

# Security Topics

## Arquitetura e Gestão de Redes

**DETI-UA**

# IP Secure Communications (IPsec Protocol)



# IPSec

- Framework of security protocols and algorithms used to secure data at the network layer
- Authentication Header (AH)
  - ♦ Ensures data integrity
  - ♦ Does not provide confidentiality
  - ♦ Provides origin authentication
  - ♦ Uses Keyed-hash mechanisms
- Encapsulating Security Payload (ESP)
  - ♦ Provides data confidentiality (encryption)
  - ♦ Data Integrity
  - ♦ Does not protect IP header
- AH and ESP use symmetric secret key algorithms, although public key algorithms are feasible



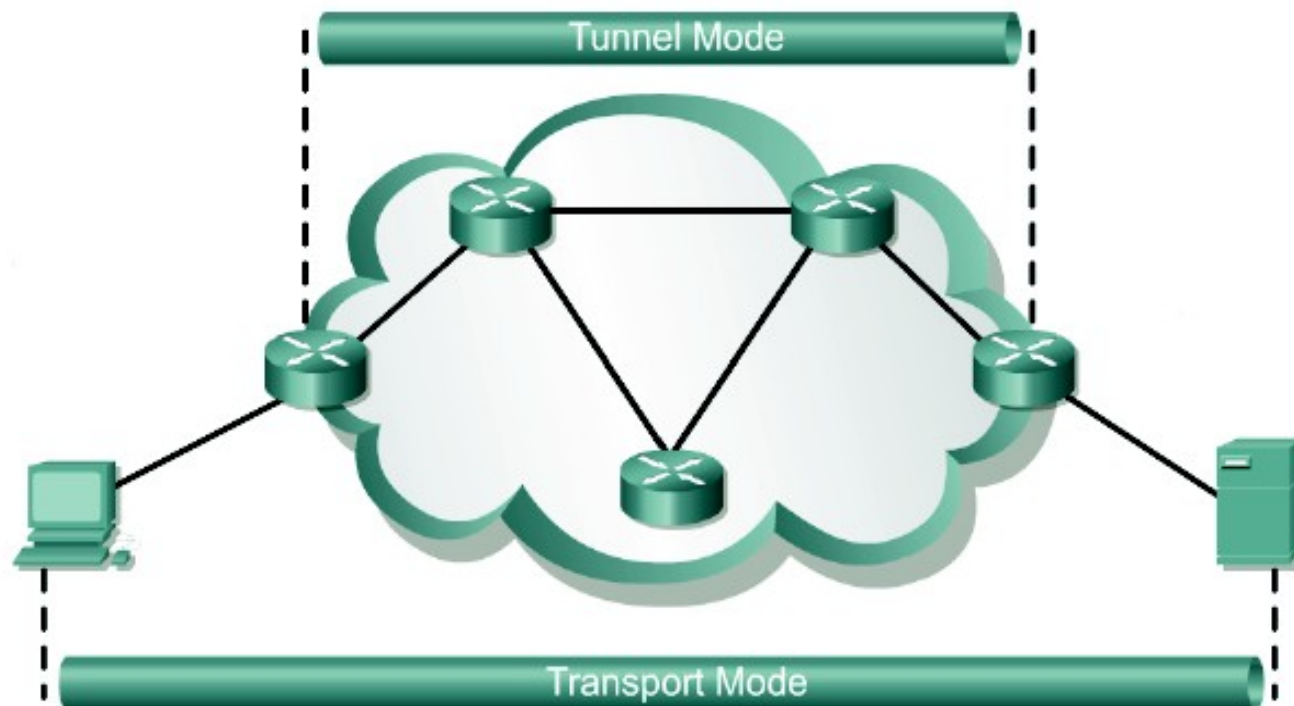
# IPSec Modes

- Tunnel

- IPSec gateways provide IPSec services to other hosts in peer-to-peer tunnels
- End-hosts are not aware of IPSec being used to protect their traffic
- IPSec gateways provide transparent protection over untrusted networks

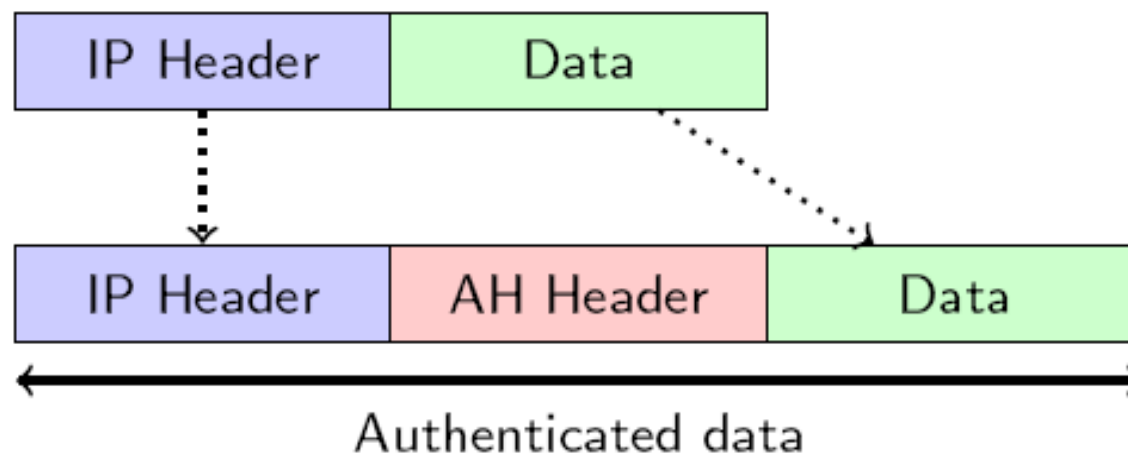
- Transport

- Each end host does IPSec encapsulation of its own data, host-to-host.
- IPSec has to be implemented on end-hosts
- The application endpoint must also be the IPSec endpoint

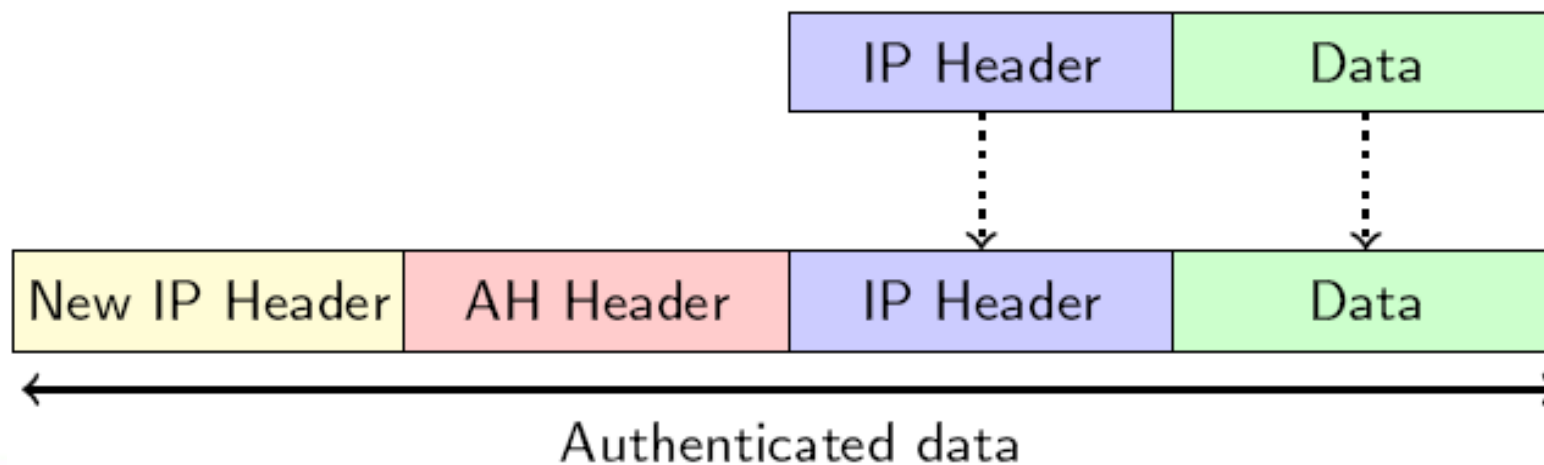


# IPSec - AH header placement

- Transport mode

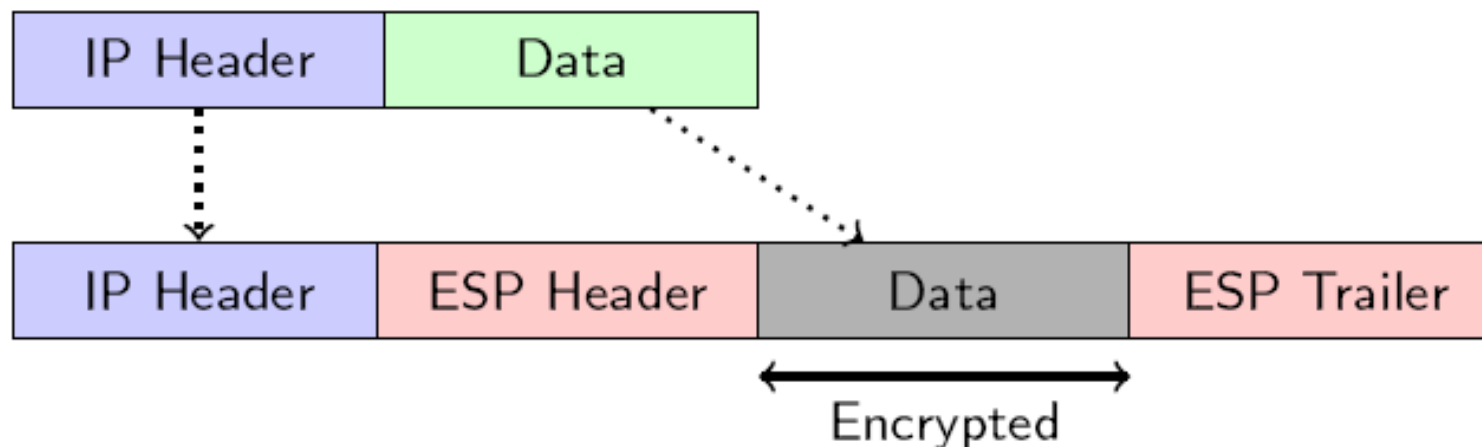


- Tunnel mode

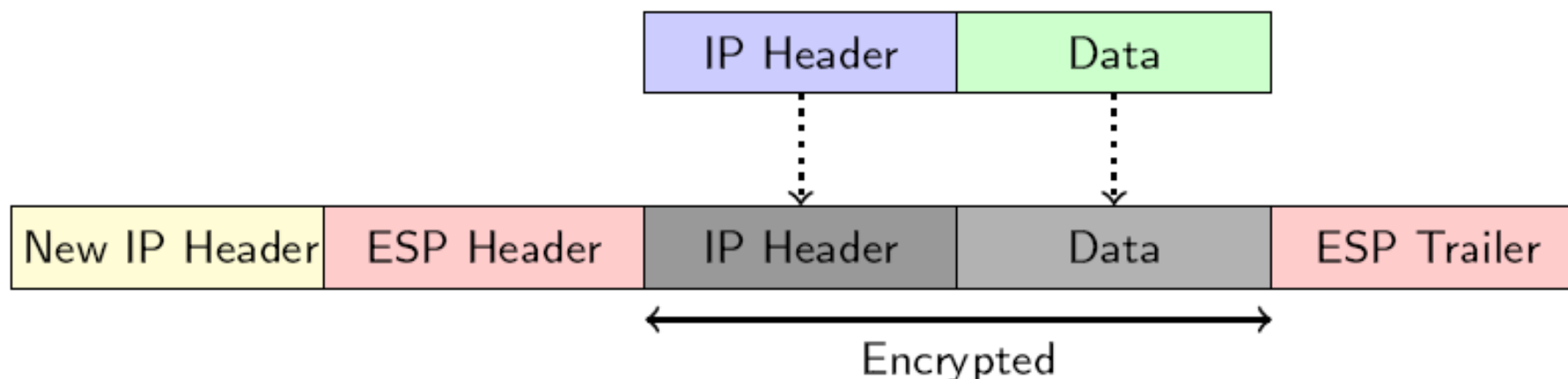


# IPSec - ESP header placement

- Transport mode



- Tunnel mode



# IPSec - Security Associations

- SAs represent a policy contract between two peers or hosts
- Describe how the peers will use IPSec security services to protect network traffic
- An SA contains the following security parameters:
  - Authentication/encryption algorithm, key length and other encryption parameters (e.g. key lifetime, ...)
  - Session keys for authentication, or HMACs, and encryption, which can be entered manually or negotiated automatically
  - A specification of network traffic to which the SA will be applied (e.g. IP traffic or only TELNET sessions)
  - IPSec AH or ESP encapsulation protocol and tunnel or transport mode





# Establishing SA and Cryptographic Keys

- ISAKMP - Internet Security Association and Key Management Protocol
  - Used to establish Security Associations (SA) and cryptographic keys
  - Separate the details of security association management (and key management) from the details of key exchange
  - Provides a framework for authentication and key exchange but does not define them
- Oakley Key Determination Protocol
  - Key-agreement protocol
  - Allows authenticated peers to exchange keying material across an insecure connection
  - Uses Diffie-Hellman
- SKEME
  - Key exchange protocol
- IKE - Internet Key Exchange
  - Is a hybrid protocol
  - Uses part of Oakley and part of SKEME in conjunction with ISAKMP



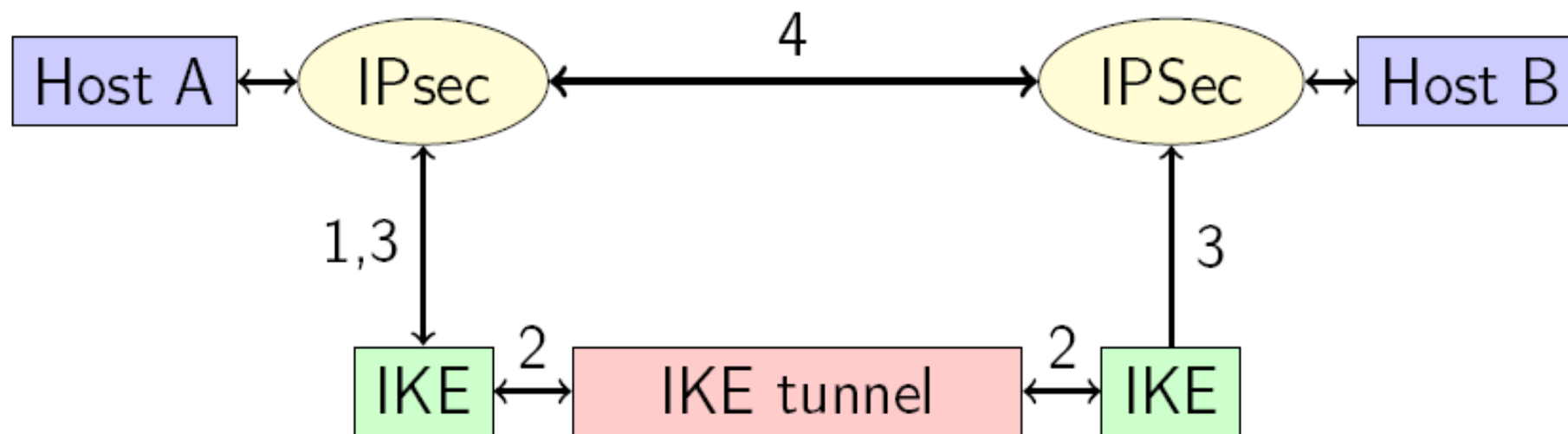


# IKE and IPsec

- Enhances IPsec by providing additional features and flexibility
- Provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations
- The IKE tunnel protects the SA negotiations. After the SAs are in place, IPsec protects data transference
- Advantages
  - Eliminates the need to manually specify IPsec security parameters at both peers
  - Allows administrators to specify a lifetime for the IPsec security association
  - Allows encryption keys to change during IPsec sessions
  - Allows IPsec to provide anti-replay services
  - Permits certification authority (CA) support for a manageable, scalable IPsec implementation
  - Allows dynamic authentication of peers
- IKE provides three methods for two-way authentication:
  - Authentication using a pre-shared secret (PSK)
  - Authentication using RSA encrypted nonces
  - Authentication using RSA signatures



# IKE and IPsec



# IKE and IPsec – Modes

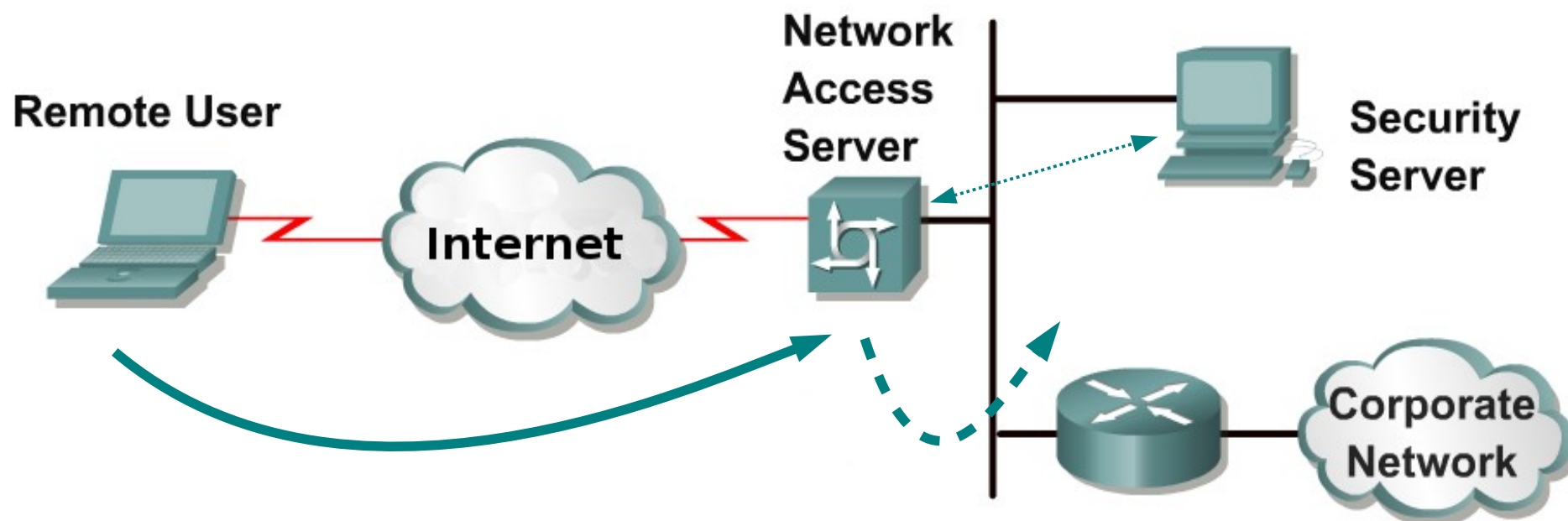
- IKE modes control an efficiency versus security tradeoff during initial IKE key exchange
- Main mode
  - ◆ Requires six packets back and forth
  - ◆ Provides complete security during the establishment of an IPsec connection
- Aggressive mode
  - ◆ Uses half the exchanges
  - ◆ Provides less security because some information is transmitted in cleartext



# Authentication Protocols



# Remote authentication



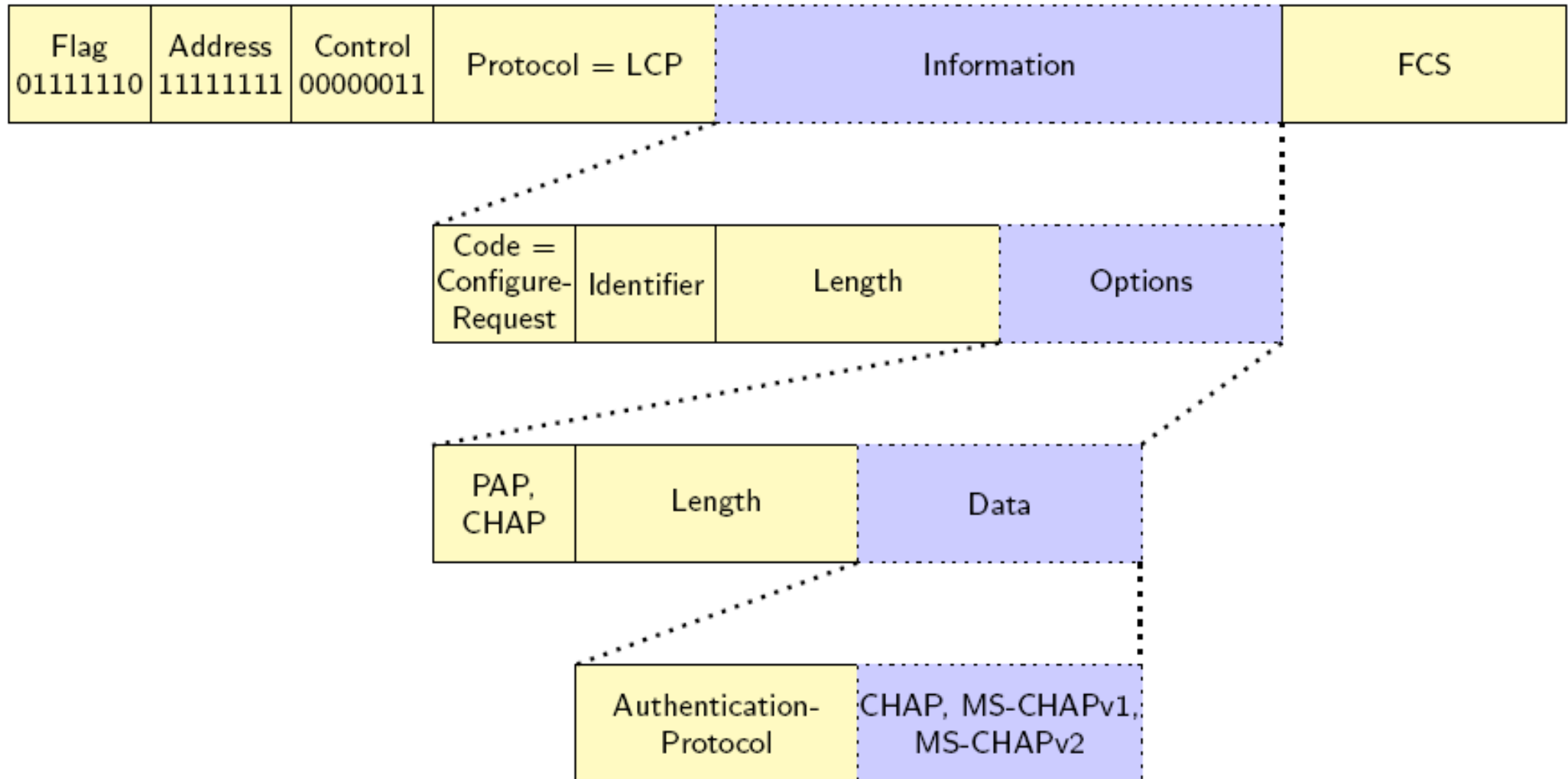
- Authentication is the security process that validates the claimed identity of an entity
  - ♦ Relying on one or more characteristics specific to that entity
- The authentication process involves at least two entities:
  - ♦ The one to be authenticated
  - ♦ The one requiring authentication (Network access server)

# PPP - Point to Point Protocol

- The Point-to-Point Protocol (PPP) emerged as an encapsulation protocol for transporting IP traffic over point-to-point links
- Defines a virtual point-to-point connection
- In conjunction with the Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) supports
  - ♦ Link configuration, quality testing and error detection
  - ♦ Assignment and management of IP addresses
  - ♦ Network layer address negotiation
  - ♦ Network protocol multiplexing
  - ♦ Data-compression negotiation
  - ♦ Authentication configuration
- PPP Frame

Flag 01111110	Address 11111111	Control 00000011	Protocol	Information	FCS
------------------	---------------------	---------------------	----------	-------------	-----

# PPP - Authentication Configuration



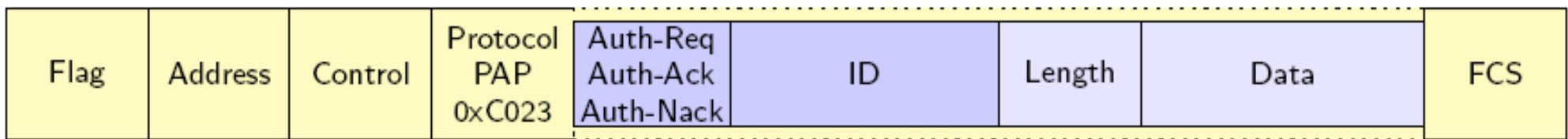
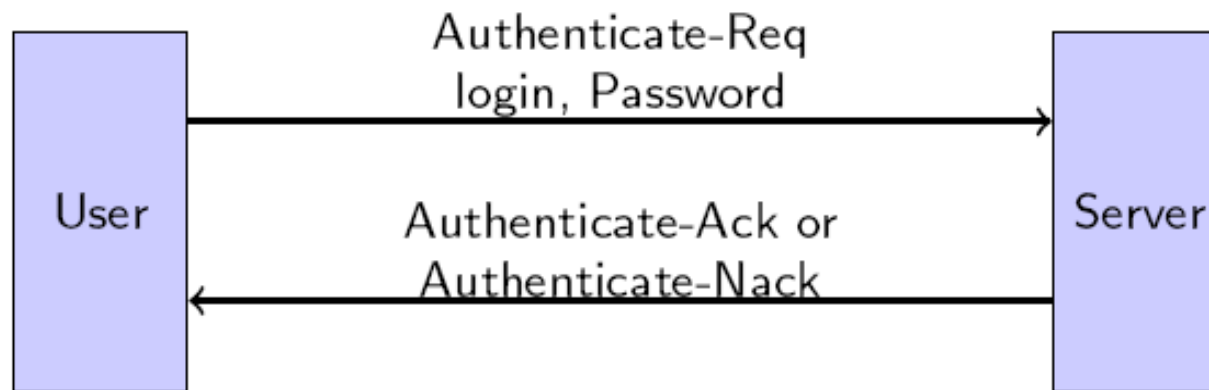
- Confirmation is made using a response with the code "Configure-Ack"





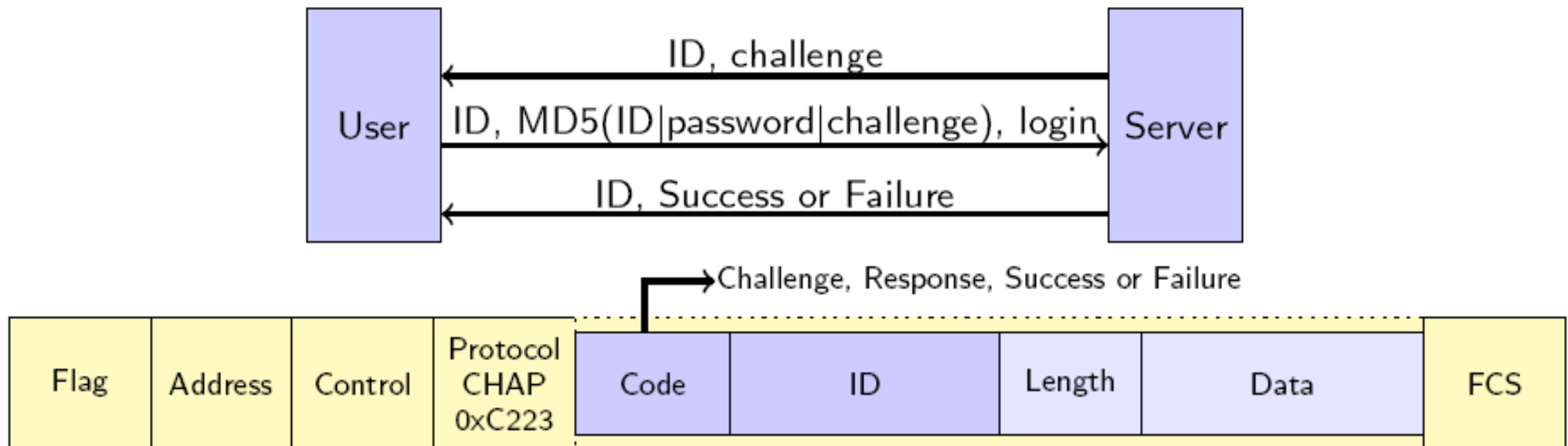
# PAP - Password Authentication Protocol

- Is a Link Control Protocol in the PPP suite
- Provides a basic method for peer authentication using a 2-way handshake
- PAP is not a strong authentication method passwords are transmitted "in the clear"
- After the link establishment phase is complete, the login and password are sent repeatedly by the peer to the authenticator until authentication is acknowledged or the connection is terminated



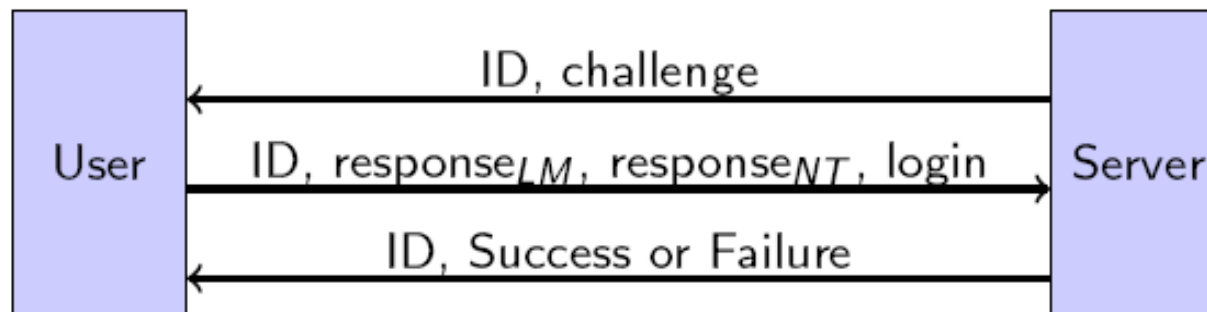
# CHAP – Challenge-Handshake Authentication Protocol

- Used to periodically verify the identity of a peer using a 3-way handshake
- After the Link Establishment phase is complete
  - The server sends a "challenge" message to the peer
  - The peer responds with an hash value (MD5)
  - The server checks the response against its own calculation of the expected hash value
- At random intervals, the server sends a new challenge to the peer



# MS-CHAP version 1

- Microsoft version of the CHAP
- Differences from CHAP
  - Designed for compatibility with Microsoft's Windows NT 3.5, 3.51 and 4.0, and
  - Microsoft networking products (e.g LAN Manager)
  - Provides a password change mechanism
  - Provides an authentication retry mechanism
  - Defines a set of failure codes returned in the Failure packet Message field



- $\text{response}_{LM} = \text{DESkey}_{LM}(\text{challenge})$ ,  $\text{key}_{LM} = \text{DES}_{\text{hash}}(\text{password})$
- $\text{response}_{NT} = \text{DESkey}_{NT}(\text{challenge})$ ,  $\text{key}_{NT} = \text{MD4}(\text{password})$



# MS-CHAP version 1 - Issues

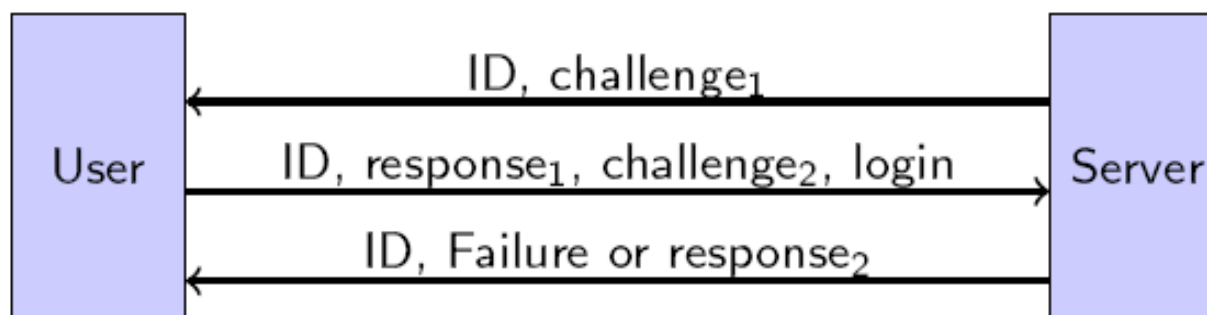
- LAN Manager encoding of the response used for backward compatibility is cryptographically weak
- Only one-way authentication is possible
- The key is based on the password. Each time the user connects with the same password, the same cryptographic key is generated



# MS-CHAP version 2

- Differences from MS-CHAPv1

- MS-CHAPv2 no longer allows LAN Manager encoded responses or password changes
- Provides two-way authentication (mutual authentication)



$response_1 = DES_{key_{NT}} (SHA-1(challenge_2|challenge_1|login))$

$key_{NT} = MD4(password)$

$response_2 = SHA-1 (SHA-1(H|response_1|M_1)|D|M_2)$

$H = MD4(key_{NT})$

$D = SHA-1(challenge_2|challenge_1|login)$

$M_1$  and  $M_2$  are constants

# TLS - Transport Layer Security Protocol

- Standardization of the SSL protocol proposed by Netscape
  - ♦ Added HMAC
- Provide privacy and data integrity between two communicating applications
- The protocol is composed of two layers
  - ♦ TLS Handshake Protocol
  - ♦ TLS Record Protocol
- TLS Handshake Protocol
  - ♦ Allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys
- TLS Record Protocol properties
  - ♦ The connection is private
  - ♦ The connection is reliable



# EAP - Extensible Authentication Protocol

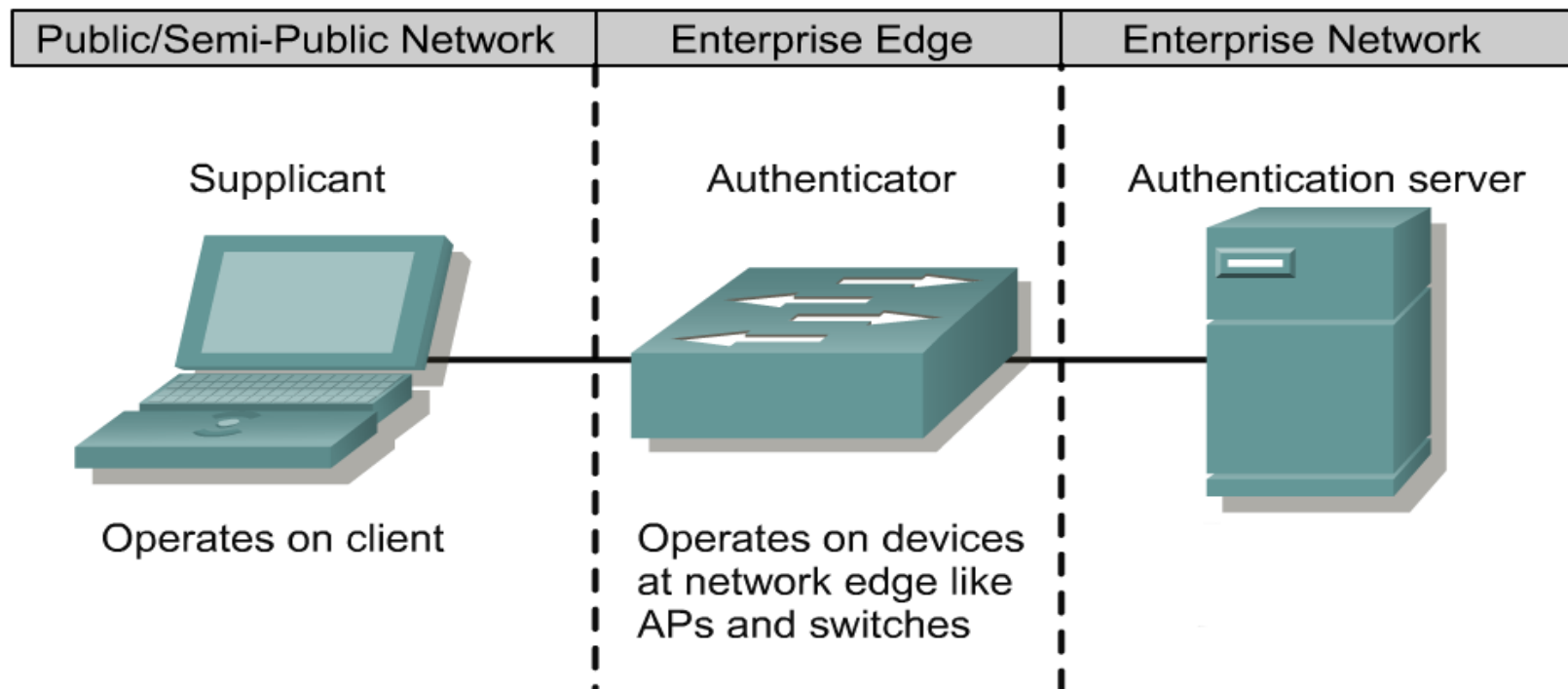
- Was designed to supplement PPP
- Provides a generalized framework for several different authentication methods
- More common methods:
  - EAP-PSK - Mutual authentication and session key derivation using a Pre-Shared Key (PSK)
  - EAP-TLS - Uses PKI to secure communication to authentication server
  - PEAP - Protected EAP (PEAP) allows hybrid authentication. PEAP employs server-side PKI authentication. For client-side authentication, PEAP can use any other EAP authentication type.
  - EAP-TTLS - Client does not need be authenticated via a PKI certificate to the server, but only the server to the client
  - LEAP - Cisco's proprietary EAP method. Uses a modified version of MS-CHAP
- EAP over LAN (EAPoL) used in 802.1x



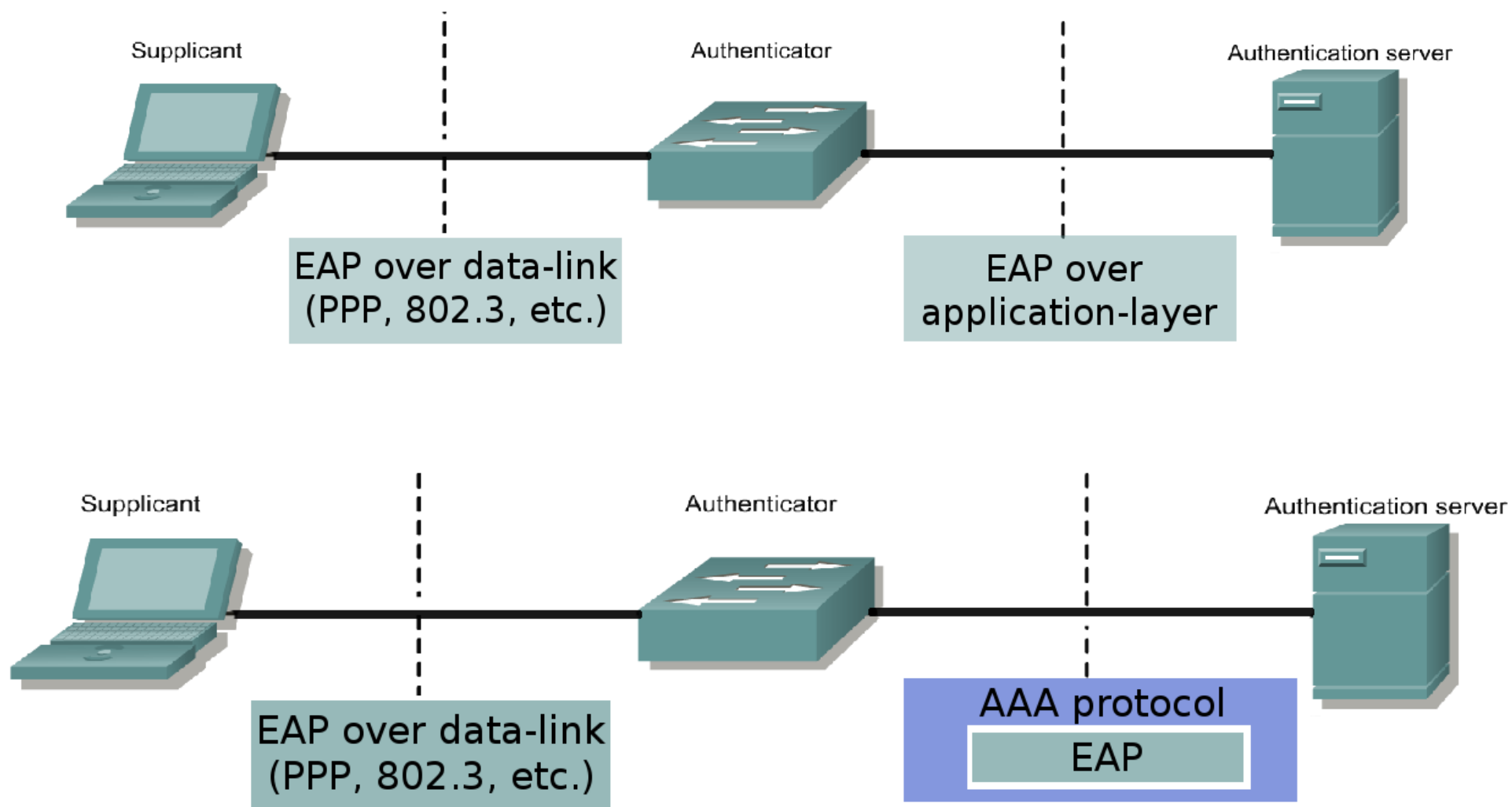


# 802.1x

- IEEE 802.1X is an IEEE Standard for Network Access Control (NAC)
- It provides an authentication mechanism to devices wishing to attach to a LAN
- It's based on the Extensible Authentication Protocol (EAP)



# 802.1x

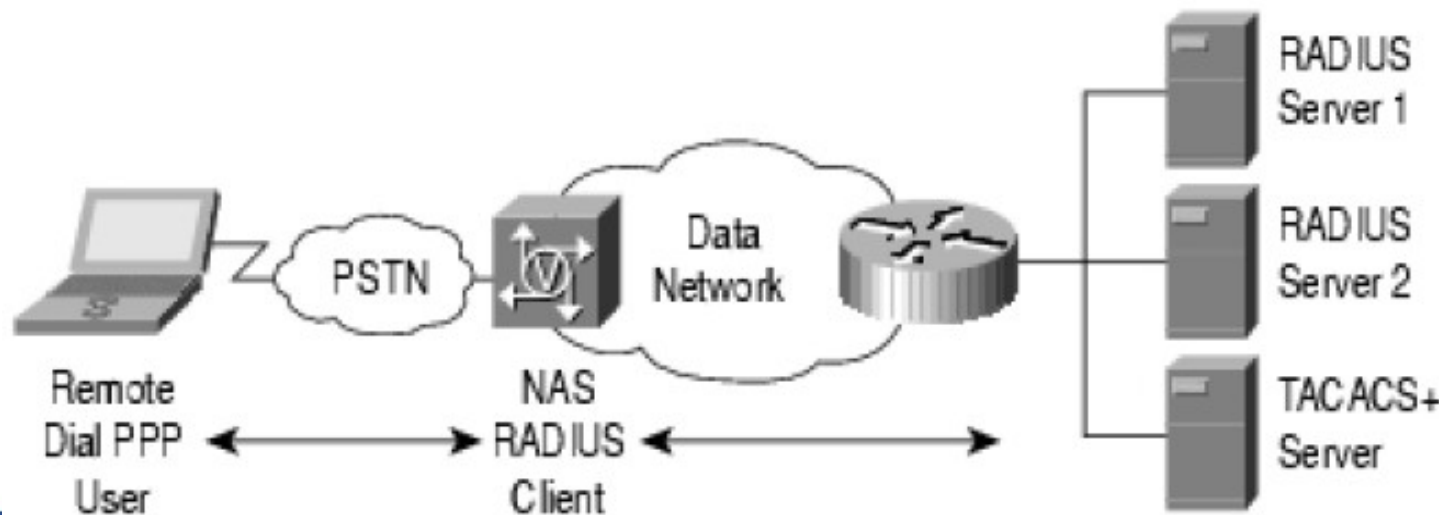


# Authentication, Authorization and Accounting



# AAA Architecture

- Enables systematic access security
  - ♦ Authentication identifies a user
  - ♦ Authorization determines what that user can do
  - ♦ Accounting monitors the network usage time for billing purposes
- Work with the network access server (NAS)
- AAA information is typically stored in an external database or remote server
- Traditional AAA Implementation



# TACACS+

- Terminal Access Controller Access Control System Plus
- Forwards username and password information to a centralized security server
- Centralized server can be either a TACACS database or a database like the UNIX password file with TACACS support
- Features
  - Separates all AAA functionalities
  - Uses TCP
  - Bidirectional authentication
  - All packet is encrypted
  - Limited accounting customization

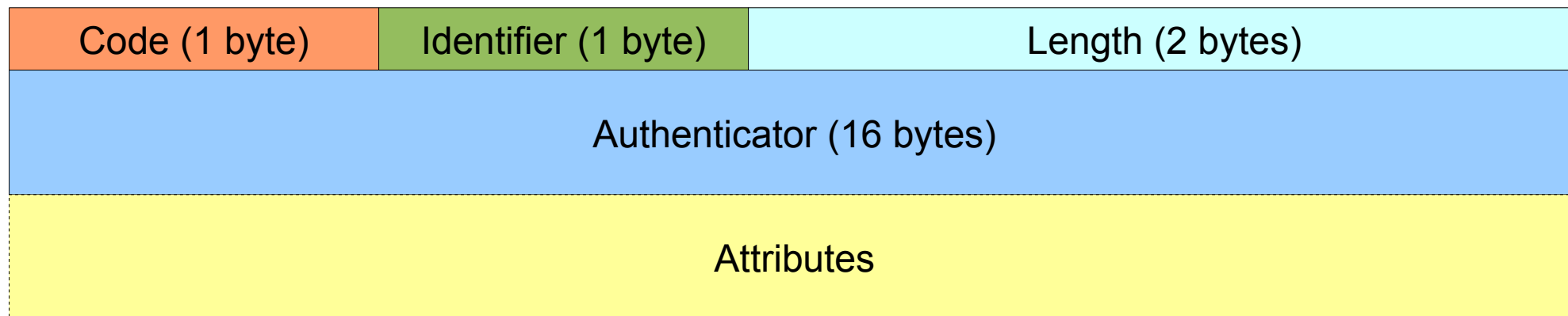


# RADIUS

- Remote Authentication Dial-In User Service
- Network access server (NAS) operates as a client of RADIUS
- RADIUS servers are responsible for
  - ◆ Receiving user connection requests
  - ◆ Authenticating the user
  - ◆ Return all configuration information necessary for the client to deliver service to the user
- Transactions between the client and RADIUS server are authenticated using a shared secret
- Supports a variety of methods to authenticate a user
  - ◆ PAP, CHAP, or MS-CHAP, UNIX login, and other authentication mechanisms
- Combines Authentication and Authorization. Separates Accounting (less flexible than TACACS+)
- Uses UDP (less robust)
- Unidirectional authentication
- Only encrypts the password (less secure)
- RADIUS accounting can hold more information



# RADIUS Packet



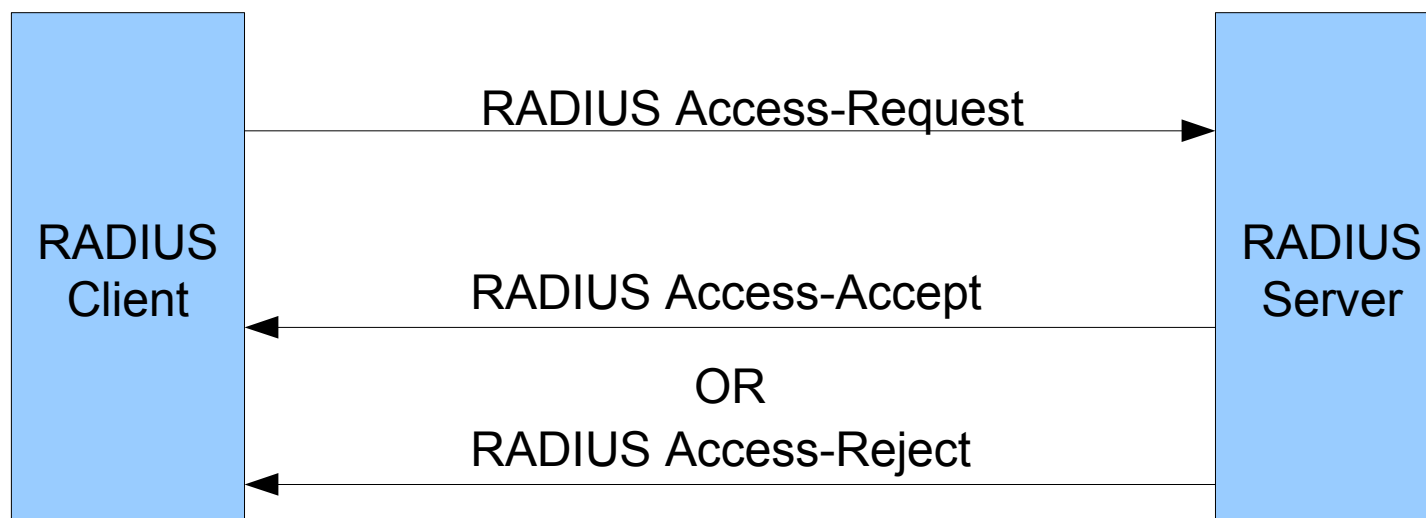
- Code - Identifies the type of RADIUS packet
  - (1) Access-Request, (2) Access-Accept, (3) Access-Reject, (4) Accounting-Request, (5) Accounting-Response and (11) Access-Challenge
- Identifier - Allows the RADIUS client to match a RADIUS response with the correct pending request (usually is implemented as a counter)
- Authenticator
  - In client Requests – Random value
  - In server Responses - MD5 Hash function of (Code,ID,Length,Request Auth,Attributes,Shared Secret)
- Attributes - Section where an arbitrary number of attribute fields can be sent (e.g. User-Name and User-Password attributes)





# RADIUS Protocol (1)

**Example - RADIUS exchange involving just a username and user password:**



- Only password is encrypted
  - The shared secret followed by the Request Authenticator is put through an MD5 hash to create a 16 octet value which is XORed with the password entered by the user
  - If the user password is greater than 16 octets, the password is broken into 16-octet blocks and additional MD5 calculations are performed

# RADIUS Protocol (2)

- The RADIUS protocol has a set of vulnerabilities
  - The Access-Request packet is not authenticated at all.
  - Many client implementations do not create Request Authenticators that are sufficiently random.
  - Many administrators choose RADIUS shared secrets with insufficient information entropy and many implementations limit the shared secret key space.



# DIAMETER

- DIAMETER is a newest framework in IETF for the next-generation AAA server
- Provides an AAA framework for Mobile-IP
- Does not use the same RADIUS protocol data unit, but is backward compatible with RADIUS to ease migration
- Bidirectional authentication
- It uses UDP but has a scheme that regulates the flow of packets
- Challenge/response attributes can be secured using end-to-end encryption and authentication
- Supports end-to-end security

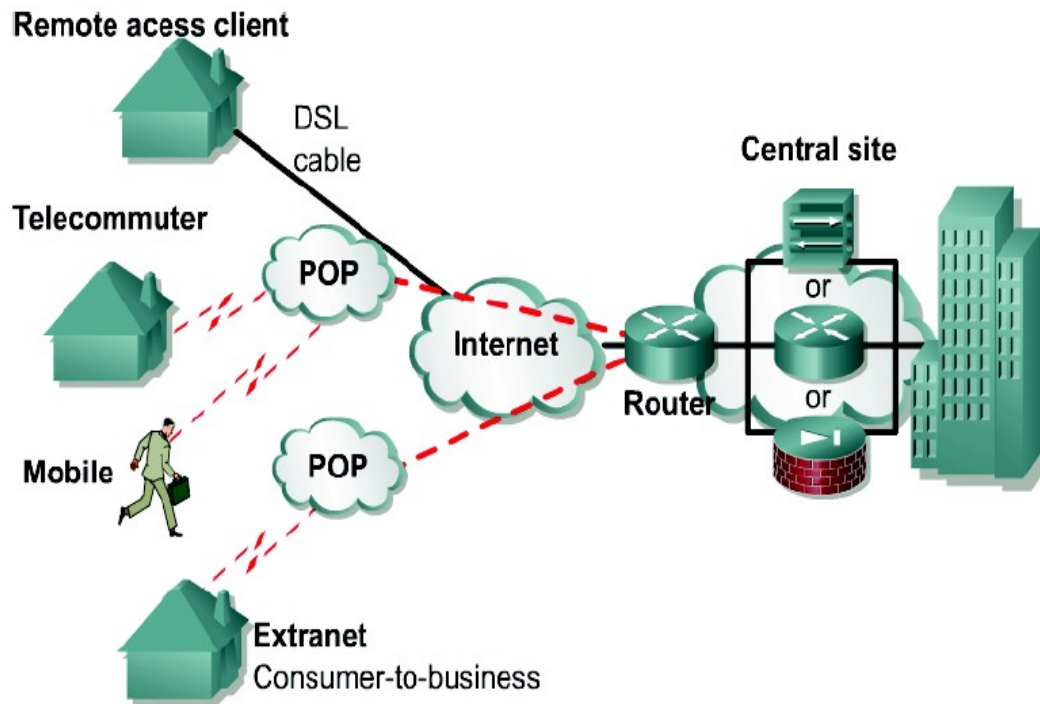


# Virtual Private Networks (VPN)

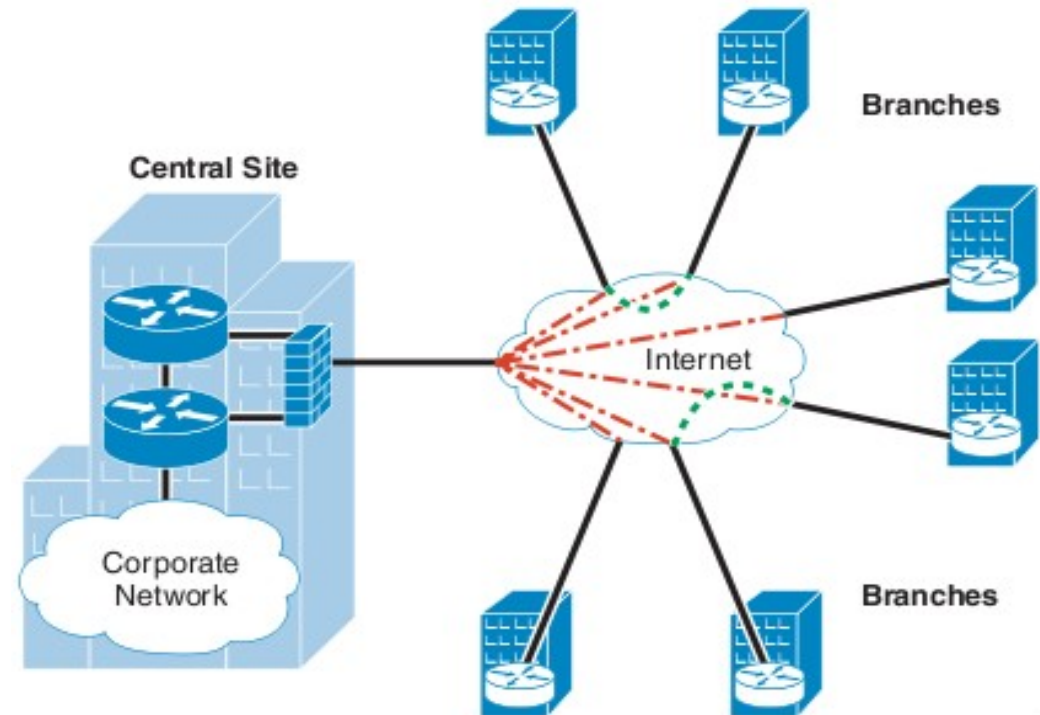


# VPN - Virtual Private Networks

- Is an encrypted connection between private networks over a public network



- Remote Access VPN



- Site-to-Site VPN

# VPN types

- Remote Access VPN

- ♦ PPTP
- ♦ L2TP/IPsec
- ♦ SSL/TLS VPN
  - ➔ Web VPN (client-less SSL VPN) – VPN client can be a standard browser
- ♦ SSH VPN
- ♦ Open VPN

- Site-to-Site VPN

- ♦ IPsec VPN
  - ➔ With static or dynamic configuration
- ♦ IPsec + GRE VPN
  - ➔ Dynamic Multipoint VPN



# Remote Access VPN - PPTP VPN

- Based on PPTP
  - ♦ PPTP packages data within PPP packets
  - ♦ Encapsulates the PPP packets within IP packets
- Uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination
- Supports authentication based on protocols PAP, EAP, CHAP, MS-CHAPv1 and MS-CHAPv2
- Uses MPPE as cipher
  - ♦ Has two different keys (one for each direction)
  - ♦ Requires MS-CHAPv2 authentication
  - ♦ Keys derived from the MS-CHAPv2's password hash and challenges
- PPTP creates a TCP control connection between the VPN client and VPN server to establish a tunnel
  - ♦ Uses TCP port 1723 for these connections
- PPTP can support only one tunnel at a time for each user





# Remote Access VPN - L2TP/IPSec VPN

- Authentication can be performed with Digital Certificates (RSA) or with the same PPP authentication mechanisms as PPTP
- Provides data integrity, authentication of origin and replay protection
- Encryption provided by IPSec (ESP protocol)
- Can support multiple, simultaneous tunnels for each user
- Slower performance than PPTP



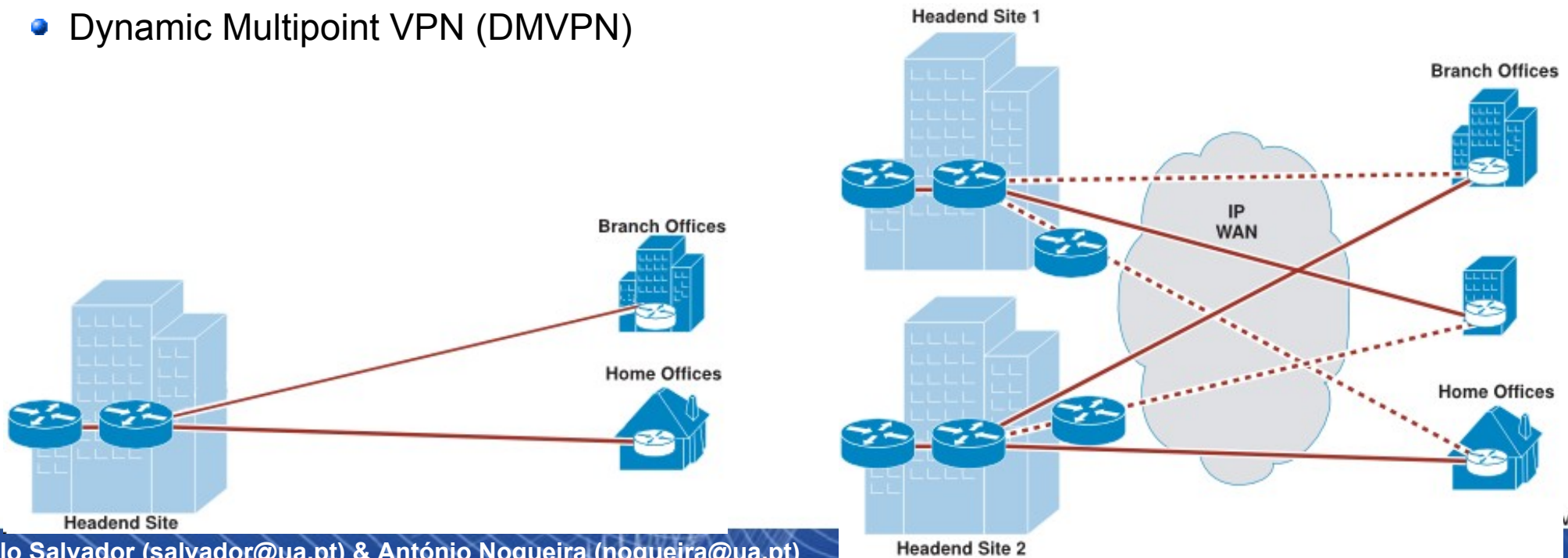
# Other Remote Access VPN types

- SSL/TLS VPN
  - ♦ SSL/TLS protocol handles the VPN tunnel creation
  - ♦ SSL/TLS is much easier to implement than IPSec and provides a simple and well-tested platform
  - ♦ RSA handshake (or DH) is used exactly as IKE in IPSec
- SSH VPN
  - ♦ VPN over a SSH connection
  - ♦ SSH tunneling - port forwarding
- OpenVPN
  - ♦ Implements a SSL/TLS VPN
  - ♦ Allows PSK, certificate, and login/password based authentication
  - ♦ Encryption provided by OpenSSL (can use all ciphers available)
  - ♦ Compatible with dynamic and NAT addresses



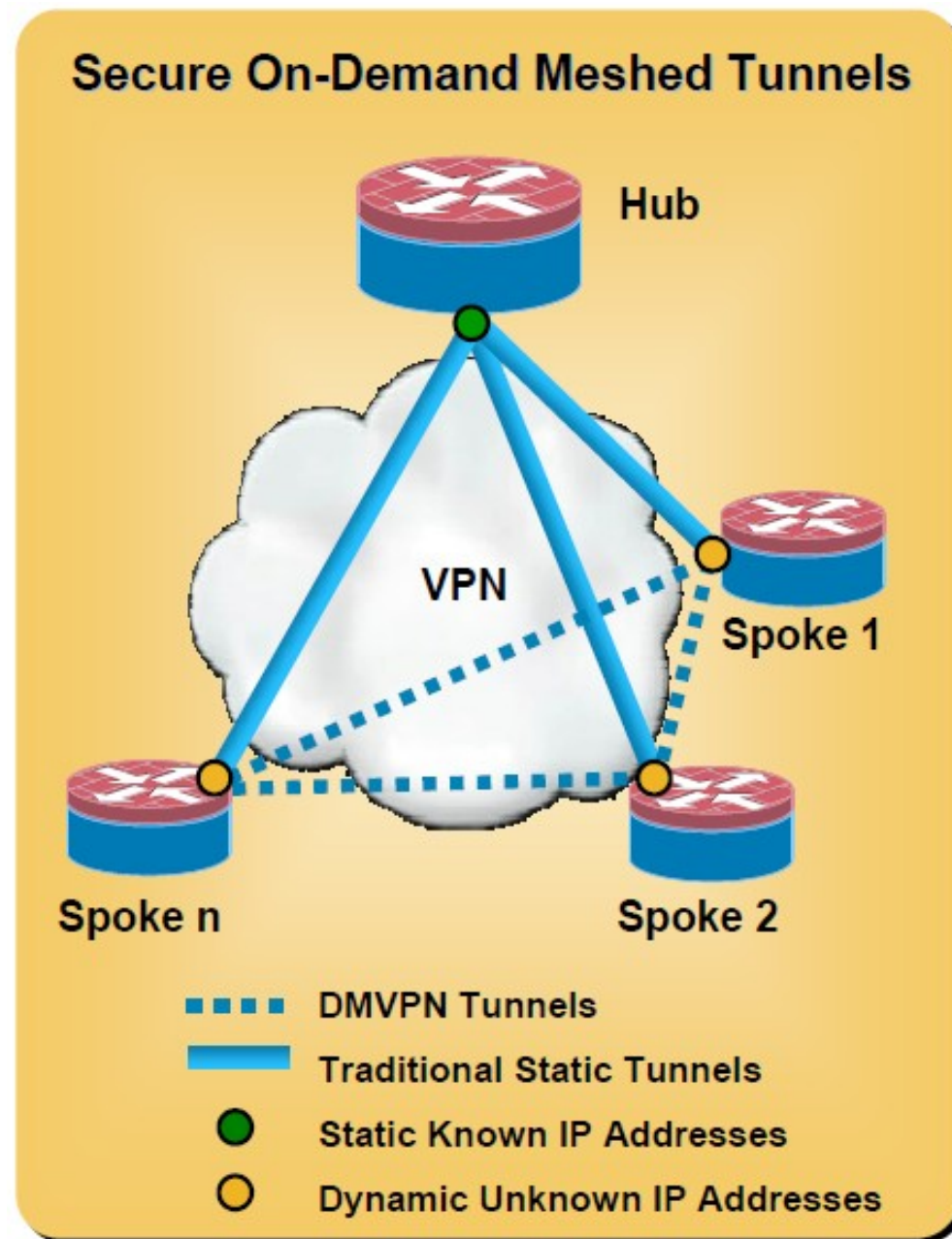
# Variants of Site-to-Site IPsec VPN

- IPsec tunnels with static configuration
  - ◆ Requires the knowledge of all peers (IP addresses and security parameters)
  - ◆ High configuration overhead
- IPsec tunnels with dynamic configuration (at the headend/hub)
  - ◆ Hub + spokes configuration
  - ◆ Generic configuration at the headend/hub
  - ◆ Easy to add new spokes
- A basic IPsec tunnel can't protect multicast traffic.
- IPsec + GRE tunnels
  - ◆ Generic Routing Encapsulation (GRE) allows the protection of multicast traffic over IPsec
- Dynamic Multipoint VPN (DMVPN)



# Dynamic Multipoint VPN

- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel



# Network Security Systems



# Network Security Systems

- Firewall
- Intrusion Prevention System (IPS)
  - ◆ Performs deep-packet inspection
- Intrusion Detection Systems (IDS)
  - ◆ Performs deep-packet inspection
- Security Appliance
  - ◆ Unified communications security
  - ◆ Firewall services
  - ◆ Real-time threat defense
  - ◆ Secure remote access
  - ◆ Secure communications services
  - ◆ Content security





# Firewalls

- A firewall provides a single point of defence between networks and protects one network from the others-
- It is a system or group of systems that enforces a control policy between two or more networks (access control, flow control and content control).
- It is a network gateway that enforces the rules of network security.
- Minimizes local vulnerabilities.
- Evaluates each network packet against the policies of network security.
- Can monitor all the network traffic and alert to any attempts to bypass security or to any patterns of inappropriate use.
- Can be hardware or software based.



# Firewalls Security/Network Services

- NAT (Network Address Translation).
- Authorization
  - ♦ Flows (packet filtering).
  - ♦ Users (application and circuit level).
- Redirecting.
  - ♦ To specif machines.
  - ♦ Proxing.
- Content analysis.
- Secure communication.
  - ♦ Site-to-site VPN.
    - IPsec.
  - ♦ Remote-access VPN.
- DoS and DDoS detection and defense.





# Types of Firewalls

- Network-Level Firewalls (L2/L3)

- Packet filtering
- Inspecting packet headers and filtering traffic based on
  - the IP address of the source and the destination, the port and the service (L3)
  - source and the destination MAC addresses (L2)

- Circuit-Level Firewalls (L4)

- Monitor TCP handshaking between packets to make sure a session is legitimate
- Traffic is filtered based on specified session rules

- Application-Level Firewalls (L4+)

- Application-level firewalls are sometimes called proxies
- Looking more deeply into the application data
- Consider the context of client requests and application responses
- Attempt to enforce correct application behavior and block malicious activity
- Application-level filtering may include protection against Spam and viruses as well, and block undesirable Web sites based on content rather than just their IP address
- Slow and resources consuming tasks

- Stateful Multi-level Firewalls (L\*)

- Filter packets at the network level and they recognize and process application-level data
- Since they don't employ proxies, they have reasonably good performance even performing deep packet analysis

- Host Level / Personal Firewalls

- Act only within a specif host
- Filter all communication layers
- Control OS processes/applications



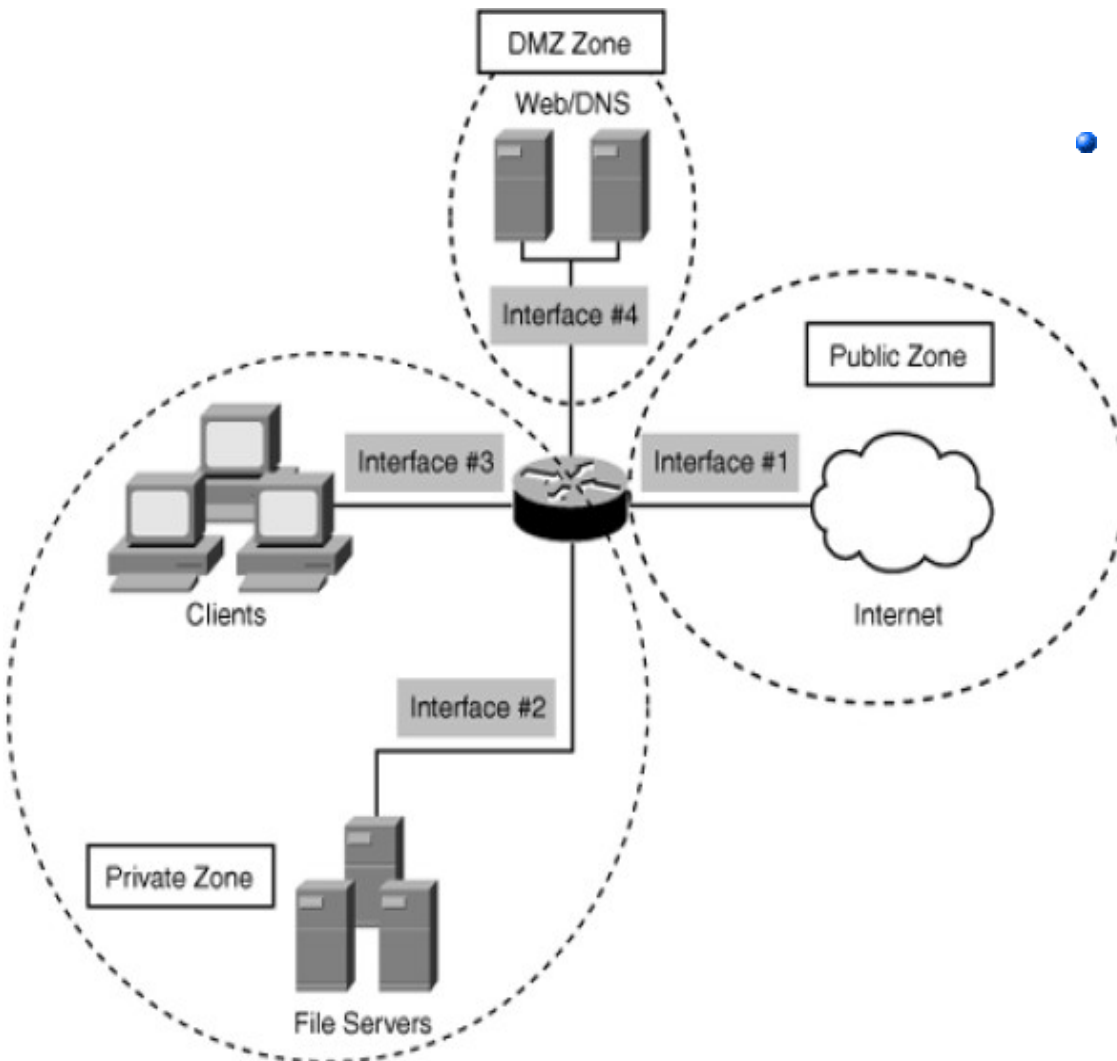
# Firewall Technologies (1)

- **Packet filtering systems** - Route packets between internal and external hosts, but do it selectively. The type of router used in a packet filtering firewall is known as a screening router.
- **Problems:**
  - ♦ Undesirable packets can be fitted to a packet rule criteria and, therefore, pass through the filter.
  - ♦ Packets can pass through the filter by being fragmented.
  - ♦ Complex rule sets are difficult to implement and maintain correctly.



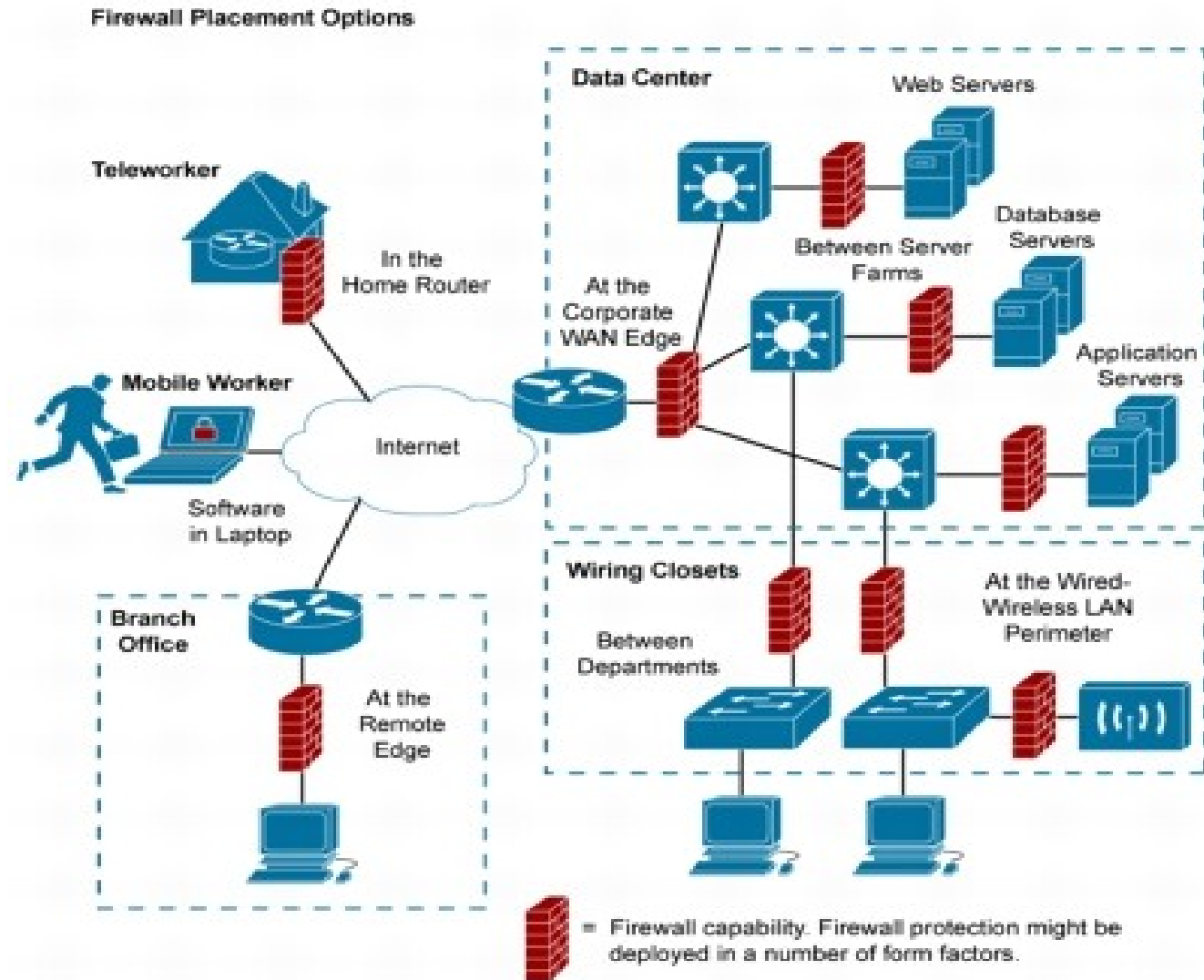
# Secure Zones - Overview

- A network can be divided in multiple secure zones with different security levels.
- A Demilitarized Zone (DMZ) is a perimeter network outside the protected internal/private network
  - ◆ Used to place public servers/services.
  - ◆ The DMZ is a "semi-protected" Zone.
    - ➔ It must be assumed that any machine placed on the DMZ is at risk.

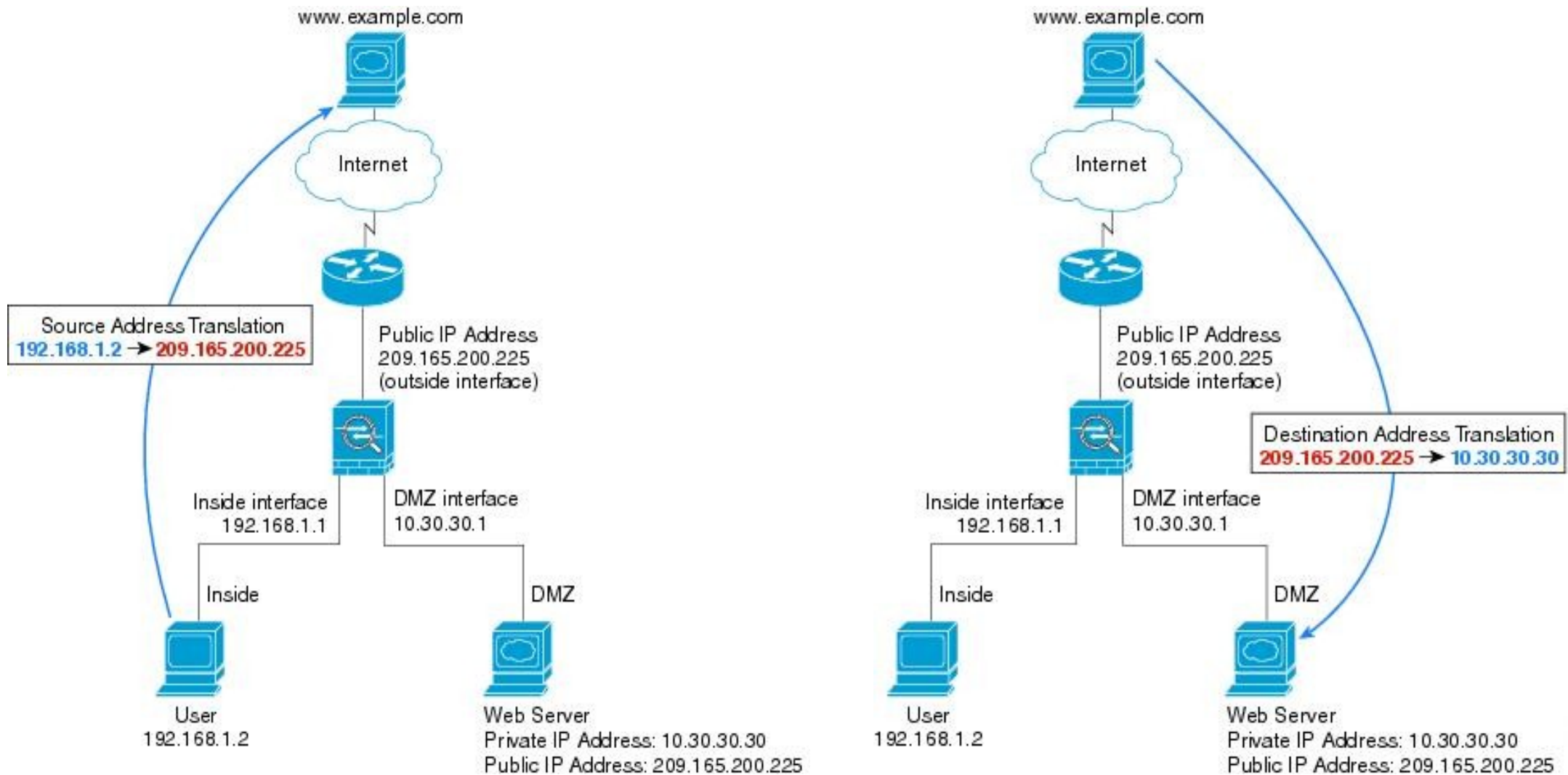


# Deploying Firewalls

- Network must be protected at multiple levels and locations



# Example DMZ Network Topology



# Multiple Security Contexts (1)

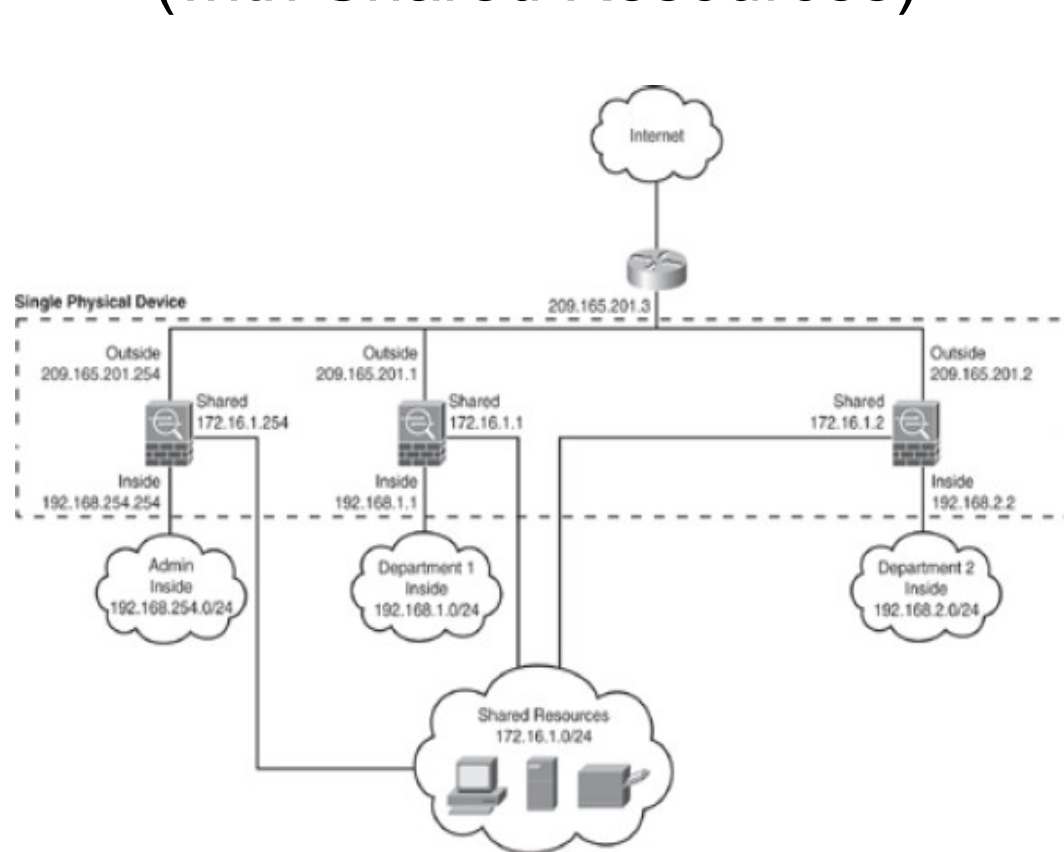
- Multiple security contexts can exist in these situations:
  - An ISP want to sell security services to many customers.
    - With multiple security contexts it is possible to an implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.
  - A large enterprise or a college campus want to keep departments completely separate.
  - An enterprise that wants to provide distinct security policies to different departments.
  - A network that requires more than one security appliance/firewall.



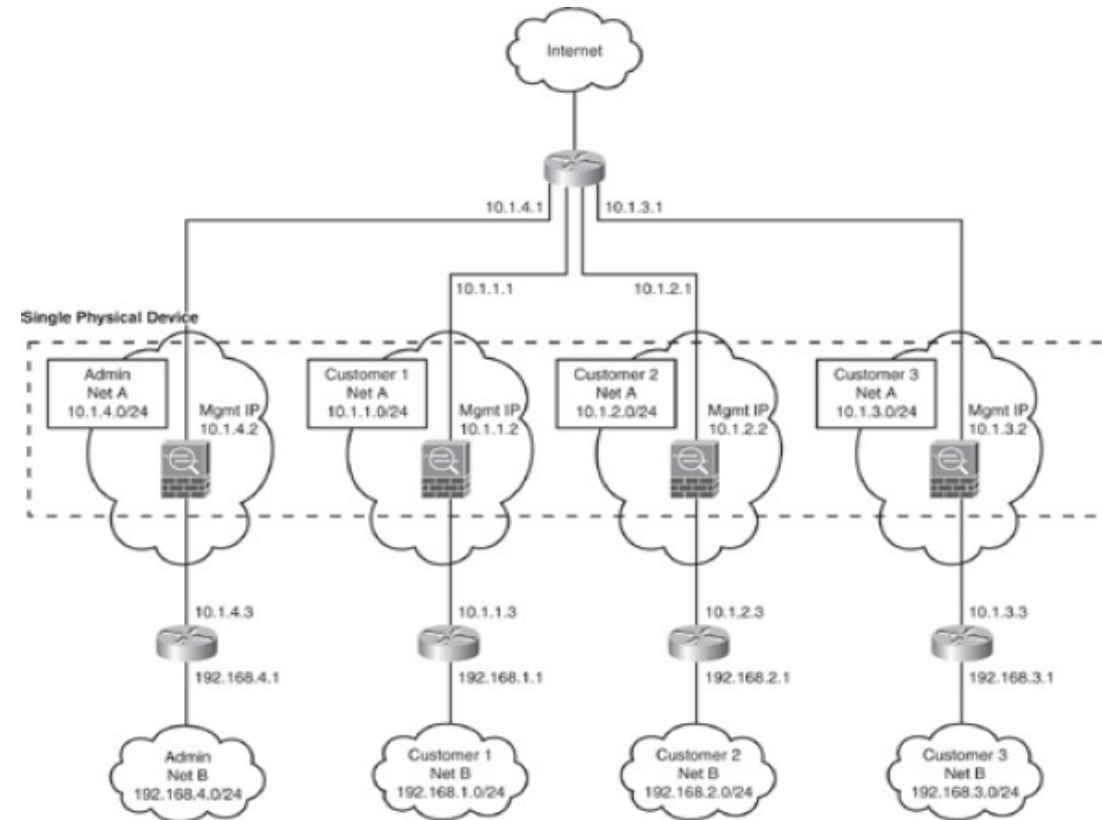


# Multiple Security Contexts (2)

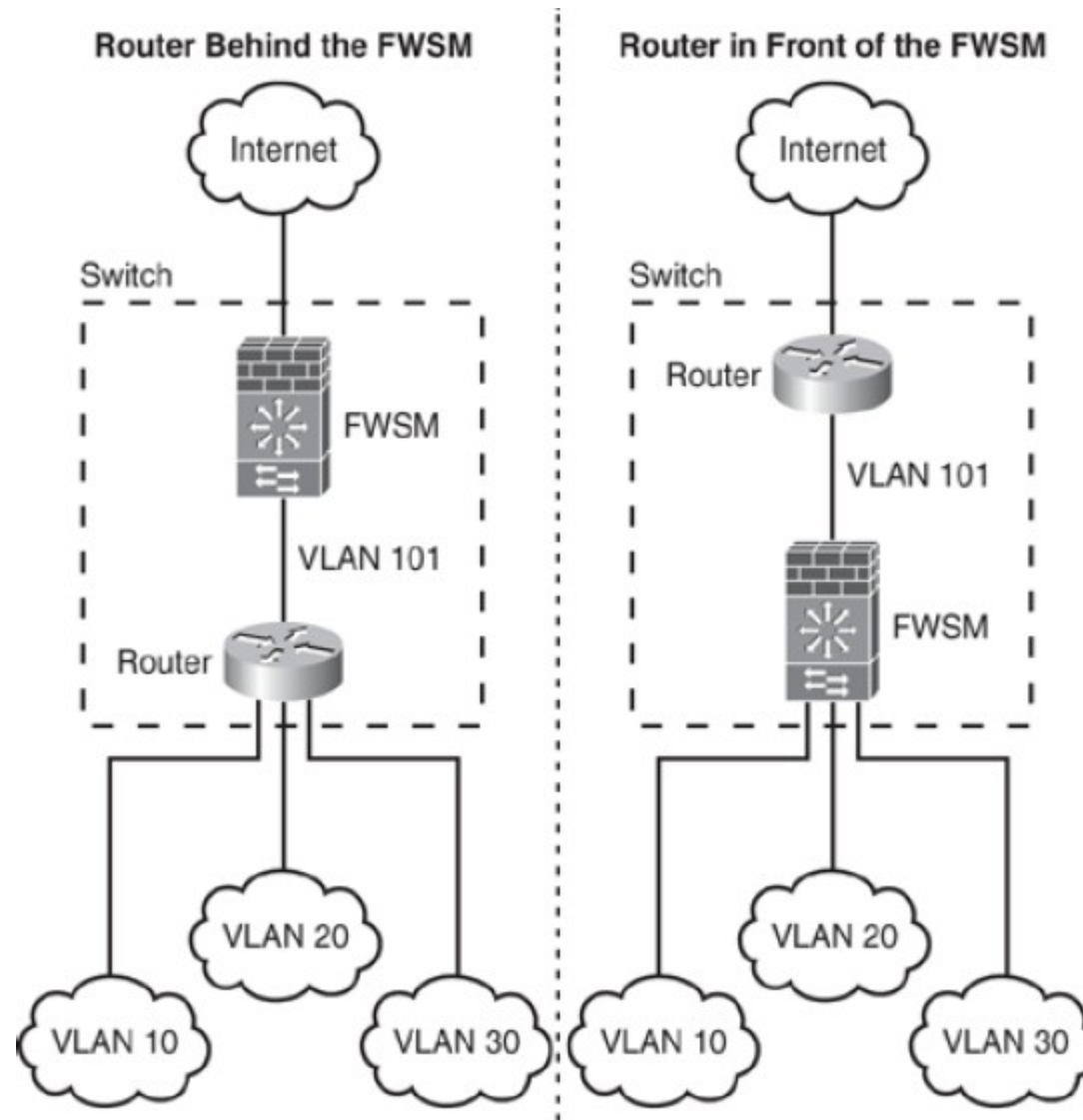
- Routed Mode  
(with Shared Resources)



- Transparent Mode



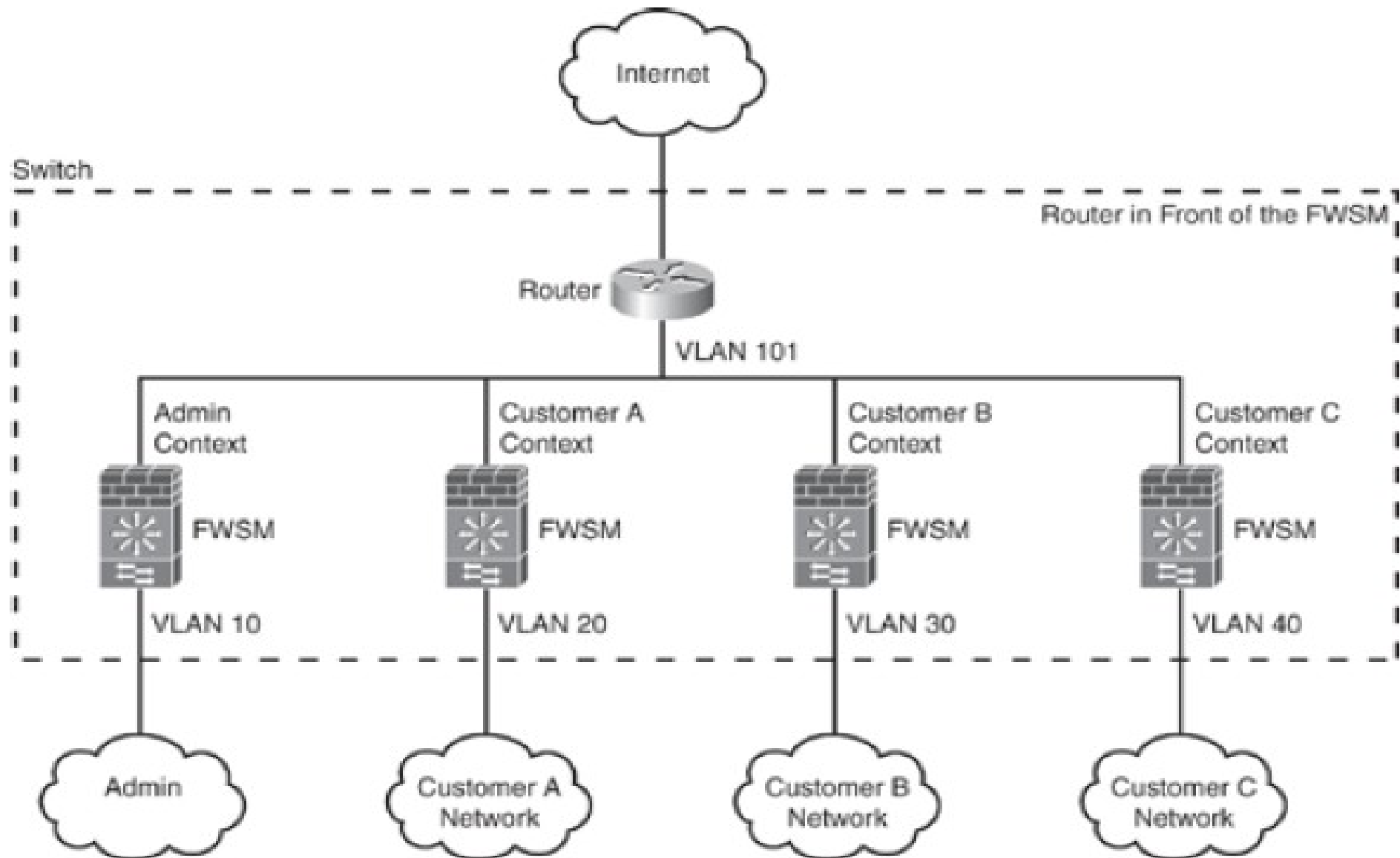
# Firewall placement - In Single Context



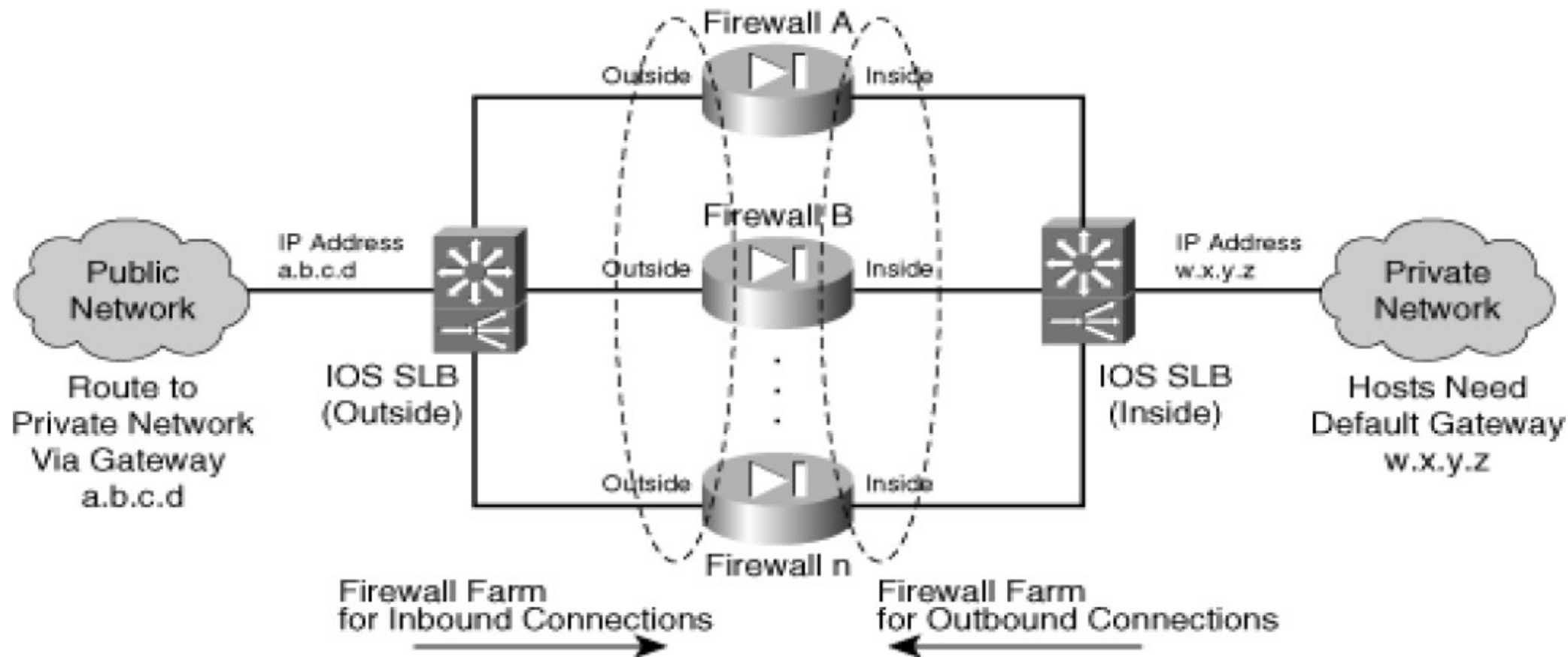
- Both solutions are acceptable!



# Firewall placement - In Multiple Context



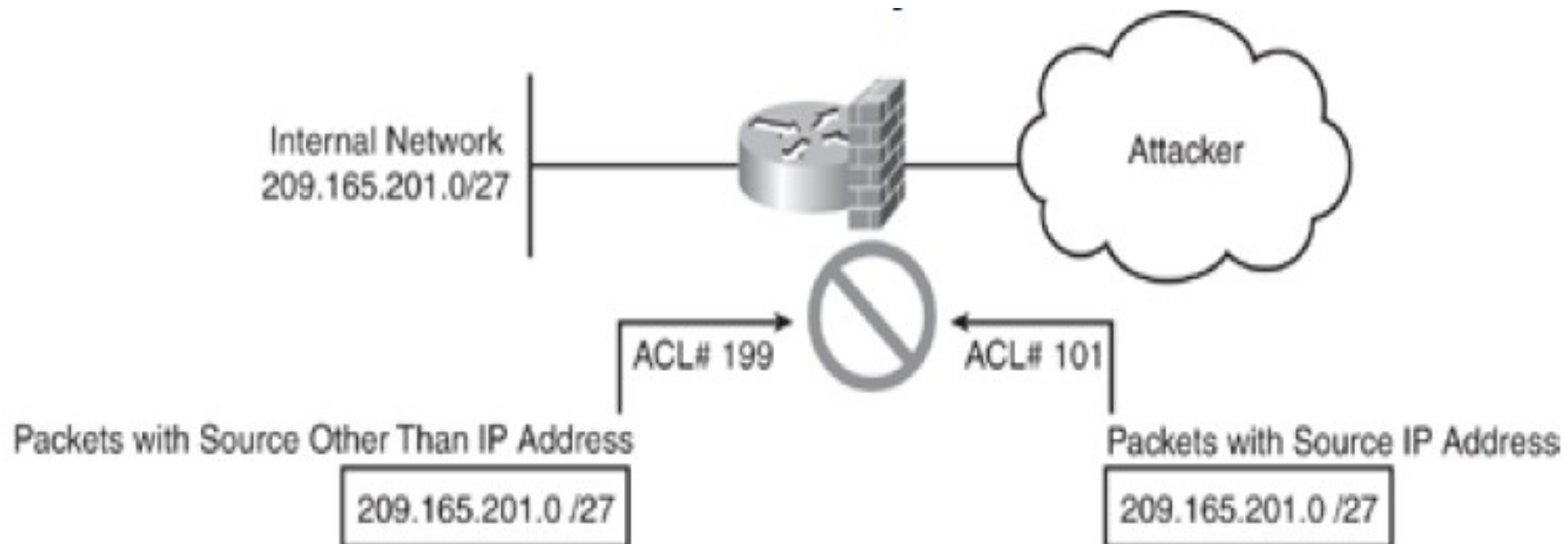
# Firewall Load-Balancing Concept



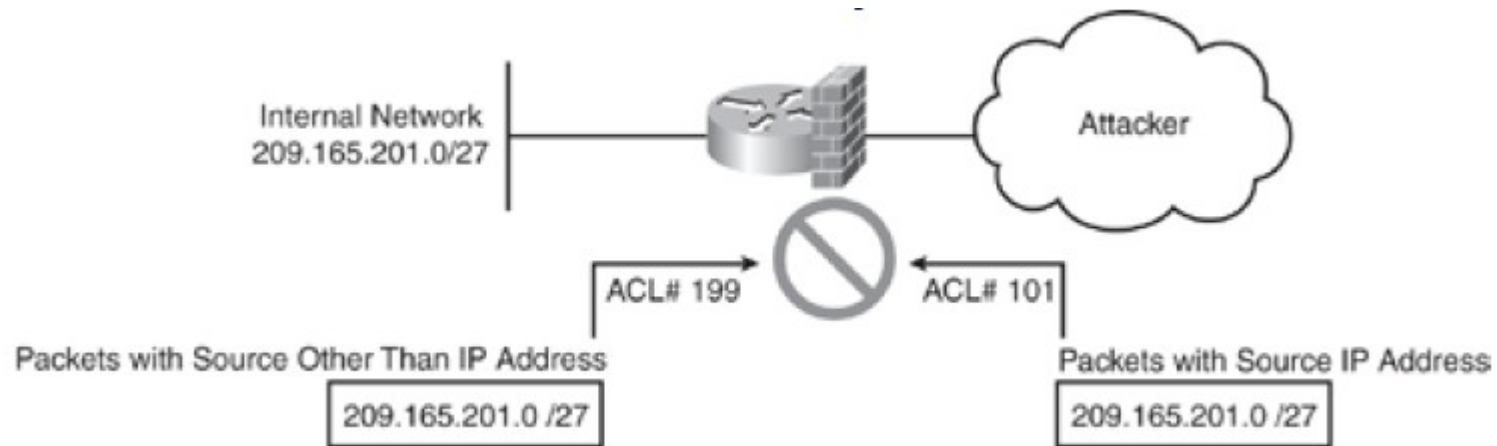
- Load-balancing equipments can distribute traffic by multiple firewalls.
  - ◆ Decrease processing and memory requirements of each firewall.
  - ◆ Makes the network less vulnerable to DoS attacks.

# IP Spoofing

- IP spoofing refers to the creation of IP packets with a forged source IP address.
  - To hide the identity of the sender or impersonate another network system.
  - Spoofing IP datagrams is a well-known problem.
  - Most spoofing is done for illegitimate purposes.



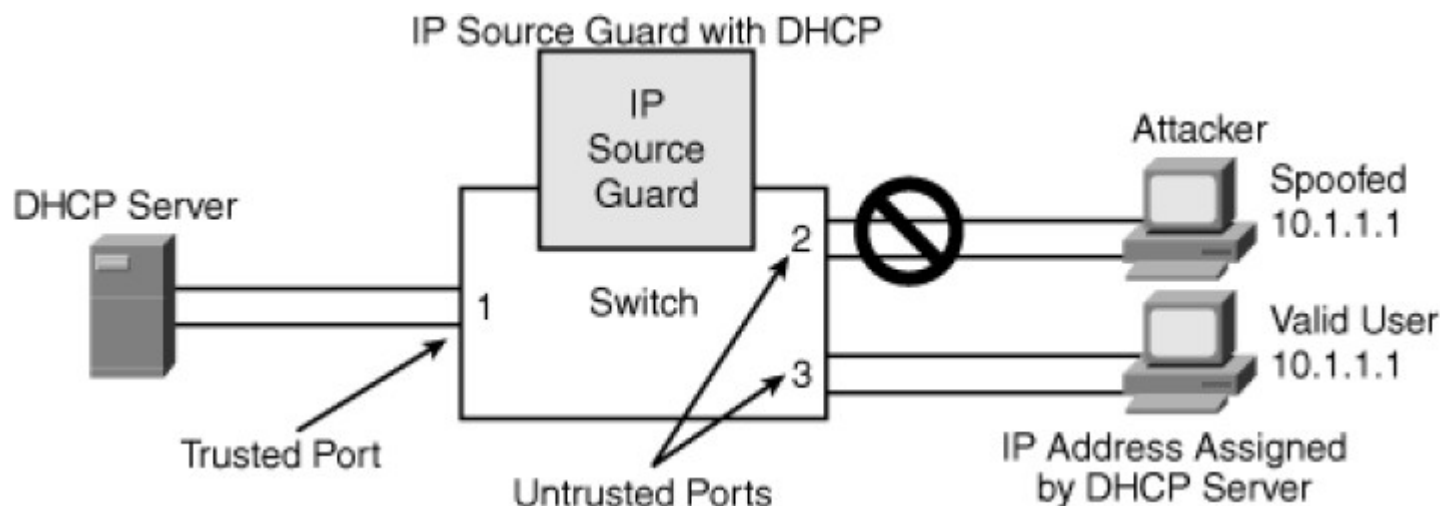
# Preventing IP Spoofing



- Deny external traffic with
  - IP source equal to protected network IP ranges.
  - IP source equal to private addresses.
  - Multicast destinations.
- Reverse Path Verification
  - Deny traffic where the source IP network is not reachable using the interface where the packet arrived.

```
Interface interface-name
 ip access-group 101 in
 ip access-group 199 out
!
access-list 101 deny ip 209.165.201.0 0.0.0.31 any
access-list 101 deny icmp any any redirect
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
access-list 101 deny ip 240.0.0.0 15.255.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 10.1.1.0 0.0.0.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 permit ip any any
!
access-list 199 permit ip 209.165.201.0 0.0.0.31 any
access-list 199 deny ip any any
```

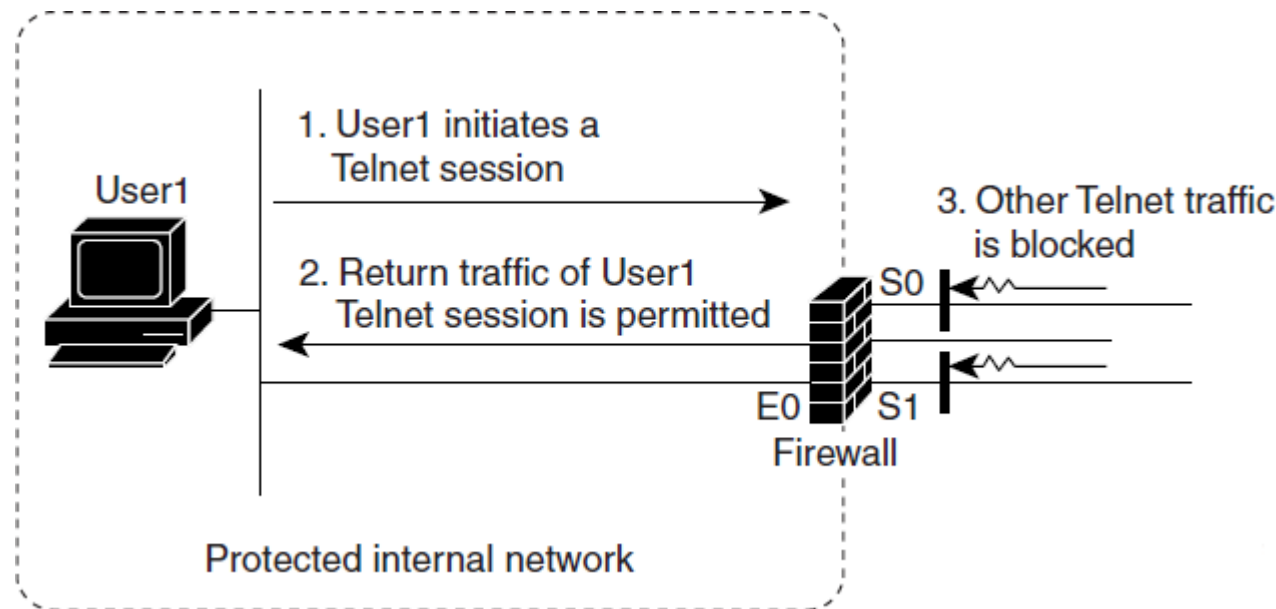
# Preventing IP Spoofing with IP Source Guard



- IP Source Guard is a Layer 2 security feature that prevents IP spoofing attacks by restricting IP traffic on untrusted Layer 2 ports to clients with an assigned IP address.
- Works by filtering IP traffic with a source IP address other than that assigned via Dynamic Host Configuration Protocol (DHCP) or static configuration on the untrusted Layer 2 ports.
- Works in combination with the DHCP and is enabled on untrusted Layer 2 ports.

# Context-Based Access Control (CBAC)

- CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information
- Permit TCP and UDP traffic through a firewall only when the connection is initiated from within the network
- Without CBAC, traffic filtering is limited to implementations that examine packets only at the network layer and transport layer

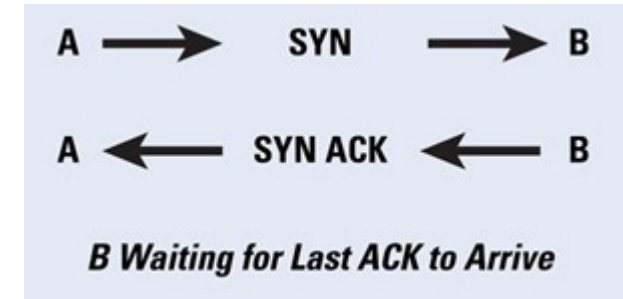




# Half-Open TCP Connection Problem

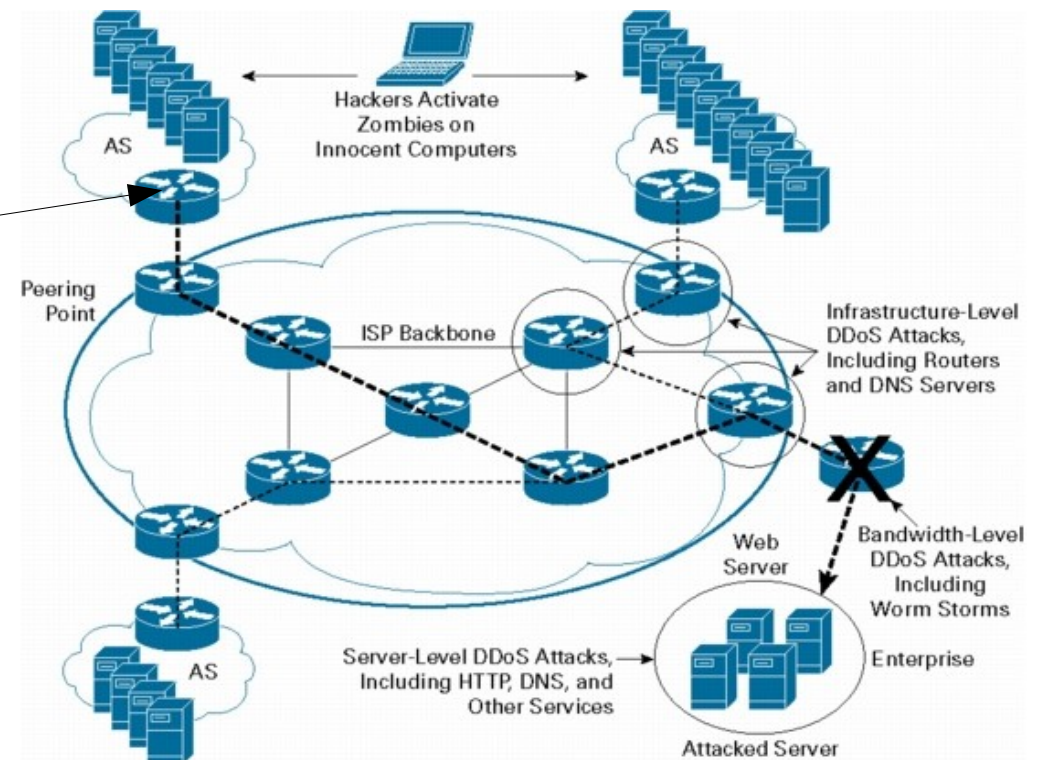
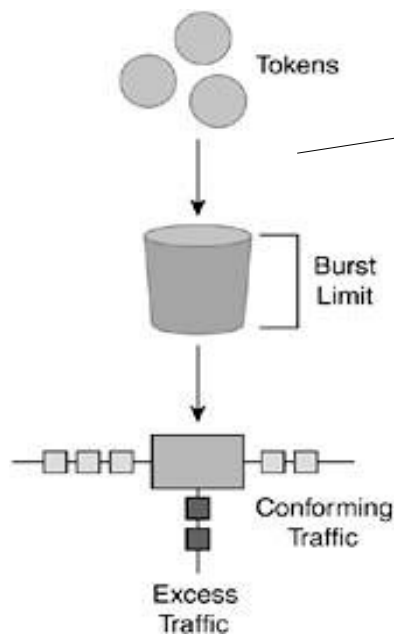
- A DoS attack commonly uses half-open TCP connections.

- Firewall keeps the state of the TCP session in memory.
- Multiple half-open TCP connections can overrun firewalls.
  - Define timeout values for half-open TCP sessions:
    - Normal: small/medium values.
    - Under attack (based on traffic thresholds): very small values.
  - May be necessary to use external means to “clean” firewall.
    - Resetting (half-open) connections from the internal servers.



# DDoS Mitigation at Source

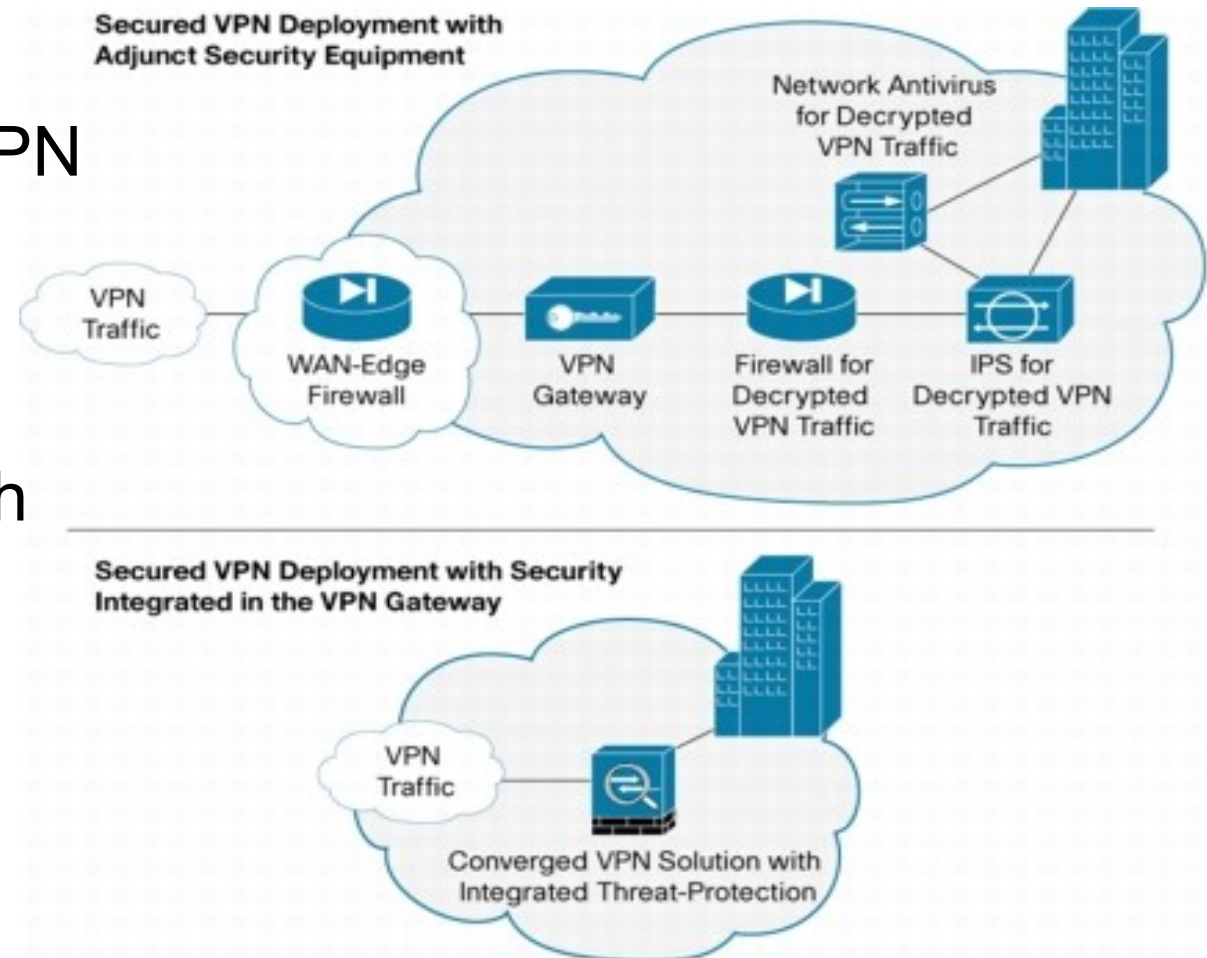
- CAR - Committed Access Rate
  - ◆ Limits (a class of traffic) traffic to a specific rate
  - ◆ Token bucket model
  - ◆ Avoids that a single source may generate/transmit traffic above a per-defined threshold





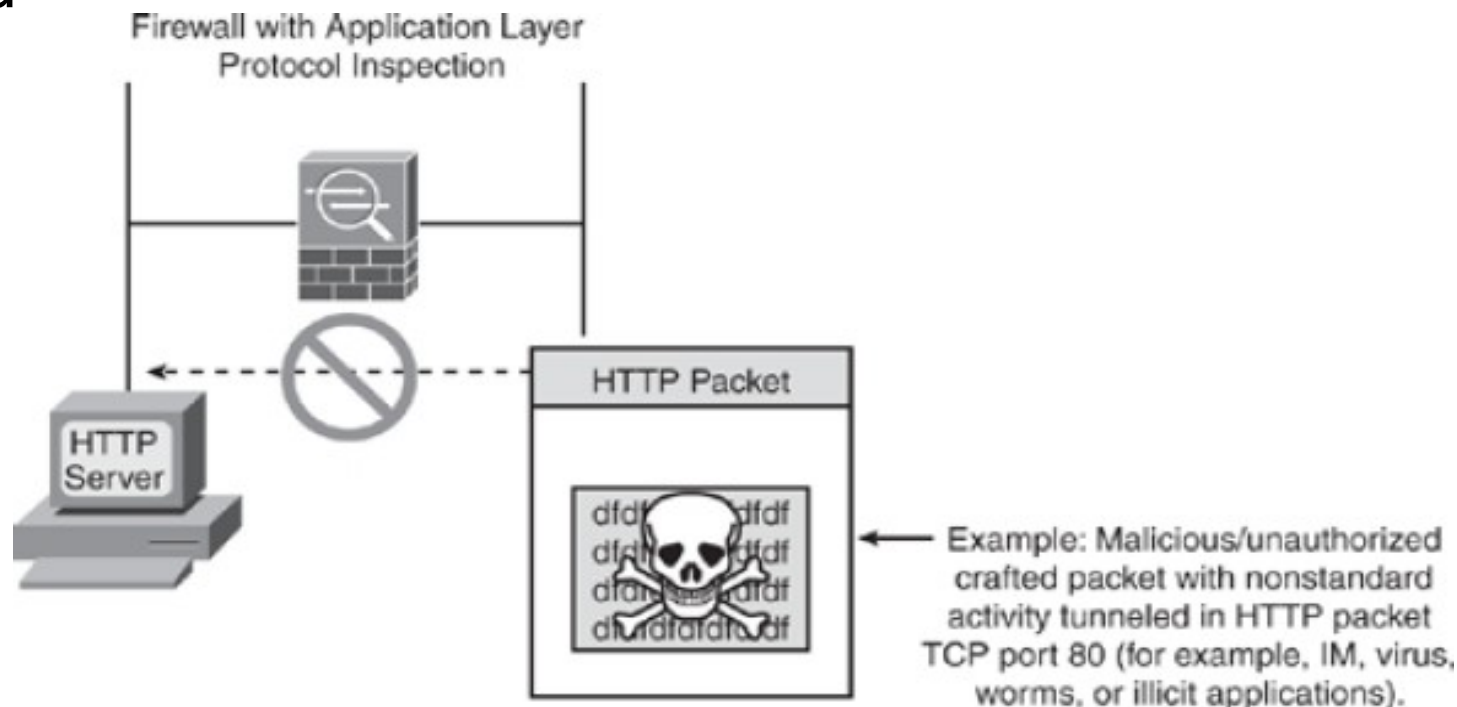
# Firewalls and Remote-Access VPN

- Firewalls need work with VPN gateways
  - To filter all traffic
  - To filter decrypt VPN traffic
- Most firewalls integrate both Security and VPN gateway services



# Application Layer Intelligence

- Application layer Intelligence provides advanced protocol inspection
- Any non-compliance operation in the payload is blocked
- Only packets with standard operation (RFC compliant) are allowed



# Firewall Performance Evaluation

- Basic Firewall

- ◆ IP Throughput

- Raw capability of the firewall to pass traffic from interface to interface

- ◆ Latency

- Time traffic delay in the firewall

- Should be measured and reported when the firewall is at its operating load

- Traditional Enterprise Firewall

- ◆ Connection Establishment Rate

- Speed at which firewalls can set up connections

- ◆ Concurrent Connection Capability

- Total number of open connections through the firewall at any given moment

- ◆ Connection Teardown Rate

- Speed at which firewalls can teardown connections and free resources

- Next Generation Firewall

- ◆ Application Transaction Rate

- Capability of the firewall to secure discrete application-layer transactions contained in an open connection

- May include application-layer gateways, intrusion prevention, or deep-inspection technology

- Application transaction rate are highly data dependent



# Cisco's Access Control Lists (ACL)

- An access list is a sequential collection of **permit** and **deny** conditions.
- Software tests packets against the conditions in an access list one by one.
- The first match determines whether the software accepts or rejects the packet.
  - ◆ Because the software stops testing conditions after the first match, the order of the conditions is critical.
- If no conditions match, the software rejects the packet.
- Can be applied to inbound or outbound traffic.



# ACL Types

- Standard

- ◆ Control traffic by the analysis of the source address of the IP packets.
- ◆ Numbered from 1 to 99
  - Example: access-list 1 permit 10.1.1.0 0.0.0.255

- Extended

- ◆ Control traffic by the analysis of the source and destination addresses and protocol of the IP packets.
- ◆ Numbered from 100 to 199
  - Example: access-list 101 permit ip any 10.1.1.0 0.0.0.255

- Named

- ◆ Allow standard and extended ACLs to be given names Intuitively identify an ACL using an alphanumeric name.
- ◆ Eliminate the number limits that exist on standard and extended ACLs.
- ◆ Named ACLs provide the ability to modify ACLs without deleting and then reconfiguring them.
  - Example: ip access-list {extended | standard} name

- Reflexive

- ◆ Allow IP packets to be filtered based on upper-layer session information.
- ◆ Communication in one direction opens doors in the opposite direction.
- ◆ Generally used to allow outbound traffic and to limit inbound traffic in response to sessions that originate inside the network.

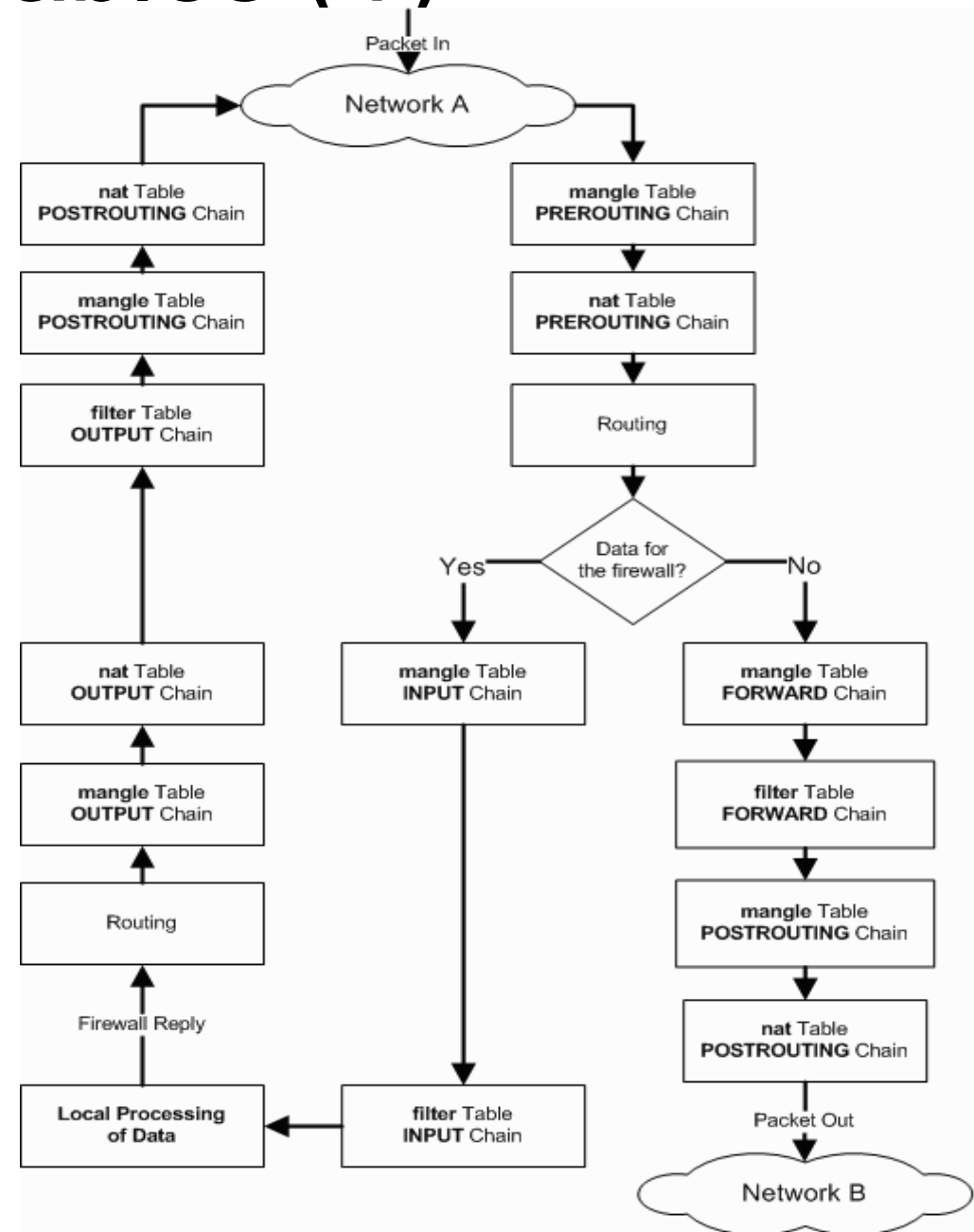
- Context-Based Access Control (CBAC)

- ◆ Inspects traffic to discover and manage state information for TCP and UDP sessions
- ◆ This state information is used to create temporary openings in the firewall access lists



# Linux IPTables (1)

- Name of the user space tool by which administrators create rules for the packet filtering and NAT modules.
- Used to set up, maintain, and inspect the tables of IP packet filtering rules within the Linux kernel.
- Has 5 default chains:
  - ◆ INPUT, OUTPUT, FORWARD
  - ◆ PREROUTING
  - ◆ POSTROUTING
- Has 3 default tables,
  - ◆ Filter, nat and mangle
- Basic decisions
  - ◆ ACCEPT, DROP, QUEUE and RETURN
- Extended decisions
  - ◆ LOG, MARK, REJECT, TOS, SNAT, DNAT, MASQUERADE, REDIRECT, etc...
- Multiple state machines
  - ◆ For example: Conntrack (connection tracker).





# Linux IPTables (2)

- In addition to the built-in chains, the user can create any number of user-defined chains within each table, which allows them to group rules logically.
- Each chain contains a list of rules,
  - ◆ When a packet is sent to a chain, it is compared against each rule in the chain in order.
- The rule specifies what properties the packet must have for the rule to match (such as the port number or IP address).
- If the rule does not match, then processing continues with the next rule.
- If, however, the rule does match the packet, then the rule's target instructions are followed (and further processing of the chain is usually aborted).
- Some packet properties can only be examined in certain chains,
  - ◆ For example, the outgoing network interface is not valid in the INPUT chain.
- Some targets can only be used in certain chains, and/or certain tables,
  - ◆ For example, the SNAT target can only be used in the POSTROUTING chain of the NAT table.
- The target of a rule can be the name of a user-defined chain or one of the built-in targets (ACCEPT, DROP, RETURN, DNAT, SNAT and MASQUERADE).
- You can think of a target in the same way as a subroutine.

