VIRTUAL PRIVATE NETWORK

By:
Er.Amit Mahajan
Introduction

- In a VPN, private communication between two or more devices is achieved through a public network the Internet. Therefore, the communication is virtually but not physically there.
- Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them.
- A VPN is a network which can transmit information over long distances effectively and efficiently.
**Introduction**

- With VPNs businesses can securely connect remote offices and remote users using cost-effective, third-party Internet access rather than expensive dedicated WAN links or long-distance remote dial links.
- Organizations can reduce WAN bandwidth costs while increasing connectivity speeds by using high-bandwidth Internet connectivity, such as Ethernet, and cable, and securing it with VPN tunnels.
- VPNs provide the highest possible level of security through encryption and authentication.
- Thus, Virtual Private Network is defined as a network that uses public network paths but maintains the security and protection of private networks.
Private Networks
vs.
Virtual Private Networks

- Employees can access the network (Intranet) from remote locations.
- Secured networks.
- The Internet is used as the backbone for VPNs
- Saves cost tremendously from reduction of equipment and maintenance costs.
- Scalability
Categories of VPN

● VPNs were broken into 4 categories-

1. **Trusted VPN**: A customer “trusted” the leased circuits of a service provider and used it to communicate without interruption. Although it is “trusted” it is not secured.

2. **Secure VPN**: With security becoming more of an issue for users, encryption and decryption was used on both ends to safeguard the information passed to and fro. This ensured the security needed to satisfy corporations, customers, and providers.

3. **Hybrid VPN**: A mix of a secure and trusted VPN. A customer controls the secure parts of the VPN while the provider, such as an ISP, guarantees the trusted aspect.

4. **Provider-provisioned VPN**: A VPN that is administered by a service provider.
A VPN enables one to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint.

To emulate a private link, the data being sent is encrypted for confidentiality.

Packets that are intercepted on the shared or public network are indecipherable without the encryption keys.

The portion of the connection in which the private data is encapsulated is known as the tunnel.

**Figure:** Tunneling
The portion of the connection in which the private data is encrypted is known as the VPN connection.

VPN connections allow users working at home or on the road to connect in a secure fashion to a remote corporate server.

The VPN architecture is shown in Figure.

The VPN connection is a point-to-point connection between the user’s computer and a corporate server.

The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites.
VPN TOPOLOGY

How a VPN works internally:

- To begin using a VPN, an Internet connection is needed;
- A specially designed router or switch is then connected to each Internet access circuit to provide access from the origin networks to the VPN.

- The VPN devices create PVCs (Permanent Virtual Circuit) through tunnels allowing senders to encapsulate their data in IP packets.
- The VPN device at the sending side takes the packet or frame and encapsulates it to move through the VPN tunnel across the Internet to the receiving end.
The process of moving the packet using VPN is transparent to both the users, Internet Service Providers (ISP) and the Internet as a whole.

When the packet arrives on the receiving end, another device will strip off the VPN frame and deliver the original packet to the destination network.

VPNs operate at either layer 2 or layer 3 of the OSI model (Open Systems Interconnection).

Layer-2 VPN uses the layer 2 frame such as the Ethernet while layer-3 uses layer 3 packets such as IP.

Layer-3 VPN starts at layer 3, where it discards the incoming layer-2 frame and generates a new layer-2 frame at the destination.

Two of the most widely used protocols for creating layer-2 VPNs over the Internet are: layer-2 tunneling protocol (L2TP) and point-to-point tunneling protocol (PPTP).

The newly emerged protocol, called Multiprotocol Label Switching (MPLS) is used exclusively in layer-3 VPNs.
1. **User Authentication:** The solution must verify the VPN client's identity and restrict **VPN access to authorized users only:** It must also provide audit and accounting records to show who accessed what information and when.

2. **Address Management:** The solution must assign a VPN client's address on the intranet and ensure that private addresses are kept private.

3. **Data Encryption:** Data carried on the public network must be rendered unreadable to unauthorized clients on the network.

4. **Key Management:** The solution must generate and refresh encryption keys for the client and the server.

5. **Multiprotocol Support:** The solution must handle common protocols used in the public network. These include IP, Internetwork Packet Exchange (IPX), and so on.
Components Of The VPN

1) SECURITY

- Companies need to keep their VPNs secure from tampering and unauthorized users.
- Some examples of technologies that VPN’s use are:
  A. IP Security (IPSec),
  B. Point-to-Point Tunneling Protocol (PPTP),
  C. Layer 2 Tunneling Protocol and
  D. Multiprotocol Label Switching (MPLS) along with Data Encryption Standard (DES), and
A). IPSec

- IPSec uses
  - data encryption standard (DES) and other algorithms for encrypting data,
  - public-key cryptography to guarantee the identities of the two parties to avoid man-in-the-middle attack,
  - and digital certificates for validating public keys.

- IPSec is focused on Web applications, but it can be used with a variety of application-layer protocols.

- It sits between IP at the network layer and TCP/UDP at the transport layer.

- Both parties negotiated the encryption technique and the key before data is transferred.
IPSec

- IPSec can operate in either transport mode or tunnel mode.

**In tunnel model,**
- Intruders can only see where the end points of the tunnel are, but not the destinations of the packet and the sources.
- IPSec encrypts the whole packet and adds a new IP packet that contains the encrypted packet. The new IP packet only identifies the destination’s encryption agent.
- When the IPSec packet arrives at the encryption agent, the new encrypted packet is stripped and the original packet continues to its destination.

**In Transport mode,**
- IPSec leaves the IP packet header unchanged and only encrypts the IP payload to ease the transmission through the Internet.
- IPSec here adds an encapsulating security payload at the start of the IP packet for security through the Internet.
- The payload header provides the source and destination addresses and control information.
PPTP uses Point-to-Point Protocol (PPP) to provide remote access that can be tunneled through the Internet to a desired site.

Tunneling allows senders to encapsulate their data in IP packets that hide the routing and switching infrastructure of the Internet from both senders and receivers to ensure data security against unwanted viewers, or hackers.

PPTP is designed to run on the Network layer of the Open systems interconnection (OSI).

It uses a voluntary tunneling method, where connection is only established when the individual user request to logon to the server.

PPTP tunnels are transparent to the service provider.
Layer Two Tunneling Protocol (L2TP) exists at the data link layer of the OSI model.

L2TP is a combination of the PPTP and Layer two Forwarding (L2F).

L2TP uses a compulsory tunneling method, where a tunnel is created without any action from the user, and without allowing the user to choose a tunnel.

A L2TP tunnel is dynamically established to a predetermined end-point based on the Network Access Server (NAS) negotiation with a policy server and the configured profile.

L2TP also uses IPSec for computer-level encryption and data authentication.
D). Multiprotocol Label Switching (MPLS)

- Multiprotocol Label Switching (MPLS) uses a label swapping forwarding structure.
- It is a hybrid architecture which attempts to combine the use of network layer routing structures and per-packet switching, and link-layer circuits and per-flow switching.
- When the packets enter the MPLS, it is assigned a local label and an outbound interface based on the local forwarding decision.
- The forwarding decision is based on the incoming label, where it determines the next interface and next hop label.
- The MPLS uses a look up table to create end-to-end transmission pathway through the network for each packet.
The second component after security is FIREWALL. Firewalls monitors traffic crossing network parameter, and protect enterprises from unauthorized access. The organization should design a network that has a firewall in place on every network connection between the organization and the Internet. Two commonly used types of firewalls are packet-level firewalls and application-level firewalls.

- **Packet-level firewall** checks the source and destination address of every packet that is trying to passes through the network.
- **Application-level firewall** acts as a host computer between the organization’s network and the Internet. Users who want to access the organization’s network must first log in to the application-level firewall and only allow the information they are authorized for.
3). MANAGEMENT

- The 3rd component is MANAGEMENT - managing security policies, access allowances, and traffic management.
- VPN’s need to be flexible to a company’s management, some companies chooses to manage all deployment and daily operation of their VPN, while others might choose to outsource it to service providers implementing a VPN.
Common Uses Of VPNs

1. Remote Access Over The Internet

- VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information.
- Figure shows a VPN connection used to connect a remote user to a corporate intranet.
- Rather than making a long distance (or 1-800) call to a corporate or outsourced network access server (NAS), the user calls a local ISP.
- Using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

Figure: Using a VPN connection to connect a remote client to a private intranet
2. Connecting Networks Over The Internet

- There are two methods for using VPNs to connect local area networks at remote sites:
  a) **Using dedicated lines to connect a branch office to a corporate LAN.**
  b) **Using a dial-up line to connect a branch office to a corporate LAN.**

In both cases, the facilities that connect the branch office and corporate offices to the Internet are local.
3. Connecting Computers Over An Intranet

- In some corporate internetworks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate internetwork.
- Although this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.

- VPNs allow the department's LAN to be physically connected to the corporate internetwork but separated by a VPN server.
US accounting firm McGladrey & Pullen has increased productivity by moving its mainly mobile workforce to a virtual private network.

To keep up with technology, McGladrey & Pullen recently replaced its direct-dial RAS infrastructure with a Virtual Private Network (VPN).

The VPN, which supports as many as 2,700 mobile or remote users, is based on AT&T WorldNet's Virtual Private Network Service (VPNS).

VPNS provides secure remote access to corporate local and wide area networks, intranets and extranets.

The VPN rollout replaced a patchwork of dial-up centres with remote-access servers each with different configurations and equipment.

The goal is to give remote users the same capabilities they would have if they were connected to the office LAN.

The first step was replacing the company's Lotus cc: Mail dial-up email server with IP dial-up connections. The old system was adequate for sending and receiving email, but IP dial-up offers more.
By using per hour billing, the firm pays for what it uses nothing more.

In their Mail layout, they had a post office in every office with modems hanging off of them.

But with the new VPN, the firm has gone to a central server to which everybody connects.

The firm found that VPN provide a shared pool of time. It saves a lot of money and it's much more efficient."

It also found that the technology changes resulted in cost savings.
Conclusion

- VPN is an emerging technology that has come a long way.
- From an insecure break off of Public Telephone networks to a powerful business aid that uses the Internet as its gateway. Secure communication is done using IPSec.
- VPN’s technology is still developing, and this is a great advantage to businesses, which need to have technology that is able to scale and grow along with them.
- With VPN businesses now have alternative benefits to offer to their employees, employees can work from home, take care of children while still doing productive, and have access work related information at anytime.
- VPN will also help to make the possibility of a business expanding its services over long distances and globally, more of a reality.
BIBLIOGRAPHY


THANK YOU