Tunneling

Tunneling is a way in which data is transferred between two networks securely. All the data being transferred is fragmented into smaller packets or frames and then passed through the tunnel. This process is different from a normal data transfer between nodes. Every frame passing through the tunnel will be encrypted with an additional layer of tunneling encryption and encapsulation, which is also used for routing the packets to the right direction. This encapsulation would then be reverted at the destination with decryption of data, which is later sent to the desired destined node.

A tunnel is a logical path between the source and the destination endpoints between two networks. Every packet is encapsulated at the source and de-capsulated at the destination. This process will keep happening as long as the logical tunnel is persistent between the two endpoints.

Tunneling is also known as the encapsulation and transmission of VPN data, or packets. IPSec tunnel mode enables IP payloads to be encrypted and encapsulated in an IP header so that it can be sent over the corporate IP internetwork or Internet.

IPSec protects, secures and authenticates data between IPSec peer devices by providing per packet data authentication. IPSec peers can be teams of hosts, or teams of security gateways. Data flows between IPSec peers are confidential and protected. The source and destination addresses are encrypted. The original IP datagram is left in tact. The original IP header is copied and moved to the left and becomes a new IP header. The IPSec header is inserted between these two headers. The original IP datagram can be authenticated and encrypted.

The tunnel is the logical path or connection that encapsulated packets travel through the transit internetwork. The tunneling protocol encrypts the original frame so that its content cannot be interpreted. The encapsulation of VPN data traffic is known as tunneling. The Transport Control Protocol/Internet Protocol (TCP/IP) protocol provides the underlying transport mechanism for VPN connectivity.
The two different types of tunneling are:

- Voluntary tunneling: With voluntary tunneling, the client starts the process of initiating a connection with the VPN server. One of the requirements of voluntary tunneling is an existing connection between the server and client. This is the connection that the VPN client utilizes to create a tunneled connection with the VPN server.
- Compulsory tunneling: With Compulsory tunneling, a connection is created between:

- Two VPN servers
- Two VPN access devices – VPN routers

In this case, the client dials-in to the remote access server, by using whichever of the following methods:

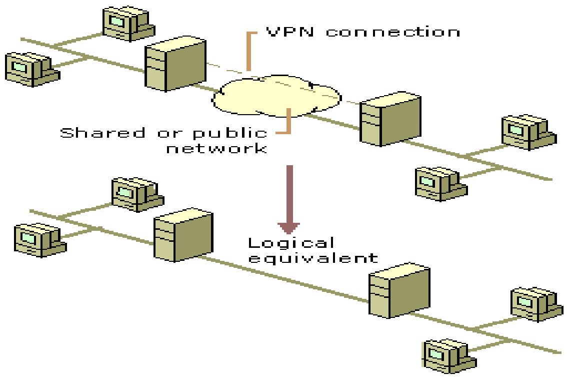
- Through the local LAN.
- Through a internet connection.

The remote access server produces a tunnel, or VPN server to tunnel the data, thereby compelling the client to use a VPN tunnel to connect to the remote resources.

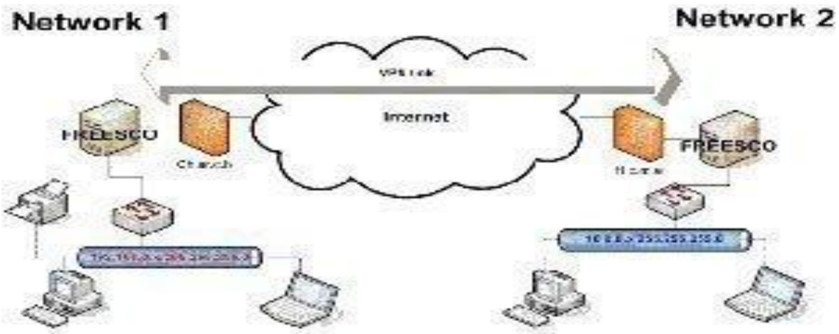
VPN tunnels can be created at the following layers of the Open Systems Interconnection (OSI) reference model:

- Data-Link Layer – layer 2: VPN protocols that operate this layer are Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP).
- Network Layer – layer 3: IPSec can operate as a VPN protocol at the Network layer of the OSI reference model.

VPN Overview



Virtual Private Networks (VPNs) provide secure and advanced connections through a non-secure network by providing data privacy. Private data is secure in a public environment. Remote access VPNs provides a common environment where many different sources such as intermediaries, clients and off-site employees can access information via web browsers or email. Many companies supply their own VPNconnections via the Internet. Through their ISPs, remote users running VPN client software are assured private access in a publicly shared environment. By using analog, ISDN, DSL, cable technology, dial and mobile IP; VPNs are implemented over extensive shared infrastructures. Email, database and office applications use these secure remote VPN connections.



A few of the main components needed to create VPN connections are listed below:

- VPN services need to be

enabled on the server.

- VPN client software has to be installed on the VPN client. A VPN client utilizes the Internet, tunneling and TCP/IP protocols to establish a connection to the network
- The server and client have to be on the same network.
- A Public Key Infrastructure (PKI)
- The server and client have to use the same:
  - ” Tunneling protocols
  - ” Authentication methods
  - ” Encryption methods.
- Centralized accounting

Remote access VPNs offer a number of advantages, including:

- Third parties oversee the dial up to the network.
- New users can be added with hardly any additional costs and with no extra expense to the infrastructure.
- Wan circuit and modem costs are eliminated.
- Remote access VPNs call to local ISP numbers. VPNs can be established from anywhere via the internet.
- Cable modems enable fast connectivity and are relatively cost efficient.
- Information is easily and speedily accessible to off-site users in public places via Internet availability and connectivity.

Tunneling Protocols Overview

The tunneling protocols are responsible for the following functions:

- Tunnel maintenance: This involves both the creation and management of the tunnel.
- VPN data transfer: This relates to the actual sending of encapsulated VPN data through the tunnel.

The tunneling protocols are:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

How Tunneling Works

There are two types of VPN connections, PPTP (Point-to-Point tunneling protocol) and L2TP (Layer 2 tunneling protocol). Both PPTP and L2TP tunnels are nothing but local sessions between two different endpoints. In case they have to communicate, the tunneling type must be negotiated between the endpoint, either PPTP or L2TP, then more configurable parameters like encryption, address assignment, compression, etc. must be configured in order to get the best possible security over the Internet based private logical tunnel communication. This communication is created, maintained, and terminated with a tunnel management protocol.

Data can be sent once the tunnel is in place and clients or the server can use the same tunnel to send and receive data across the internetwork. The data transfer depends upon the tunneling protocols being used for the transfer. For example, whenever the client wants to send data or payload (the packets containing data) to the tunneling server, the tunnel server adds a header to each packet. This header packet contains the routing information that informs the packet about the destination across the internetwork communication. Once the payload is received at the destination, the header information is verified. After, the destination tunnel server sends the packet to the destined node, client, or server.

Point-to-Point Protocol (PPP)

It is very obvious that the PPTP and L2TP protocols are fully dependent upon PPP connection and it is very much important to understand and examine PPP a little more closely. Initially, PPP was designed to work with only dial-up connections or dedicated connections. If the data transfer is happening over PPP connection, then the packets going over PPP are encapsulated within PPP frames and then sent across or transmitted over to the destination dial-up or PPP server.

There are four distinct phases of negotiation in a PPP connection. Each of these four phases must complete successfully before the PPP connection is ready to transfer user data.

- Phase 1: PPP Link Establishment First step is where PPP uses the LCP or Link Control Protocol to connect to the destination network. Apart from establishing the connection, LCP is also responsible for maintaining and terminating the connection. For example, during this phase 1, LCP connects to the destination and prepares the authentication protocol which will be used in phase 2. Next step would be to negotiate and find out if these two nodes in a PPP connection would agree on any compression or encryption algorithm. If the answer is yes then the same is implemented in Phase 4.
- Phase 2: A User Authentication Second step is where the user credentials are sent to the remote destination for authentication. There are different secure authentication programs. The secure authentication method must be used to safeguard the user credentials. If using PAP (password Authentication Protocol) for authorizing user credential, the user information is passed in plain clear text that can be captured easily. This is the only time that the user must take utmost care in handling his/her credential

from any theft. If for any reason an intruder captures these credentials, once the user connection is authenticated, the intruder will trap the communication, disconnect the original user, and take control of the connection.

- Phase 3: PPP Callback Control The Microsoft implementation of PPP includes an optional callback control phase. This phase uses the Callback Control Protocol (CBCP) immediately after the authentication phase. If configured for callback, both the remote client and NAS disconnect after authentication. The NAS then calls the remote client back at a specified phone number. This provides an additional level of security to dial-up connections. The NAS allows connections from remote clients physically residing at specific phone numbers only. Callback is only used for dial-up connections, not for VPN connections.
- Phase 4: Invoking Network Layer Protocol(s) Once the previous phases have been completed, PPP invokes the various network control protocols (NCPs) that were selected during the link establishment phase (Phase 1) to configure protocols that the remote client uses. For example, during this phase, IPCP is used to assign a dynamic address to the PPP client. In the Microsoft implementation of PPP, the Compression Control Protocol (CCP) is used to negotiate both data compression (using MPPC) and data encryption (using MPPE).

Data Transfer

Once the four phases of PPP negotiation have been completed, PPP begins to forward data to and from the two peers. Each transmitted data packet is wrapped in a PPP header that the receiving system removes. If data compression was selected in phase 1 and negotiated in phase 4, data is compressed before transmission. If data encryption is selected and negotiated, data is encrypted before transmission. If both encryption and compression are negotiated, the data is compressed first then encrypted.

Point-to-Point Tunneling Protocol (PPTP)

PPTP encapsulates PPP frames in IP datagram for transmission over an IP internetwork such as the Internet. PPTP can be used for remote access and router-to-router VPN connections.

PPTP or Point-to-Point tunneling protocol works over TCP ports, which are also used for tunnel management and GRE or Generic Routing Encapsulation protocol to encapsulate any PPP frames that will later be used to send data through the tunnel. Compression or encryption will depend on the tunnel configuration.
Point-to-Point Tunneling Protocol (PPTP), an extension of Point-to-Point Protocol (PPP), encapsulates PPP frames into IP datagrams to transmit data over an IP internetwork. To create and manage the tunnel, PPTP utilizes a TCP connection. A modified version of Generic

Route Encapsulation (GRE) deals with data transfer by encapsulating PPP frames for tunneled data. The encapsulated tunnel data can be encrypted and/or compressed. However, PPTP encryption can only be utilized when the authentication protocol is EAP-TLS or MS-CHAP. This is due to PPTP using MPPE to encrypt VPN data in a PPTP VPN, and MPPE needing EAP-TLS or MS-CHAP generated encryption keys.
The authentication methods supported by PPTP are the same authentication mechanisms supported by PPP:

- PAP
- CHAP
- MS-CHAP
- EAP

Layer Two Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) is a combination of the benefits and features of PPTP and Cisco's Layer 2 Forwarding (L2F) protocol. L2TP encapsulates PPP frames, and sends encapsulated data over IP, frame relay, ATM and X.25 networks. With L2TP, the PPP and layer two end-points can exist on different devices. L2TP can also operate as a tunneling protocol over the Internet. L2TP uses UDP packets and a number of L2TP messages for tunnel maintenance. UDP is used to send L2TP encapsulated PPP frames as tunneled data.

While L2TP can provide encryption and compression for encapsulated PPP frames, you have to use Microsoft's implementation of L2TP with the IPSec security protocol. When L2TP is used with IPSec, the highest level of security is assured. This includes data confidentiality and integrity, data authentication, as well as replay protection. IPSec protects the packets of data and therefore provides security on insecure networks such as the Internet. This is due to IPSec securing the actual packets of data, and not the connection used to convey the data. IPSec utilizes encryption, digital signatures and hashing algorithms to secure data.

IPSec provides the following security features:

- Authentication; digital signatures are used to authenticate the sender.
- Data integrity; hash algorithms ensure that data has not been tampered with while in transit.
- Data privacy; encryption ensures that data cannot be interpreted while in transit.
- Repay protection; protects data by preventing unauthorized access by any attackers who resend data.
- The Diffie-Hellman key agreement algorithm is used to generate keys. This makes it possible for confidential key agreement to occur.

- Non-repudiation; public key digital signatures authenticate the origin of the message.

The two IPSec protocols are:

- Authentication Header (AH); provides data authentication, data integrity and replay protection for data.
- Encapsulating Security Payload (ESP); provides data authentication, data confidentiality and integrity, and replay protection.

Source: http://www.tech-faq.com/tunneling.html