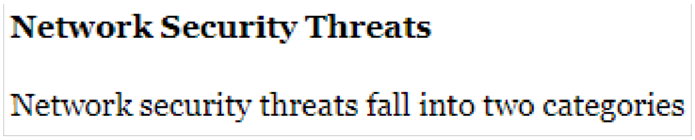
UNIT 5

Security and Privacy

- **Network Security**
- **Firewall**
- **VPN**

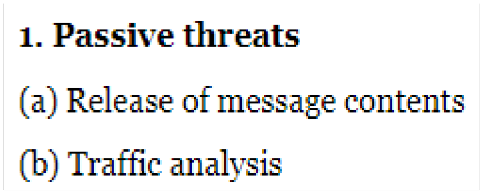
Network security

- Computer Security means to protect information.
- It deals with prevention and detection of unauthorized actions by users of a computer.
- In simple words security is defined as *"Protecting information system from unintended access"*
- Network security measures are needed to protect data during their transmission and to guarantee that data transmissions are authentic



Network Security Threats

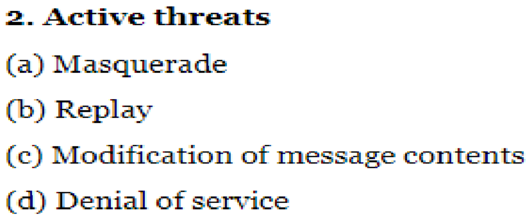
Network security threats fall into two categories



1. Passive threats

(a) Release of message contents

(b) Traffic analysis



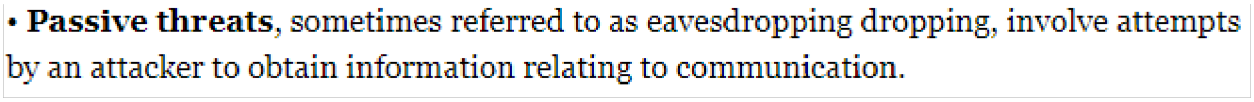
2. Active threats

(a) Masquerade

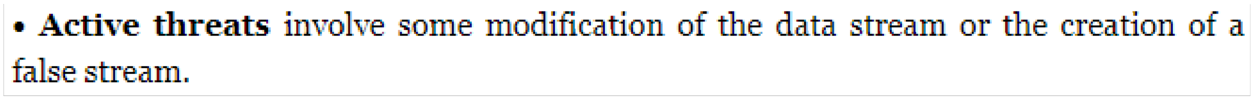
(b) Replay

(c) Modification of message contents

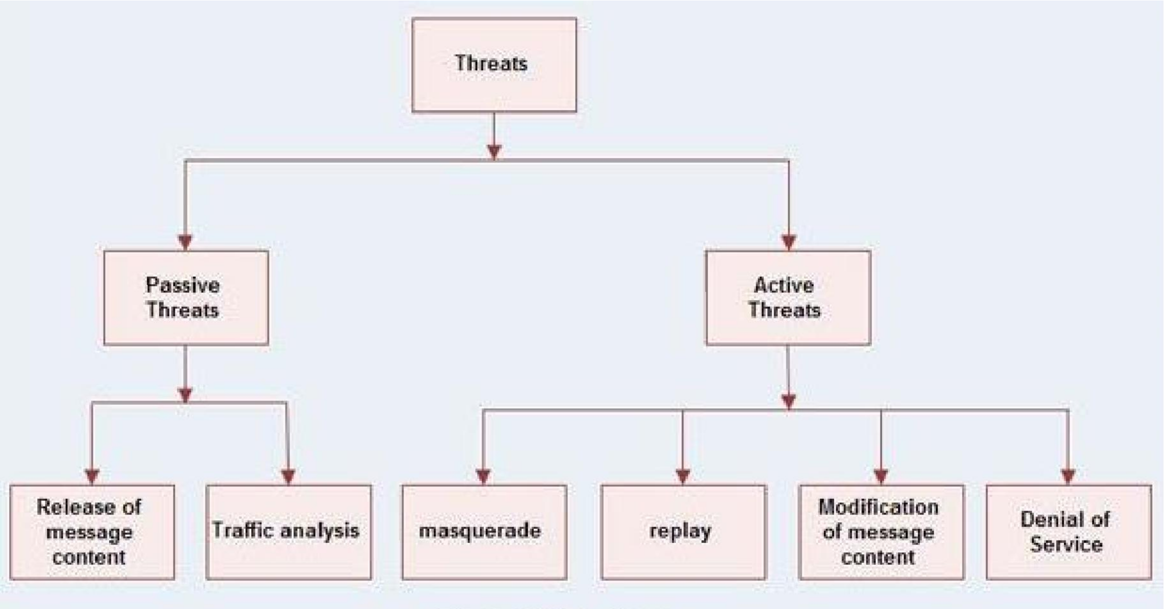
(d) Denial of service



• **Passive threats**, sometimes referred to as eavesdropping dropping, involve attempts by an attacker to obtain information relating to communication.



• **Active threats** involve some modification of the data stream or the creation of a false stream.



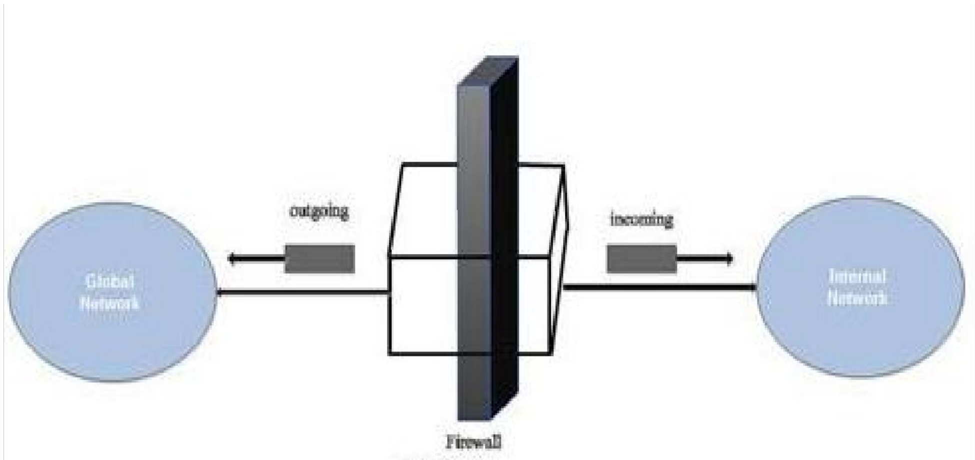
Security threats

Firewall

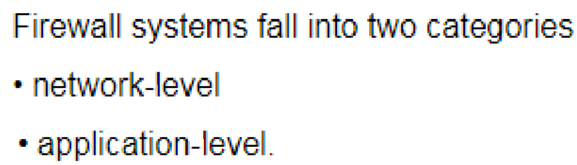
- A firewall is a device installed between the internet network of an organization and the rest of Internet.
- When a computer is connected to Internet, it can create many problems for corporate companies.
- Most companies put a large amount of confidential information online.
- Such an information should not be disclosed to the unauthorized persons
- Second problem is that the virus, worms and other digital pests can breach the security and can destroy the valuable data.

- The main purpose of a firewall is to separate a secure area from a less secure area and to control communications between the two.
- Firewall also controlling inbound and outbound communications on anything from a single machine to an entire network
- On the Other Hand Software firewalls, also sometimes called personal firewalls, are designed to run on a single computer.

- These are most commonly used on home or small office computers that have broadband access, which tend to be left on all the time
- A software firewall prevents unwanted access to the computer over a network connection by identifying and preventing communication over risky ports
- Computers communicate over many different recognized ports, and the firewall will tend to permit these without prompting or alerting the user.

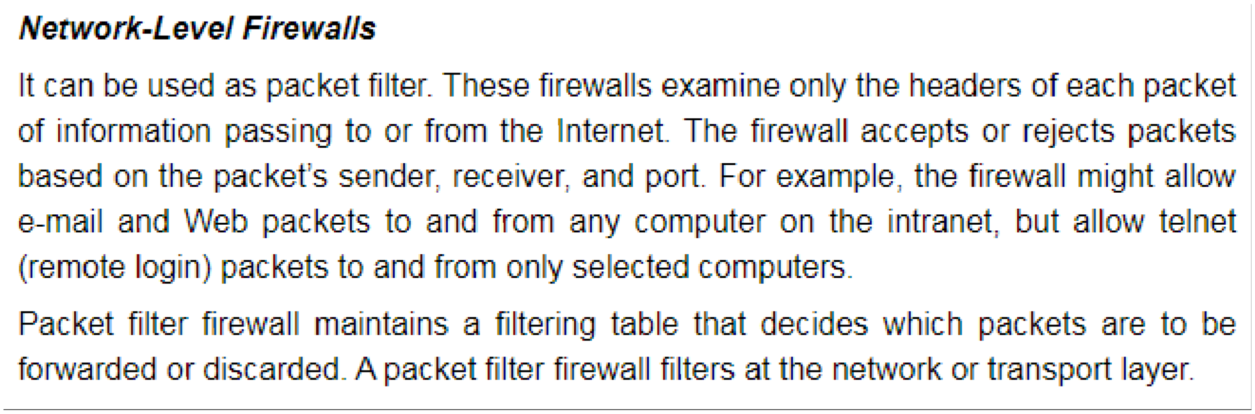


Firewall



Firewall systems fall into two categories

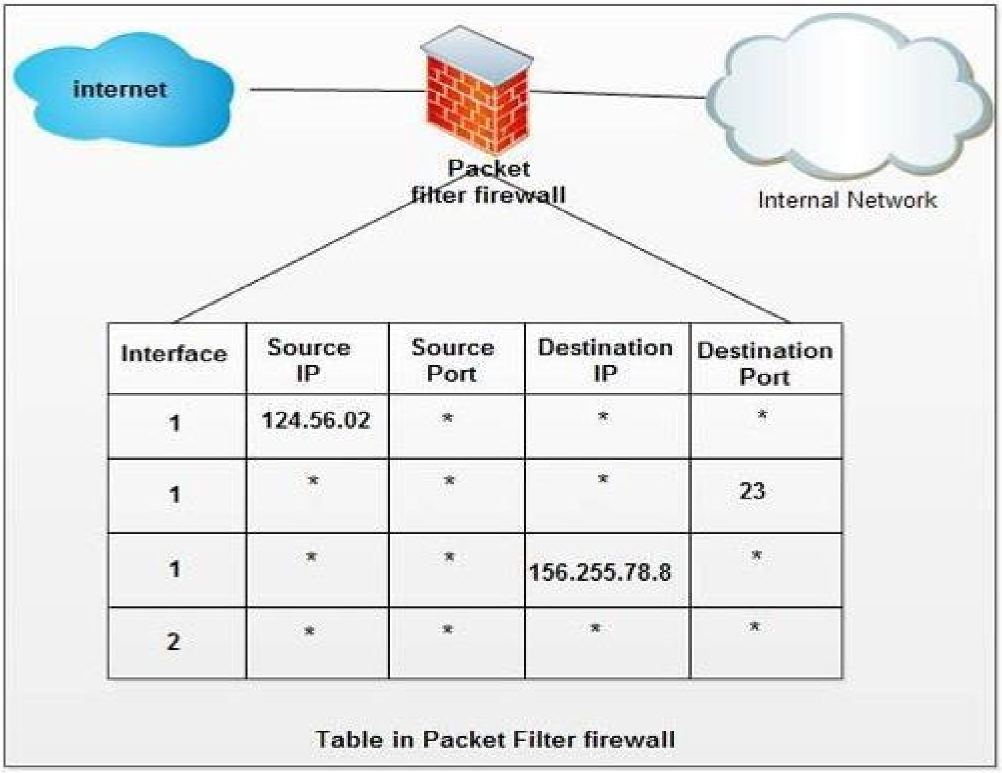
- network-level
- application-level.



Network-Level Firewalls

It can be used as packet filter. These firewalls examine only the headers of each packet of information passing to or from the Internet. The firewall accepts or rejects packets based on the packet's sender, receiver, and port. For example, the firewall might allow e-mail and Web packets to and from any computer on the intranet, but allow telnet (remote login) packets to and from only selected computers.

Packet filter firewall maintains a filtering table that decides which packets are to be forwarded or discarded. A packet filter firewall filters at the network or transport layer.



Interface	Source IP	Source Port	Destination IP	Destination Port
1	124.56.02	*	*	*
1	*	*	*	23
1	*	*	156.255.78.8	*
2	*	*	*	*

Table in Packet Filter firewall

As shown in fig. the packets are filtered according to following specifications :

1. Incoming packets from network 124.56.0.2 are block (* means any).
2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
3. Incoming packets for internal host 156.255.7.8.8 are blocked.
4. Outgoing packets destined for an HTTP server (port 80) are blocked i.e. employees of organization are not allowed to browse the internet and cannot send any HTTP request.

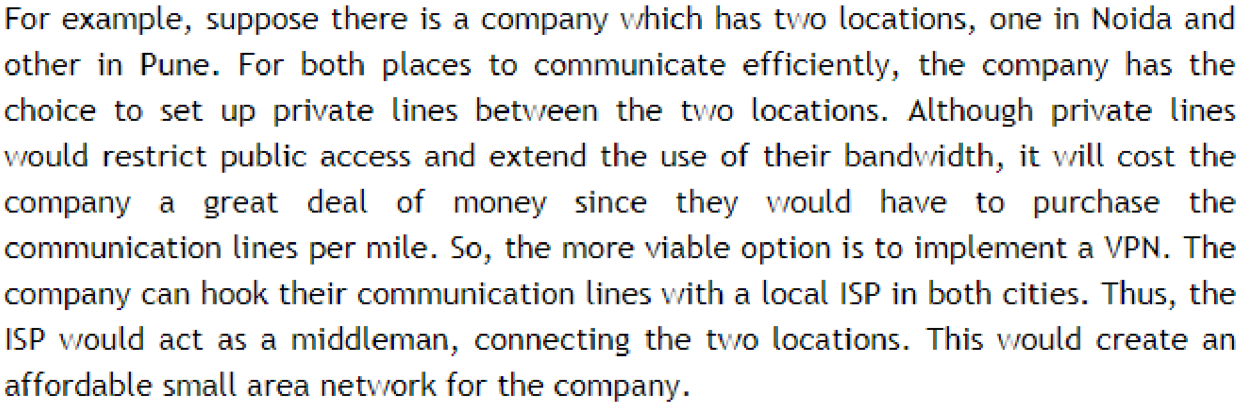
Application-Level Firewalls

These firewalls handle packets for each Internet service separately, usually by running a program called a *proxy server,* which accepts e-mail, Web, chat, newsgroup, and other packets from computers on the intranet, strips off the information that identifies the source of the packet, and passes it along to the Internet.

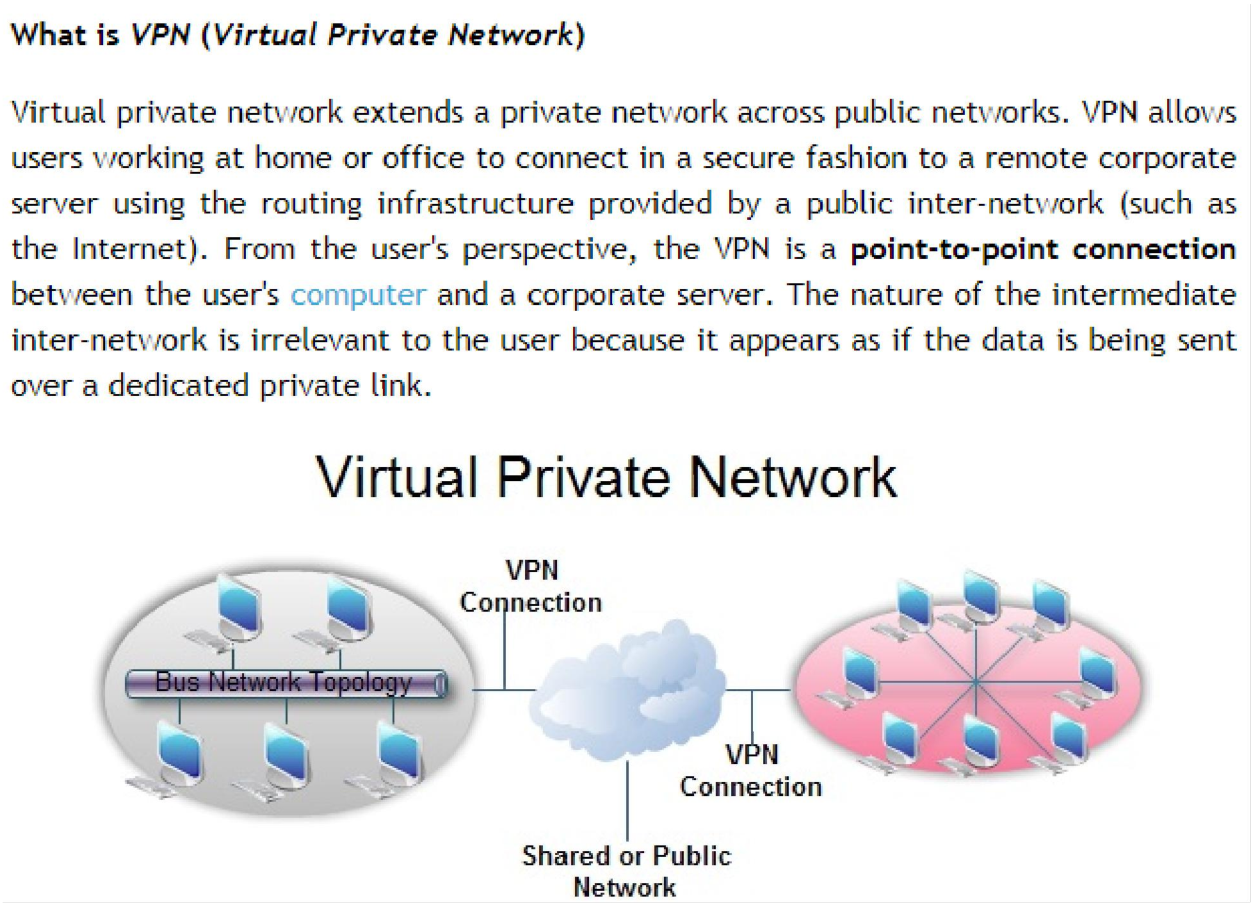
When the replies return, the proxy server passes the replies back to the computer that sent the original message. A proxy server can also log all the packets that pass by, so that you have a record of who has access to your intranet from the Internet, and vice versa.

VPN

- **VPN (Virtual Private Network) Definition**: VPN meaning that it is a private point-to-point connection between two machines or networks over a shared or public network such as the internet.
- A Virtual Private Network is a combination of software and hardware.
- VPN (Virtual Private Network) technology, can be use in organization to extend its safe encrypted connection over less secure internet to connect remote users, branch offices, and partner private, internal network
- VPN turn the Internet into a simulated private WAN.
- It uses “virtual” connections routed through the internet from a business’s private network to the remote site.
- A Virtual Private Network is a technology which creates a network, and that network is virtually private
- The letter V in VPN stands for “virtual” means that it shares physical circuits with other traffic and it has no corresponding physical network.

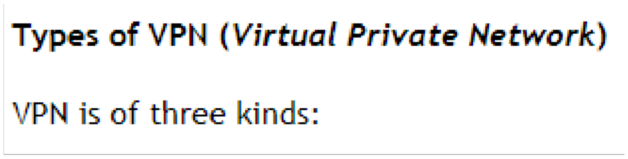


For example, suppose there is a company which has two locations, one in Noida and other in Pune. For both places to communicate efficiently, the company has the choice to set up private lines between the two locations. Although private lines would restrict public access and extend the use of their bandwidth, it will cost the company a great deal of money since they would have to purchase the communication lines per mile. So, the more viable option is to implement a VPN. The company can hook their communication lines with a local ISP in both cities. Thus, the ISP would act as a middleman, connecting the two locations. This would create an affordable small area network for the company.



What is *VPN* (*Virtual Private Network*)

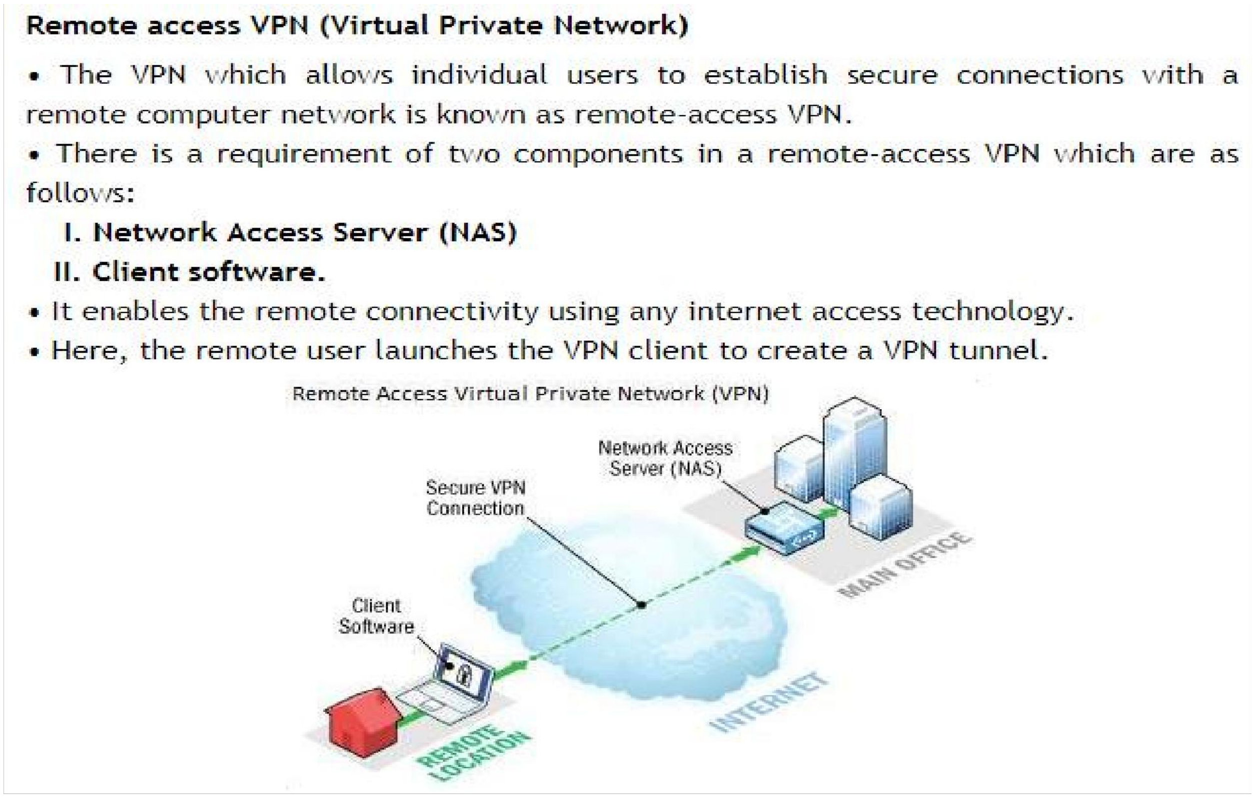
Virtual private network extends a private network across public networks. VPN allows users working at home or office to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public inter-network (such as the Internet). From the user's perspective, the VPN is a **point-to-point connection** between the user's computer and a corporate server. The nature of the intermediate inter-network is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.



Types of VPN (*Virtual Private Network*)

VPN is of three kinds:

1. Remote Access VPN
2. Intranet VPN
3. Extranet VPN



Remote access VPN (Virtual Private Network)

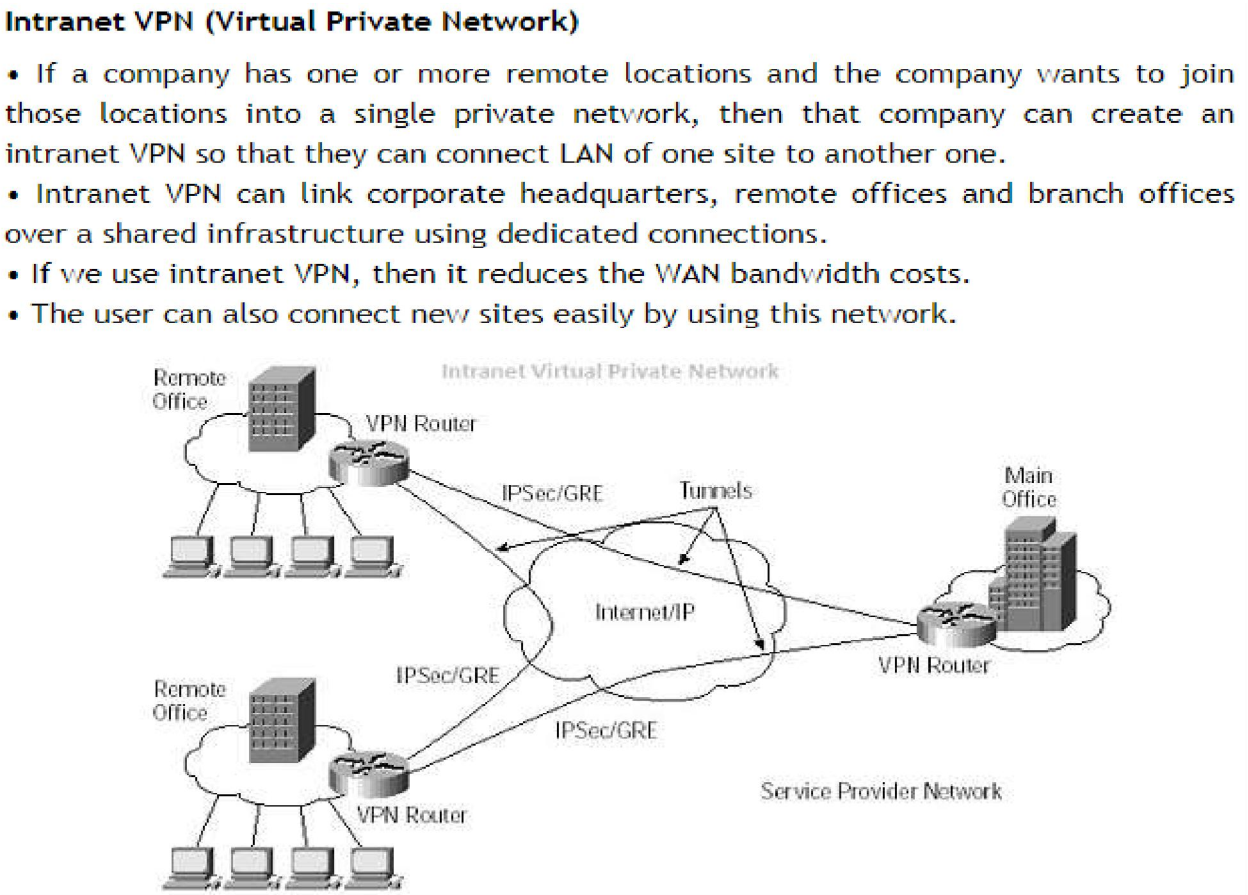
- The VPN which allows individual users to establish secure connections with a remote computer network is known as remote-access VPN.
- There is a requirement of two components in a remote-access VPN which are as follows:

  I. **Network Access Server (NAS)**

  II. **Client software.**

- It enables the remote connectivity using any internet access technology.
- Here, the remote user launches the VPN client to create a VPN tunnel.

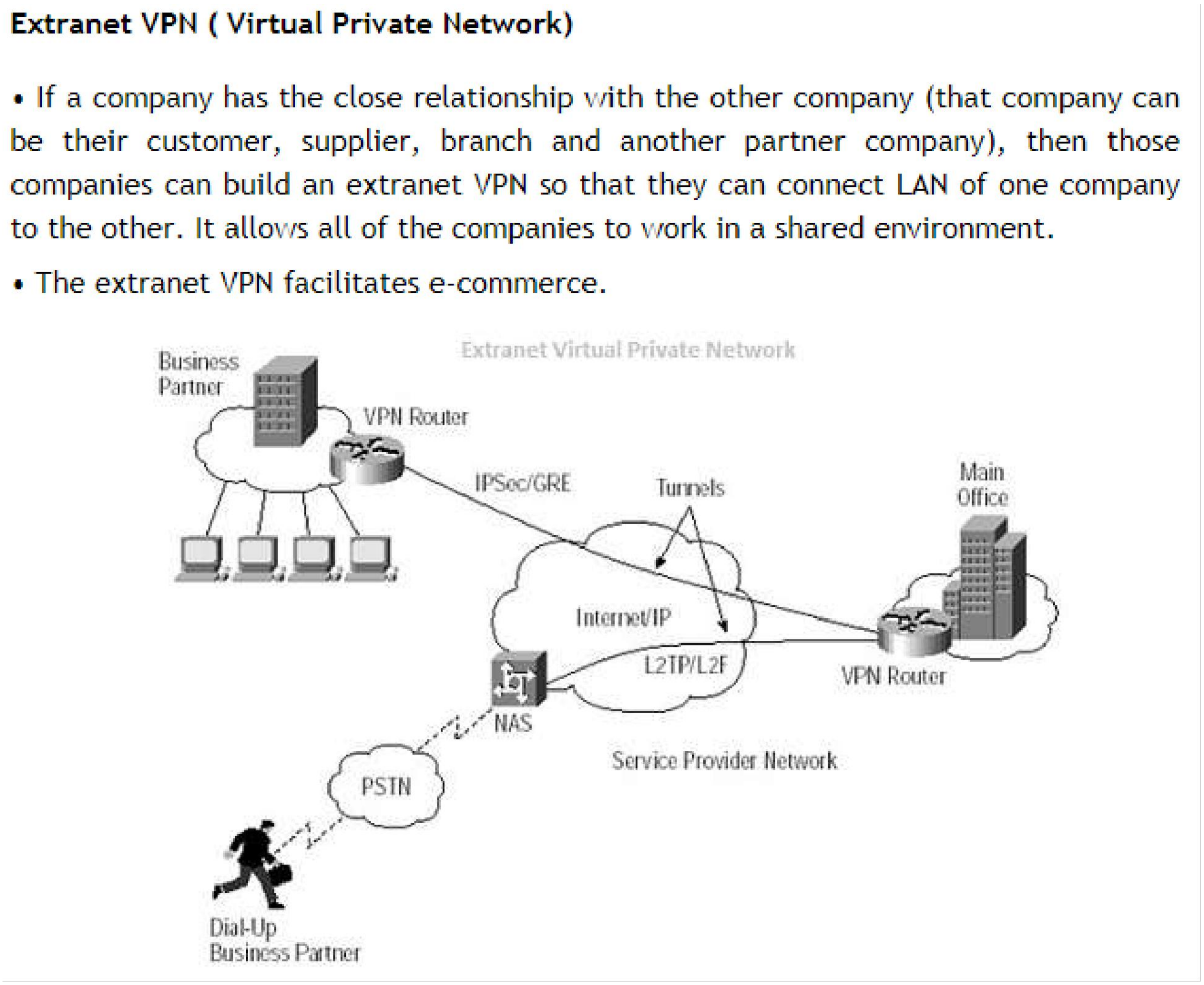
Remote Access Virtual Private Network (VPN)



Intranet VPN (Virtual Private Network)

- If a company has one or more remote locations and the company wants to join those locations into a single private network, then that company can create an intranet VPN so that they can connect LAN of one site to another one.
- Intranet VPN can link corporate headquarters, remote offices and branch offices over a shared infrastructure using dedicated connections.
- If we use intranet VPN, then it reduces the WAN bandwidth costs.
- The user can also connect new sites easily by using this network.

Intranet Virtual Private Network



Extranet VPN (Virtual Private Network)

- If a company has the close relationship with the other company (that company can be their customer, supplier, branch and another partner company), then those companies can build an extranet VPN so that they can connect LAN of one company to the other. It allows all of the companies to work in a shared environment.
- The extranet VPN facilitates e-commerce.

Extranet Virtual Private Network