Virtual Private Network

What is a VPN ?

- A technology that creates a network that is physically public, but virtually private.
- VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties.

NEED OF VPN ?

- Earlier there was

1. **Private Network .**

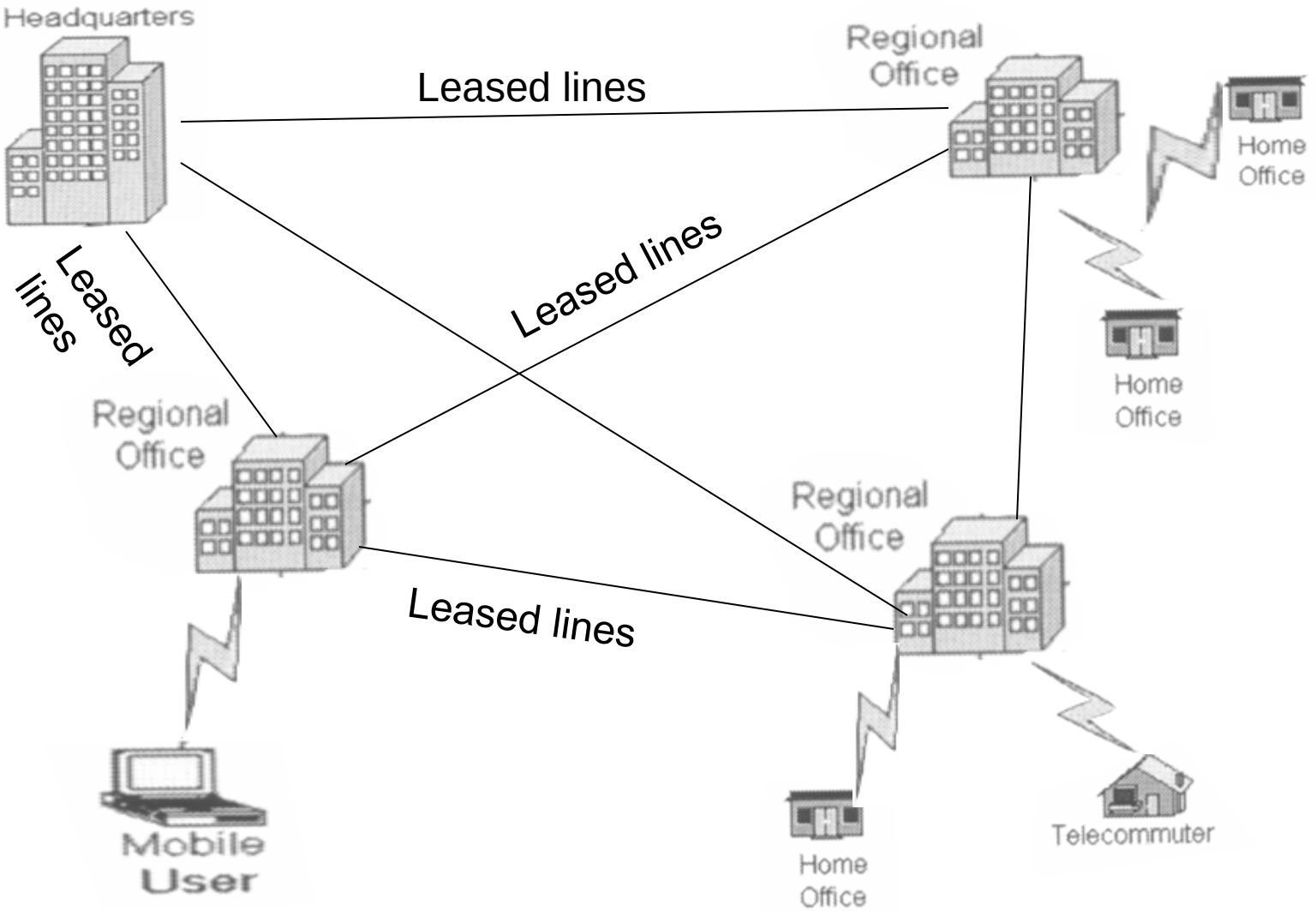
- Completely isolated network is established.
- It creates its own TCP\IP internet .
- Leased lines .

- Isolated from world .
- Costlier .

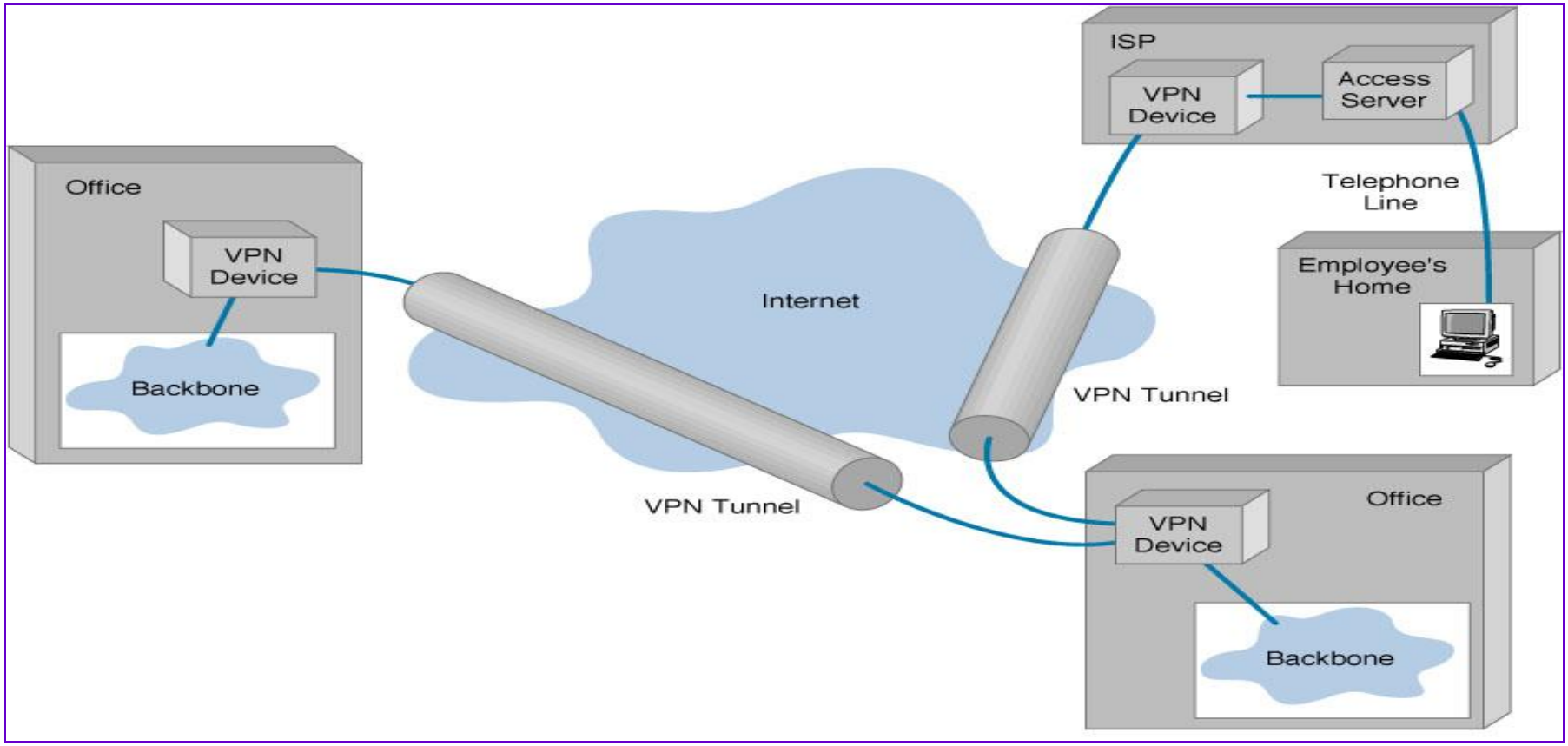
HYBRID NETWORK

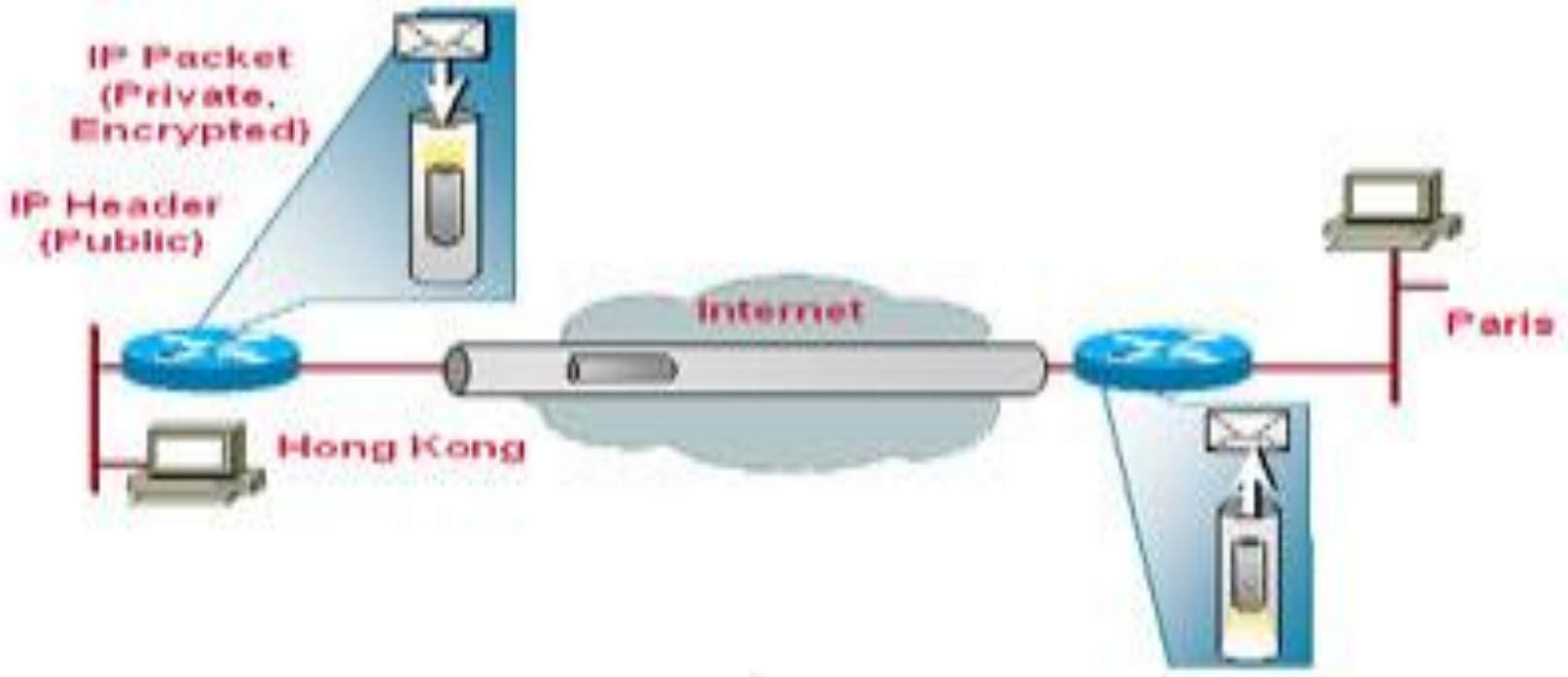
- Uses advantages of private and global internet.
- Privatization is done by leased lines .
- Cost inefficient .

TRADITIONAL SYSTEM



Virtual Private Networks (VPN)
Basic Architecture




IP Packet
(Private,
Encrypted)
IP Header
(Public)
Internet
Paris
Hong Kong

IN VPN -

- A virtual private network (VPN) is a secure way of connecting to a private Local Area Network at a remote location, using the Internet or any unsecure public network to transport the network data packets privately, using encryption. The VPN uses authentication to deny access to unauthorized users, and encryption to prevent unauthorized users from reading the private network packets. The VPN can be used to send any kind of network traffic securely, including voice, video or data.

VPN IS -

- VIRTUAL .
- PRIVATE .
- NETWORK .

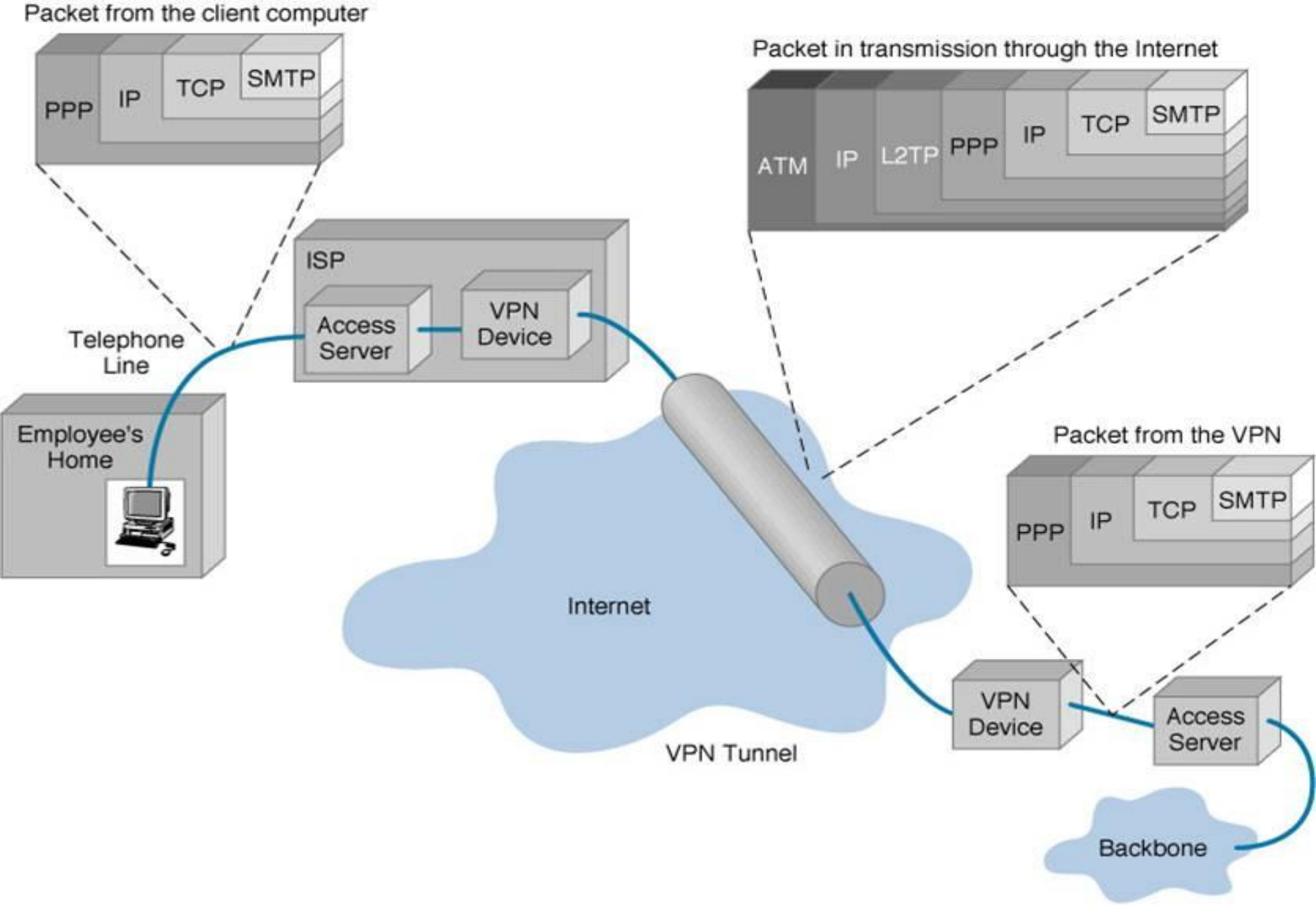
REQUIREMENTS OF VPN

- TUNNELING.
- ENCRYPTION.
- ENCAPSULATION.
- AUTHENTICATION.
- FIREWALL.

TUNNELING

What is Tunneling ?

- Virtual private network technology is based on the idea of tunneling.
- VPN tunneling involves establishing and maintaining a logical network connection .
- Tunneling is the process of placing an entire packet within another packet before it's transported over the Internet.
- That outer packet protects the contents from public view and ensures that the packet moves within a virtual tunnel.


Packet from the client computer
PPP
IP
TCP
SMTP
Packet in transmission through the Internet
ATM
IP
L2TP
PPP
IP
TCP
SMTP
ISP
Access Server
VPN Device
Telephone Line
Employee's Home
Internet
Packet from the VPN
PPP
IP
TCP
SMTP
VPN Device
Access Server
VPN Tunnel
Backbone

- **On this connection**, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.
  - allows senders to encapsulate their data in IP packets that hide the routing and switching infrastructure of the Internet
  - to ensure data security against unwanted viewers, or hackers.

Type Of Tunneling

1.Voluntary.

2. compulsory.

VOLUNTARY

- In voluntary tunneling, the VPN client manages connection setup.
- The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs).
- Then, the VPN client application creates the tunnel to a VPN server over this live connection.

Compulsory

- In compulsory tunneling, the carrier network provider manages VPN connection setup.
- When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server.
- From the client point of view, VPN connections are set up in just one step

CONTI . . .

- Compulsory tunneling hides the details of VPN server connectivity from the VPN clients and effectively transfers management control over the tunnels from clients to the ISP.

- In return, service providers must take on the additional burden of installing and maintaining FEP devices.

VPN Tunneling Protocols

- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)
- Internet Protocol Security (IPsec)

Point-to-Point Tunneling Protocol (PPTP)

- It’s the most widely supported VPN method among Windows users and it was created by Microsoft in association with other technology companies.
- compared to other methods, PPTP is faster and it is also available for Linux and Mac users. .
- Voluntary tunneling method.

Layer Two Tunneling Protocol (L2TP)

- **L2TP** (**L**ayer **2** **T**unneling **P**rotocol) it's another tunneling protocol that supports VPNs.

- The difference between PPTP and L2TP is that the second one provides not only d*ata confidentiality but also data integrity*.

- L2TP was developed by Microsoft and Cisco as a combination between PPTP and

Internet Protocol Security (IPSec)

- IPsec is actually a collection of multiple related protocols.
- It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP.
- IPsec exists at the network layer (Layer Three) of the OSI model.

Encryption

What is Encryption?

- Encryption is the process of encoding data so that only a computer with the right decoder will be able to read and use it.

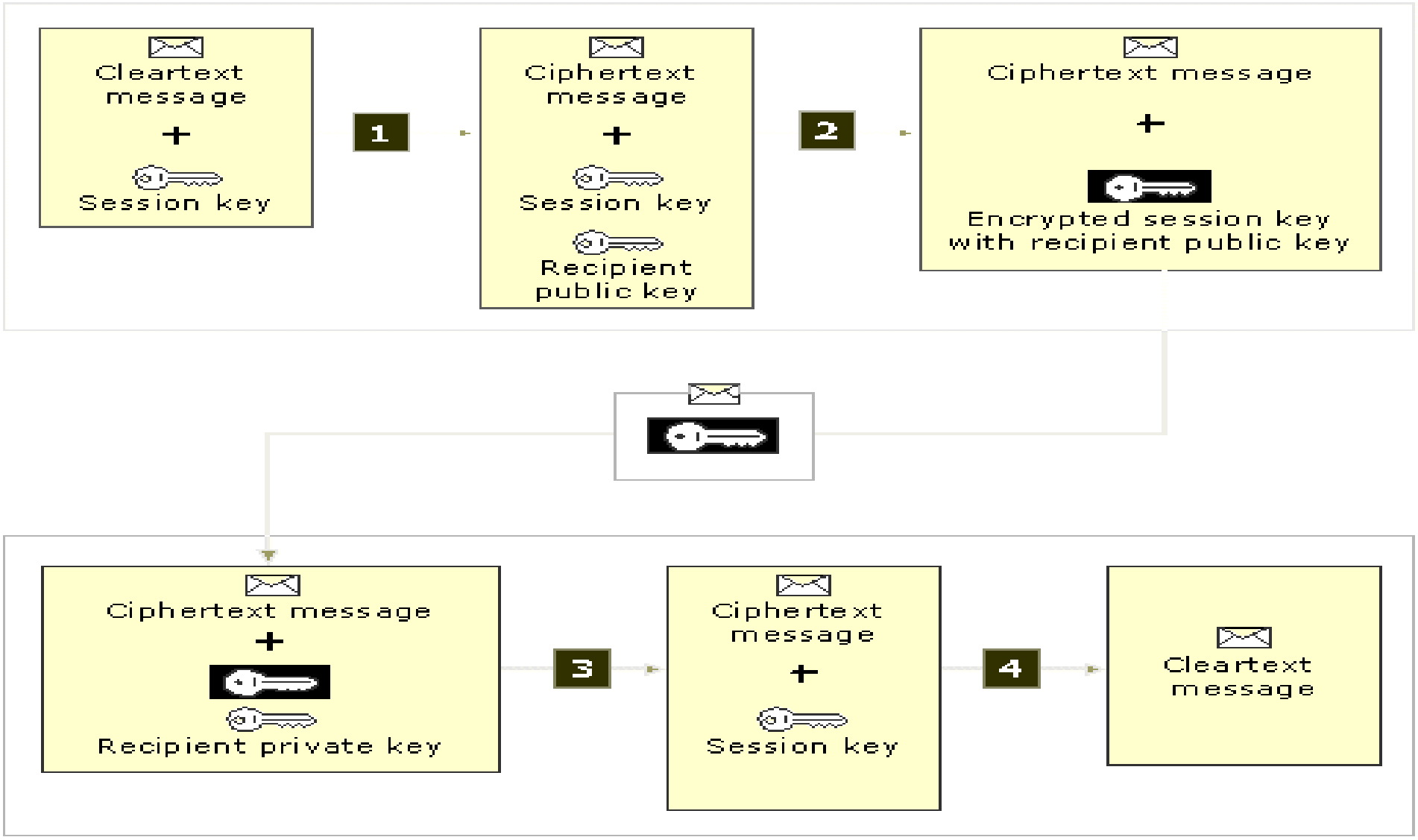
- The VPN client at each end of the tunnel encrypt the data entering the tunnel and decrypt it at the other end .

Types Of Encryption

There are most two common forms of encryption

- 1 . symmetric-key encryption
- 2 . public-key Encryption

How encryption takes place



Authentication

- Authentication process determine if the sender is the authorized person and if the data has been redirect or corrupted .

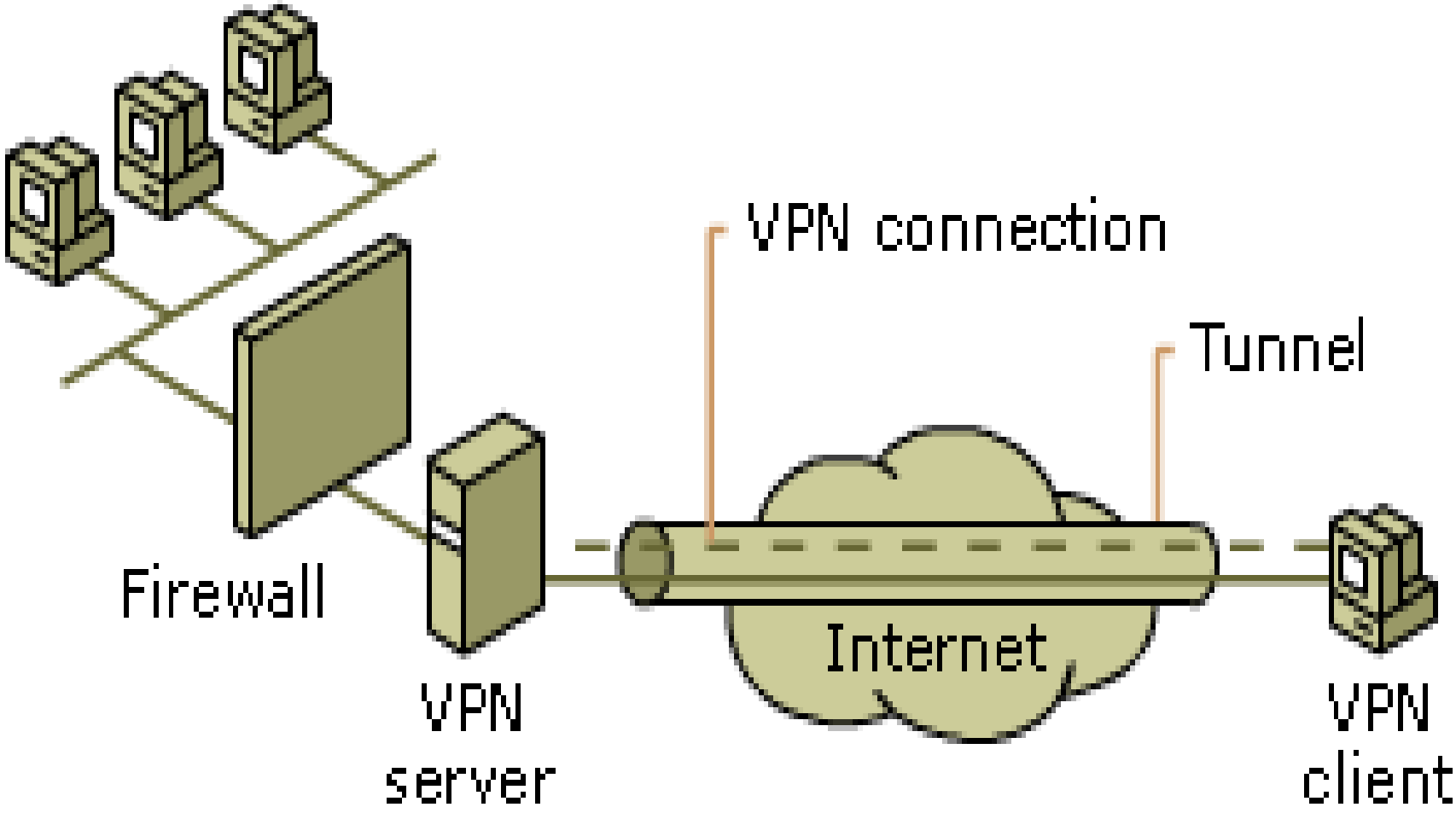
- There are 2 levels of Authentication.

  - Computer-Level Authentication
  - User-level Authentication

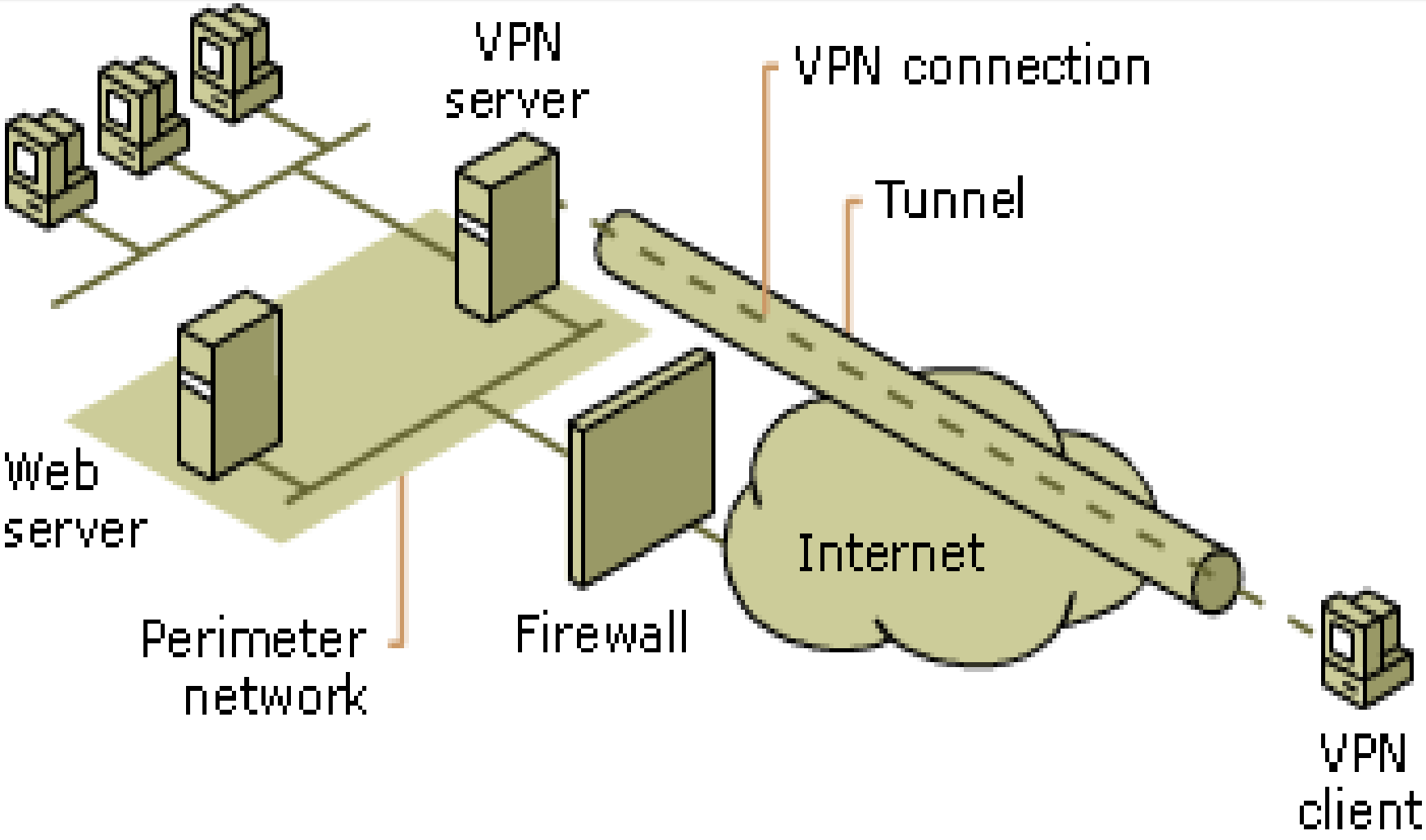
Firewall configuration

- Firewall provides network security and business continuity .
- It prevents attacks, and secures your data communications with multiple parallel Virtual Private Network (VPN) connections.
- There are two approaches to using a firewall with a VPN server:
- **VPN server in front of the firewall**..
- **VPN server behind the firewall**..

VPN server in front of the firewall.



VPN server behind the firewall

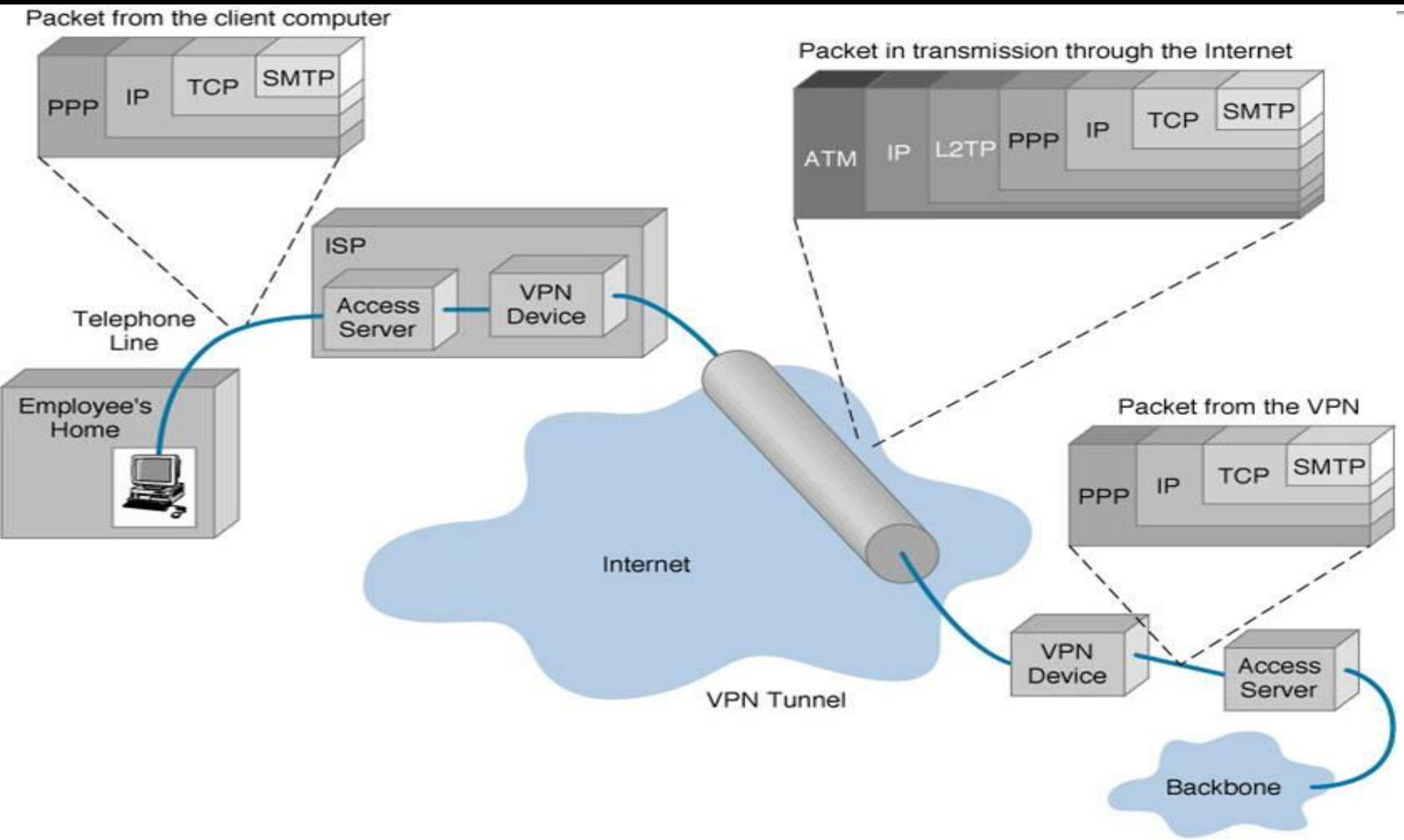


Encapsulation

- For data encapsulation, VPN relies on either of the following technologies like GRE , IPSec, L2F,PPTP and L2TP .

- In which IPsec and PPTP are more popular.

Example of packet encapsulation



Secure VPN requirements

- All traffic on the secure VPN must be encrypted and authenticated.
- The security properties of the VPN must be agreed to by all parties in the VPN.
- No one outside the VPN can affect the security properties of the VPN.

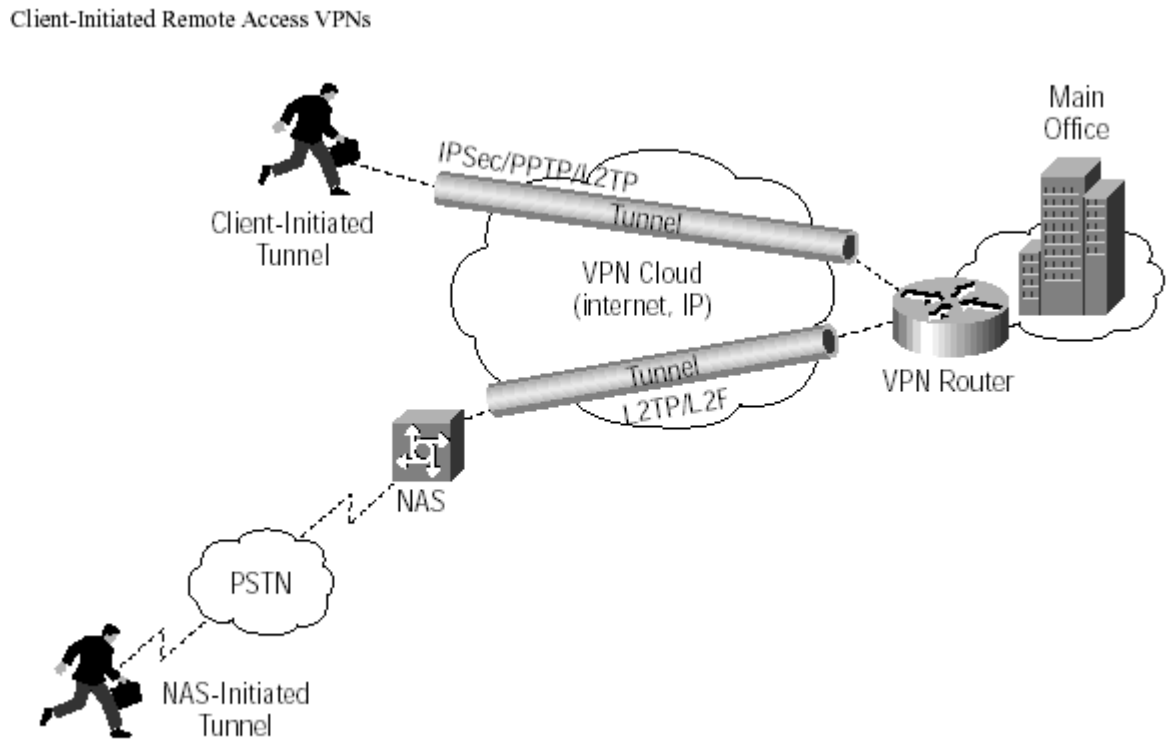
Types of VPNs

- Remote access VPN
- Intranet VPN
- Extranet VPN

Remote access VPN

- A **remote-access VPN** allows individual users to establish secure connections with a remote computer network.
- There are two components required in a remote-access VPN. The first is a **network access server**(NAS).
- The other required component of remote-access VPNs is client software

Remote Access VPN

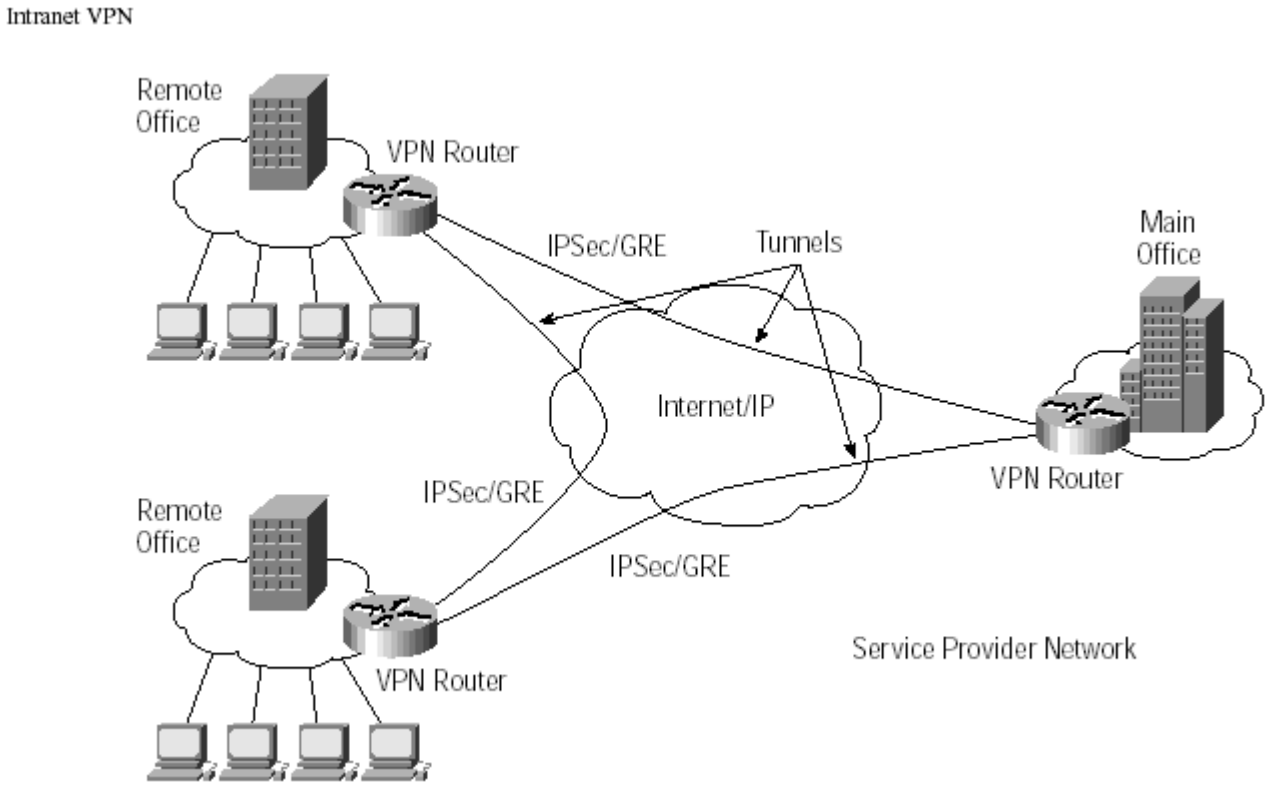


Intranet VPN

- Intranet VPNs link corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections.

- The benefits of an intranet VPN are as follows:
  - Reduces WAN bandwidth costs
  - Connect new sites easily

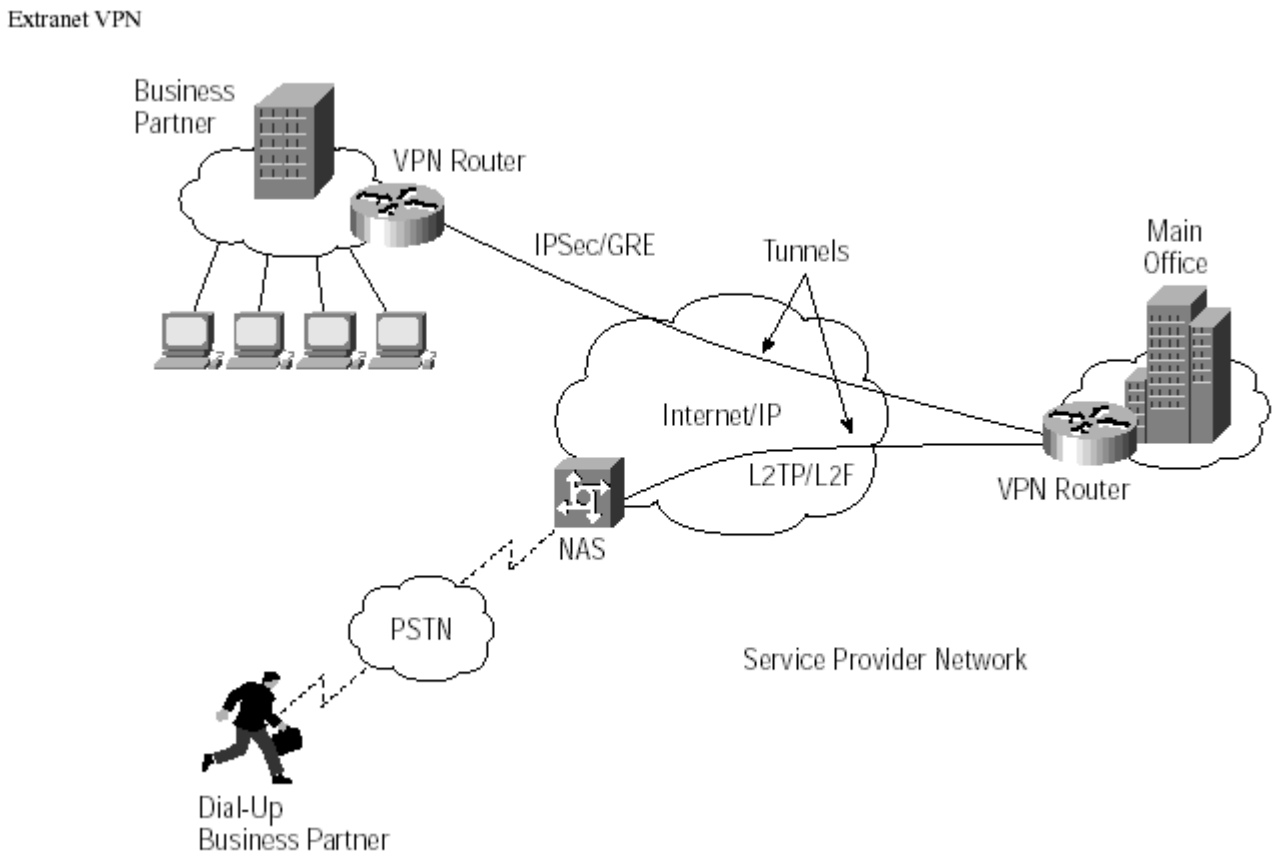
Intranet VPN



Extranet VPN

- Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. In this example, the VPN is often an alternative to fax, snail mail, or EDI. The extranet VPN facilitates e-commerce.

Extranet VPN



VPN ADVANTAGES

- **Security** -- The VPN should protect data while it's traveling on the public network. If intruders attempt to capture the data, they should be unable to read or use it.

- **Reliability** -- Employees and remote offices should be able to connect to the VPN with no trouble at any time (unless hours are restricted), and the VPN should provide the same quality of connection for each user even when it is handling its maximum number of simultaneous connections.

- **Cost Savings**

- Eliminating the need for expensive long-distance leased lines
- Reducing the long-distance telephone charges for remote access.
- Transferring the support burden to the service providers
- Operational costs

- : **Scalability**

  - Flexibility of growth
  - Efficiency with broadband technology

Disadvantages of VPN

- VPNs require **detailed understanding** of network security issues and careful installation / configuration to ensure sufficient protection on a public network like the Internet.

- The **reliability and performance** of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.

- VPN products and solutions from different vendors have not always been **compatible** due to issues with VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give as great a cost savings.