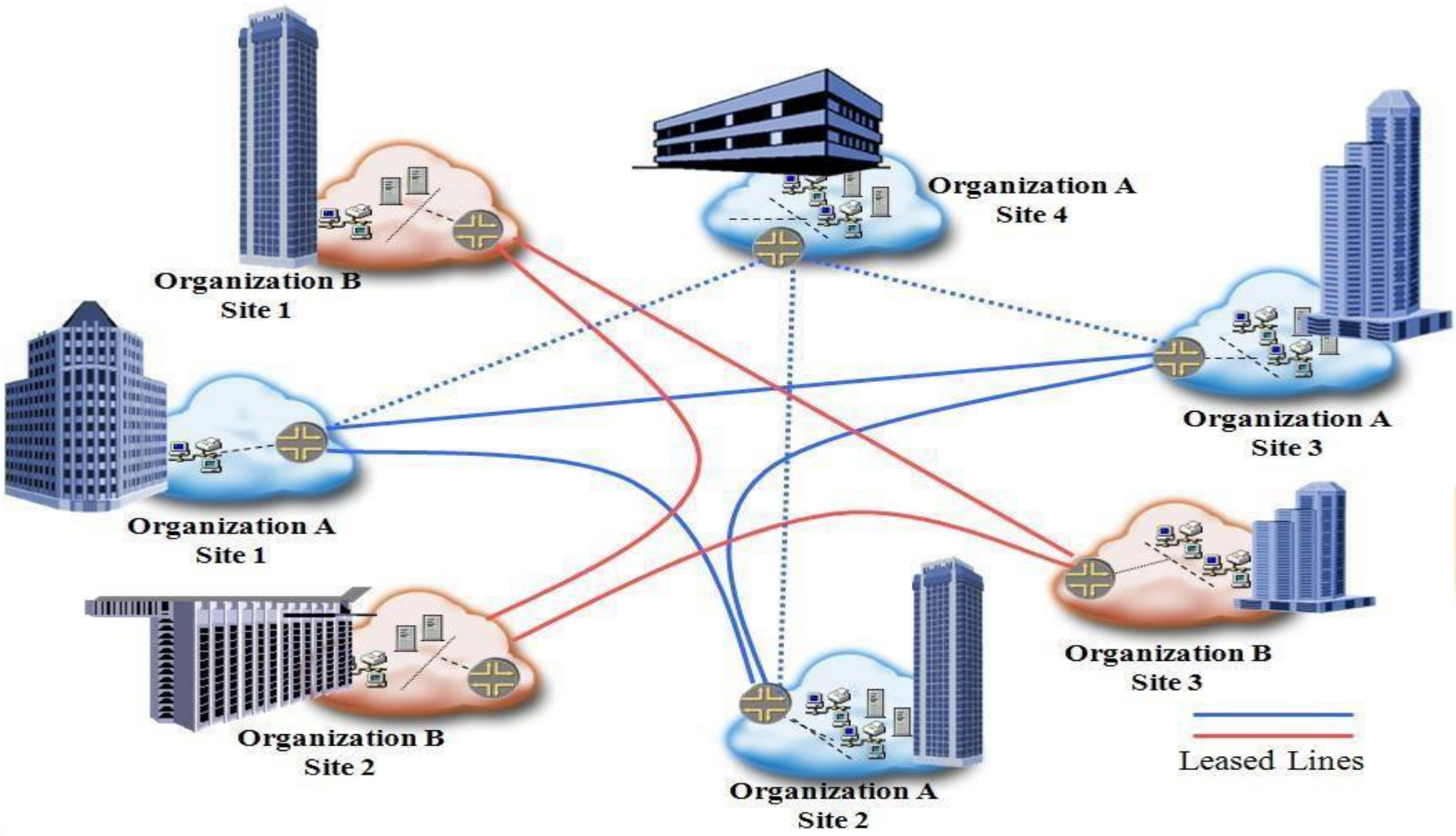
VPN: Virtual Private Network

- Virtual Private Network (VPN) is defined as network connectivity deployed on a shared infrastructure with the same policies and security as a private network.
- A VPN can be between two end systems, or it can be between two or more networks.
- A VPN can be built using tunnels and encryption. VPNs can occur at any layer of the TCP/IP protocol stack.
- A VPN is an alternative WAN infrastructure that replaces or augments existing private networks that use leased-line or enterprise-owned networks

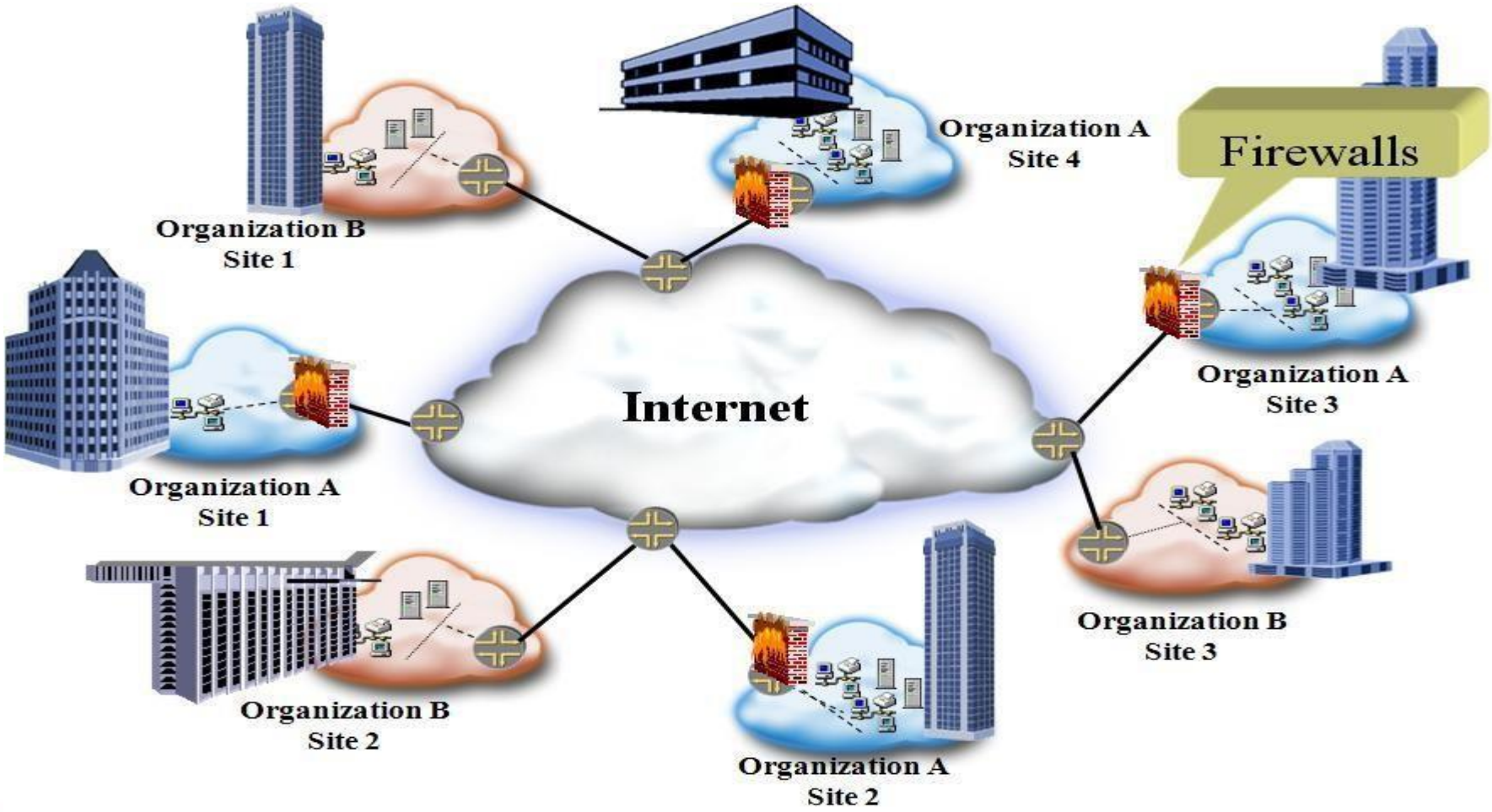
Private Networks



Private Networks (Cont.)

- **Advantages:**
  - Leased lines are secured
  - Privacy and QoS Guaranteed
- **Disadvantages**
  - Leased lines are very expensive
  - No of links required grows exponentially if full mesh connectivity is required and network expands.
  - More CPE ports are required
  - Network complexity increases as network grows. All existing sites requires reconfiguration in case of a new site addition.

Virtual Private Network



Critical Functions of VPN

VPNs provide three critical functions:

- Confidentiality (encryption) – The sender can encrypt the packets before transmitting them across a network.
  - By doing so, no one can access the communication without permission. If intercepted, the communications cannot be read.
- Data integrity – The receiver can verify that the data was transmitted through the Internet without being altered.
- Origin authentication – The receiver can authenticate the source of the packet, guaranteeing and certifying the source of the information.
- Access Control: Restricting unauthorized users from the network

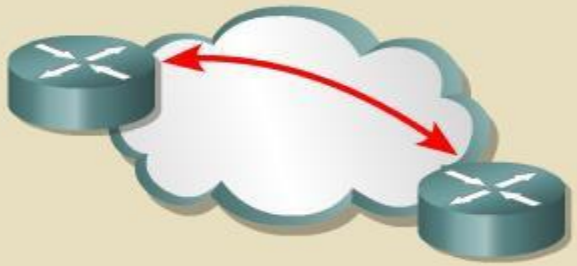
Benefits of VPN Technology

The primary benefits include:

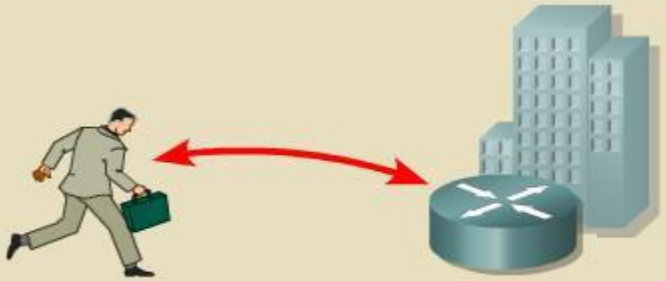
- VPNs offer lower cost than private networks.
  - LAN-to-LAN connectivity costs are typically reduced by 20 to 40 percent over domestic leased-line networks.
- VPNs offer flexibility for enabling the Internet economy.
  - VPNs are inherently more flexible and scalable network architectures than classic WANs.
- VPNs offer simplified management burdens compared to owning and operating a private network infrastructure.
- VPN provide Tunnel Network Topology which results in the reduction of management compared to conventional ATM/Frame Relay (Both uses Virtual Circuit Switching Technologies)

VPN Usage Scenarios

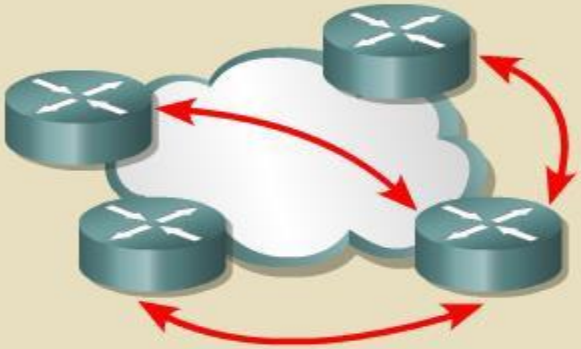
Router to router



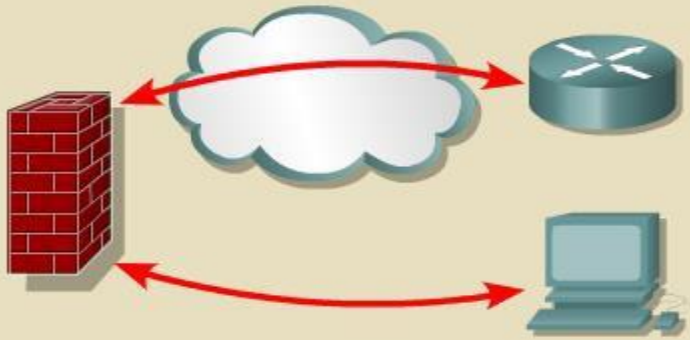
PC to router/concentrator



One router to many routers



PC to firewall



VPN Solutions

- Site-to-Site VPNs are an alternative WAN infrastructure that used to connect branch offices, home offices, or business partners' sites to all or portions of a company's network.
- Intranet VPNs provide full access to company's network
- Extranet VPNs provide business partners with limited access to a company's network
- Secure VPNs use Internet as a corporate communication medium. Data is encrypted before sending, moved over to Internet, and then decrypted at the receiving end.
- Encryption creates a security 'tunnel' that can't be attacked

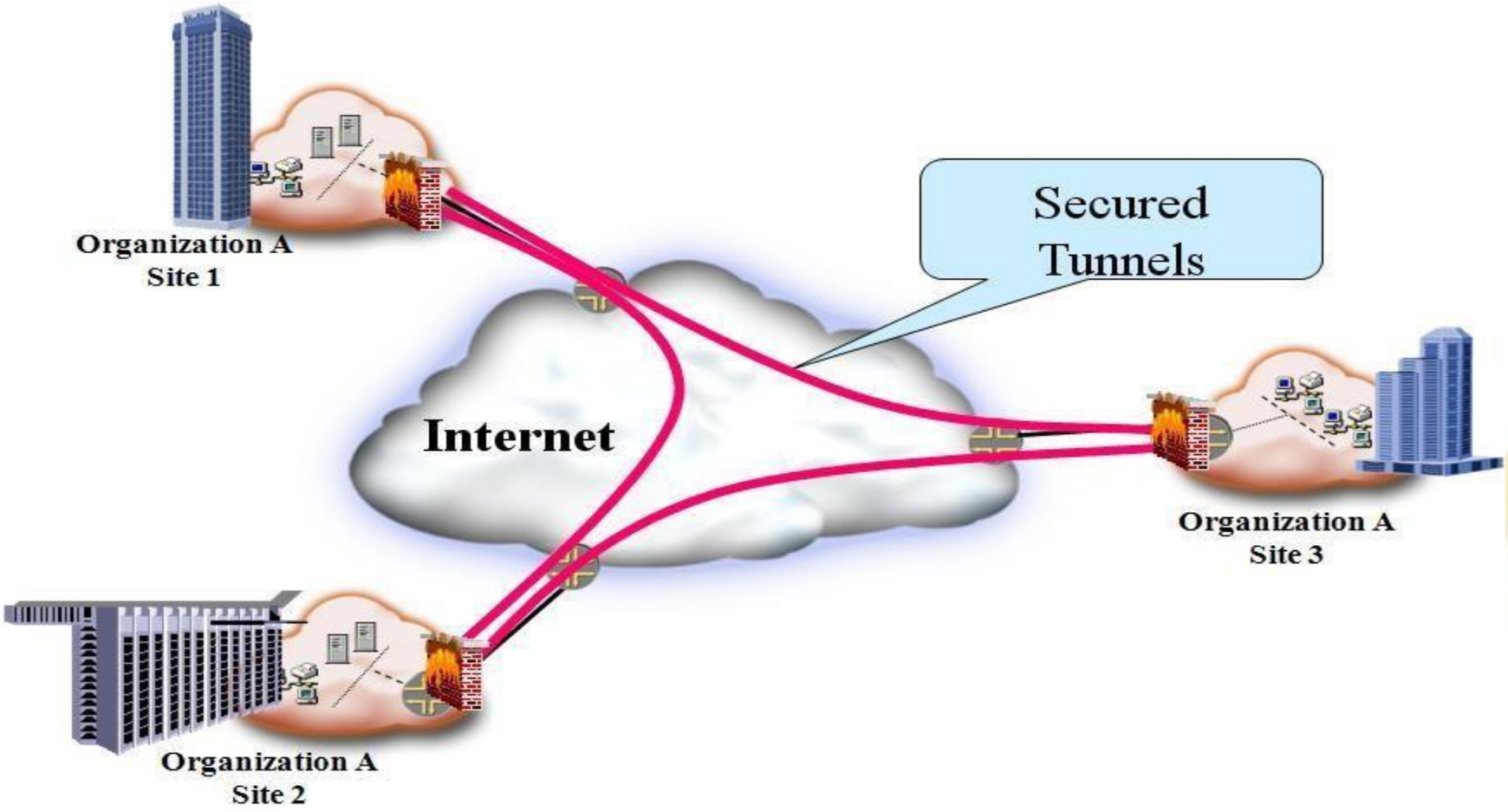
VPN Solutions (Cont.)

- Router based VPNs – adding encryption support to existing router(s) can keep the upgrade costs of VPN low.
- Firewall based VPNs – workable solution for small networks with low traffic volume.
- Software based VPNs – good solution for better understanding a VPN, software runs on existing servers and share resources with them

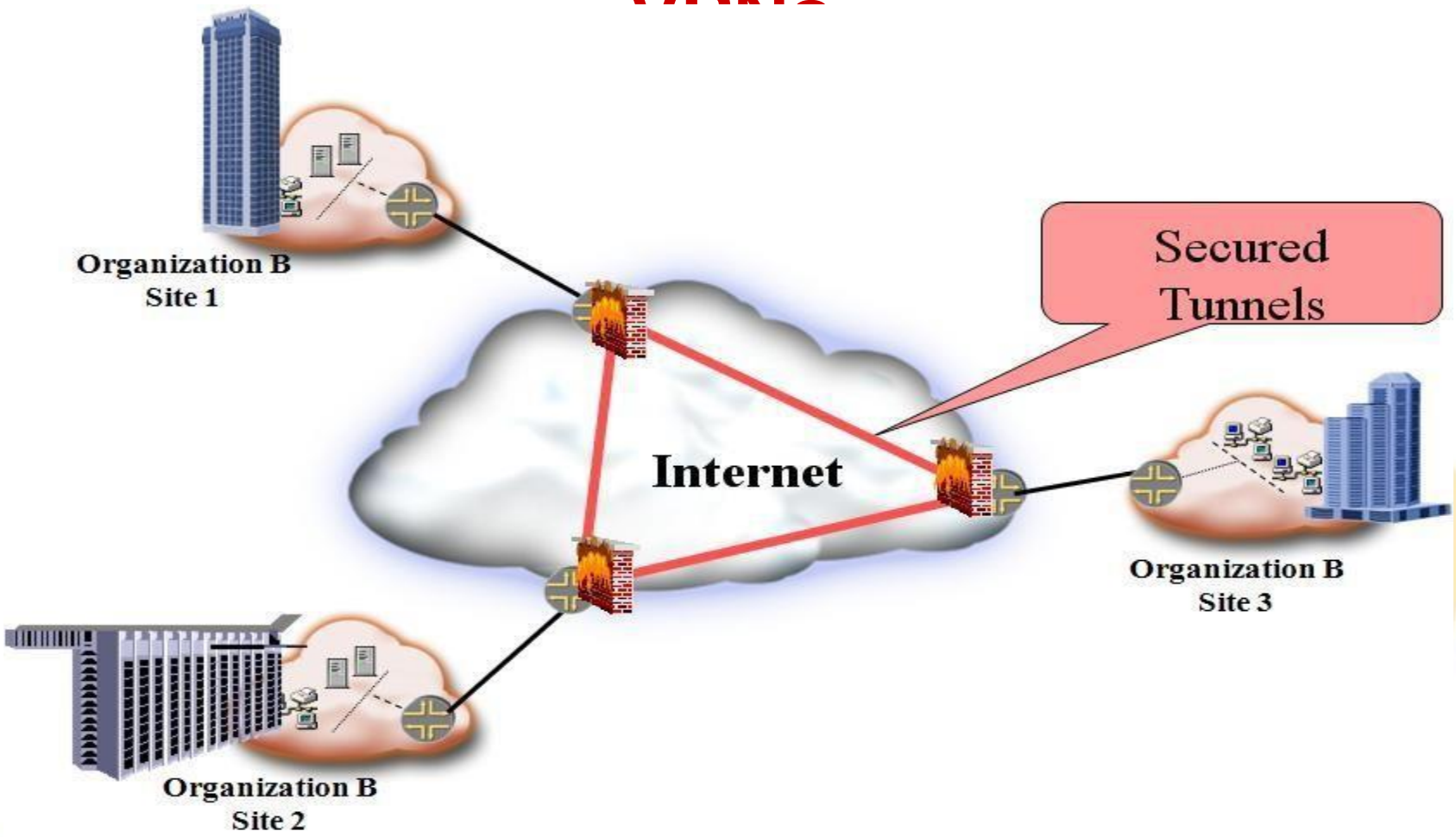
VPN Categories

- **VPN can be classified in two categories**
  - Customer Provisioned
    - VPN Tunnels originate and terminate at customer premises
    - Provisioning of equipment and allied activities is the
    - responsibility of the customer
    - Provider may not be aware of the VPN tunneling through his
    - network
  - Provider Provisioned
    - VPN Tunnels originate and terminate at the service
    - provider's edge
    - Responsibilities of creating and maintaining these tunnels
    - lies with the provider

Customer Provisioned VPNs



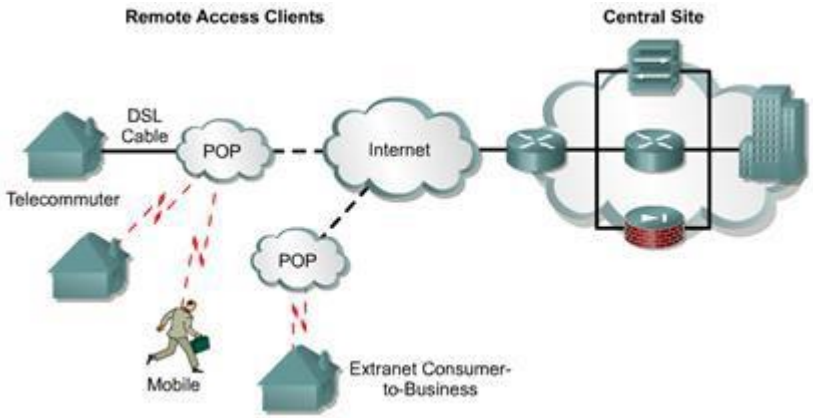
Provider Provisioned VPNs



Remote Access VPNs

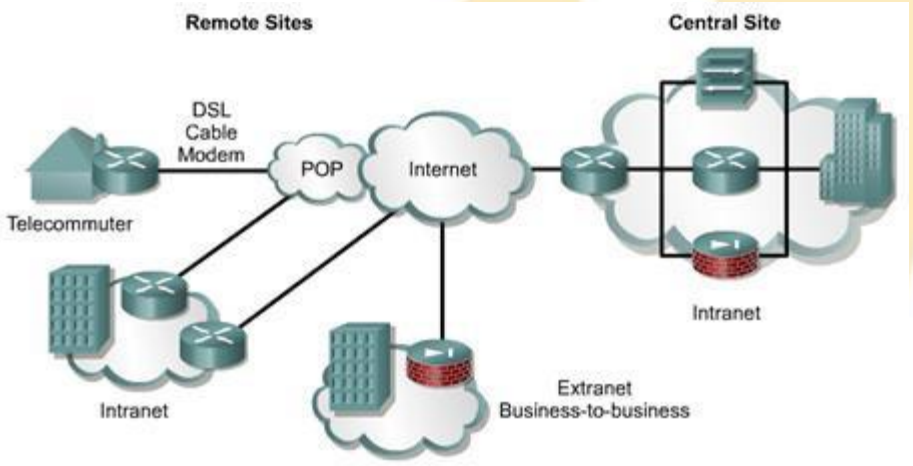
Client Initiated

- Remote users use clients to establish a secure tunnel across a shared ISP network to the enterprise.

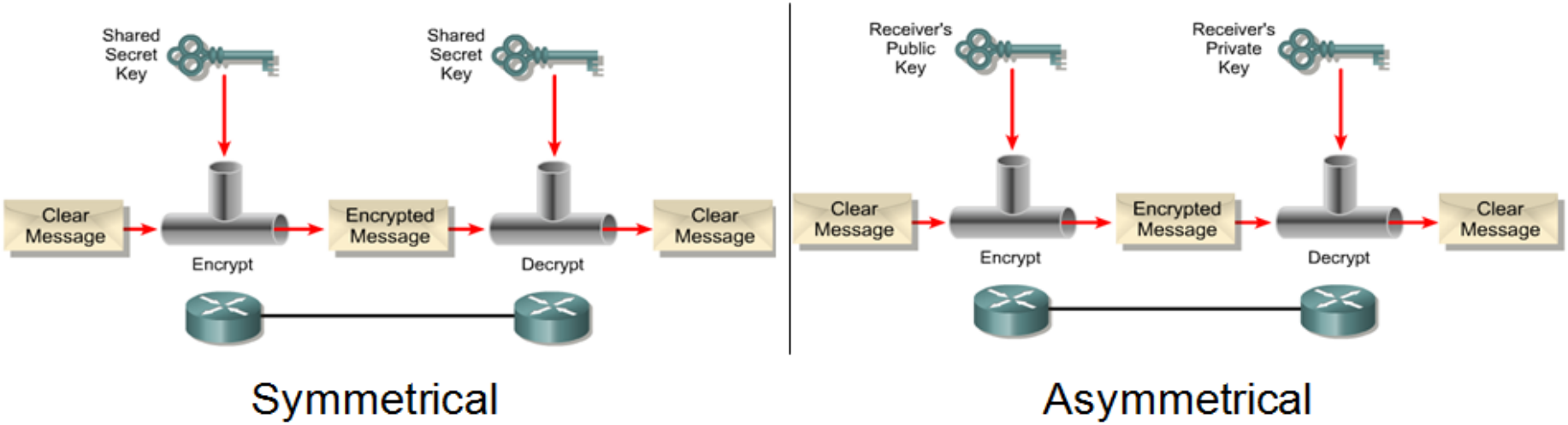


Network Access Server Initiated

- Remote users dial in to an ISP. NAS establishes a secure tunnel to the enterprise private network that might support multiple remote user-initiated sessions.



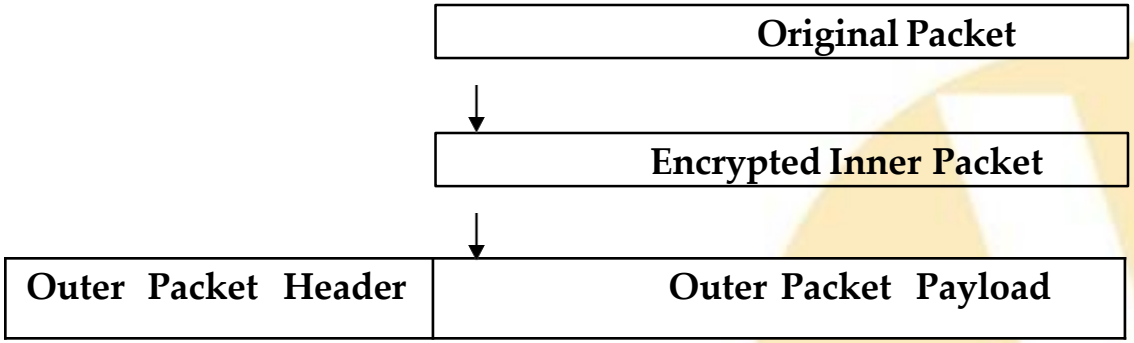
Encryption Algorithms (from EE450)



- Symmetrical algorithm – A shared key algorithm that is used to encrypt and decrypt a message.
  - Use the same key to encrypt and decrypt the message.
- Asymmetrical algorithm – Uses a pair of keys to secure encrypt and decrypt a message.
  - Uses one key to encrypt and a different, but related, key to decrypt.

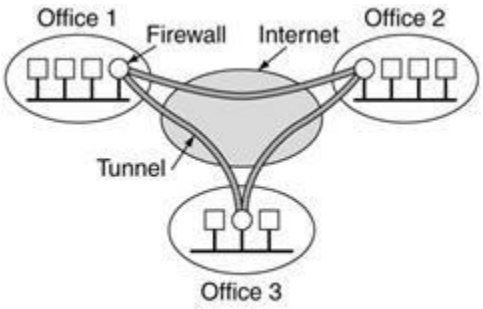
Tunneling

A virtual point-to-point connection made through a public network. It transports encapsulated Packets.

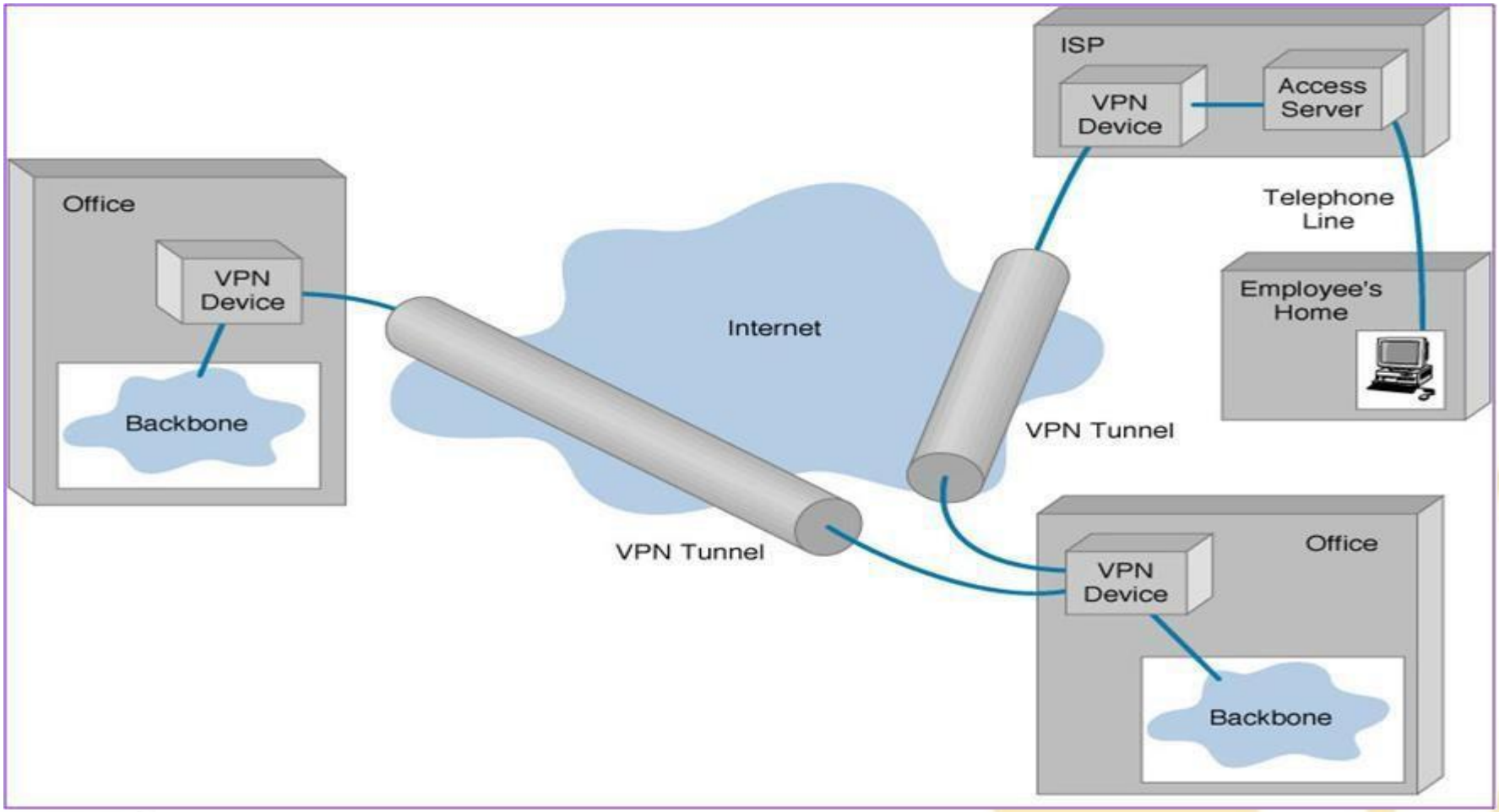


VPN Gateways & Tunnels

- A VPN Gateway is a Network device that provides encryption and authentication service to multiple hosts attached to it.
- All communications (from the public Internet) to internal hosts must flow through the gateway.
- Two Types of VPN Tunnels:
  - PC to Gateway (for remote access)
  - Gateway to Gateway (Typical for LAN-LAN connectivity)

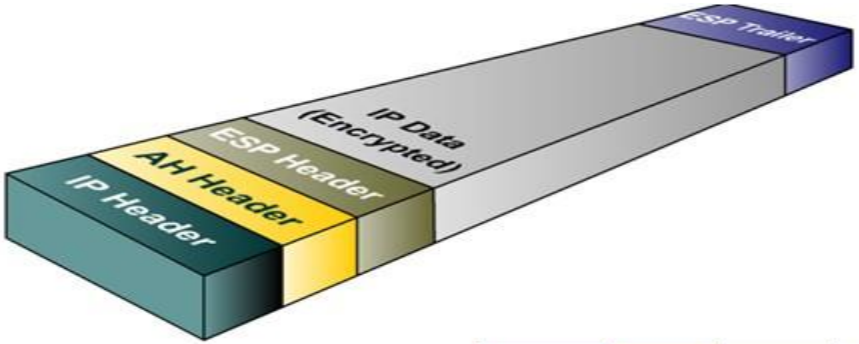


VPN Tunneling



IPsec Overview

IPsec is used to enhance IP with security

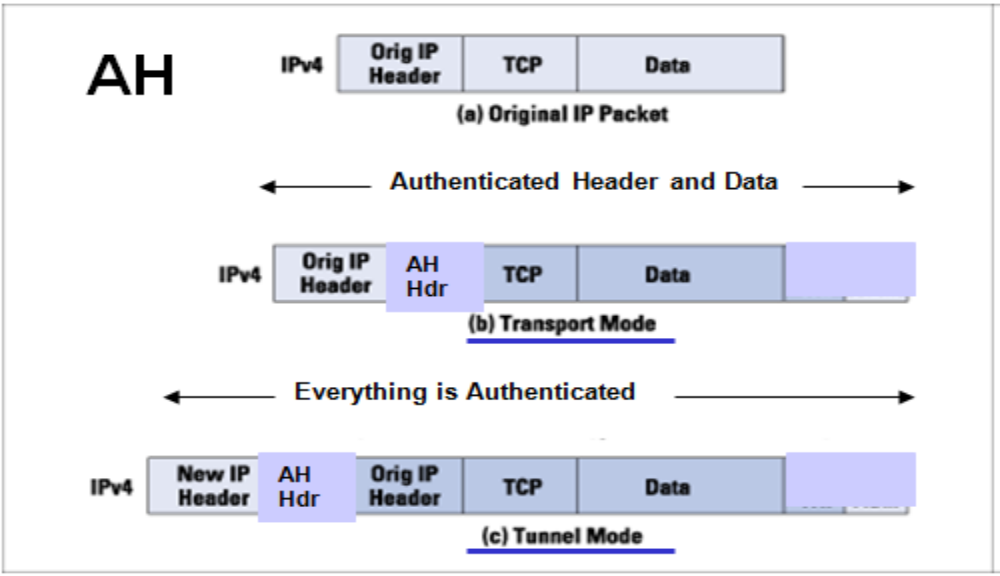


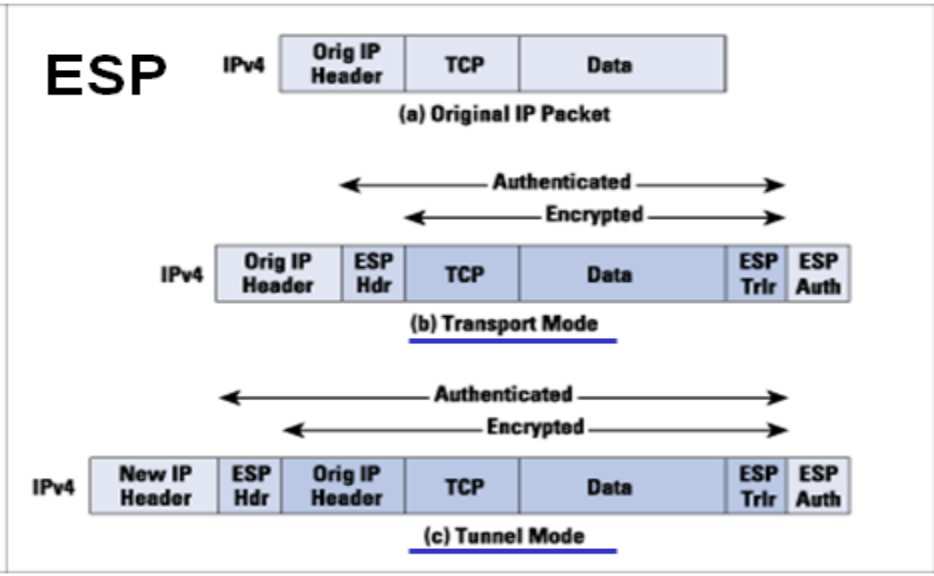
- IPSec was designed to work at Layers 3 and 4.
- Using different options can:
  - Authenticate
  - Check for data integrity
  - Encrypt the payload portion of IP
- IPSec can be used between:
  - Two gateways
  - Two hosts
  - Host and its gateway
- Two primary protocols:
  - Authentication Header (AH)
  - Encapsulation Security Protocol (ESP)

IPsec

- Provides a method of setting up a secure channel for protected data exchange between two devices.
- More flexible and less expensive than end-to end and link encryption methods.
- Employed to establish virtual private networks (VPNs) among networks across the Internet.
- IPSec uses two basic security protocols:
  - Authentication Header (AH): Authenticating Protocol
  - Encapsulating Security Payload (ESP): ESP is an authenticating and encrypting protocol that provide source authentication, confidentiality, and message integrity.

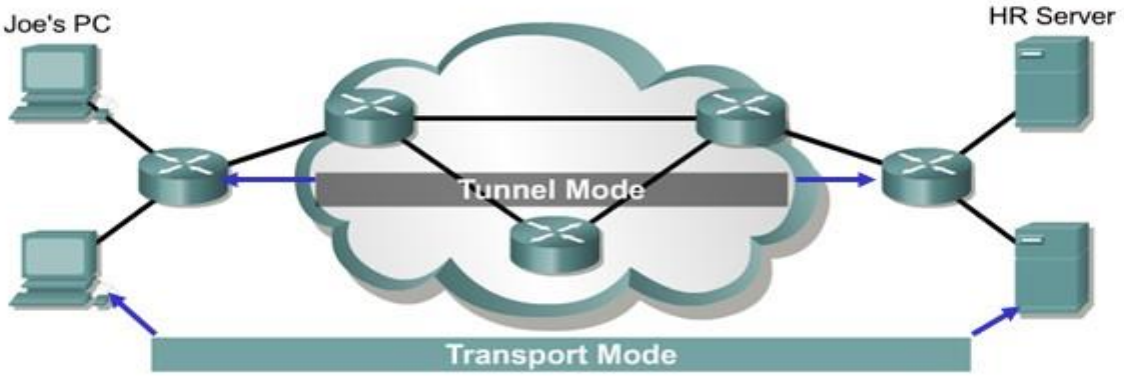
Tunnel Mode vs. Transport Mode





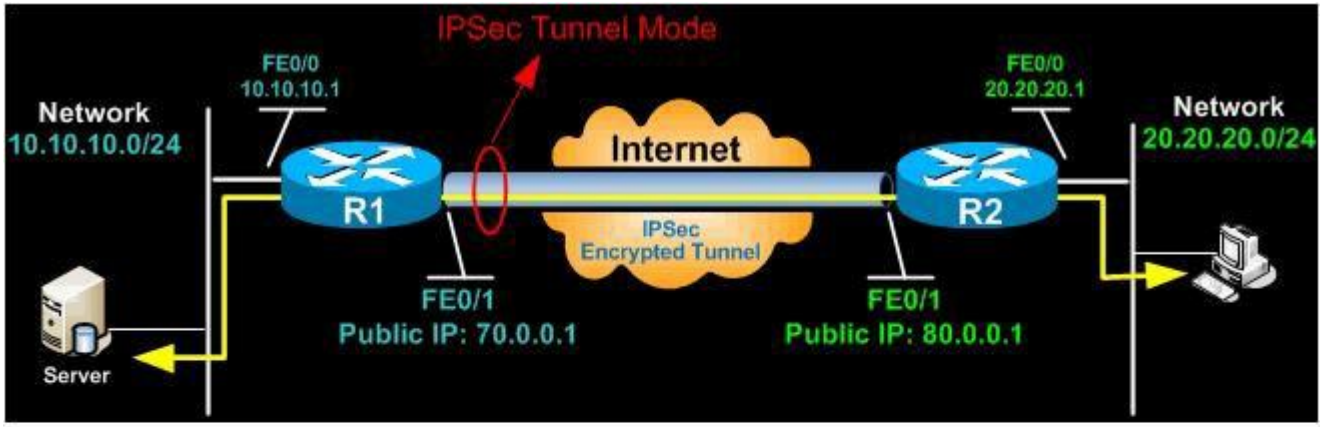
- Both AH and ESP can operate in two modes:
  - Transport Mode
  - Tunnel Mode (default)
- **Transport Mode** – The original IP packet is put through the ESP and/or AH options and then the original IP header is reused with the packet, which would be the original packet plus added information from ESP and/or AH.
- **Tunnel mode** – The original IP packet is put through the ESP and/or AH options and the a new IP header is created for the new packet, which is a combination of the original packet plus ESP and/or AH information plus a new IP header.

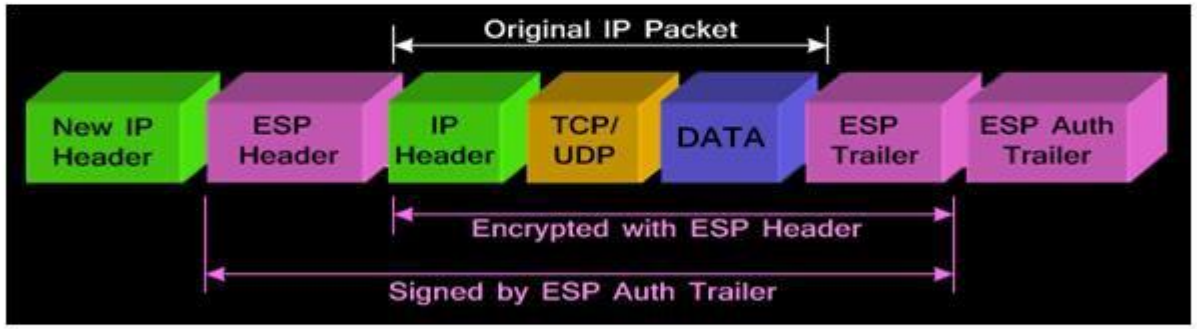
Tunnel Mode vs. Transport Mode (Cont.)

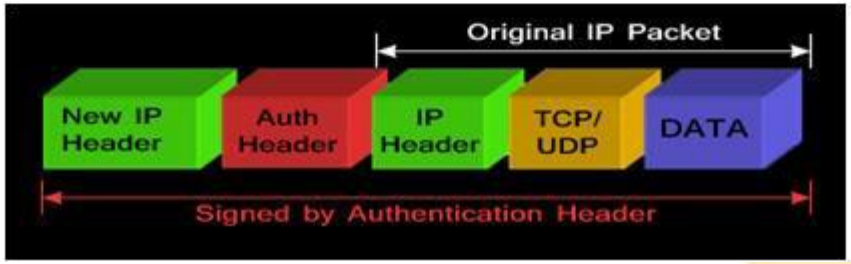


- In **transport mode end hosts do IPSec** encapsulation of their own data (host-to-host) therefore IPSec has to be implemented on each of the end-hosts.
  - The application endpoint must be also the IPSec endpoint.
  - ESP transport mode is **used between hosts.**
- In **tunnel mode IPSec gateways provide IPSec** services to other hosts in peer-to-peer tunnels, and end-hosts are not aware of IPSec being used to protect their traffic.

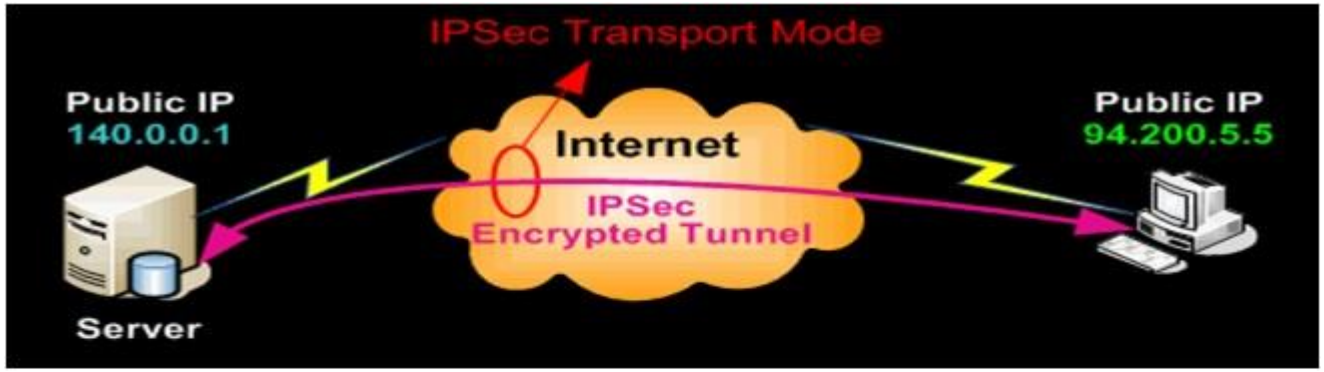
ESP and AH in IPsec Tunnel Mode

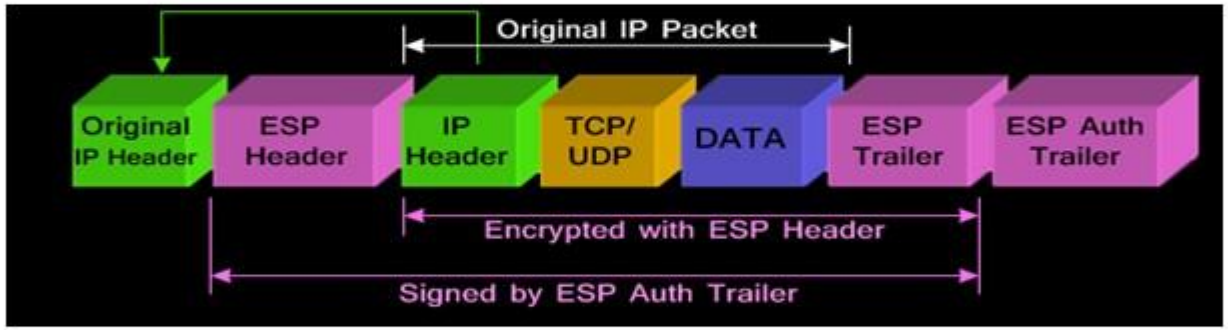


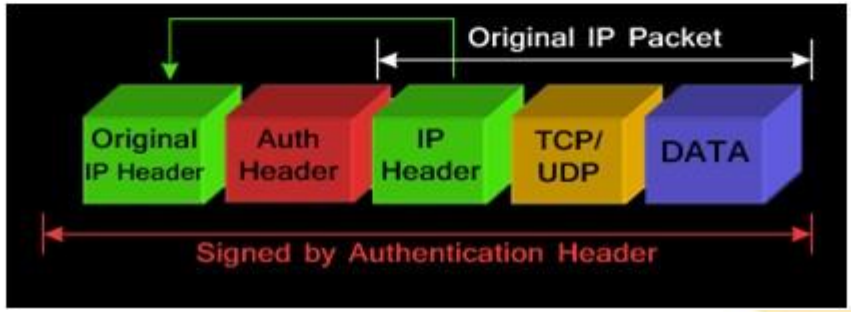




ESP and AH in IPsec Transport Mode







VPN Components

- There are four components to a VPN network.
  - The Internet
  - Security Gateways
    - Sit between public and private networks preventing unauthorized intrusion (Firewalls, routers, integrated VPN hardware and software.)
    - May provide tunneling and encrypt private data.
  - Security Policy Servers
    - Maintains Access control lists that the security gateway uses to determine which traffic is authorized. For example, some systems use a RADIUS server for these policies.
  - Certificate Authorities
    - These are used to confirm the authenticity of shared keys among sites. Companies might choose to maintain their own digital certificate server or might use an external agency of creating an extranet.