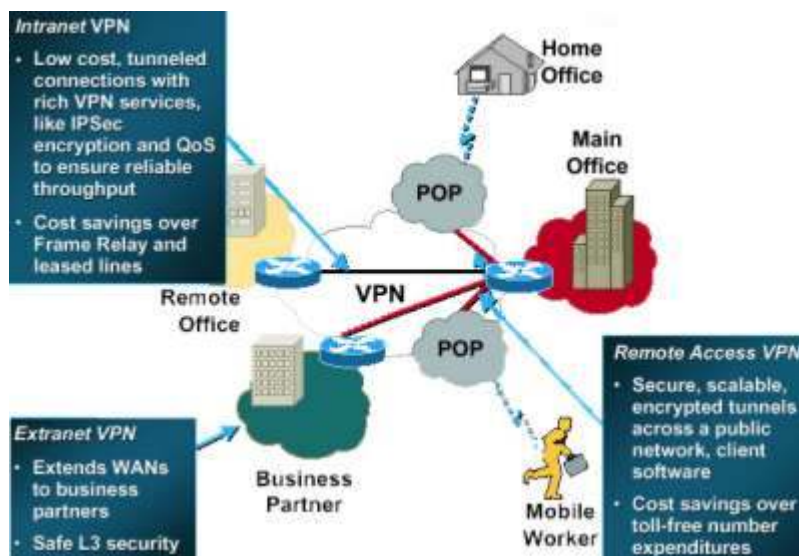


Fig: Types of Virtual Private Networks

Remote Access VPN:

In this VPN client is initiated. Remote Access VPN is intended for salesmen equipped with laptops and telecommuters that will connect intermittently from vary diverse locations (homes, hotels, conference halls...). The key factor of remote access VPN is flexibility as performance and bandwidth are usually minimal and less of an issue. More than encryption, authentication will be the main security concern for remote access vpn.

How VPN Work:

VPNs create "virtual" point-to-point connections using a technique called tunneling. VPN tunnel acts like a "pipe" which penetrates through a network to connect two points using public network through ISP. VPN tunneling encrypts data into standard TCP/IP packets and encapsulates it for safe transmission across the Internet. The following steps illustrate how the communication will happen over a Virtual Private Network.

- Connection establishes through ISP.
- The VPN client software on computer initiates a connection with the VPN server.
- The VPN server encrypts the data on the connection so it cannot be read by others while it is in transit.
- The VPN server decrypts the data and passes it on to other servers and resources.

Security Issues:

Securing a network requires a lot of issues to be considered. The most important requirements for secure communications are: Confidentiality, Data Integrity and Authentication.

- Confidentiality means that the information exchanged between the parties must be secretly scrambled, preventing unauthorized eavesdroppers from comprehending the message content.
- Data Integrity is the ability of the receiving party to verify that the message arrived without any changes made by an intruder.
- Authentication means that the party receiving a message is able to verify that the message is authentic by verifying the message origin.

For incorporating confidentiality into a communication link encryption is used. The encryption itself is also called cipher. The original message is called plain text. The plain text is encrypted in a secret manner into another message that is unreadable to everyone but the communicating parties. The encrypted message is called "Cipher text". For enabling security into a VPN one of the following methods are employed:

- Secured Socket Layer(SSL)
- IPSec (IP Security)

Secured Socket Layer (SSL):

The SSL standard is not a single protocol, but rather a set of accepted data transfer routines that are designed to protect the integrity of transmitted messages. SSL relies on certificates - digital identification cards - and keys. Certificates include the name of the certificate authority that issued the certificate, the name of the entity to which the certificate was issued, the entity's public key, and time stamps that indicate the certificate's expiration date.

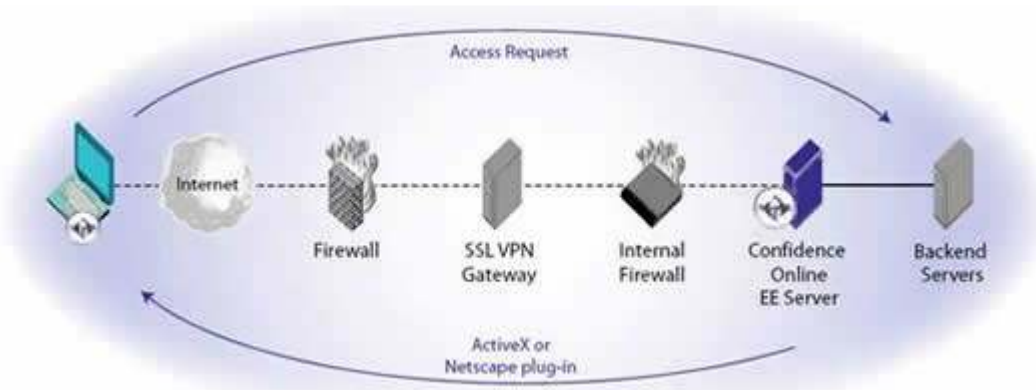


Fig: Secured Socket Layer Virtual Private Network

SSL is best used as the remote access and mobile access VPNs while IPsec is the best to create VPNs among fixed sites. Using an SSL VPN, the connection between the remote user and the internal resource happens via a Web connection at the application-layer, as opposed to IPSec VPNs' open □tunnel□ at the network-layer. The use of SSL is ideal for the remote and mobile user because:

- SSL does not need to be downloaded onto the device being used to access corporate resources.
- SSL does not need to be configured by the end user.
- SSL is available wherever there is a standard Web browser, which exists on any computer and many mobile devices.

In SSL there exist several kinds of algorithms for enabling the above features. The main cryptographic algorithms in SSL are

Symmetric Key Algorithm:

In symmetric key algorithm same key is used for both encryption and decryption.

Public Key Algorithm:

In Public key algorithm two different keys are used one is used for encryption, which is public and the other used for decryption, which is private and known to only the receiving party. Here, any one can transfer the message but the only a specific party is allowed to decrypt the message. There are several variations in Public Key Algorithm like using block ciphers etc. Data Integrity and Message Authentication can also be incorporated into a public key algorithm by using hash keys. More security will be incorporated by using Cipher Block Chaining(CBC) Methods.

IPSec:

IPSec is a suite of protocols designed to secure communication at the network layer. It provides two traffic security protocols, the Authentication Header(AH) and the Encapsulating Security Payload(ESP). Each AH/ESP protocol can work in either Transport or Tunnel mode. The AH and ESP protocols differ in that AH provides authentication while ESP provides confidentiality and optional authentication. Transport mode is used for host to host communications where the IP header is not protected. In applications such as VPN, Tunnel mode is employed.

Tunneling:

VPNs use the tunneling capability of IPSec to transparently move private data across the public Internet. Tunneling treats entire packets from a private internet work as payload data that must be transported across a public transport network.

A VPN gateway acts as one end of a "tunnel," encapsulating entire packets from the private inter-network in new IP packets before they travel across the public Internet. The new packets, carrying the private source and destination addresses, are simply directed to a second VPN gateway that protects the other end of the transmission. The receiving gateway then recognizes and disassembles the encapsulated packet before passing its contents on to the correct address on the private internet work.

The private network resources on each internal network, whether single machines or entire internet works, remain unaware of the fact that the Internet is being used as a transmission medium. A VPN gateway forms the foundation of a secure Internet-based portal to those resources, since it is designed to unconditionally reject all Internet traffic that is not tunneled IPSec. A variety of different network devices and software products can act as VPN gateways, including VPN access servers, VPN routers, and computers with VPN client software installed.

Advantages and Disadvantages of Using VPNs:

Advantages:

- VPNs enable secure broadband connections.
- VPNs make it easy to manage T1 lines, phone and data lines and remote access terminals.
- VPNs can create significant communication savings in particular when lots of remote users dial in from outside the local calling area.
- IP-based VPN can keep IT management costs down. Dynamic configuration ensures adaptability to changing network configuration and needs.

Disadvantages:

- VPNs may provide less bandwidth than by using direct lines.
- VPN is more prone to Internet connectivity problems. To ensure maximum availability it may be wise to secure on-call specialized support services, typical ISP support may not prove efficient enough.
- VPN being mostly Internet-based, it is dependent on connections to be up. If your ISP is down, so is your VPN. Emergency dial-in access may be used as limited, temporary back-up.

Compiled by: Venkata Ramana Murty R
ramana.murty@vassure.com