Acknowledgements: Most of the slides are taken from the Internet

Virtual Private Networks

Cunsheng Ding

HKUST

Hong Kong

Internet layers

Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc…	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

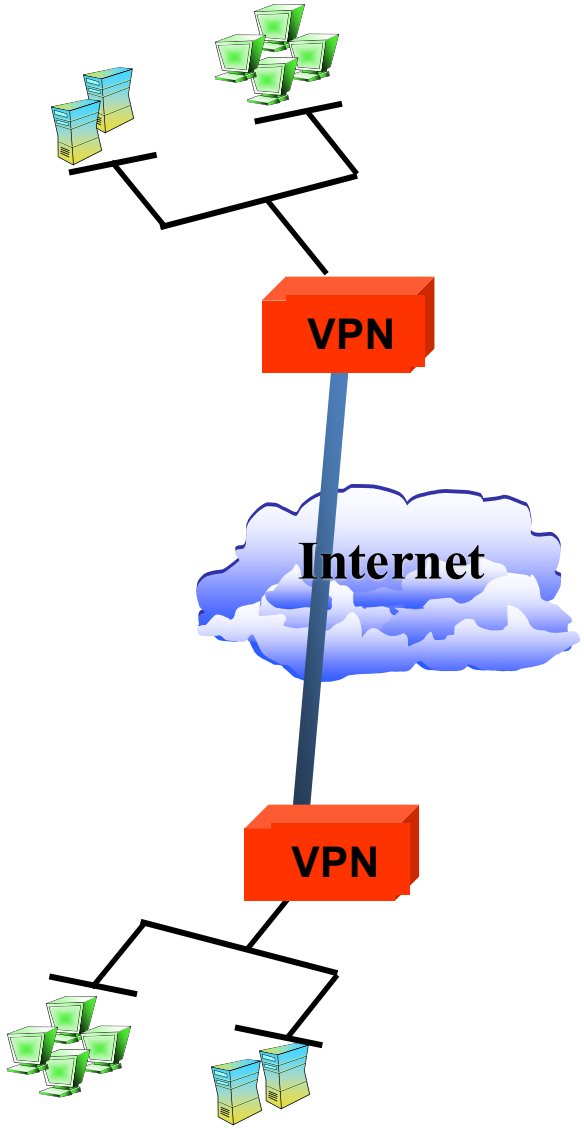
Data Link Layer Protocols: Ethernet, PPP, Frame Relay, ATM

Point-to-Point Protocol (PPP)

- In computer networking, PPP is a data link protocol used to establish a direct connection between two routers without any host or any other networking in between.
- It can provide connection authentication, transmission encryption (using ECP), and compression.
- PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET.
- PPP is also used over Internet access connections.
- Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol.

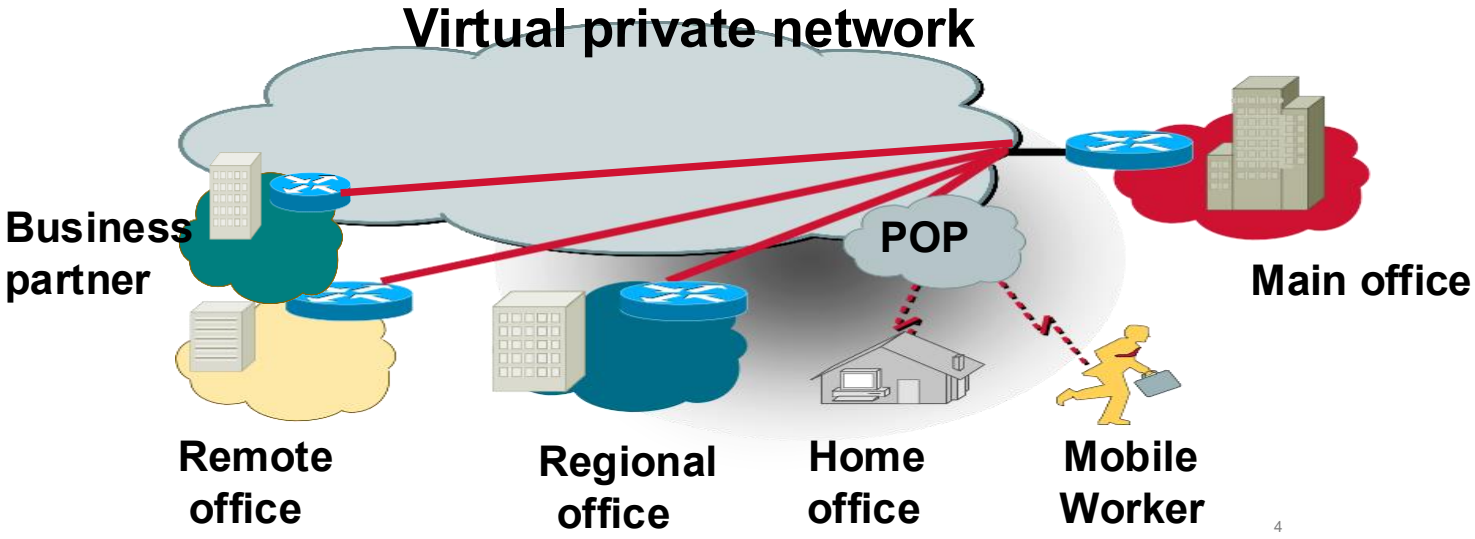
What Is a VPN?

- A VPN is a private connection over an open network
- It provides authentication, data integrity and confidentiality
- It is virtual because it exists as a virtual entity within a public network
- It is private because it is confined to a set of private users



What Is a VPN?

Connectivity deployed on a shared infrastructure with the same policies and ”performance" as a private network



POP (Point of Presence): an access point from one place to the rest of the Internet

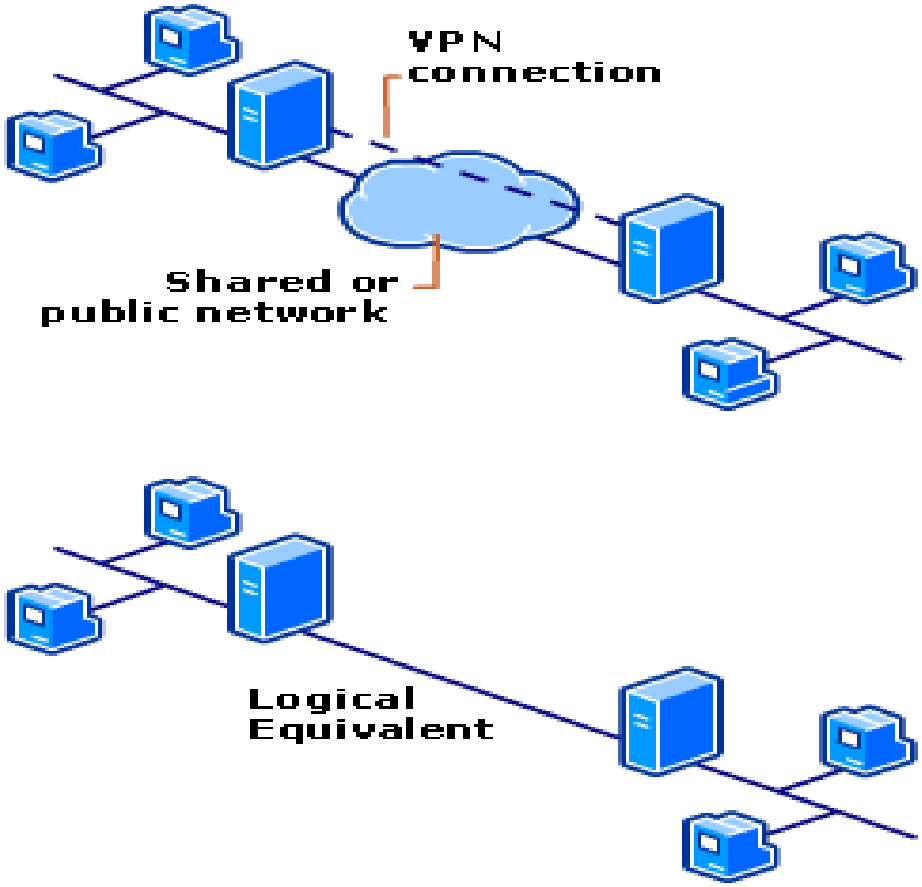
VPN Scenarios (I)

- A VPN client uses a special TCP/IP-based or UDP/IP-based protocol, called a tunneling protocol, to make a virtual call to a virtual port on a VPN server.
- In a typical VPN deployment, a client initiates a virtual point-to-point connection to a remote access server over the Internet.
- The remote access server answers the call, authenticates the caller, and transfers data between the VPN client and the organization’s private network.

VPN Scenarios (II)

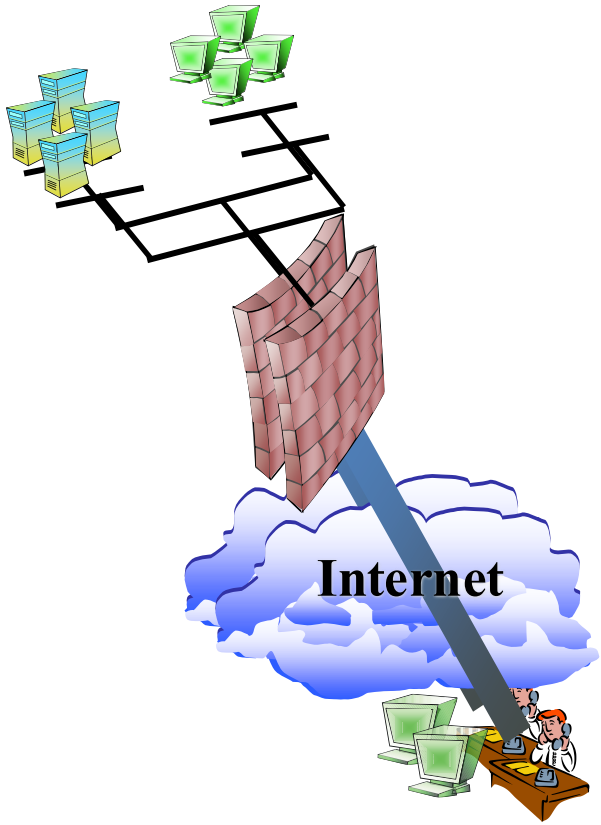
- To emulate a point-to-point link, data is encapsulated, or wrapped, with a header. The header provides routing information that enables the data to traverse the shared or public network to reach its endpoint.
- To emulate a private link, the data being sent is encrypted for confidentiality.
- Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The link in which the private data is encapsulated and encrypted is known as a *VPN connection*.

A VPN Connection



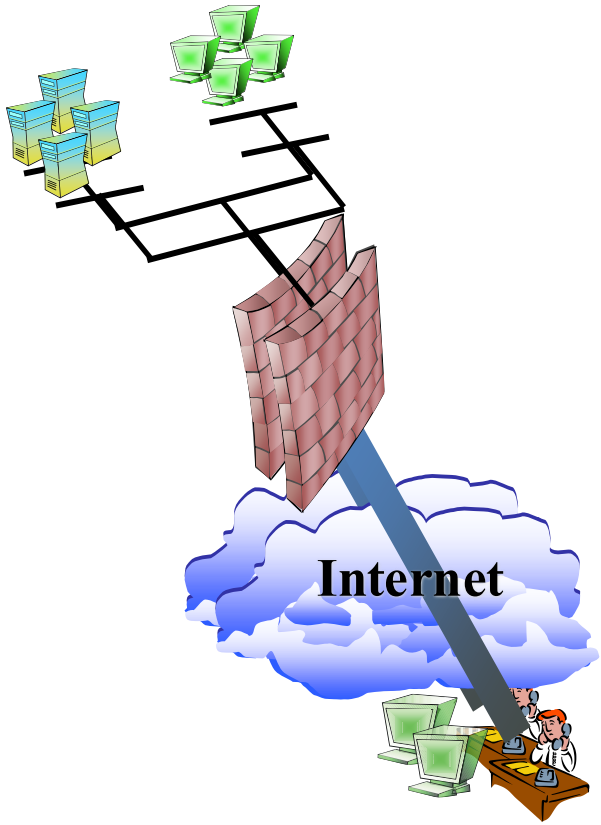
Types of VPNs

- Remote Access VPN
  - Provides access to internal corporate network over the Internet
  - Reduces long distance, and technical support costs



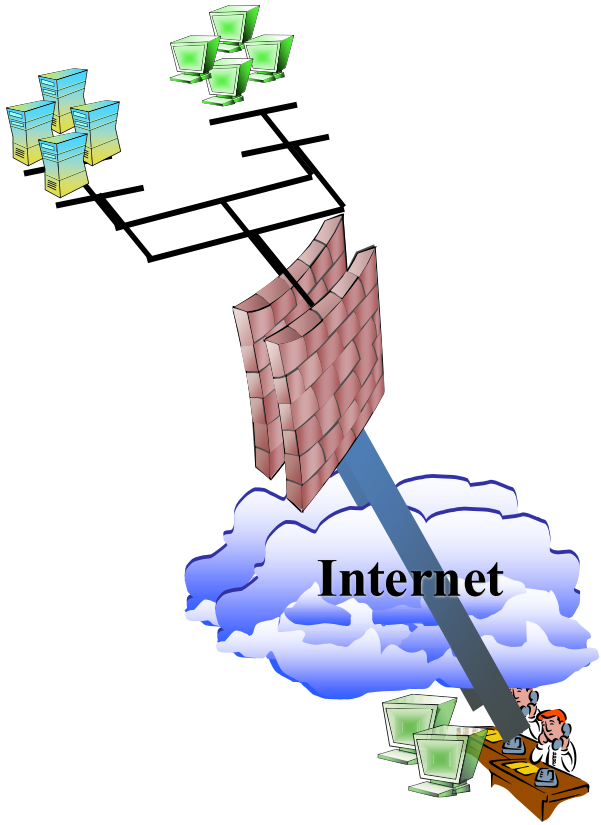
Remote Access VPN

- Remote access VPN connections enable users working at home or on the road to access a server on a private network using the infrastructure provided by a public network, such as the Internet.



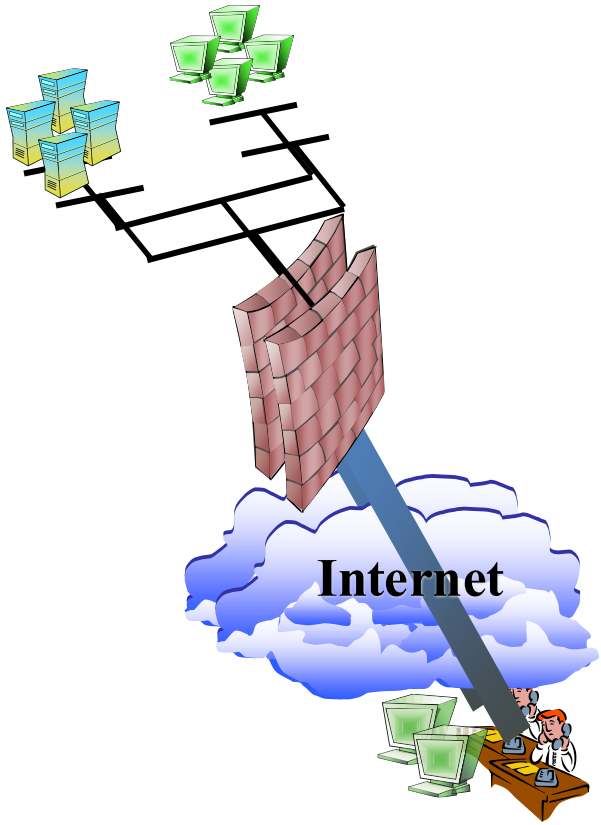
Remote Access VPN

- From the user's perspective, the VPN is a point-to-point connection between the computer (the VPN client) and an organization's server.



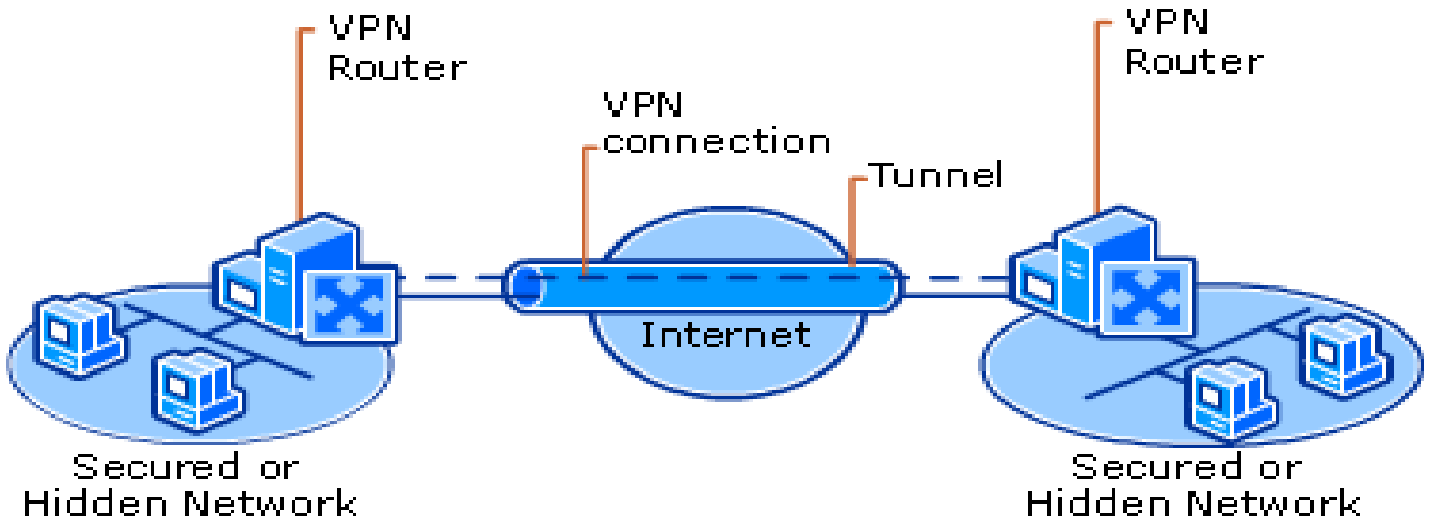
Remote Access VPN

- The exact infrastructure of the shared or public network is irrelevant because it appears logically as if the data is sent over a *dedicated private link*.
  - Because the VPN connection is secure



Types of VPNs

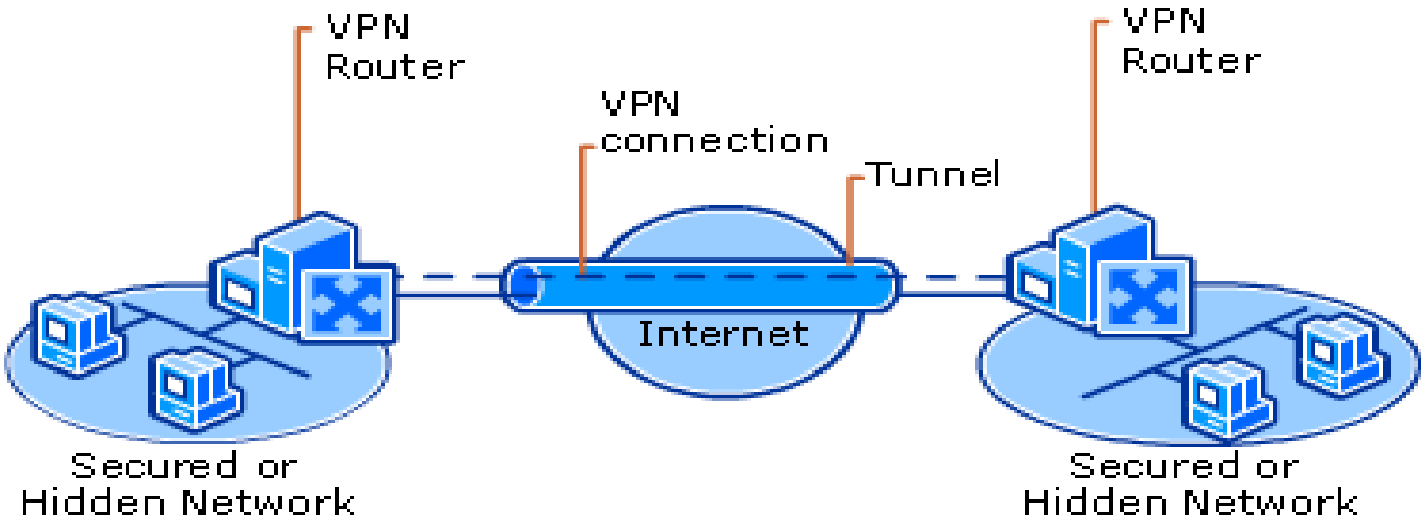
- Site-to-Site VPN
  - Connects multiple offices over the Internet
  - Reduces dependencies on “frame relay” and “leased lines”



Frame Relay is a standardized wide area network (WAN) technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology.
A leased line is an allocated circuit between two points of communication.

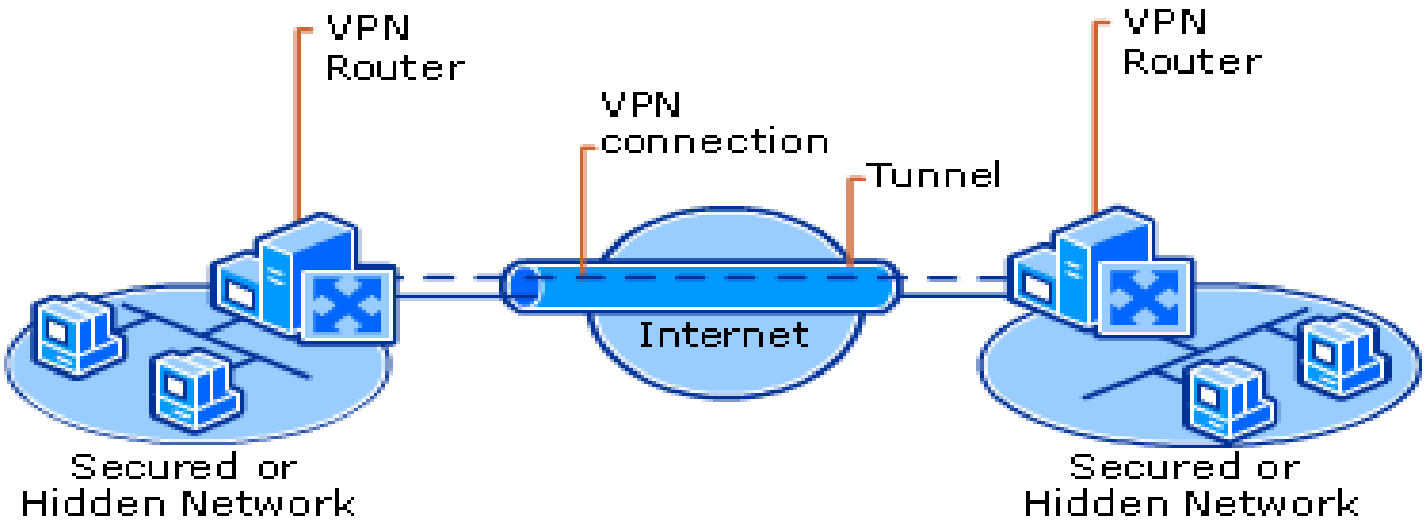
Site-to-Site VPN

- Site-to-site VPN connections (also known as router-to-router VPN connections) enable organizations to have routed connections between separate offices or with other organizations over a public network while helping to maintain secure communications.



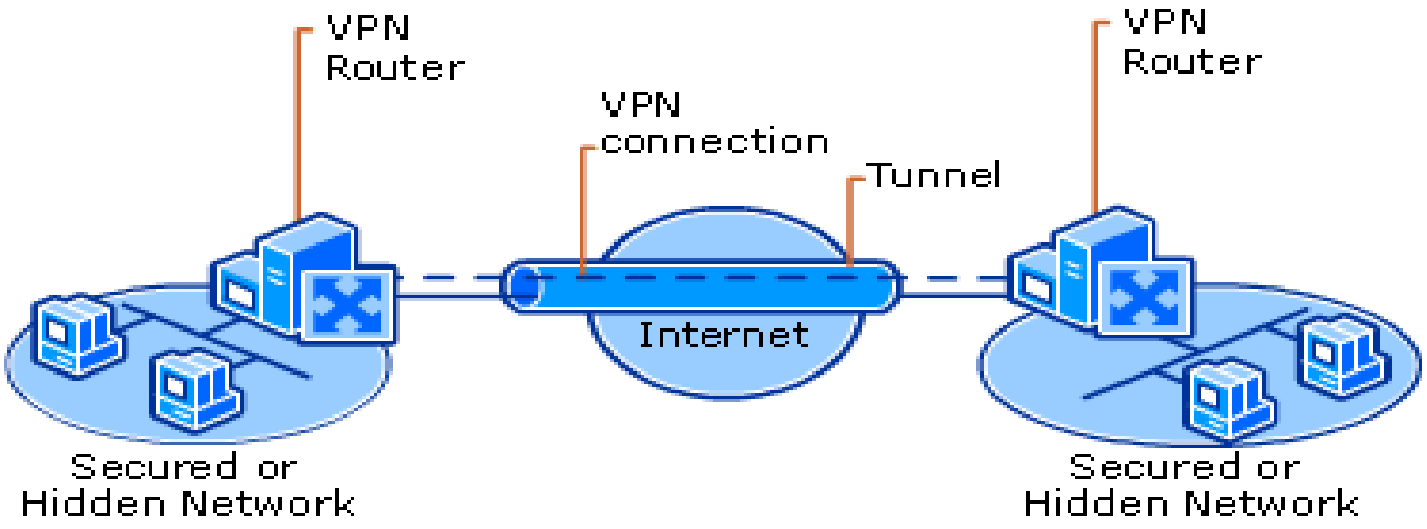
Site-to-Site VPN

- A routed VPN connection across the Internet logically operates as a *dedicated WAN link,*
  - because the VPN connection is secure.



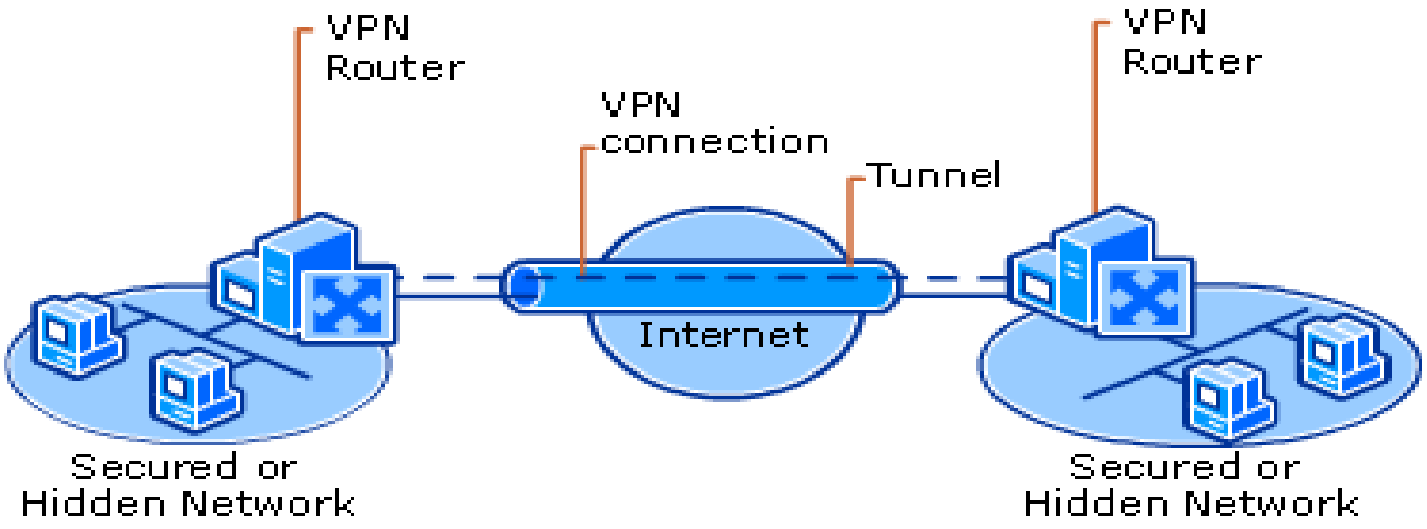
Site-to-Site VPN

- When networks are connected over the Internet, a router forwards packets to another router across a VPN connection.



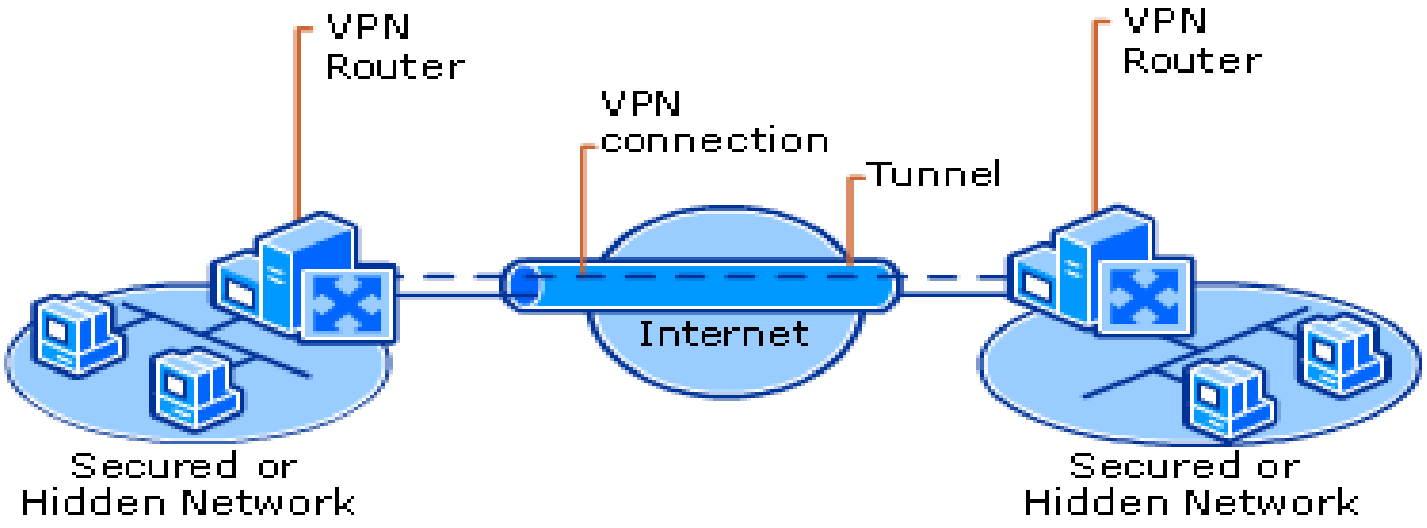
Site-to-Site VPN

- To the routers, the VPN connection operates as a data-link layer link.



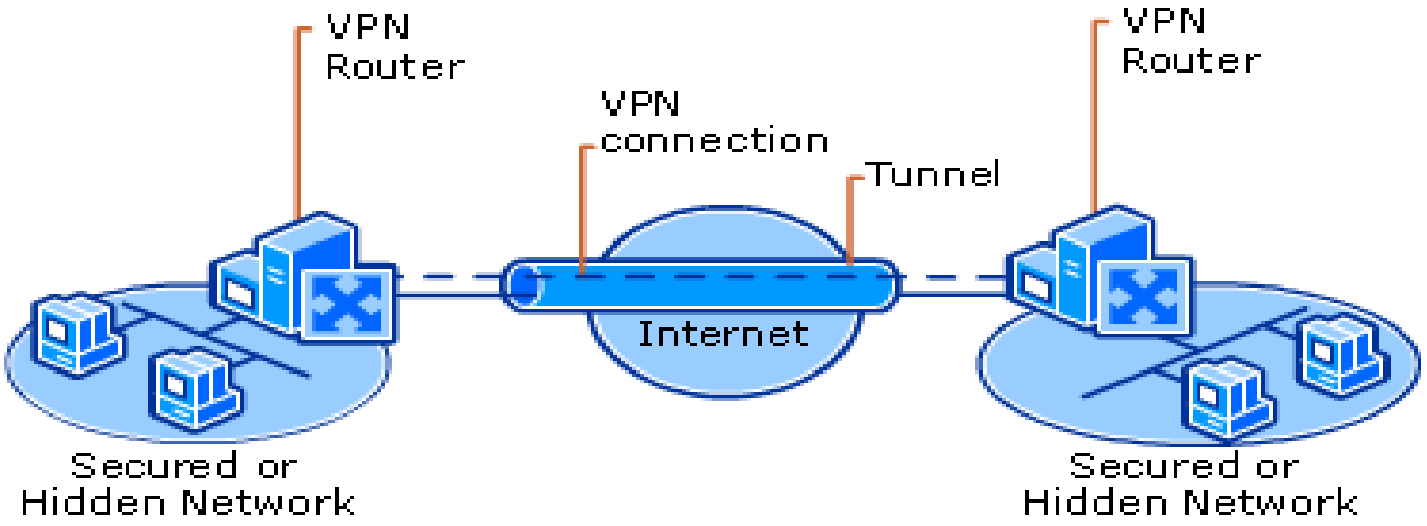
Site-to-Site VPN

- A site-to-site VPN connection connects two portions of a private network.
- The VPN server provides a routed connection to the network to which the VPN server is attached.



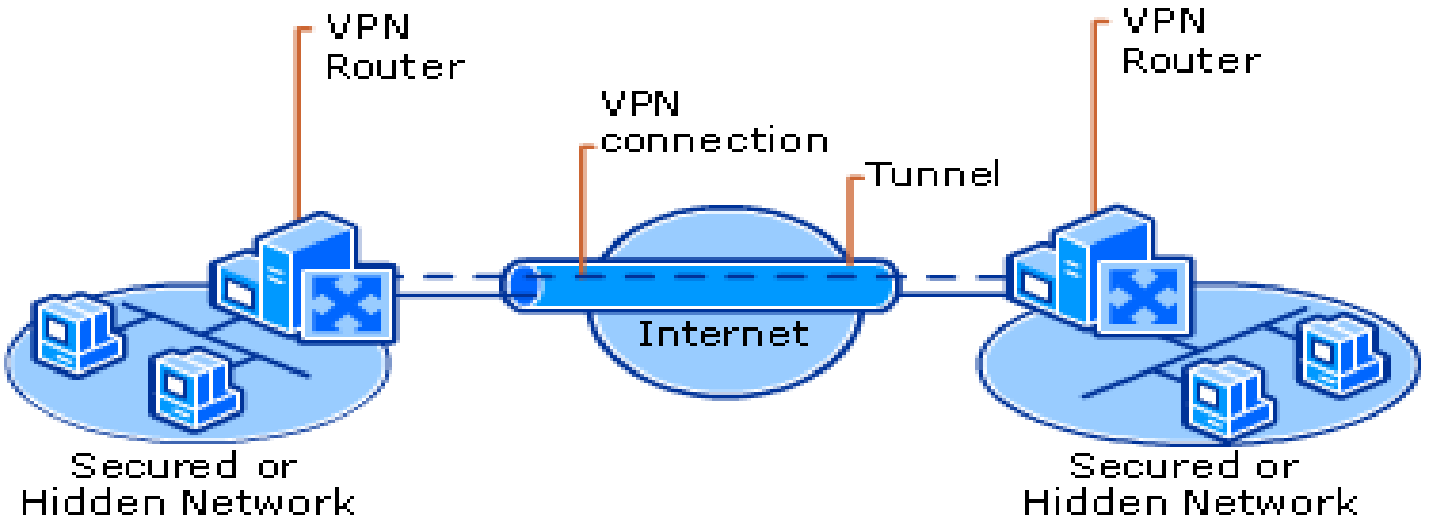
Site-to-Site VPN

- The calling router (the VPN client) authenticates itself to the answering router (the VPN server).
- For mutual authentication, the answering router authenticates itself to the calling router.

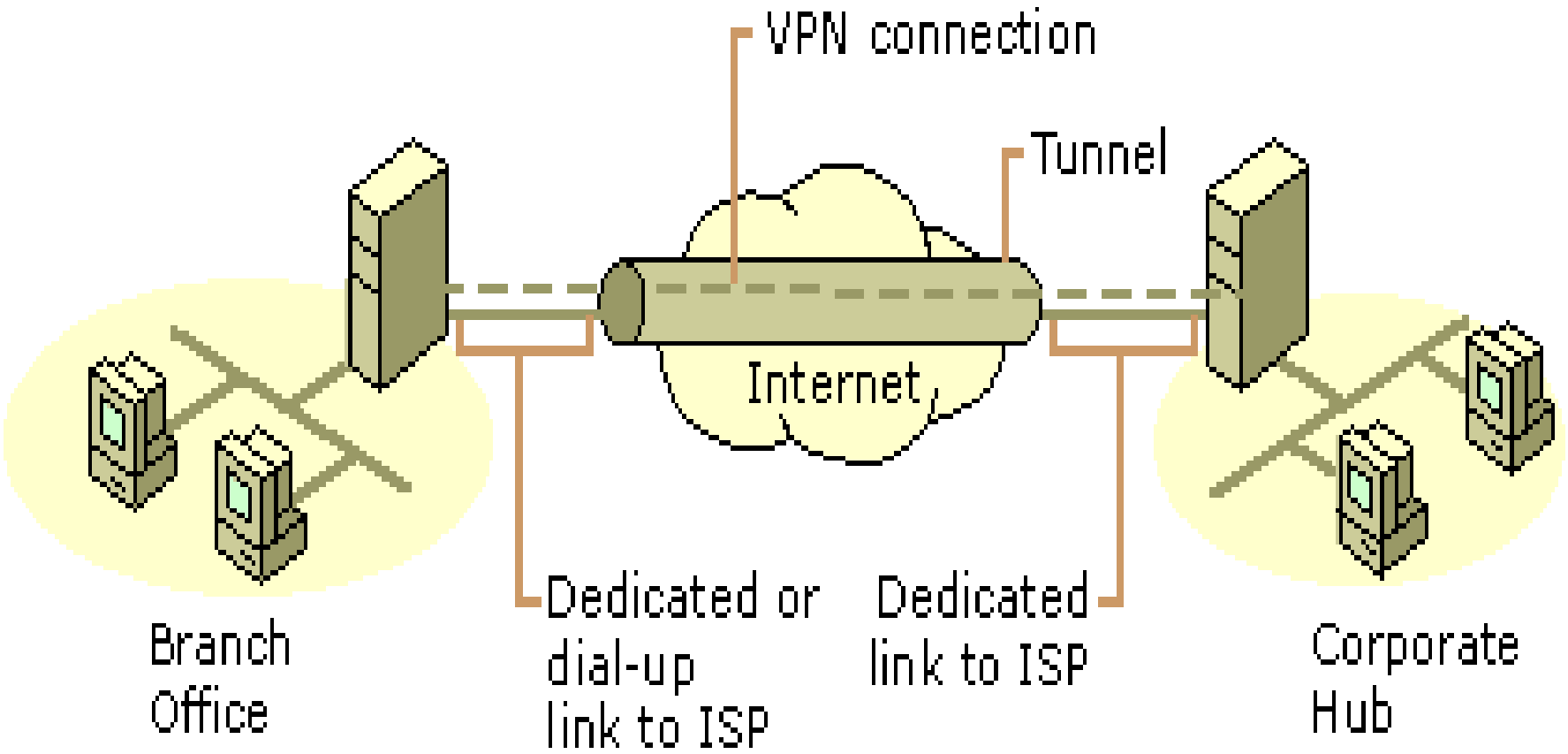


Site-to-Site VPN

- In a site-to site VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers.

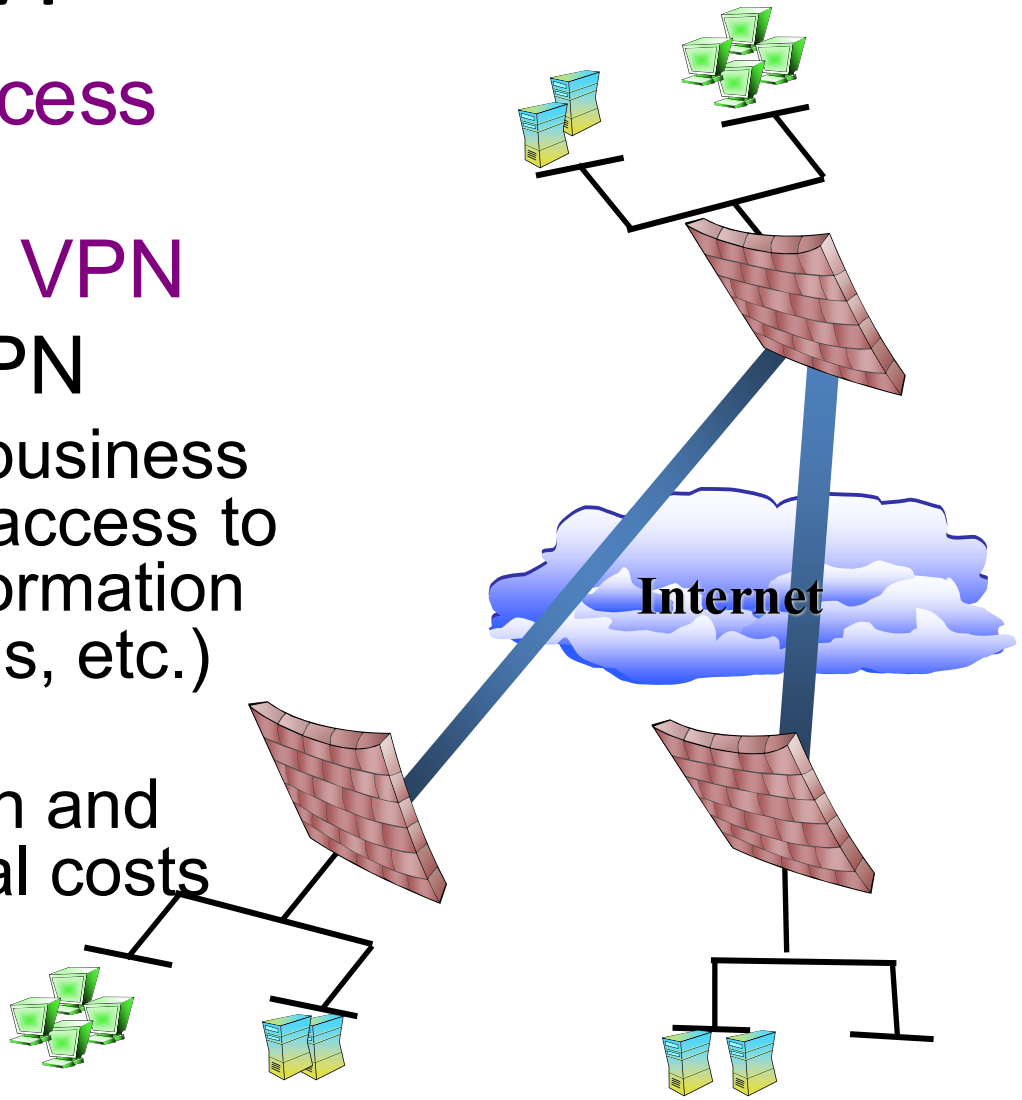


Site to Site VPN Connection



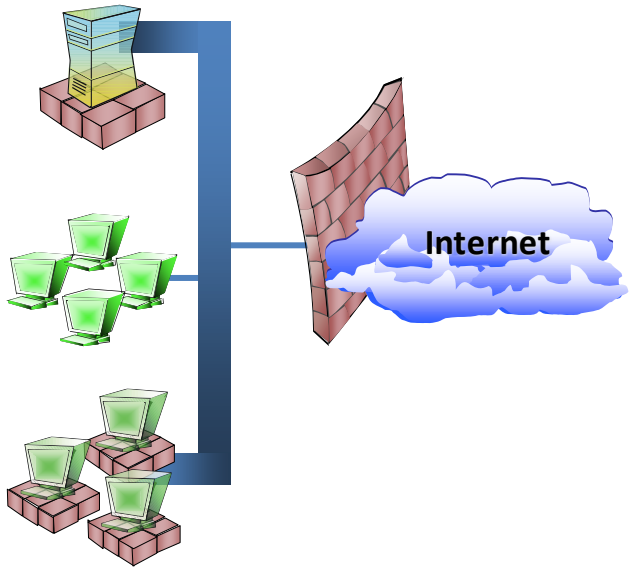
Types of VPNs

- Remote Access VPN
- Site-to-Site VPN
- Extranet VPN
  - Provides business **partners** access to critical information (sales tools, etc.)
  - Reduces transaction and operational costs



Types of VPNs

- Remote Access VPN
- Site-to-Site VPN
- Extranet VPN
- Intranet (Client-Server) VPN
  - Protects sensitive **internal** communications
  - HKUST: **Juniper Pulse Secure**
  - Most attacks originate within an organization

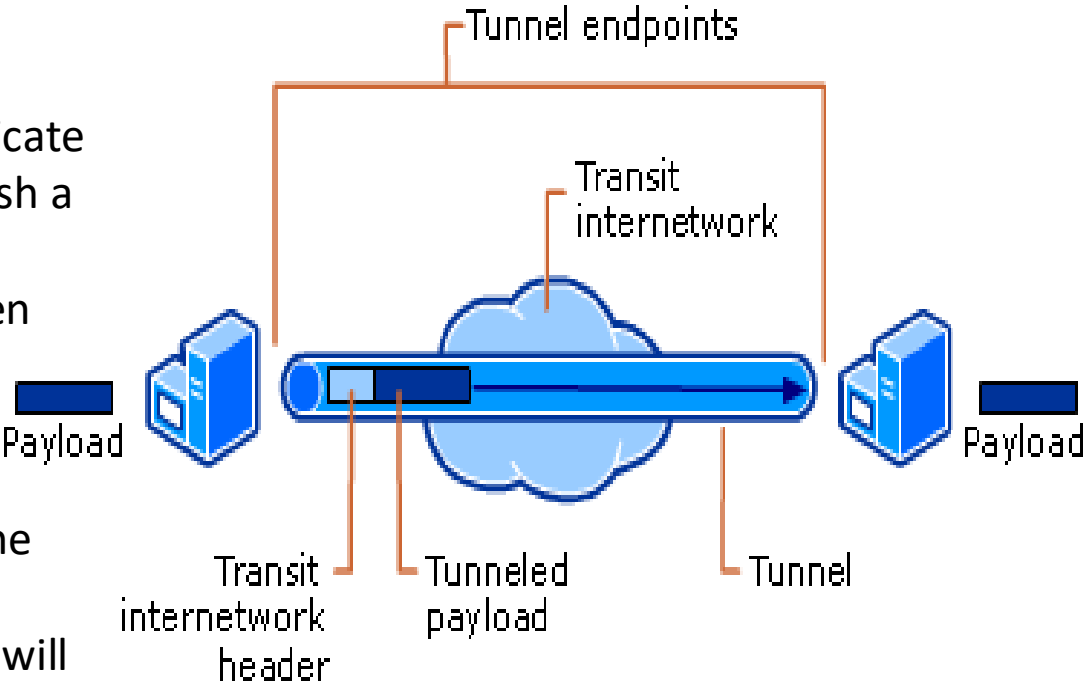


Establishing a Secure Tunnel

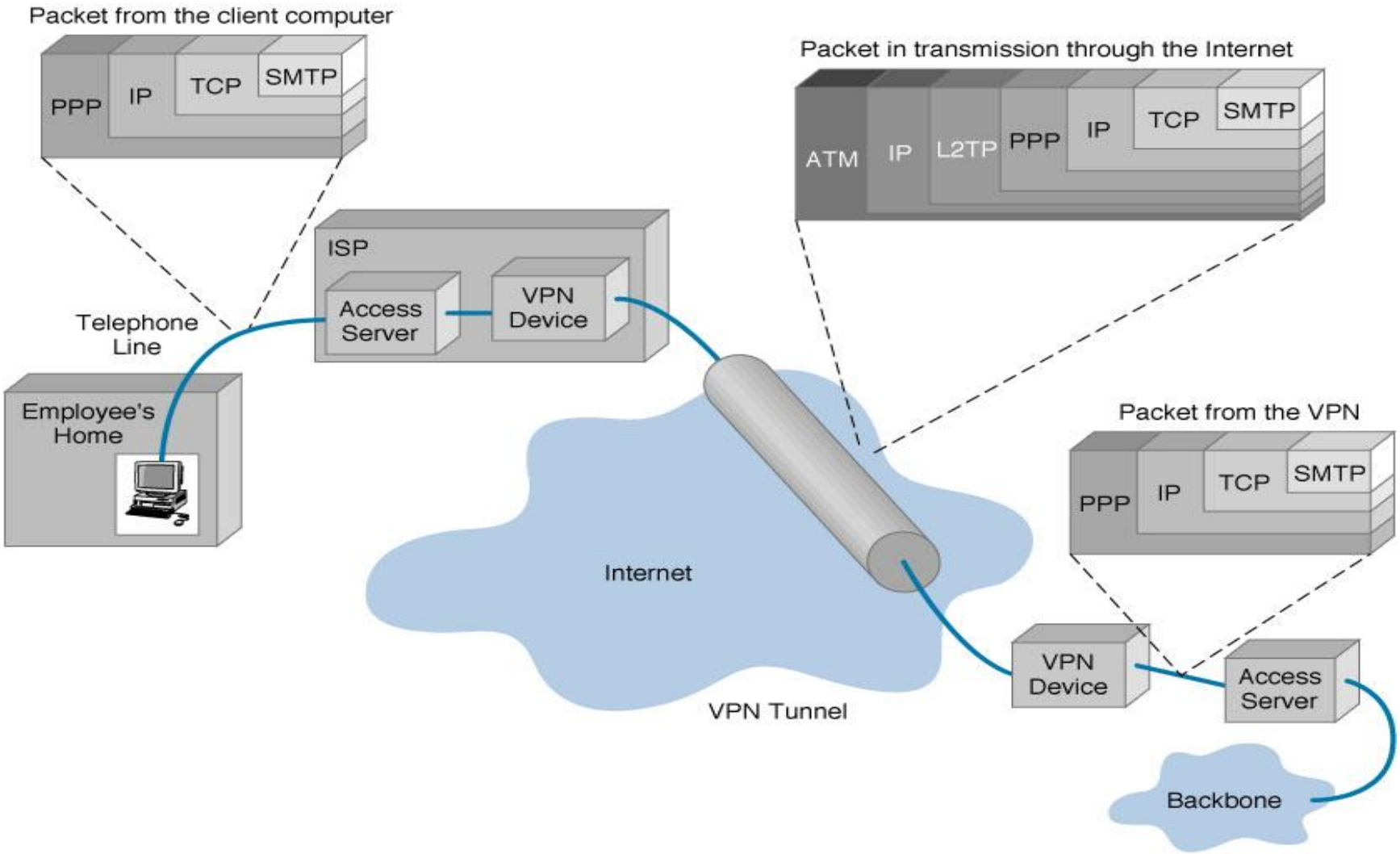
- Two Tunneling protocols can be used
  - PPTP (Point to Point Tunneling Protocol)
  - L2TP (Layer Two Tunneling Protocol)
  - Tunneling encapsulates frames in an extra header to be passed over the internet appearing as normal frames. The process includes:
    - Encapsulation (adding extra frame), transmission, Decapsulation

A Pictorial Description of Tunneling

1) The two VPNs authenticate each other and establish a secure tunnel.
2) The payload data is then encapsulated.
3) The encapsulated data is then transmitted via the secure tunnel to the VPN server.
4) Finally, the VPN server will decapsulate the received data



VPN Encapsulation of Packets



Tunneling Protocols

- Both tunneling protocols support the following methods, as they are based on PPP:
  - User authentication
  - Dynamic address assignment
  - Data compression
  - Data encryption
  - Key management

Tunneling Protocols cont.

- Each tunneling protocol is built on PPP (Point to Point Protocol)
  - 4 Phases
    - 1) Link Establishment - a physical link between ends
    - 2) User Authentication – Password protocols used
      - PAP, CHAP, MS-CHAP (details omitted here)
    - 3) Call Back Control – optional
      - Disconnects and server calls back after authentication
    - 4) Data Transfer Phase – exactly what it sounds like

Tunneling Protocols cont.

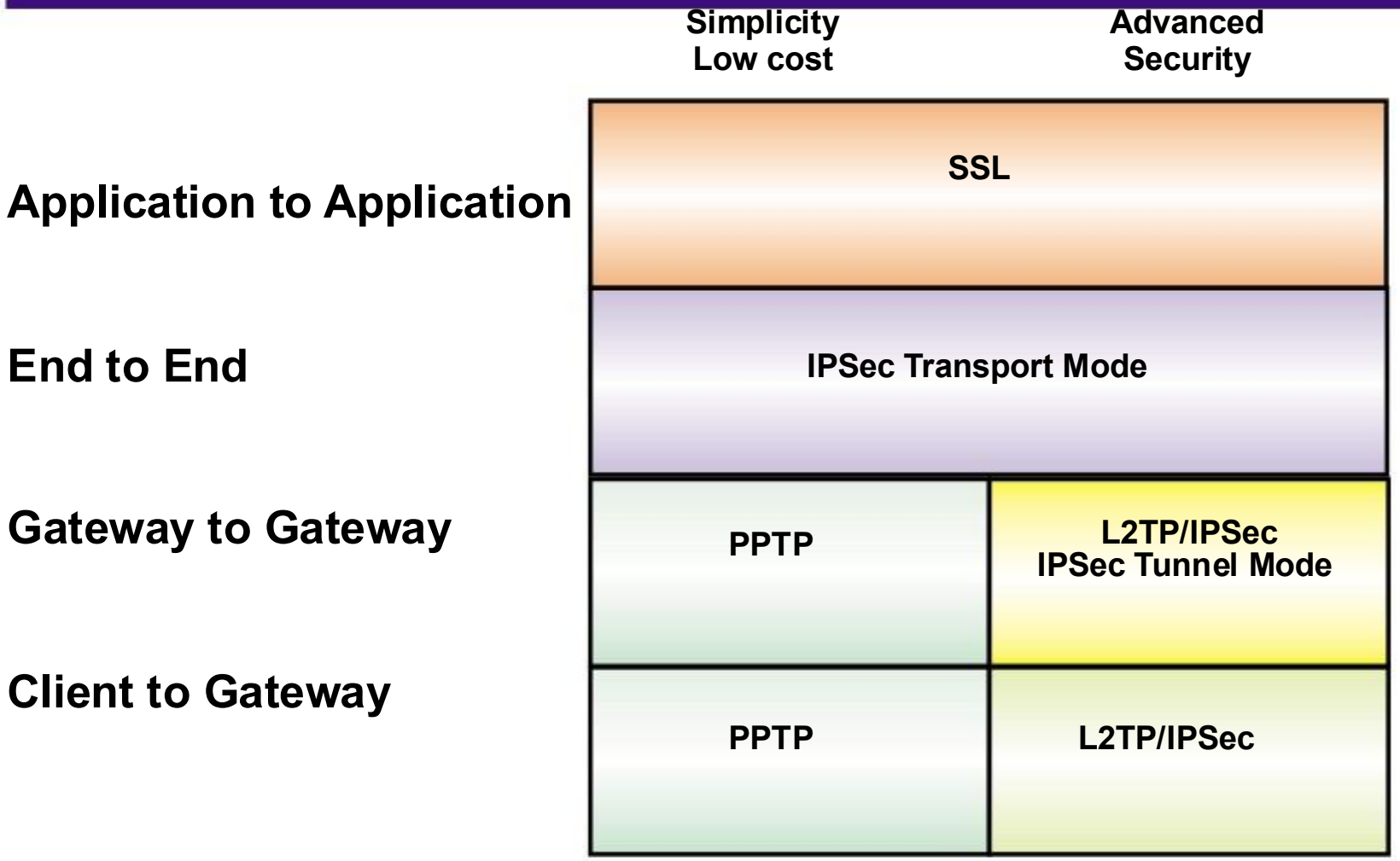
- PPTP
  - Uses IP datagrams for encapsulation
  - Uses TCP for tunnel maintenance
  - Its specification does not describe encryption or authentication futures and relies on the PPP being tunneled to implement security.
  - However, the most common PPTP implementation shipping with the Microsoft Windows product families implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack.

Tunneling Protocols cont.

- L2TP
  - In computer networking, Layer 2 Tunneling Protocol is a tunneling protocol used to support VPNs or as part of the delivery of services by ISPs.
  - It does not provide any encryption by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.
  - It uses data in IP, ATM, Frame Relay, X.25 for encapsulation
    - IP when going over internet
  - It uses UDP for tunnel maintenance

Packet switching: ATM (Asynchronous Transfer Mode), Frame relay, X.25

Summary of VPN Technologies



Remark: Since PPTP-based VPNs are not secure enough, they are rarely used nowadays!

Benefits of Using VPN

- A VPN can expand globally.
- The operational cost of an organization can be reduced.
  - No dedicated lines are necessary
- A VPN has scalability
  - Add new sites, users quickly
- Technology is on the end systems, which makes it more scalable
- There is no single point of failure

Appendix

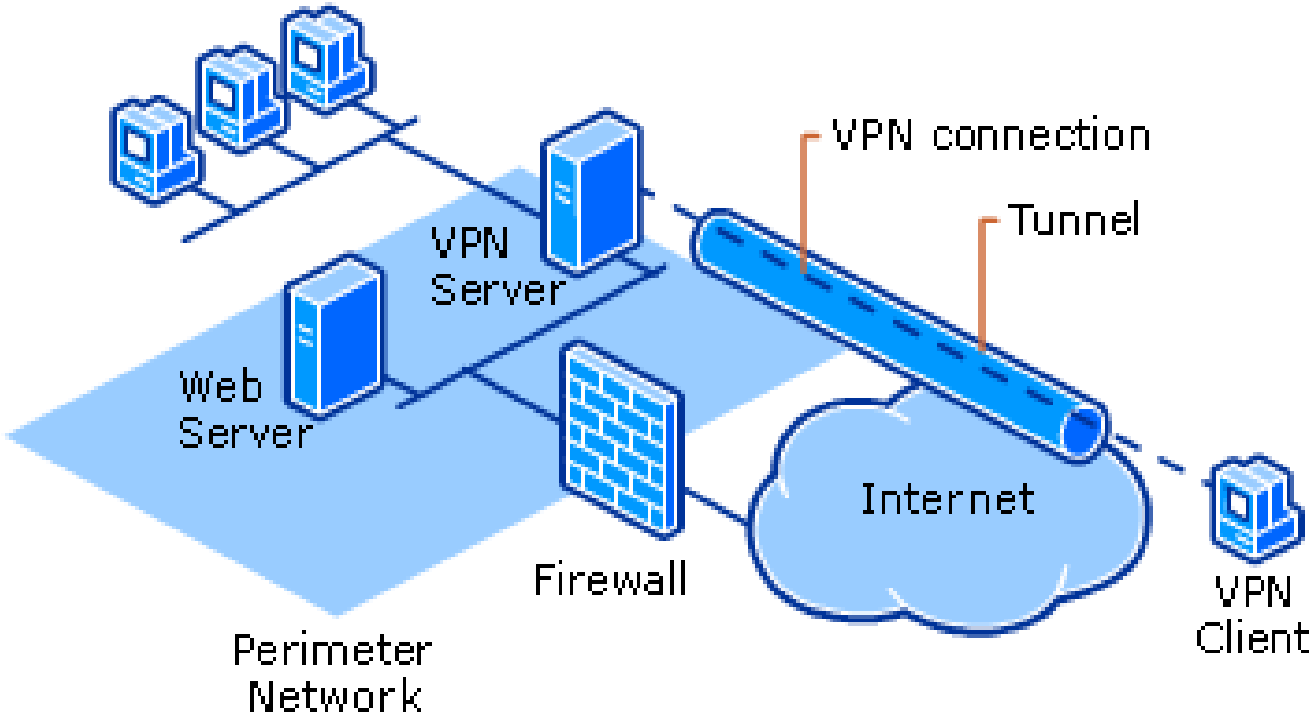
VPN and Firewalls

- The routing service of a VPN supports a variety of inbound and outbound packet-filtering features that block certain types of traffic.
- The filtering options include the following: TCP port, UDP port, IP protocol ID, Internet Control Message Protocol (ICMP) type, ICMP code, source address, and destination address.
- A VPN server can be placed behind a firewall or in front of a firewall.
- These two approaches are described below.

VPN Server Behind a Firewall

- In the most common configuration, the firewall is connected to the Internet, and the VPN server is an intranet resource that is attached to the perimeter network. The VPN server has an interface on both the perimeter network and the intranet.
- In this scenario, the firewall must be configured with input and output filters on its Internet interface that allow tunnel maintenance traffic and tunneled data to pass to the VPN server.
- Additional filters can allow traffic to pass to Web, FTP, and other types of servers on the perimeter network. For an additional layer of security, the VPN server should also be configured with PPTP or L2TP/IPSec packet filters on its perimeter network interface.

VPN Server Behind a Firewall



VPN Server in Front of a Firewall

- In this case, packet filters must be added to the VPN server's Internet interface to allow only VPN traffic to and from the IP address of that interface.
- For inbound traffic, when the tunneled data is decrypted by the VPN server, it is forwarded to the firewall. Through the use of its filters, the firewall allows the traffic to be forwarded to intranet resources. Because the only traffic that crosses the VPN server is generated by authenticated VPN clients, in this scenario, firewall filtering can be used to prevent VPN users from accessing specific intranet resources. Because Internet traffic allowed on the intranet must pass through the VPN server, this approach also prevents the sharing of FTP or Web intranet resources with non-VPN Internet users.

VPN Server in Front of a Firewall

