VPN: VIRTUAL PRIVATE NETWORK

Presented by, Sreehari.R.B.
Contents

• Introduction
• How VPN works?
• Tunneling
• VPN Security
• Requirements of VPN
• Applications of VPN
• Advantages
• Applications
• Conclusion
•
What is VPN?

- Virtual
- Private
- Network
Introduction

• Virtual Private Network is a private communication network usually used within a company or by different companies to communicate and exchange data over the network.

• In VPN the messages are carried on a public network (i.e., internet) using standard protocols or over a service provider’s network.
• The main purpose of VPN is to provide a cost efficient way of private networking compared to traditional private networking techniques.

• A VPN makes it possible to have protected sharing of sensible data through a public network.

• In order to perform the data transfer safely, VPN uses special tunneling processes and complex encryption procedures.
How VPN works?

• A VPN works by using a shared public infrastructure while maintaining privacy through security procedures and tunneling protocols.

• In VPN the data are passed through a “tunnel”, in which a data which is not properly encrypted cannot be entered.

• An additional level of security involves encrypting not only the data but also the originating and receiving network address.
Tunneling

- Tunneling is the process of placing an entire packet within another packet and sending it over a network.

- Tunneling requires three different protocols:
  - **Carrier protocol** - The protocol used by the network that the information is traveling over.
  - **Encapsulating protocol** - The protocol that is wrapped around the original data.
  - **Passenger protocol** - The original data being carried.
The truck is the carrier protocol, the box is the encapsulating protocol and the computer is the passenger protocol.
Tunneling

- Virtual private network technology is based on the idea of tunneling.

- VPNs rely on tunneling to create a private network that reaches across the Internet.

- By tunneling process only the recipient at the other end of transmission can see or access the data inside the protective encryption shell.
• Tunneling encrypts and encapsulates our own network protocols within IP.

• The protocols of the outer packet is understood by the network and two end points called tunneling interface, where the packets enters and exits the network.

• For example, you can place a packet that uses a protocol not supported on the Internet (such as NetBeui) inside an IP packet and send it safely over the Internet.
Tunneling protocols used in VPN

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security
VPN Security

• A well-designed VPN uses several methods for keeping your connection and data secure:
  1. Firewalls
  2. Encryption
  3. IPSec
  4. AAA Server
Firewalls:

- A firewall provides a strong barrier between the private network and the Internet.
- We can set firewalls to restrict the number of open ports, what type of packets is passed through and which protocols are allowed through.
Encryption

- Encryption is the process of converting data to a secret code for transmission over an unsecured network.

- Most computer encryption systems belong in one of two categories:
  - Symmetric-key encryption
  - Public-key encryption
Symmetric-key encryption:

- In symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer.

- In this technique you should know which computers will be talking to each other so you can install the key on each one.
Public key encryption:

- Public-key encryption uses a combination of a private key and a public key.
- The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it.
- To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key.
Internet Protocol Security (IPsec)

• Internet Protocol Security (IPSec) provides enhanced security features such as better encryption algorithms and more comprehensive authentication.

• IPSec has two encryption modes: tunnel and transport modes.

• Tunnel encrypts the header and the payload of each packet.

• While transport only encrypts the payload.
IPsec

- Only systems that are IPSec compliant can take advantage of this protocol.
- All devices must use a common key.
- IPSec can encrypt data between various devices, such as:
  - Router to router
  - Firewall to router
  - PC to router
  - PC to server
AAA Servers

• AAA (authentication, authorization and accounting) servers are used for more secure access in a remote-access VPN environment.

• When a request to establish a session comes in from a dial-up client, the request is proceed to the AAA server. AAA then checks the following:
  – Who you are (authentication)
  – What you are allowed to do (authorization)
  – What you actually do (accounting)
Applications of VPN

1) Remote Access

• Business professionals who travel frequently or who often work at home after hours find this solution to be of great benefit to their ability to get things done.

• No matter where they are, secure access to their entire business is only a local telephone call away.

• This is also a useful solution for cases where key personnel need to be away from the office for an extended period of time.
Applications of VPN

2) Site-to-Site Connectivity

• The global business of today’s marketplace often requires companies to establish regional and international branch offices.

• Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network.
A VPN may be implemented in several ways:

1. LAN-to-LAN

   If a company has one or more remote locations that they wish to join in a single private network, they can create a VPN, to connect LAN to LAN.
2. Remote user-to-LAN

The VPN client allows telecommuters and traveling users to communicate on the central network of an organization and access servers from many different locations.

3. Within an intranet

With Intranet VPN, gateways at various physical locations within the same business negotiate a secure communication channel across the Internet.
Advantages:

- Greater scalability.
- Mobility.
- Security.
- Reliability.
- Easy to add/remove users.
- Reduced long-distance telecommunications costs.
- Network management.
- Policy Management.
Requirements of VPN

- VPN services need to be enabled on the server.
- VPN client software has to be installed on the VPN client.
- The server and client have to be on the same network.
- The server and client have to use the same:
  - Tunneling protocols
  - Authentication methods
  - Encryption methods
Where it is used.

- VPNs are normally implemented (deployed) by businesses or organizations rather than by individuals.

- **Healthcare:** enables the transferring of confidential patient information within the medical facilities & health care provider.

- **Manufacturing:** allow suppliers to view inventory & allow clients to purchase online safely.

- **Retail:** able to securely transfer sales data or customer info between stores & the headquarters.
Conclusion

• Thus VPN is an outgrowth of the Internet technology, which will transform the daily method of doing business faster than any other technology.

• A Virtual Private Network, or VPN, typically uses the Internet as the transport backbone to establish secure links with business partners, extend communications to regional and isolated offices, and significantly decrease the cost of communications.
THANK YOU