Virtual Private Networking (VPN)

Roll No. - 45-49
Group VII
Intro To VPN

- **Virtual Private Network** as name suggests, safely and securely transfers information from one network to another system.
- Organizations which are connected by a single logical network via Routers & WAN technologies
- They are inter-connected to do PRIVATE data sharing.
- Supports telecommuters, branch offices, & off site partners, hence most vital part of corporate IT world.
Need Of VPN

• In this world internet is the most essential thing to do communication & data transfers.

• But for some organizations which are spreading over the world need one thing, a way to maintain fast, reliable & secured communication.

• WAN has fast speed, High performance but less security, reliability & too expensive.

• For that Virtual Private Network is the best possible solution.
In short, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. 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.
Features OF VPN

• Security
• Reliability
• Scalability
• Network management
• Policy management
Connections in VPN

- **Intranet VPN**
  - Low cost, tunneled connections with rich VPN services, like IPSec encryption and QoS to ensure reliable throughput
  - Cost savings over Frame Relay and leased lines

- **Extranet VPN**
  - Extends WANs to business partners
  - Safe L3 security

- **Remote Access VPN**
  - Secure, scalable, encrypted tunnels across a public network, client software
  - Cost savings over toll-free number expenditures
• Remote Access-

Better known as Virtual Private Dial-up Network (VPDN)
This is Remote user-to-LAN connection
Mostly Organizations outsource ESP (Enterprise Service Provider) which sets Network Access Server (NAS) & provides the remote users with desktop client software for their computers. The telecommuters can then dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network. (e.g. Call Center)

Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.
- **Site to Site** - Connection b/w multiple site via Internet

It is divided in two parts

<table>
<thead>
<tr>
<th>Intranet Based</th>
<th>Extranet Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Private network between</td>
<td>Network between two companies (ie</td>
</tr>
<tr>
<td>Company’s remote locations.</td>
<td>Partner, Customer, etc) so that</td>
</tr>
<tr>
<td></td>
<td>working is in shared environment</td>
</tr>
<tr>
<td>Connection can be LAN - LAN</td>
<td>Connection can be LAN - LAN</td>
</tr>
</tbody>
</table>
Requirements of VPN

- **User Authentication** - VPN accessed should be restricted to authorized users only.

- **Address Management** - Ensuring that the private address are kept private.

- **Data Encryption** - Data carried must be unreadable to unauthorized users.
• **Multi protocol Support**: The solution must be able to handle common protocols used in the public network. These include Internet Protocol (IP), internet packet exchange (IPX) and so on.
How does VPN work?

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

- In effect, by encoding data at the sending end and decoding it at the receiving end, the protocols send the data through a 'tunnel' that cannot be 'entered' by data that is not properly encrypted.

- An additional level of security involves encoding not only the data, but also the originating and receiving network addresses.
Tunneling is the process of placing an entire packet within another packet and sending it over a network, its noting but point-point topology.

At Tunnel interfaces, the packet enters and exits the network.

It Requires three protocols-
1. Carrier protocol
2. Encapsulating protocol
3. Passenger protocol
• **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: Site - Site**

**GRE (generic routing encapsulation):**

Normally encapsulating protocol that provides the framework for how to package the passenger protocol for transport over the carrier protocol, IP based. Information on what type of packet you are encapsulating and information about the connection between the client and server.

**IPSec (IP Security):**

Sometimes instead of GRE IPSec is used. It is the encapsulating protocol, IPSec works well on both remote-access and site-to-site VPN.
Tunnelling: Site-to-Site VPN
Tunneling normally takes place using PPP (carrier for other IP protocols when communicating over the network between the host and a remote system)

**L2F (Layer 2 Forwarding):** L2F will use any authentication scheme supported by PPP.

**PPTP (Point-to-Point Tunneling Protocol):** supports 40-bit and 128-bit encoding and will use any authentication scheme supported.

**L2TP (Layer 2 Tunneling Protocol):** Combining features of both PPTP and L2F, L2TP also fully supports IPSec.
Types Of VPN Services

- **L1 Services:**
  1. VPWS

- **L2 Services:**
  1. VPLS
  2. Pseudo Wire (PW)
  3. IPLS

- **L3 Services:**
  1. BGP/MPLS VPN
  2. Virtual Router VPN
- **Layer 1 Service:**
  VPWS: The provider does not offer a full routed or bridged network, but components from which the customer can build customer-administered networks. VPWS are point-to-point. They can be Layer 1 emulated circuits with no data link structure.

- **Layer 2 Services:**
  PW (Pseudo Wiring): PW is similar to VPWS, but it can provide different L2 protocols at both ends.
Virtual Private LAN Services (VPLS): Allow multiple tagged LANs to share common Data. Not useful for customer-owned facilities. emulates the full functionality of a traditional LAN. The remote LAN segments behave as one single LAN.
• **L3 Services:**

**BGP/MPLS VPN:** PE disambiguates duplicate addresses in a single routing instance. Extensions are used to advertise routes, which are of the form of 12-byte strings, beginning with an 8-byte and ending with a 4-byte IPv4 address.

**Virtual LAN:** The PE contains a virtual router instance per VPN. Opposed to BGP/MPLS techniques as multiple virtual routers belong to one and only one VPN.
VPN Security

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

Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Most computer encryption systems belong in one of two categories:

- Symmetric-key encryption
- Public-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.
- Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one.
• **Symmetric key** encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information.

• **The code provides the key to decoding the message.**

• The sending computer encrypts the document with a symmetric key, then encrypts the symmetric key with the public key of the receiving computer.

• The receiving computer uses its private key to decode the symmetric key. It then uses the symmetric key to decode the document.
• **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.

• A very popular public-key encryption utility is called **Pretty Good Privacy (PGP)**, which allows you to encrypt almost anything.
3. Internet Protocol Security

Protocol (IPSec):

- IPSec provides enhanced security features such as better encryption algorithms and more comprehensive authentication.
- IPSec has two encryption modes: tunnel and transport.
  - Tunnel encrypts the header and the payload of each packet while transport only encrypts the payload. Only systems that are IPSec compliant can take advantage of this protocol. Also, all devices must use a common key and the firewalls of each network must have very similar security policies set up.
- IPSec can encrypt data between various devices, such as:
  - Router to router
  - Firewall to router
  - PC to router
  - PC to server
Benefits of VPN

A well-designed VPN can greatly benefit a company. For example, it can:

- Extend geographic connectivity
- Improve security
- Reduce operational costs versus traditional WAN
- Reduce transit time and transportation costs for remote users
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support
- Provide broadband networking compatibility
- Provide faster ROI (return on investment) than traditional WAN
How VPN differ from ordinary networks

- Virtual Private Networks allow any valid remote user to become part of a corporate central network, using the same network scheme and addressing as users on this central network.
- Each Corporate central network can also be responsible for validating their own users, despite the fact that they are actually dialing into a public network.
• The Internet Service Provider can give each of their customer's a unique dial-up telephone number, which will distinguish their service from any other. But this is depends on the software that will be used by the remote user.
Mobile VPNs are designed for mobile and wireless users. They integrate standards-based authentication and encryption technologies to secure data transmissions to and from devices and to protect networks from unauthorized users. Designed for wireless environments, Mobile VPNs are designed as an access solution for users that are on the move and require secure access to information and applications over a variety of wired and wireless networks. Mobile VPNs allow users to roam seamlessly across IP-based networks and in and out of wireless coverage areas without losing application sessions or dropping the secure VPN session.
VPN Challenges

• Setting up the infrastructure before deploying VPN:
  Many of the branch offices operated on dial-up connections, which were slow and often unreliable.

  So the first step was to get 24x7 connectivity using DSL or similar technology.
Paucity of IT staff at remote locations:

Since many of the branch offices were small and/or recently set up, there was no dedicated IT staff at remote locations.

The challenge was to build a solution that was literally 'plug-and-play' - that could be easily setup, deployed and managed, with an option for remote manageability as well in case advanced troubleshooting was required.
Reliability of the ISP connection and support for dial-up backup:

In many locations, if the main ISP connection was down, the connectivity to the head office was maintained via dial-up.

It was a prerequisite that the VPN solution work not just on the regular ISDN or DSL connection, but also on the dial-up, so that application uptime could be maintained.
Since this was a real-time application, the end users would have to get a reasonable response time, or else they might abandon the use of the application. The response time depends on several factors besides the VPN solution, such as the coding in the software application, the quality of the ISP connection, the volume of data being transferred by the application and the general level of congestion on the Internet pipe itself.

Keeping all these factors in mind and yet providing an interface, which would not cause the user to lose patience with it, was one of the foremost issues that needed to be addressed.
Since the implementation of the VPN involved opening up the IT infrastructure of the branches to the Internet, a firewall solution to protect the branch network was also required. But as there was no budgetary provision for a separate firewall, the VPN appliance was required to provide firewall functionality as well.

The firewall had to be simple to configure and manage, that is, meet all the requirements of the VPN solution.
User acceptance:

A major challenge faced during the implementation of this IT and security project was to gain the acceptance of remote users throughout the country to switch from a decentralized, batch process-oriented manual system to a centrally administered and managed real-time system.

This was achieved by educating end users about the use and benefits of VPN and training.
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 for an increasingly mobile workforce. VPNs serve as private network overlays on public IP network infrastructures such as the Internet.
Today, VPNs are equally appealing to companies of all sizes. Even small businesses are finding compelling reasons to implement VPNs.

The primary purposes of the VPN客观性 are:

- Promote the products of its members to the press and to potential customers
- Increase interoperability between members by showing where the products interoperate
- Serve as the forum for the VPN manufacturers throughout the world
- Help the press and potential customers understand VPN technologies and standards
BIBLIOGRAPHY

- www.scribd.com
- www.wikipedia.org
- www.howstuffworks.com
- www.google.com
THANK YOU