
# VPN

# &

# Remote Networking

# Topics To Cover :

- Introduction to Virtual Private Network
- Types of VPN
- VPN Tunneling
- VPN Protocols (IPSec, L2TP, PPTP, SSTP, IKEv2)
- VPN Security
- Connection to VPN

Mirox
Reinforce Your Security

# ❑ Introduction to Virtual Private Network

- To access a private network remotely.

- Extends a private network across a public network.

- Enables users to send and receive data across shared or public networks.

- VPNs may allow employees to securely access a corporate intranet while located outside the office.

- Securely connect geographically separated offices of an organization, creating one cohesive network.


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

- Establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

- 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.

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

# Use Of VPN:


- Public networks, and in particular public wireless networks, provide an easy way for hackers and malicious users to listen in ("sniff") on network usage.

- Allow them to see:

  - What web pages you are viewing.
  - Steal username and passwords.
  - Steal session information to be able to log into sites.
  - Man in the Middle attack.

- Using a VPN protects data from such kind of attacks, as the network traffic is authenticated and encrypted, making it secures and private.

# How does a VPN works ?

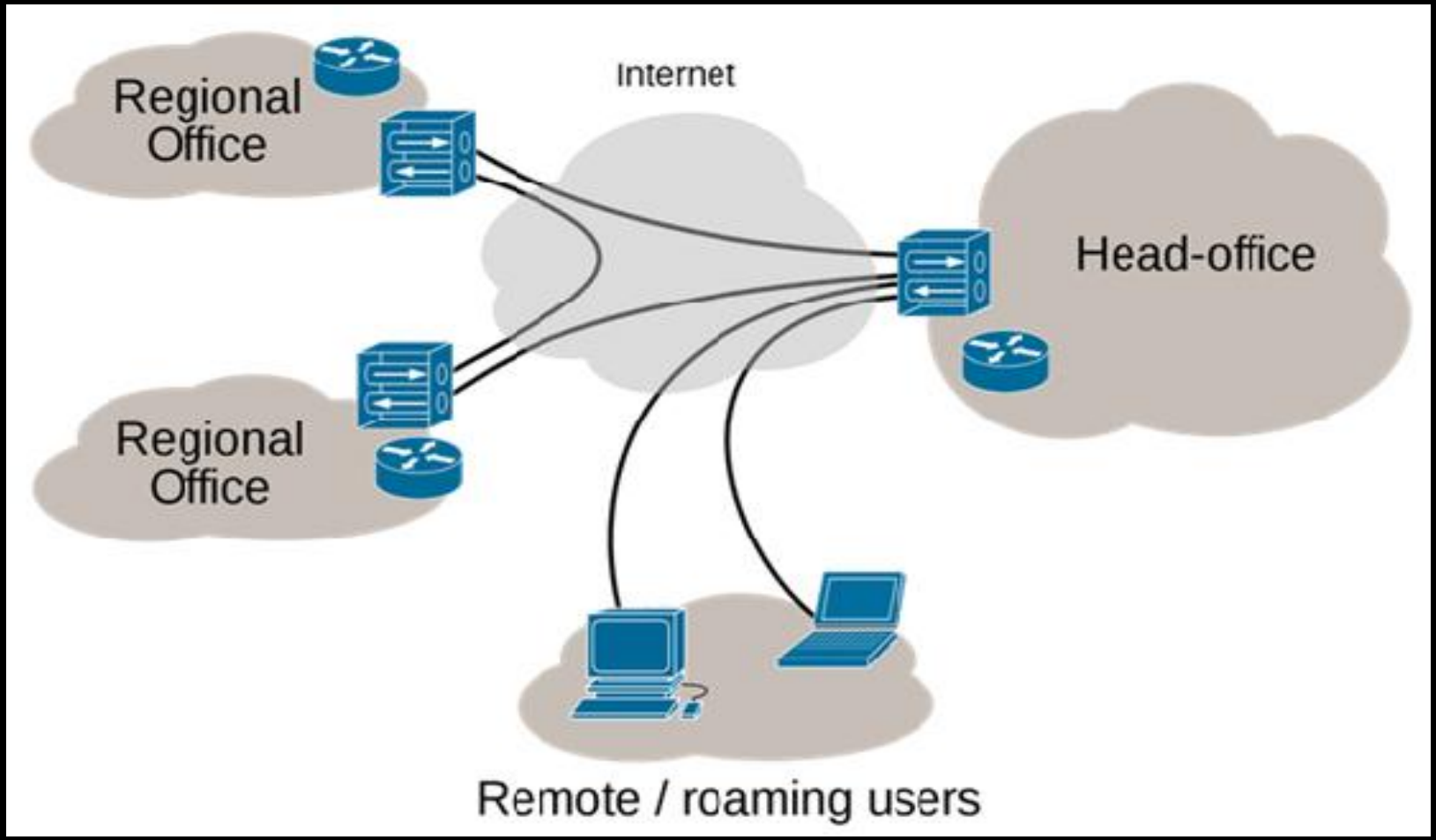
- VPN consists of two components:
  - VPN Client & VPN Server

- A VPN client is the software that allows a user to connect their computer to the VPN server and establish the VPN connection.

- It is installed on the user's computer and communicates with the VPN server to create a secure link for the user's network traffic.

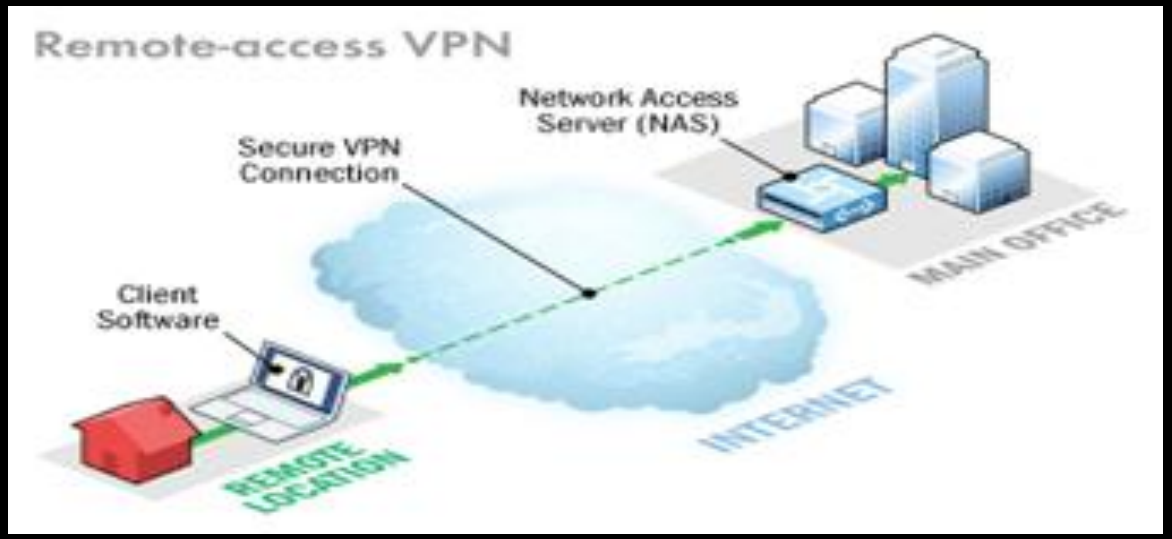
- The VPN Client is what the end user uses to control their VPN connection.

# ❑ Types of VPN


Regional Office
Internet
Head-office
Regional Office
Remote / roaming users

- There are two basic VPN types:
  - Remote Access VPN
  - Site to Site VPN

- Remote Access VPN




- Remote access VPN allows a user to connect to a private network and access its services and resources remotely.

- Remote Access VPN is useful for business users as well as home users.

- VPN services to bypass regional restrictions on the Internet and access blocked websites.

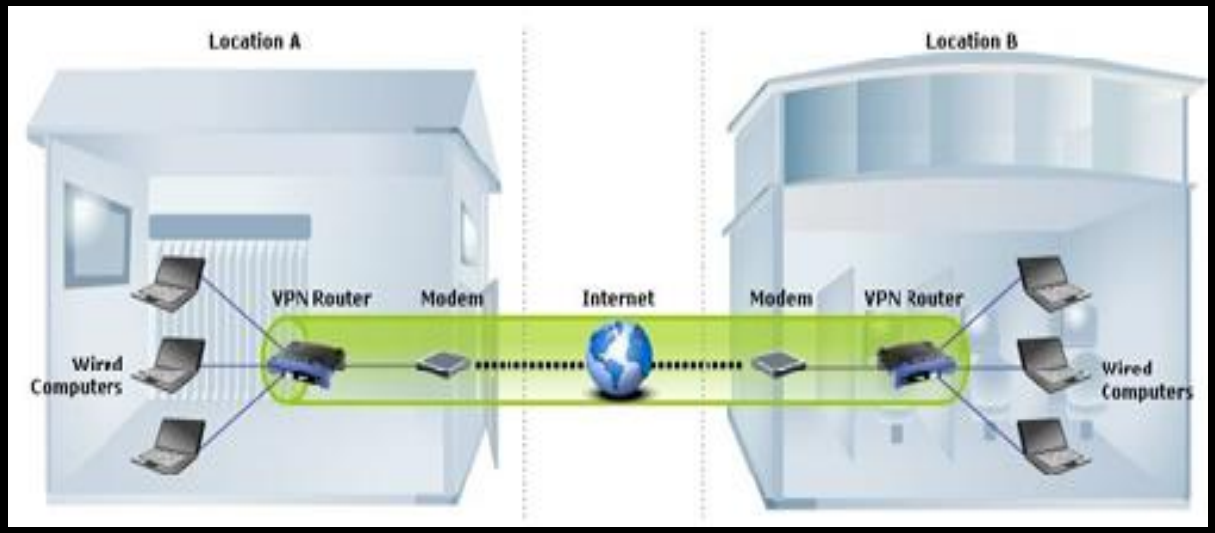
- The remote access VPN is supported by L2F, PPTP, L2TP and IPsec tunneling protocols.

- Another name for this type of VPN is Virtual Private Dial-up Network (VPDN).

- Two components required in a Remote Access VPN:

  - Network Access Server (NAS) also called a media gateway.
  - Remote-Access Server (RAS).

- Site to Site VPN




➢ A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporate.

➢ Companies, with offices in different geographical locations, use Site-to-site VPN.

➢ The communication between the two routers starts only after an authentication is validated between the two.

- Two sub-kinds of site-to-site virtual private networks:

    1. Intranet Site-to-Site VPN
    2. Extranet Site-to-Site VPN


1. Intranet Site-to-Site VPN:

- In Intranet Site-to-Site VPN when different private networks of a single organization are clubbed together over the internet.
- Can be used to share resources across various office locations of the company.

2. Extranet Site-to-Site VPN:

- Connect the corporate networks belonging to different organizations.
- Collaborating on a project involving resources from both the organizations.

## ❑ VPN Tunneling

➢ Tunneling is a network technology that enables the encapsulation of one type of protocol packet within the datagram of a different protocol.

➢ VPN connections can use Point-to-Point Tunneling Protocol (PPTP) packets to encapsulate and send private network traffic.

➢ For PPTP and Layer Two Tunneling Protocol (L2TP), a tunnel is similar to a session.

➢ Both of the tunnel endpoints must agree to the tunnel and must negotiate configuration variables, such as address assignment, encryption, or compression parameters.


- A tunnel management protocol is used as the mechanism to create, maintain, and terminate the tunnel.

- There are two types of tunneling:

1. Voluntary Tunneling
2. Compulsory Tunneling

1. Voluntary Tunneling

   - A user or client computer can issue a VPN request to configure and create a voluntary tunnel.

   - Voluntary tunneling occurs when a client computer or routing server creates a virtual connection to the target tunnel server.

   - Require only IP connectivity between the VPN client and VPN server.

## 2. Compulsory Tunneling

- In compulsory tunneling, a VPN-capable remote access server configures and creates a compulsory tunnel.

- A compulsory tunnel, the user's computer is not a tunnel endpoint.

- The dial-up access server, between the user's computer and the tunnel server is the tunnel endpoint and acts as the tunnel client.

- The computer or network device providing the tunnel for the client computer is variously known as a Front End Processor (FEP) for PPTP or an L2TP Access Concentrator (LAC) for L2TP.

- Once the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel.

## ❑ VPN Protocols


➢ There are five Protocols:

1. Internet Protocol Security or IPSec
2. Layer 2 Tunneling Protocol (L2TP)
3. Point – to – Point Tunneling Protocol (PPTP)
4. Secure Socket Tunneling Protocol (SSTP)
5. IKEv2

1. Internet Protocol Security or IPSec

- IPSec is introduced to promise information transfer securely over unprotected IP arrangement in layer three of OSI.

- IPSec ensures data integrity, privacy through encryption and authentication for accurate authorization in network.

- Never allow intended intruder to hack data and make changes for confidential data transmitted.

- Authentication header (AH) and encapsulated security payload (ESP) are two security protocols used by IP sec for providing its services.

- The security of IP through IP sec is done by key management that can be automatically set or manually set up.

## 2. Layer 2 Tunneling Protocol (L2TP)

- This protocol is enables the PPP frames wrapped to be transmitted through internet protocol or other networks.

- The authentication of this L2TP is similar to that of point to point protocol which allows data subjected to encapsulation.

- As it is combination of both PPTP and L2F (layer 2 forwarding) the data of PPP frames are wrapped and stored in PPP header along with L2TP header.

- Entire information of this L2TP is encapsulated and stored in UDP header along with source, destination addresses.

- All these individual encapsulation are collectively wrapped up into IP header and in parallel obtaining source, destination IP addresses of VPN server and client.

## 3. Point – to – Point Tunneling Protocol (PPTP)

- PPTP or Point-to-Point Tunneling Protocol creates a tunnel and encapsulates the data packet.

- It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection.

- PPTP is one of the most widely used VPN protocol and has been in use since the time of Windows 95.

- Apart from Windows, PPTP is also supported on Mac and Linux.

4. Secure Socket Tunneling Protocol (SSTP)

- This is a transport layer protocol" this protocol has different cryptographic abilities that assure data integrity, privacy and security.

- Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP traffic through an SSL/TLS channel.

- It requires a web browser that is initiated virtually on every computer that allows protected channel among network and remote system.

- The authentication is achieved by this protocol through digital certificates at time of hand shake between client remote system and server.

- This protocol in virtual private network is considered as "self signed digital certificate".

5. IKEv2 (Internet Key Exchange version 2)

- IKEv2 is a tunneling protocol that uses the IPsec Tunnel Mode protocol over UDP port 500.

- An IKEv2 VPN provides resilience to the VPN client when the client moves from one wireless hotspot to another or when it switches from a wireless to a wired connection.

- The use of IKEv2 and IPSec allows support for strong authentication and encryption methods.

- IKEv2 encapsulates datagrams by using IPsec ESP (Encapsulating Security Payload) or AH (Authentication Header) headers for transmission over the network.

- The message is encrypted with one of the following protocols: Advanced Encryption Standard (AES) 256, AES 192, AES 128, and 3DES encryption algorithms.

## ❑ VPN Security

- VPN uses encryption to provide data confidentiality.

- Once connected, the VPN makes use of the tunneling mechanism to encapsulate encrypted data into a secure tunnel.

- Packets passed over a public network in this way are unreadable without proper decryption keys, thus ensuring that data is not disclosed or changed in any way during transmission.

- Users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks.

- Point to Point Tunneling Protocol ( PPTP) and Layer 2 Tunneling Protocol (L2TP) both can link a remote computer to a network, but only L2TP offers strong security.

- To allow home users to connect to the office network via VPN, consider viruses or other security threats that could come from the user's home.

- One way to address this risk is by giving home users a computer that is owned and maintained by the organization, so is certified as up-to-date and virus-free.

- Key is shared only between the VPN's server and clients, using a sub-protocol called Encapsulation Header to hide certain packet information, including the sender's identity, during transmission.

Steps to secure VPN:

- Use the strongest possible authentication method for VPN access.
- Limit VPN access to those with a valid business reason, and only when necessary.
- Provide access to selected files through intranets or extranets rather than VPNs.
- Enable e-mail access without requiring VPN access.
- Provide strong antivirus, antispam and personal firewall protection to the remote users.
- Quarantine users from the time to they connect to the VPN until their computer has been verified as safe.
- Forbid the use of other VPNs and remote-control software while connected to your VPN.
- Secure remote wireless networks.

## ❑ Connection to VPN

1. Internet-based VPN Connections
2. Intranet-based VPN Connections

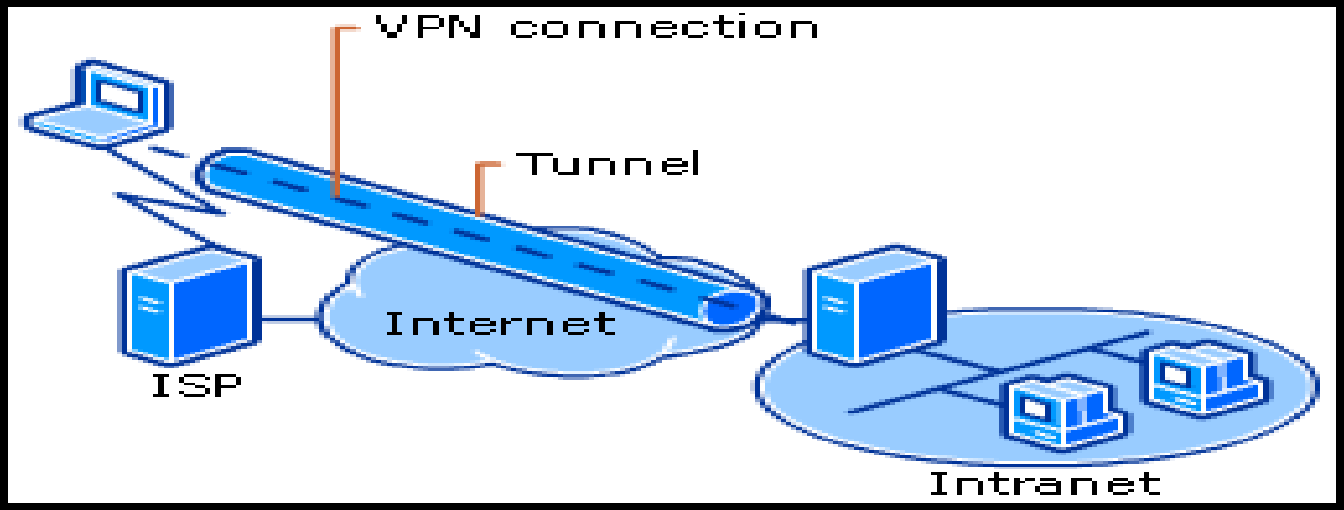
1. Internet-based VPN Connections:

- Using an Internet-based VPN connection, an organization can avoid long-distance charges while taking advantage of the global availability of the Internet.

## Remote Access VPN Connections over the Internet:

- A Remote Access VPN connection over the Internet enables a remote access client to initiate a dial-up connection to a local ISP instead of connecting to a corporate or outsourced Network Access Server (NAS).

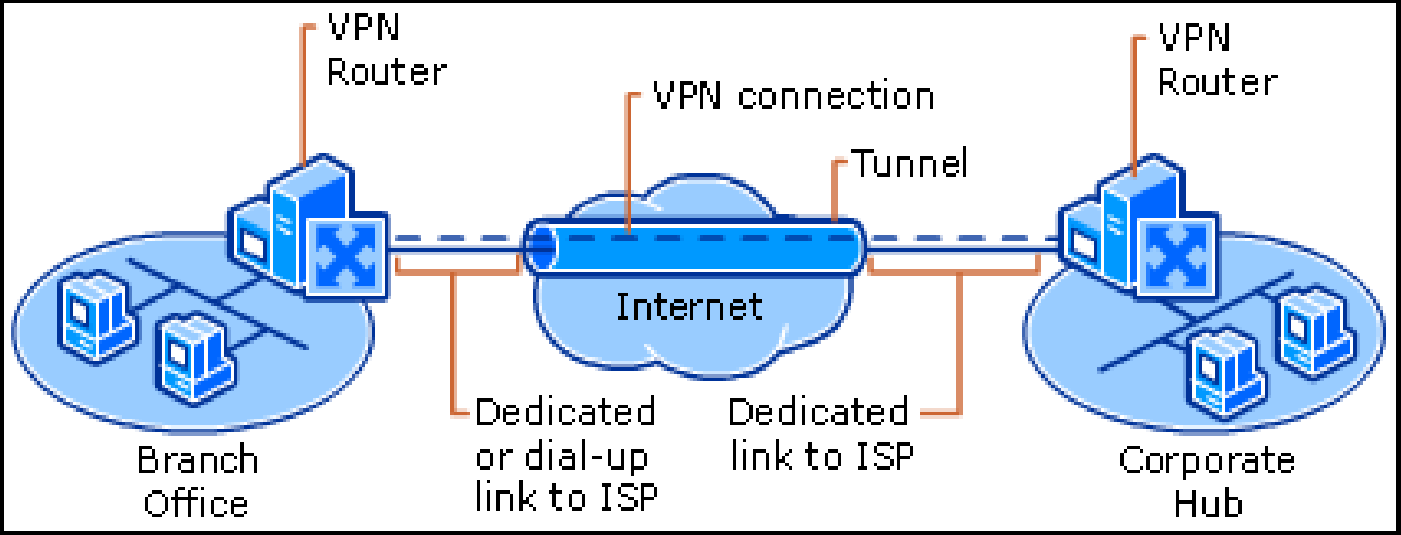
VPN Connecting a Remote Client to a Private Intranet



## Site-to-Site VPN Connections over the Internet:

- A router forwards packets to another router across a VPN connection. To the routers, the VPN connection operates as a data-link layer link.

VPN Connecting Two Remote Sites across the Internet



## 2. Intranet-based VPN Connections:

- The Intranet-based VPN connection takes advantage of IP connectivity in an organization's Local Area Network (LAN).

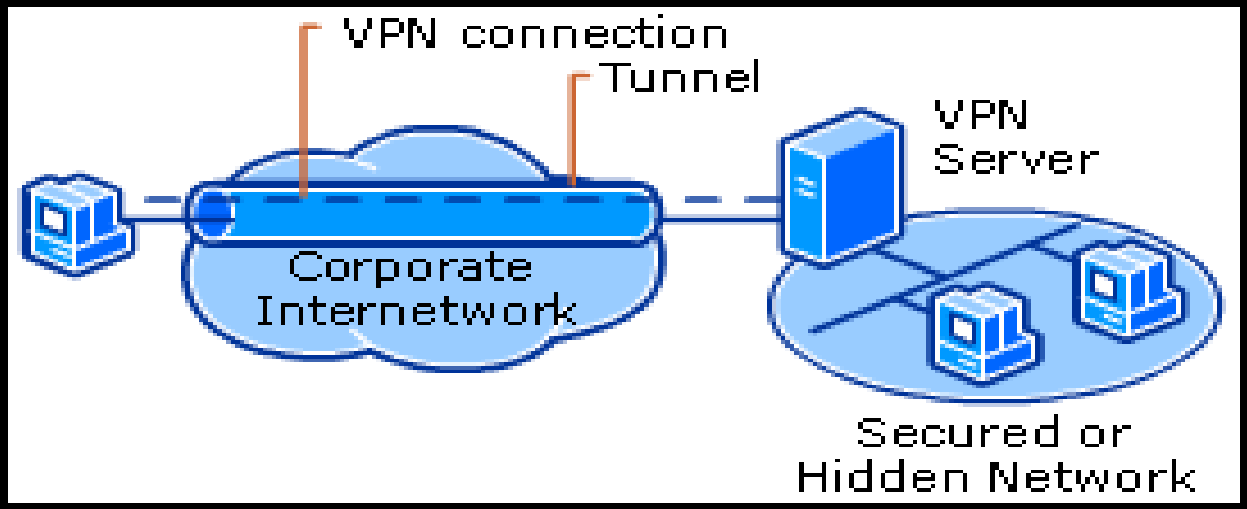
### Remote Access VPN Connections over an Intranet

- VPN server can be used to separate the network segments.

- The VPN server does not provide a direct routed connection between the corporate intranet and the separate network segment (e.g. Inter Dept.).

- Users on the corporate intranet with appropriate permissions can establish a remote access VPN connection with the VPN server and gain access to the protected resources.

# VPN Connection Allowing Remote Access to a Secured Network over an Intranet

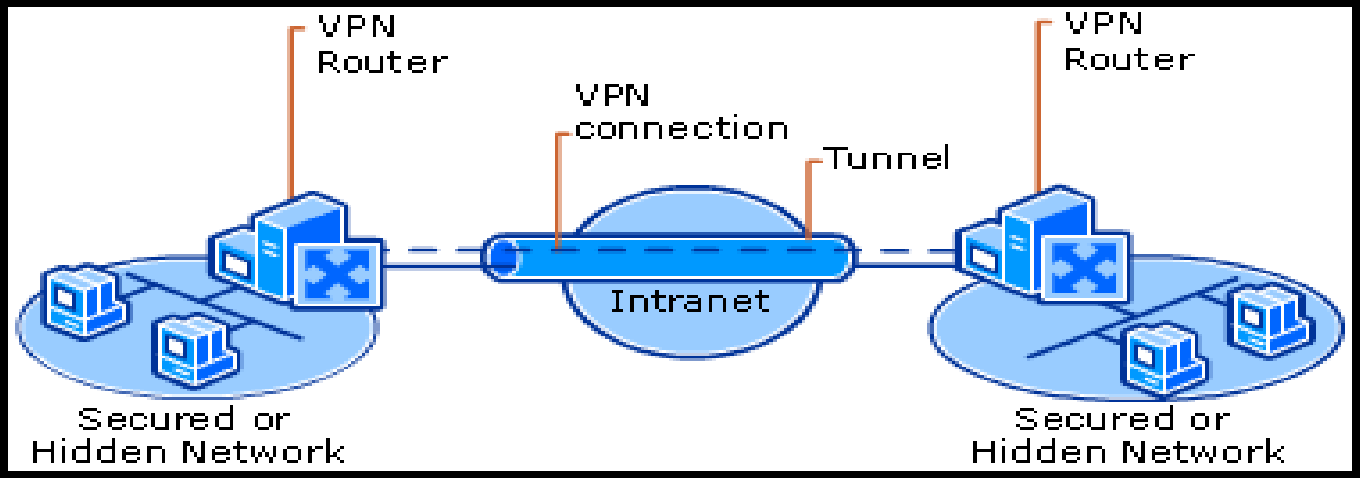


# Site-to-Site VPN Connections over an Intranet

- Two networks can be connected over an intranet using a site-to-site VPN connection.

- Two departments in separate locations, whose data is highly sensitive, to communicate with each other.

VPN Connecting Two Networks over an Intranet




THANK YOU !!!