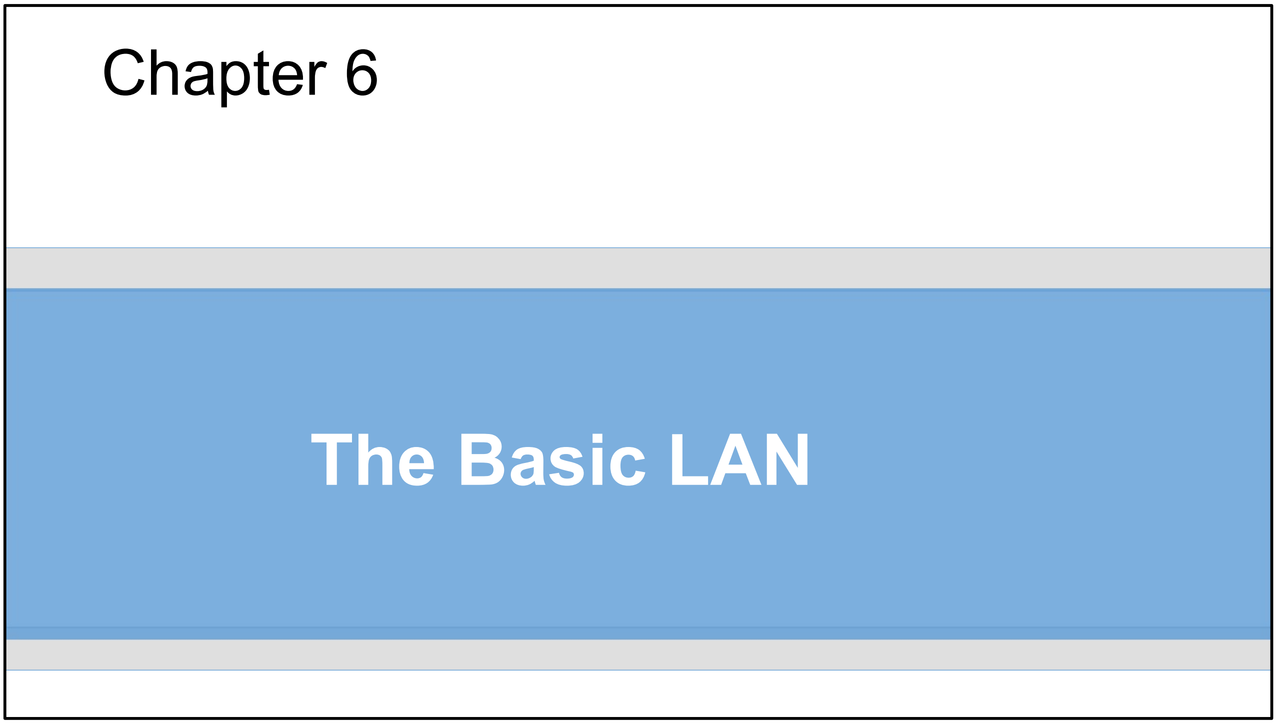
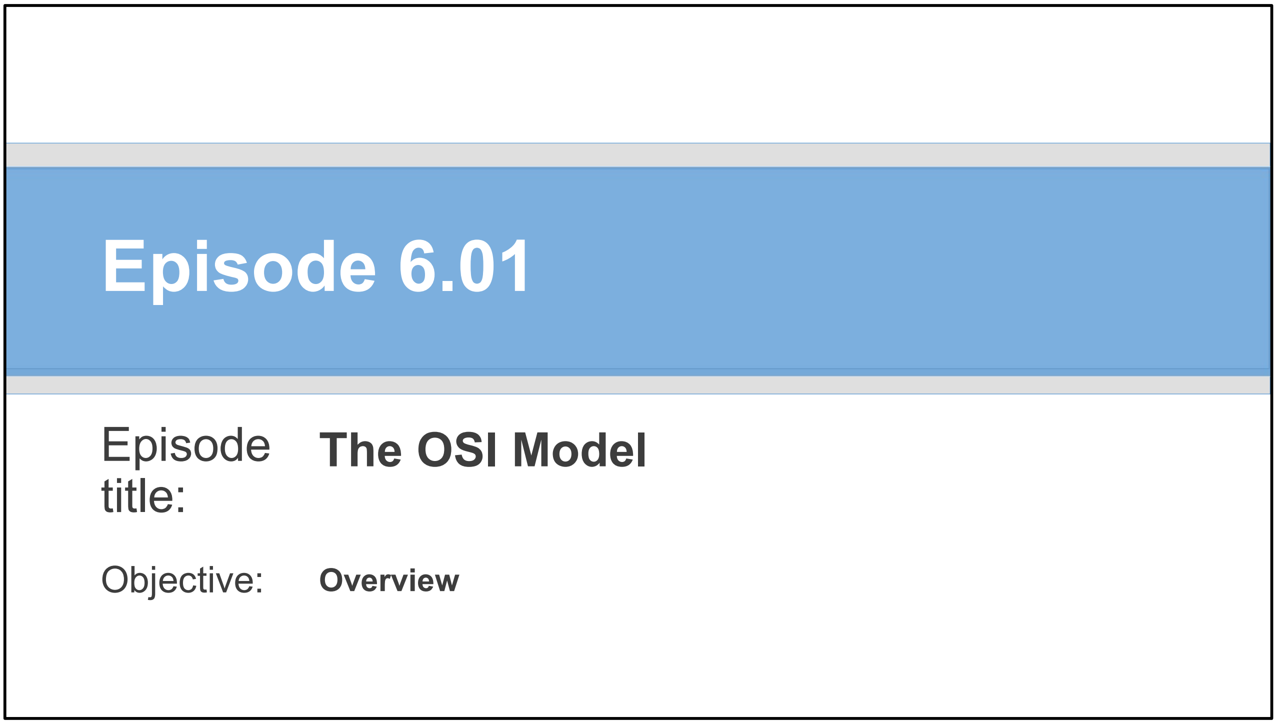


Chapter 6

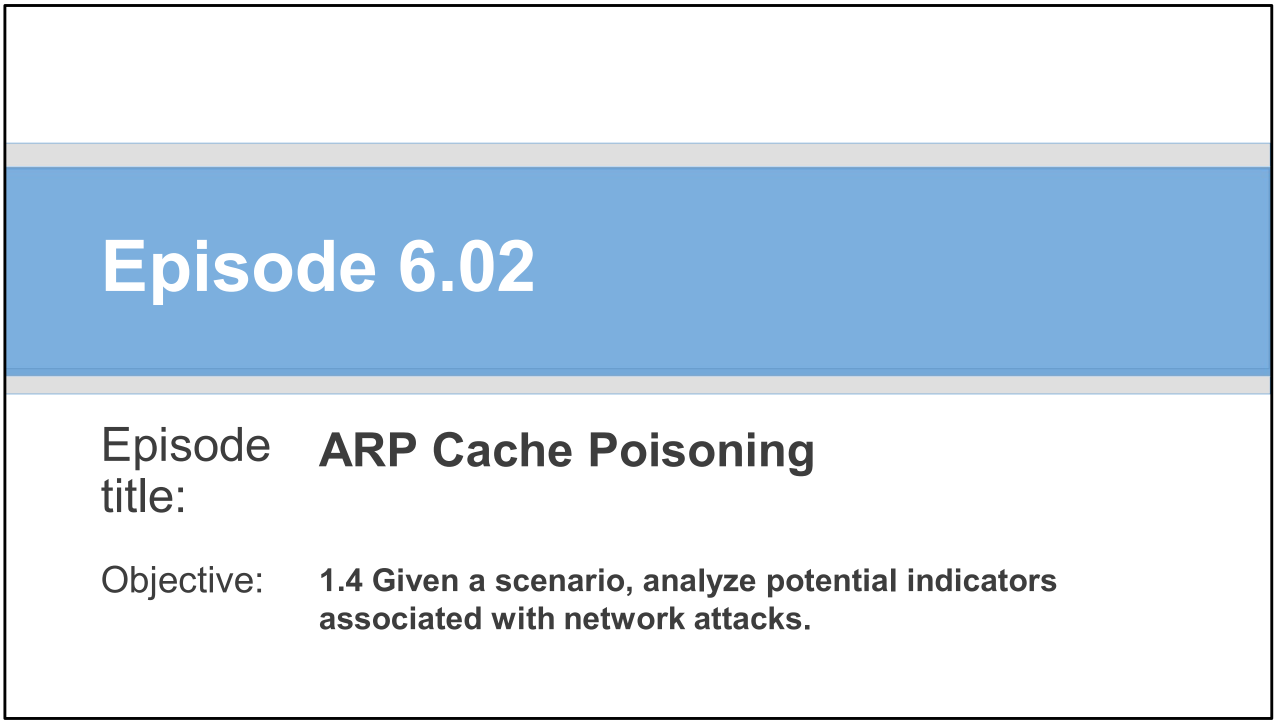
The Basic LAN



Episode 6.01

Episode title: **The OSI Model**

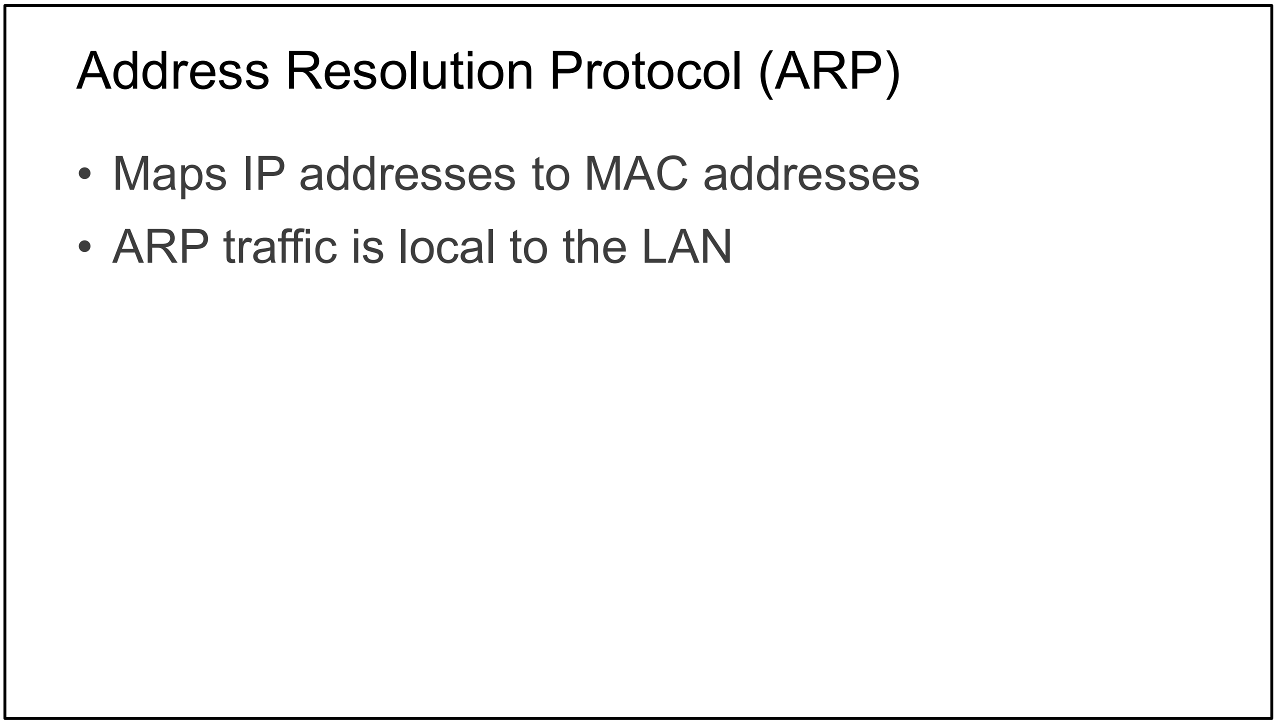
Objective: **Overview**



Episode 6.02

Episode title: **ARP Cache Poisoning**

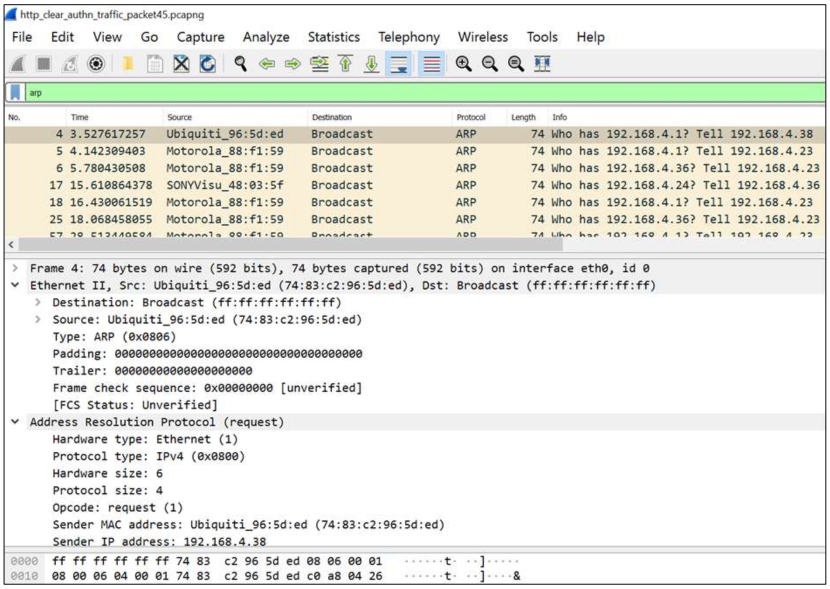
Objective: **1.4 Given a scenario, analyze potential indicators associated with network attacks.**



Address Resolution Protocol (ARP)

- Maps IP addresses to MAC addresses
- ARP traffic is local to the LAN

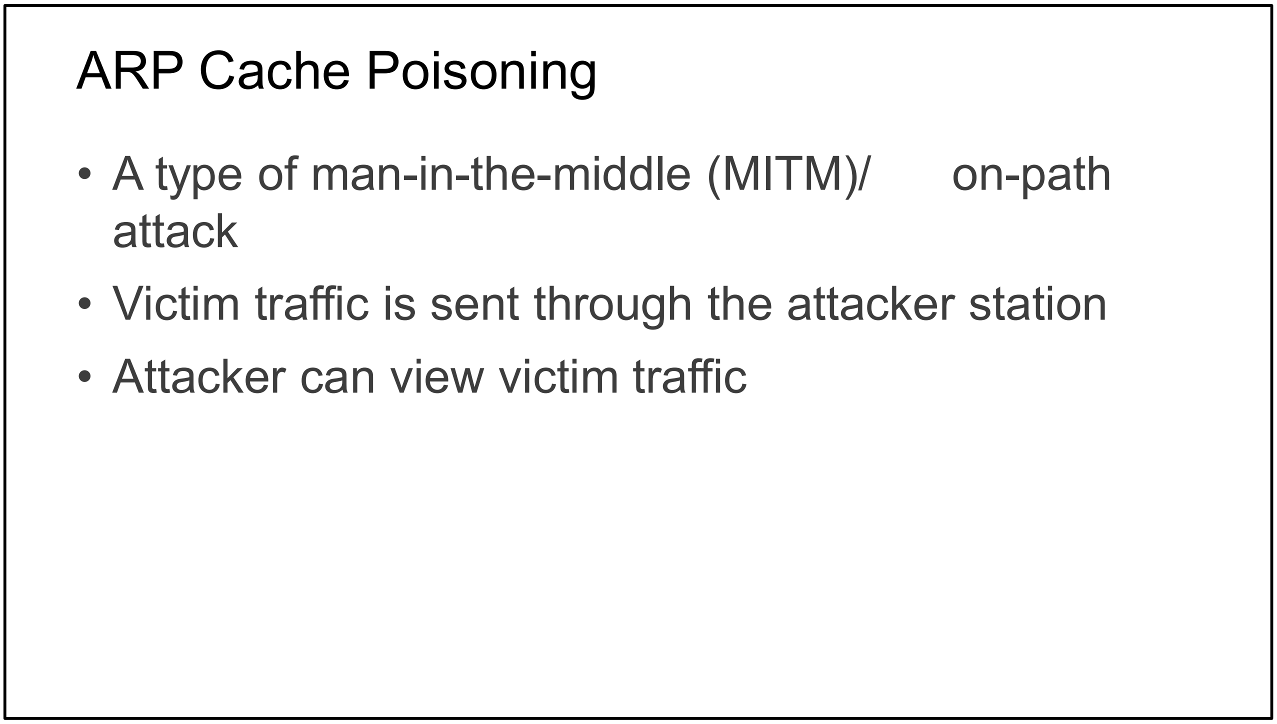
Demo ARP Packet Capture



```
No.     Time          Source              Destination   Protocol  Length Info
      4 3.527617257   Ubiquiti_96:5d:ed   Broadcast     ARP           74 Who has 192.168.4.1? Tell 192.168.4.38
      5 4.142309403   Motorola_88:f1:59   Broadcast     ARP           74 Who has 192.168.4.1? Tell 192.168.4.23
      6 5.780430508   Motorola_88:f1:59   Broadcast     ARP           74 Who has 192.168.4.36? Tell 192.168.4.23
     17 15.610864378  SONYVisu_48:03:5f   Broadcast     ARP           74 Who has 192.168.4.24? Tell 192.168.4.36
     18 16.430061519  Motorola_88:f1:59   Broadcast     ARP           74 Who has 192.168.4.1? Tell 192.168.4.23
     25 18.068458055  Motorola_88:f1:59   Broadcast     ARP           74 Who has 192.168.4.36? Tell 192.168.4.23
     57 28.513449584  Motorola_88:f1:59   Broadcast     ARP           74 Who has 192.168.4.1? Tell 192.168.4.23
```

```
> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
v Ethernet II, Src: Ubiquiti_96:5d:ed (74:83:c2:96:5d:ed), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: Ubiquiti_96:5d:ed (74:83:c2:96:5d:ed)
      Type: ARP (0x0806)
      Padding: 000000000000000000000000000000000000
      Trailer: 00000000000000000000
      Frame check sequence: 0x00000000 [unverified]
      [FCS Status: Unverified]
v Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: Ubiquiti_96:5d:ed (74:83:c2:96:5d:ed)
      Sender IP address: 192.168.4.38
```

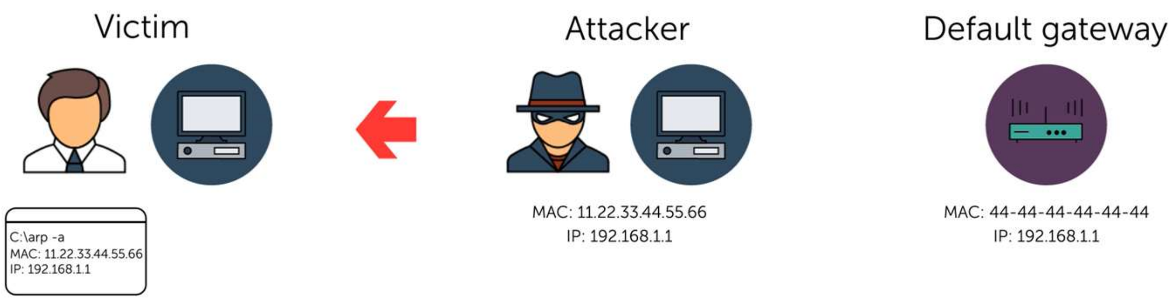
```
0000  ff ff ff ff ff ff 74 83  c2 96 5d ed 08 06 00 01   ······t· ··]·····
0010  08 00 06 04 00 01 74 83  c2 96 5d ed c0 a8 04 26   ······t· ··]····&
```



ARP Cache Poisoning

- A type of man-in-the-middle (MITM)/ on-path attack
- Victim traffic is sent through the attacker station
- Attacker can view victim traffic

ARP Cache Poisoning



Victim

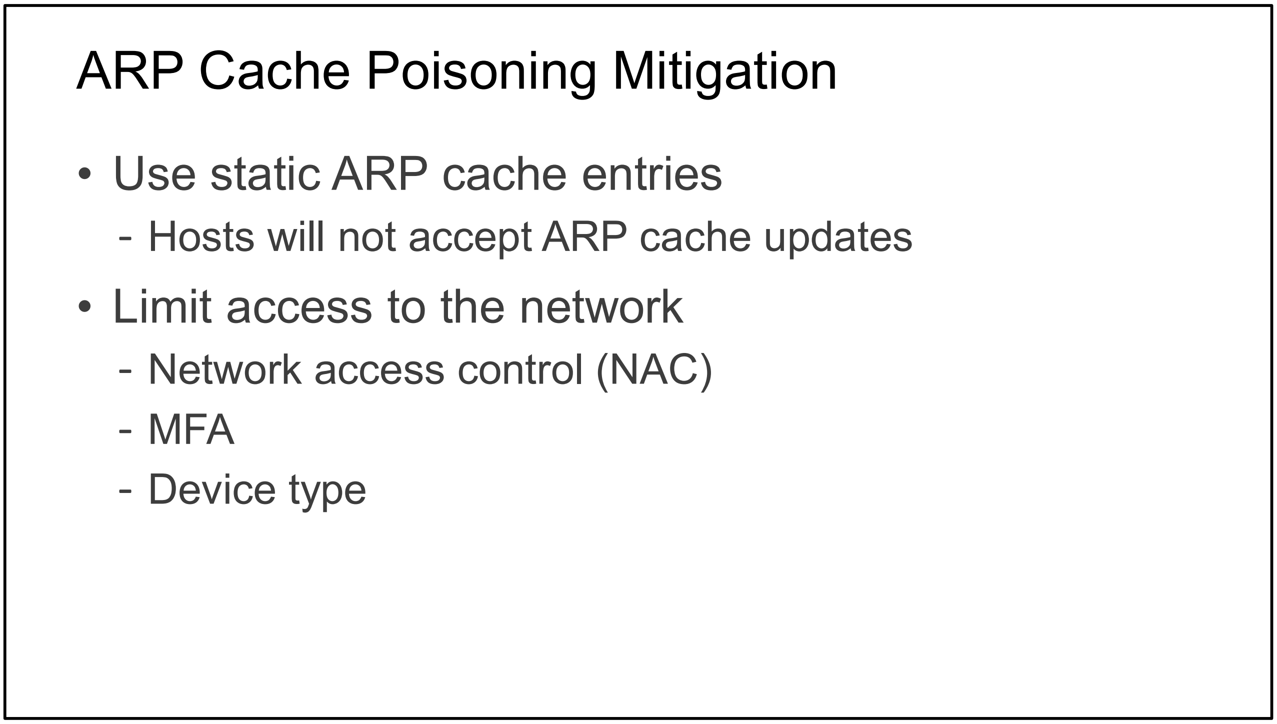
```
C:\arp -a
MAC: 11.22.33.44.55.66
IP: 192.168.1.1
```

Attacker

MAC: 11.22.33.44.55.66
IP: 192.168.1.1

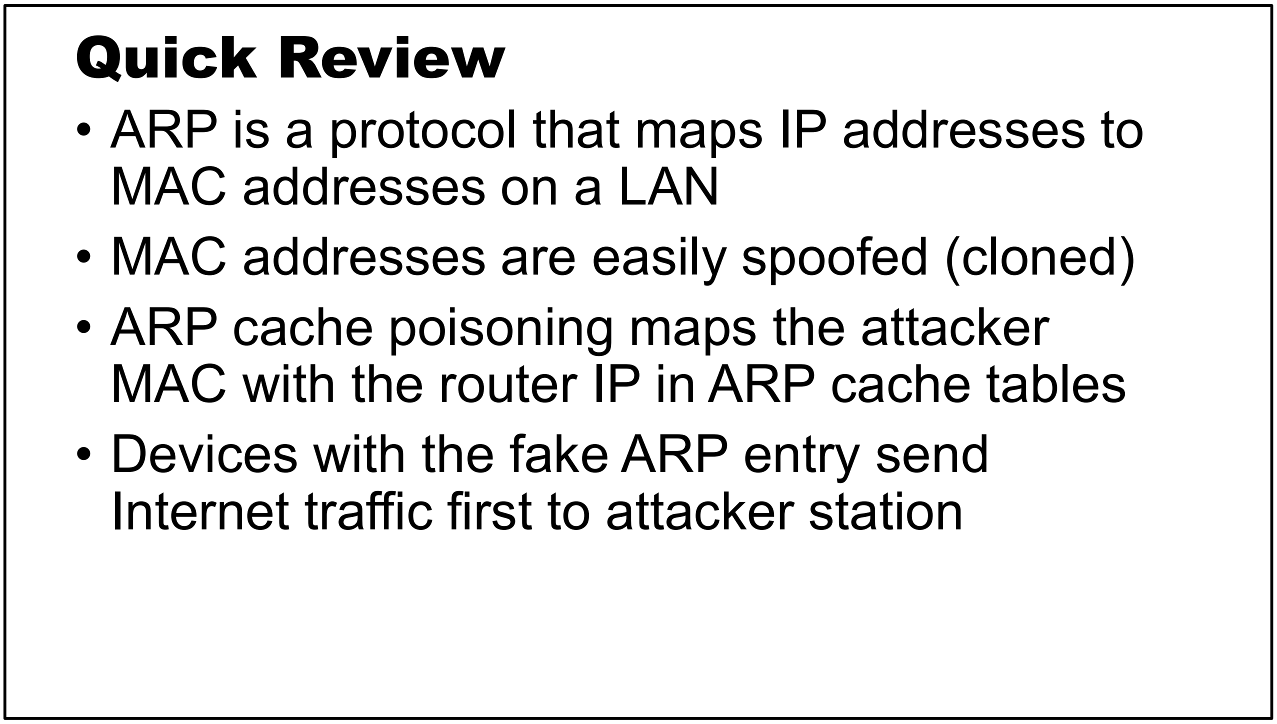
Default gateway

MAC: 44-44-44-44-44-44
IP: 192.168.1.1



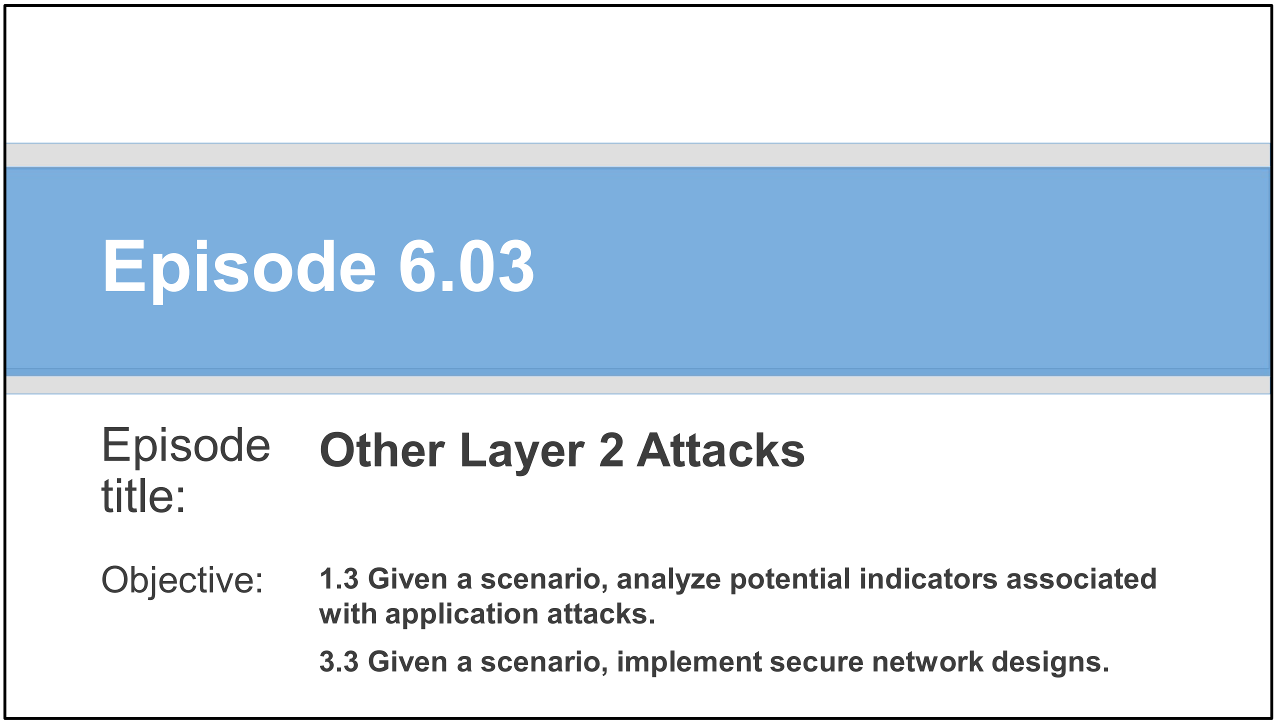
ARP Cache Poisoning Mitigation

- Use static ARP cache entries
  - Hosts will not accept ARP cache updates
- Limit access to the network
  - Network access control (NAC)
  - MFA
  - Device type



Quick Review

- ARP is a protocol that maps IP addresses to MAC addresses on a LAN
- MAC addresses are easily spoofed (cloned)
- ARP cache poisoning maps the attacker MAC with the router IP in ARP cache tables
- Devices with the fake ARP entry send Internet traffic first to attacker station

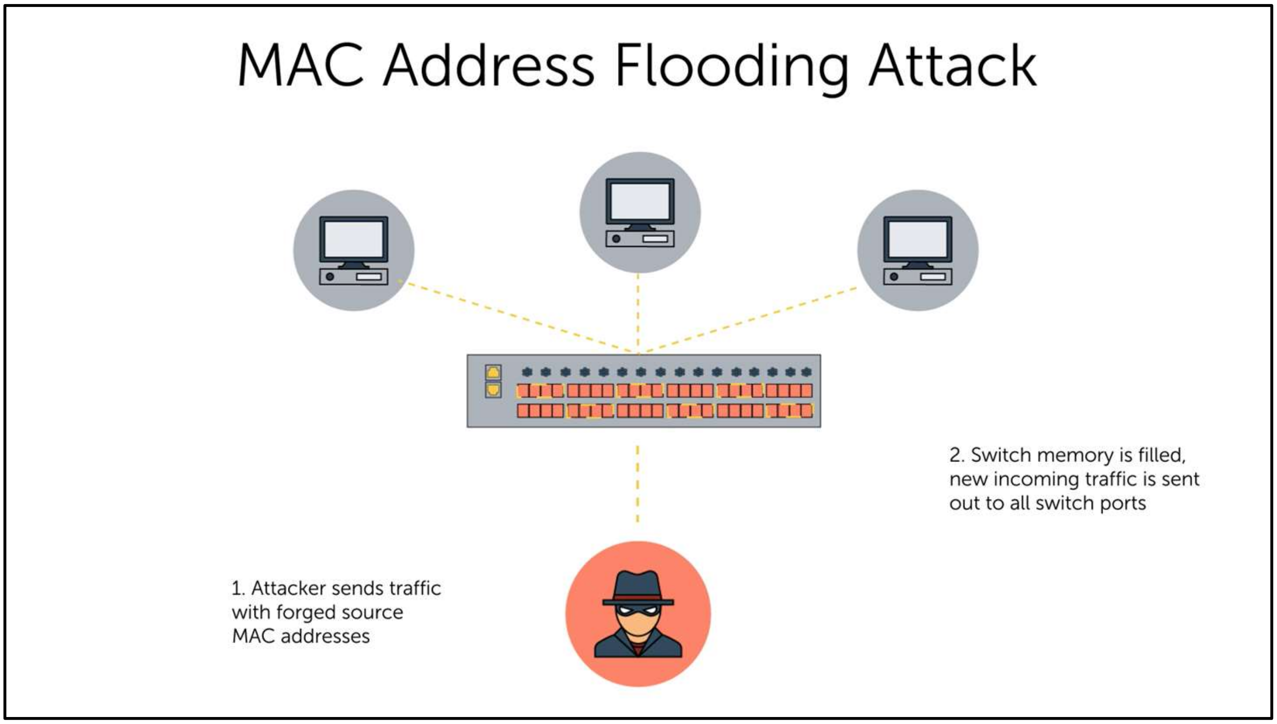


Episode 6.03

Episode title: **Other Layer 2 Attacks**

Objective: **1.3 Given a scenario, analyze potential indicators associated with application attacks.**

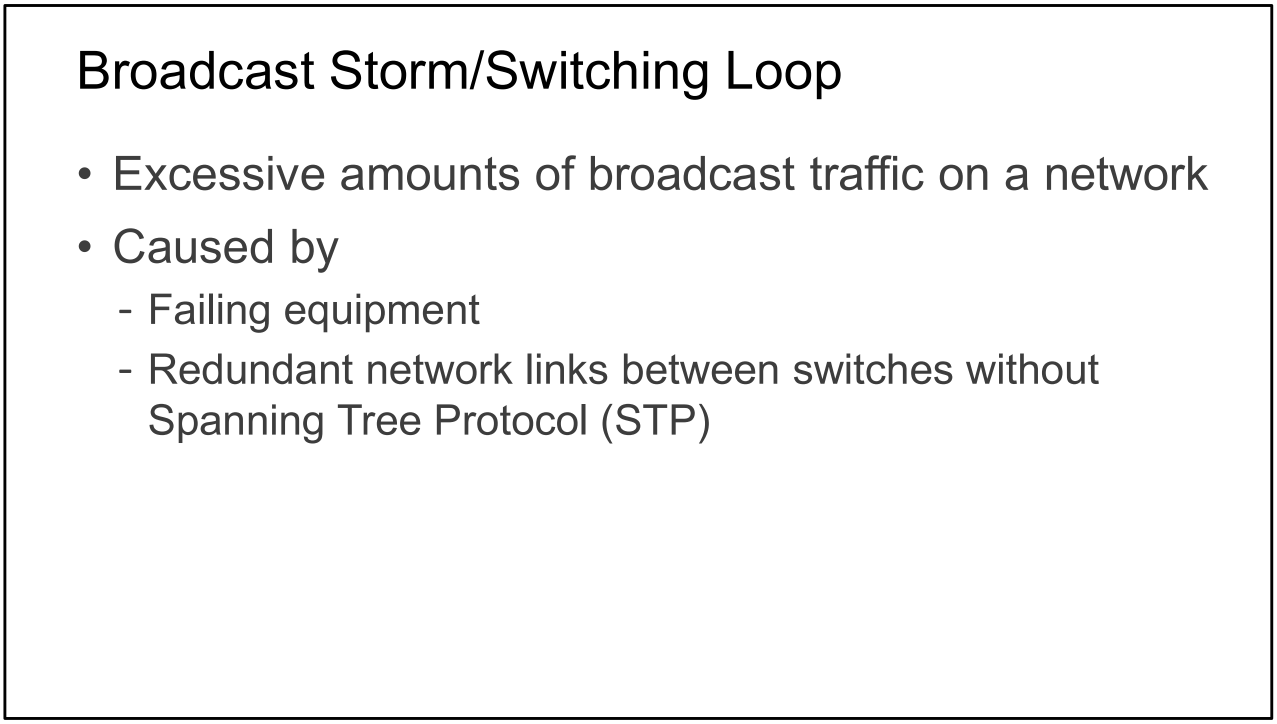
3.3 Given a scenario, implement secure network designs.



MAC Address Flooding Attack

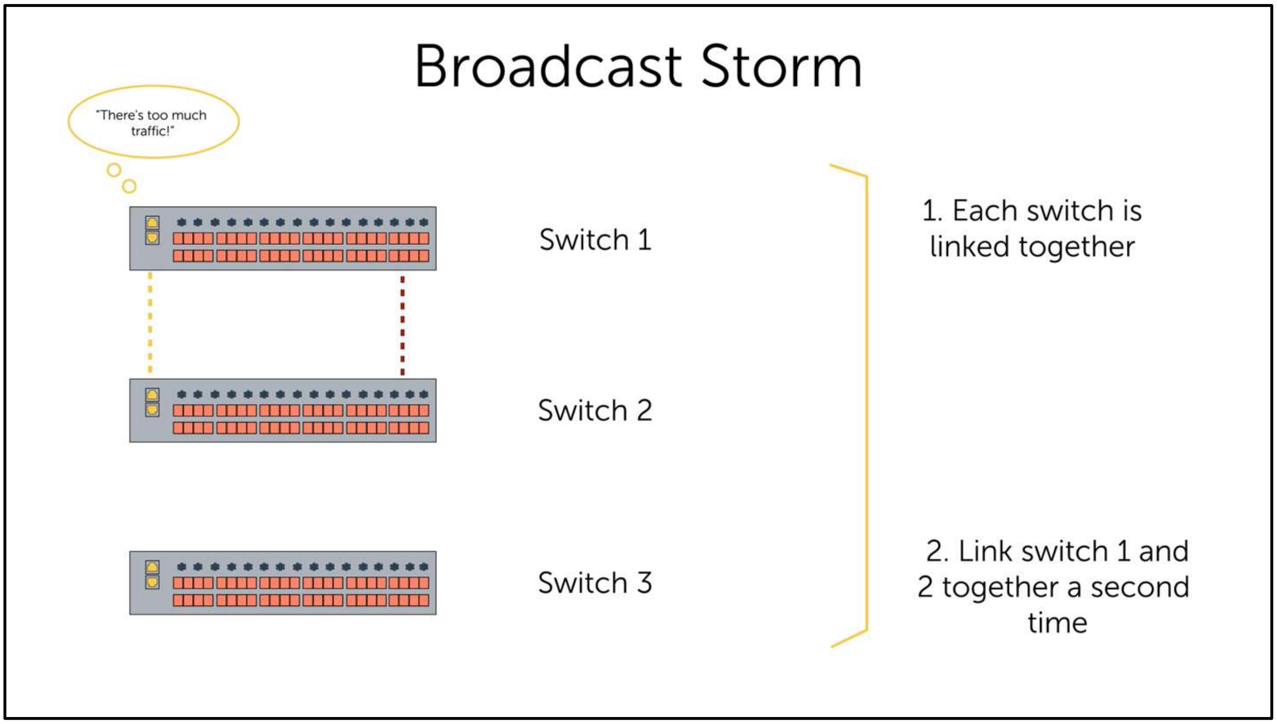
2. Switch memory is filled, new incoming traffic is sent out to all switch ports

1. Attacker sends traffic with forged source MAC addresses



Broadcast Storm/Switching Loop

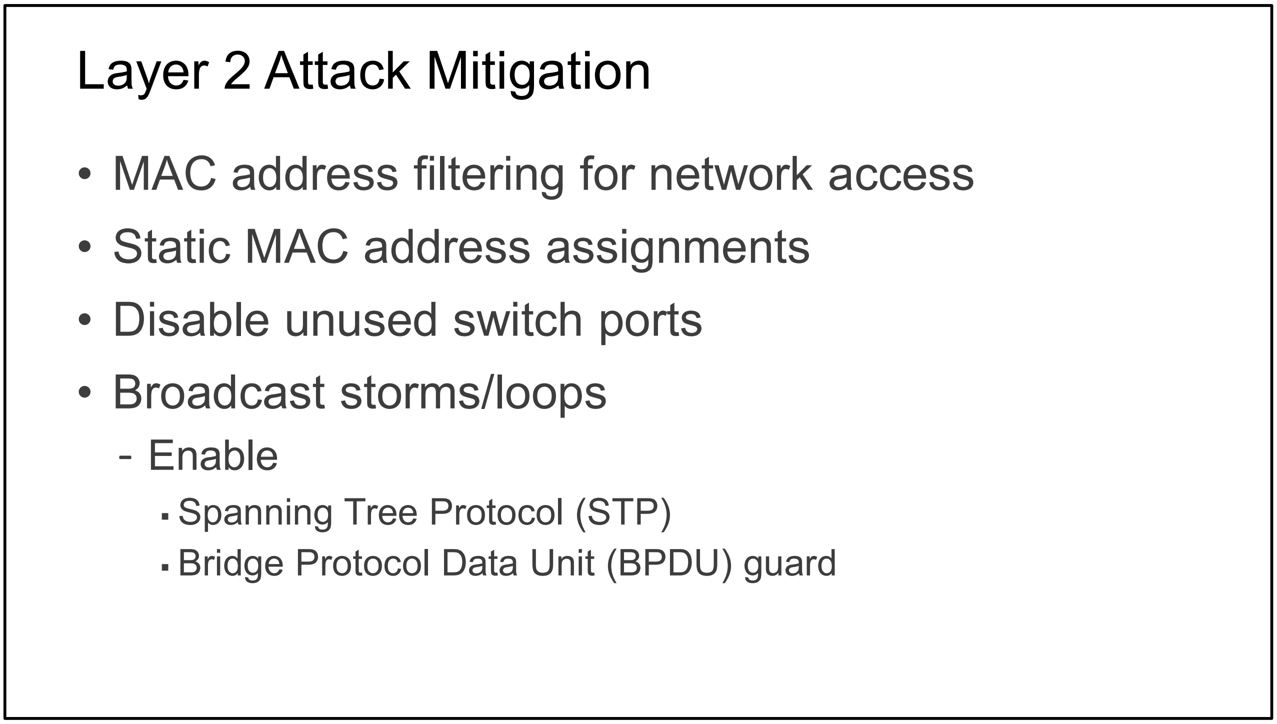
- Excessive amounts of broadcast traffic on a network
- Caused by
  - Failing equipment
  - Redundant network links between switches without Spanning Tree Protocol (STP)



Broadcast Storm

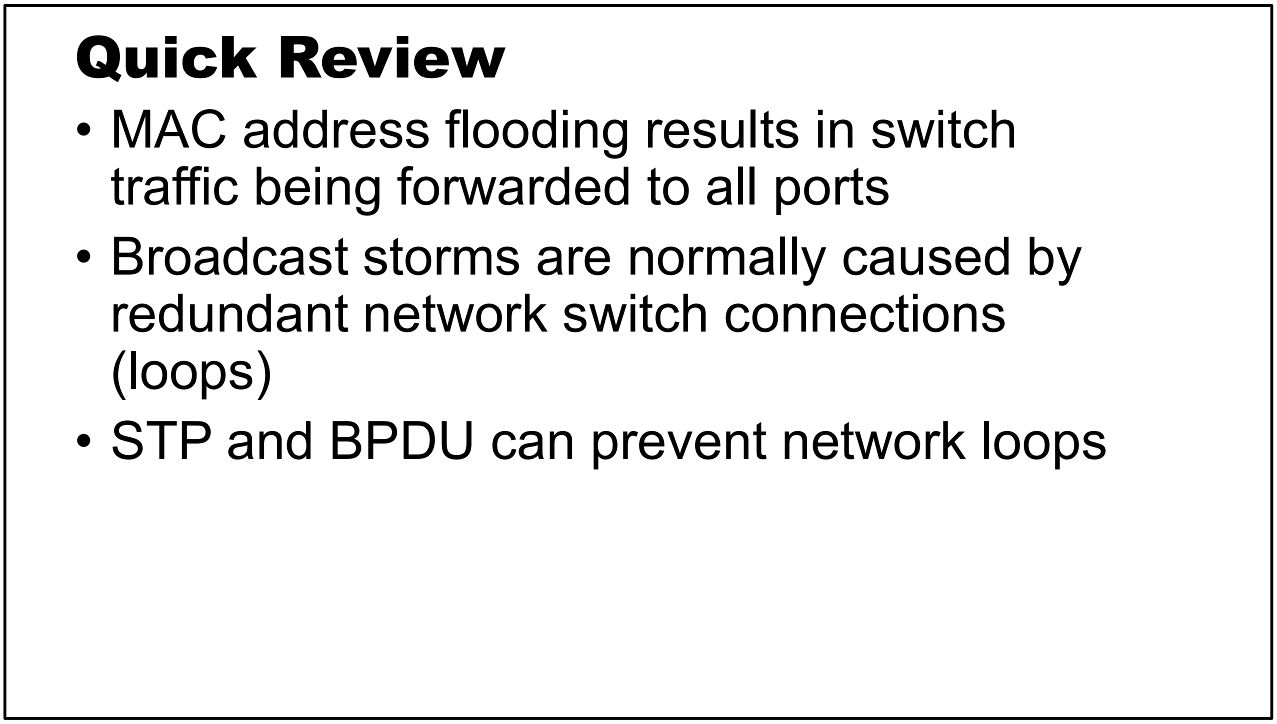
1. Each switch is linked together

2. Link switch 1 and 2 together a second time



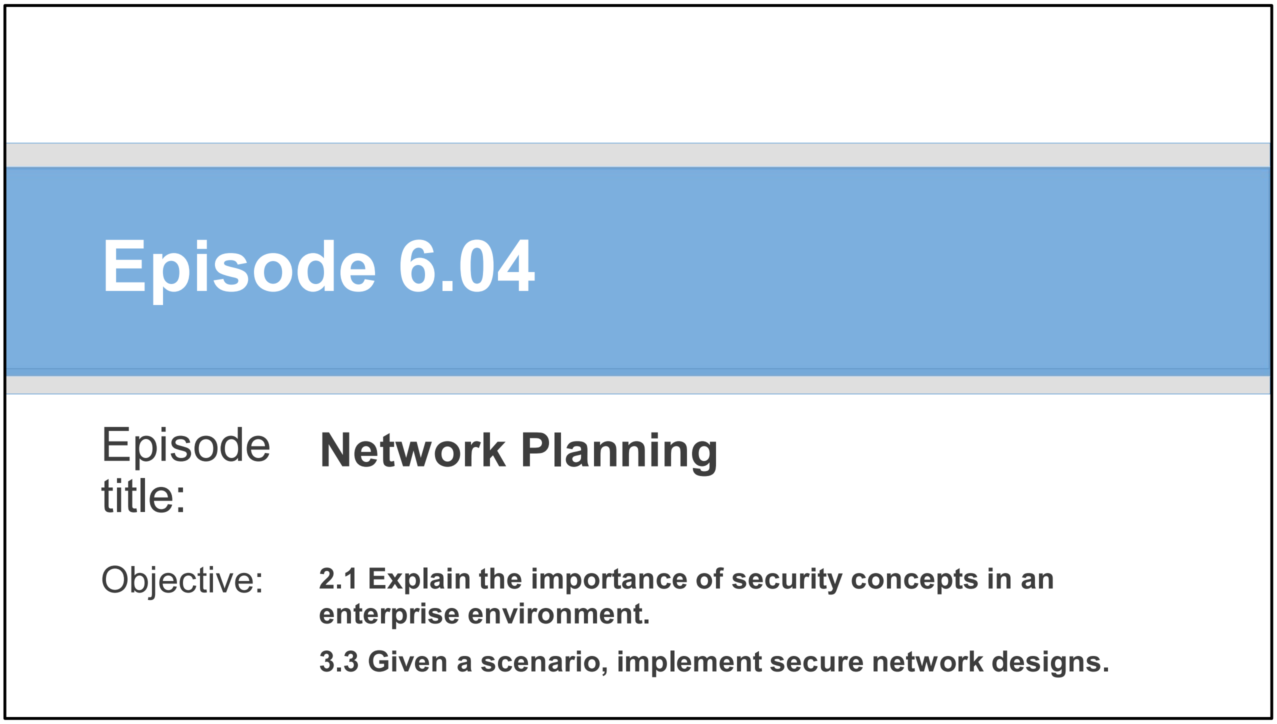
Layer 2 Attack Mitigation

- MAC address filtering for network access
- Static MAC address assignments
- Disable unused switch ports
- Broadcast storms/loops
  - Enable
    - Spanning Tree Protocol (STP)
    - Bridge Protocol Data Unit (BPDU) guard



Quick Review

- MAC address flooding results in switch traffic being forwarded to all ports
- Broadcast storms are normally caused by redundant network switch connections (loops)
- STP and BPDU can prevent network loops

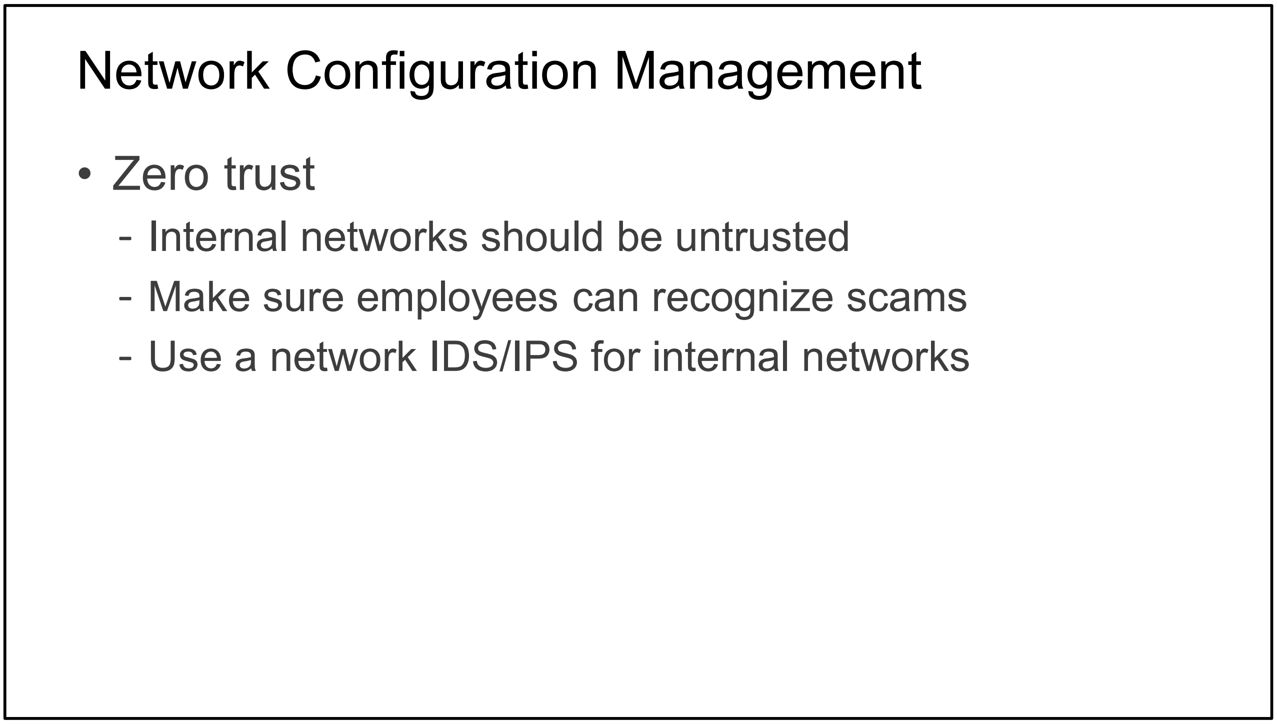


Episode 6.04

Episode title: **Network Planning**

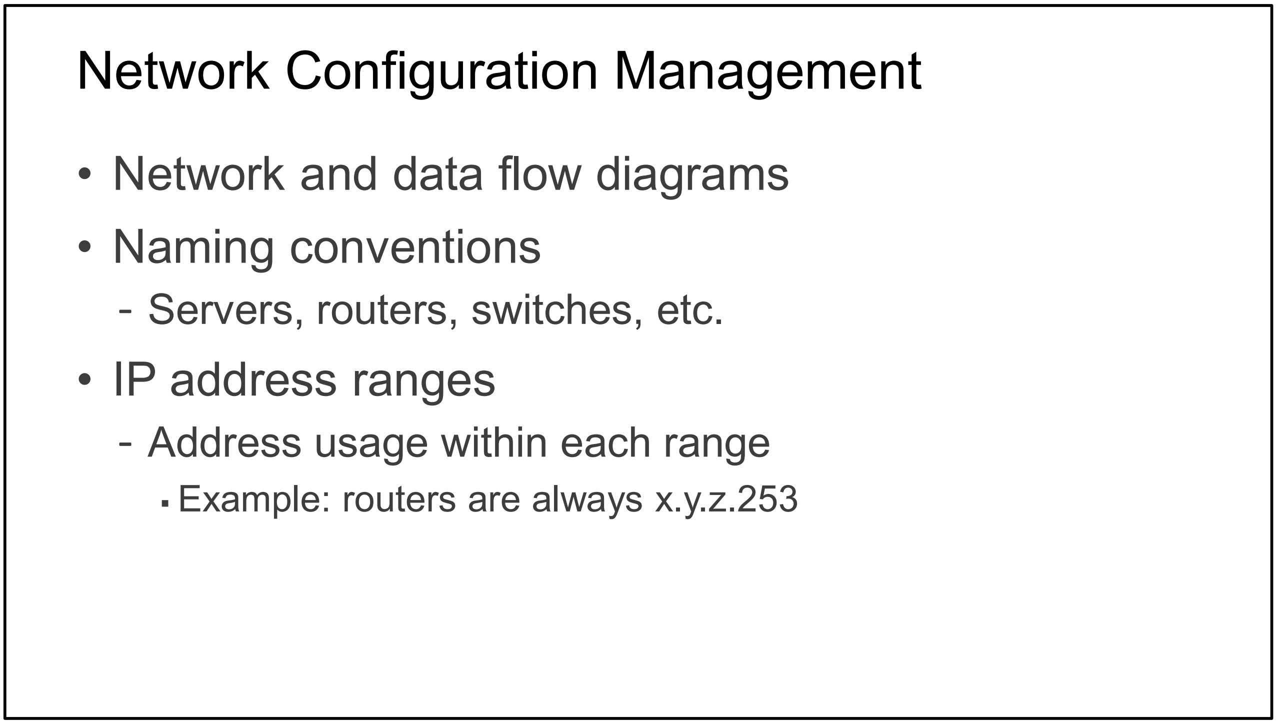
Objective: **2.1 Explain the importance of security concepts in an enterprise environment.**

3.3 Given a scenario, implement secure network designs.



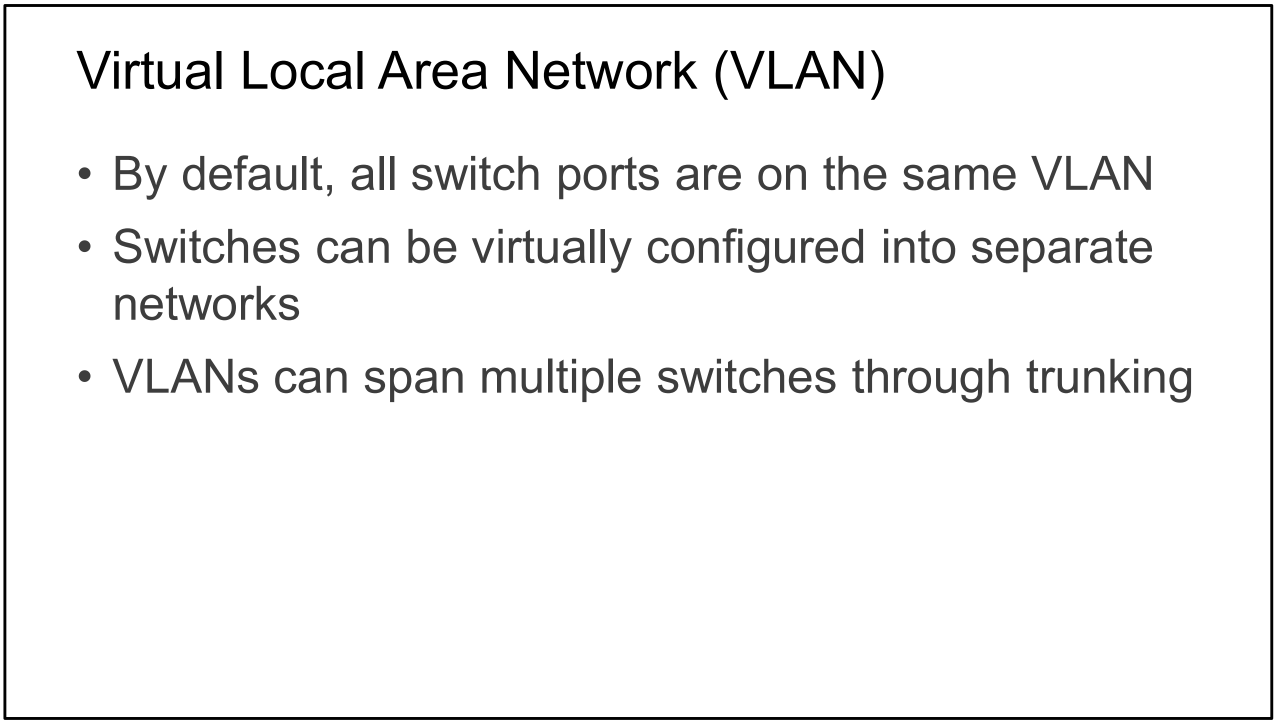
Network Configuration Management

- Zero trust
  - Internal networks should be untrusted
  - Make sure employees can recognize scams
  - Use a network IDS/IPS for internal networks



Network Configuration Management

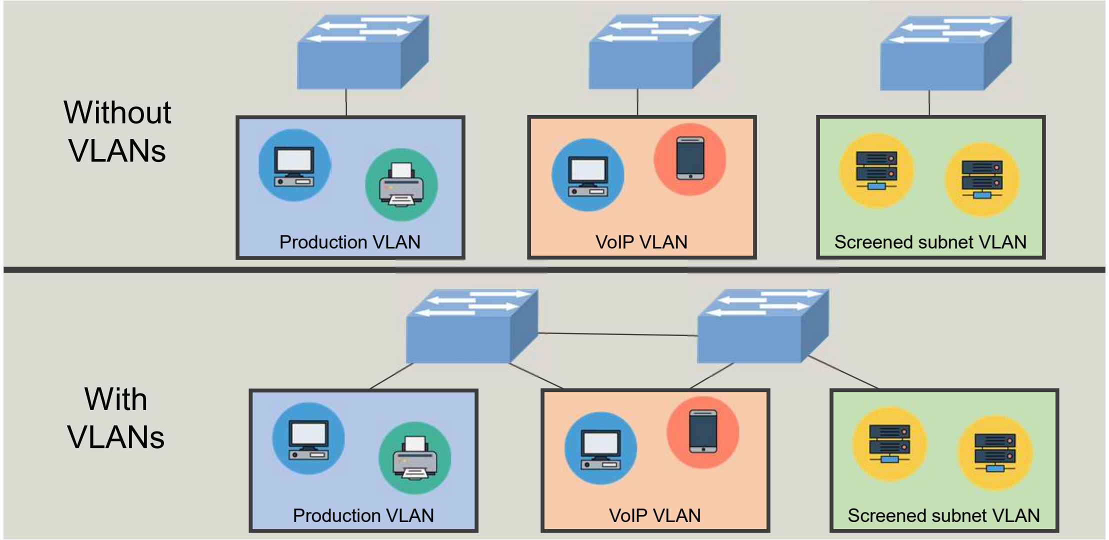
- Network and data flow diagrams
- Naming conventions
  - Servers, routers, switches, etc.
- IP address ranges
  - Address usage within each range
    - Example: routers are always x.y.z.253



Virtual Local Area Network (VLAN)

- By default, all switch ports are on the same VLAN
- Switches can be virtually configured into separate networks
- VLANs can span multiple switches through trunking

VLANs



Without VLANs

Production VLAN

VoIP VLAN

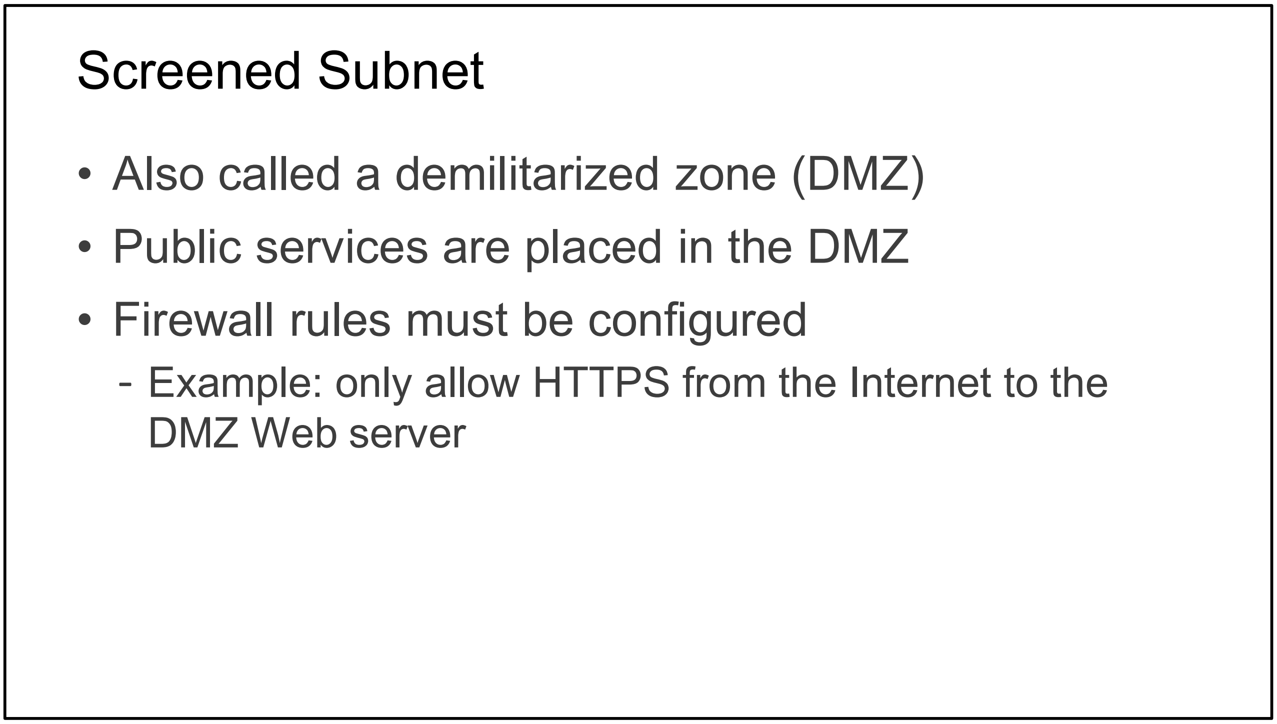
Screened subnet VLAN

With VLANs

Production VLAN

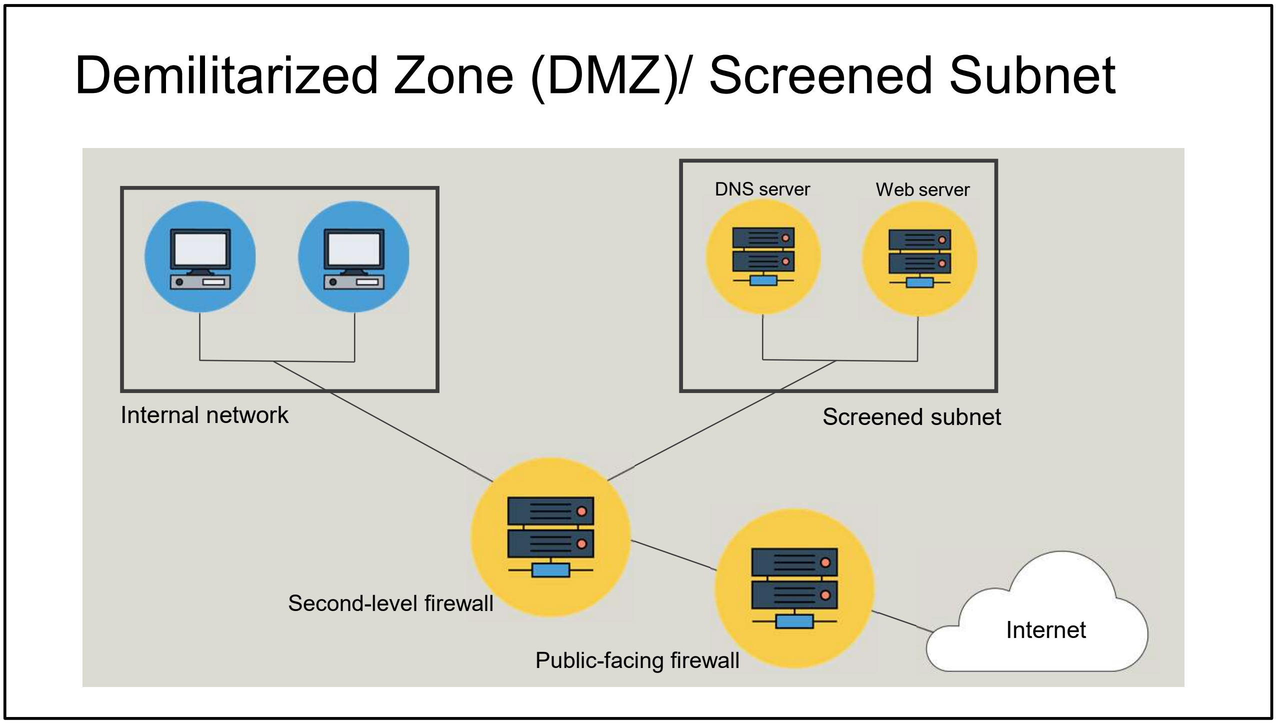
VoIP VLAN

Screened subnet VLAN

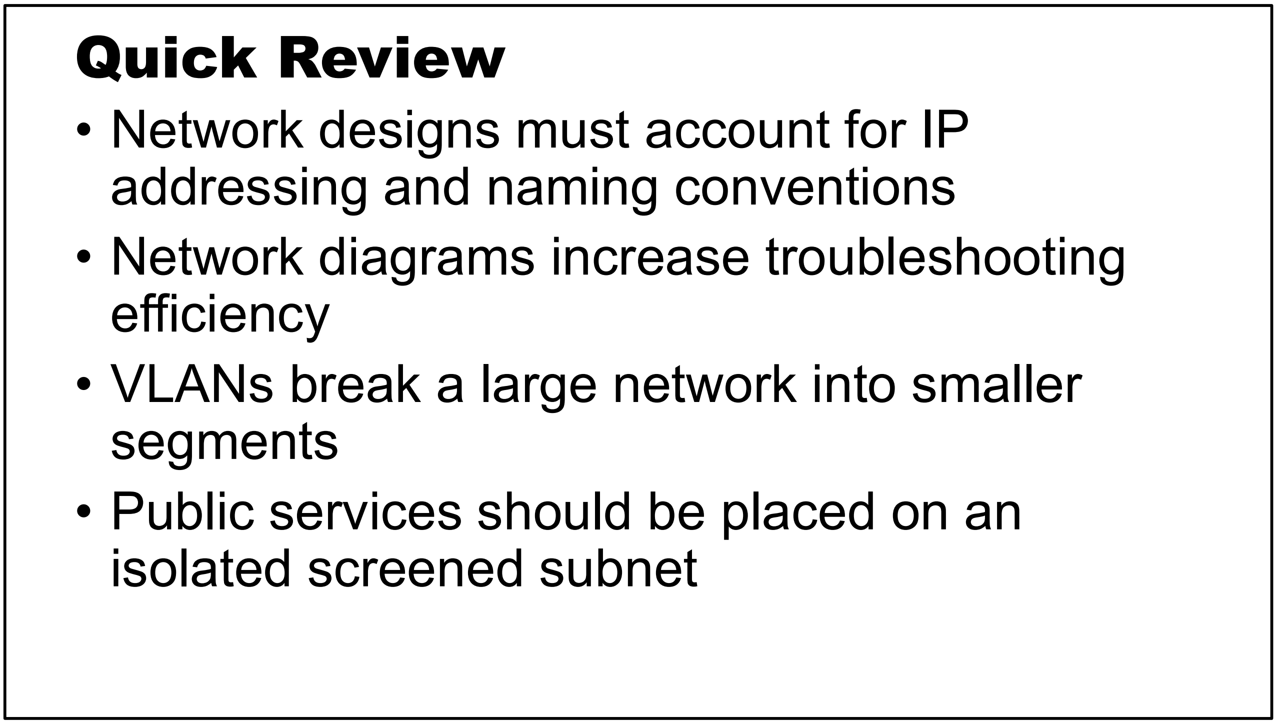


Screened Subnet

- Also called a demilitarized zone (DMZ)
- Public services are placed in the DMZ
- Firewall rules must be configured
  - Example: only allow HTTPS from the Internet to the DMZ Web server

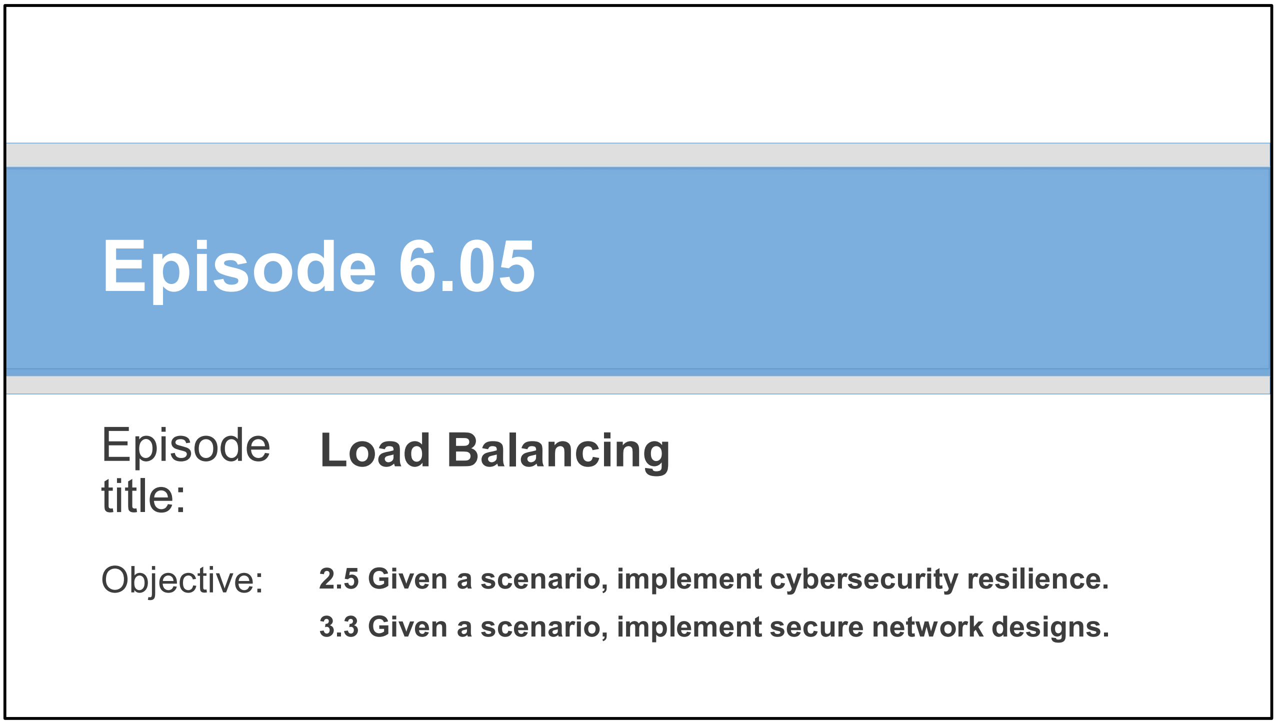


Demilitarized Zone (DMZ)/ Screened Subnet



Quick Review

- Network designs must account for IP addressing and naming conventions
- Network diagrams increase troubleshooting efficiency
- VLANs break a large network into smaller segments
- Public services should be placed on an isolated screened subnet

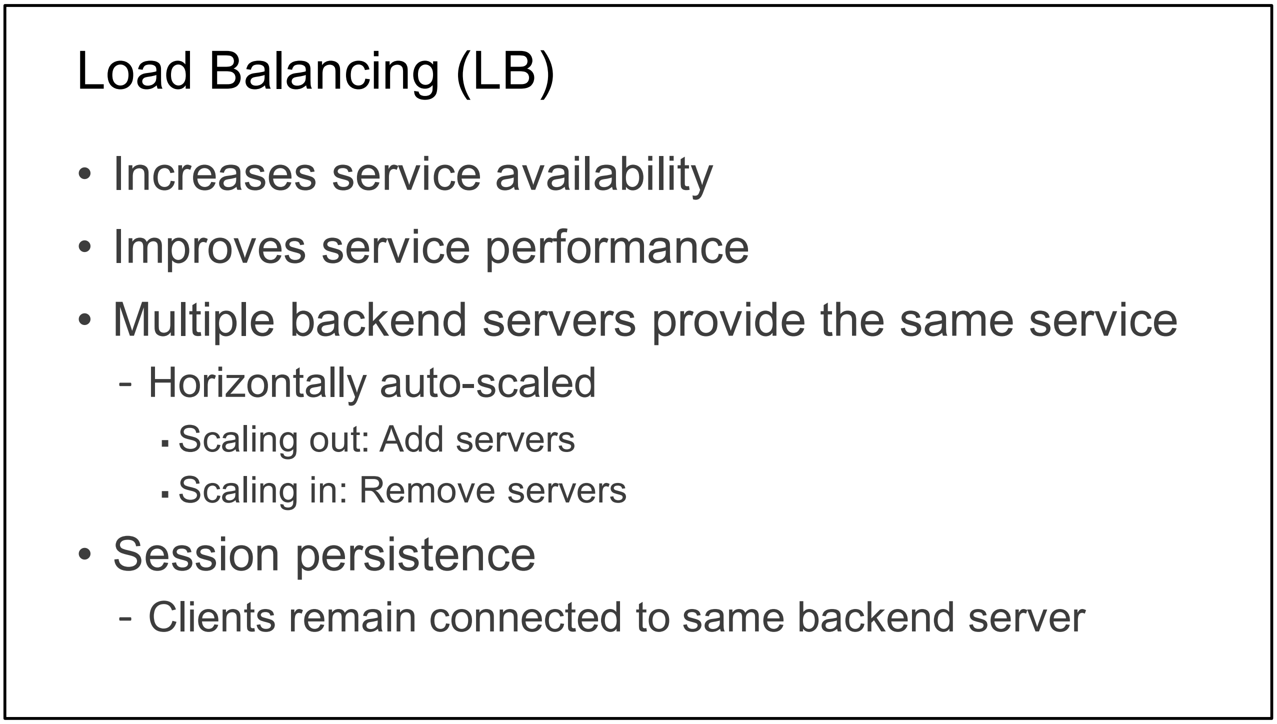


Episode 6.05

Episode title: **Load Balancing**

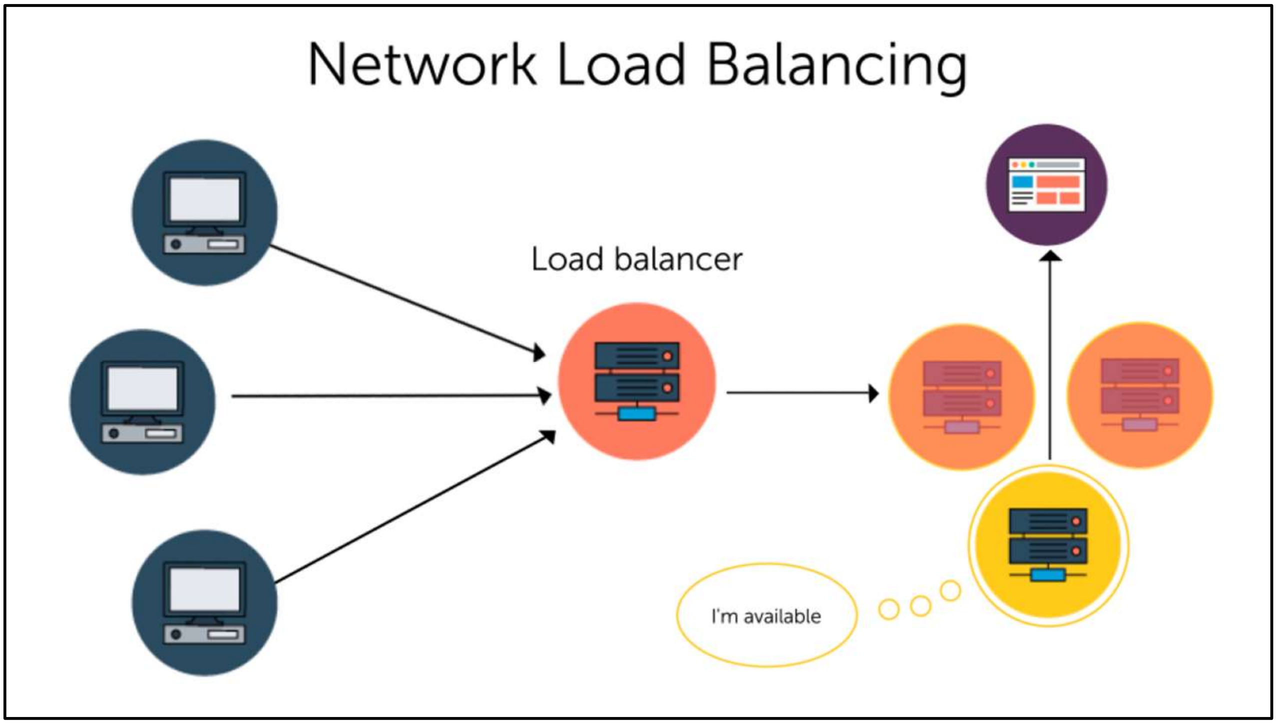
Objective: **2.5 Given a scenario, implement cybersecurity resilience.**

3.3 Given a scenario, implement secure network designs.

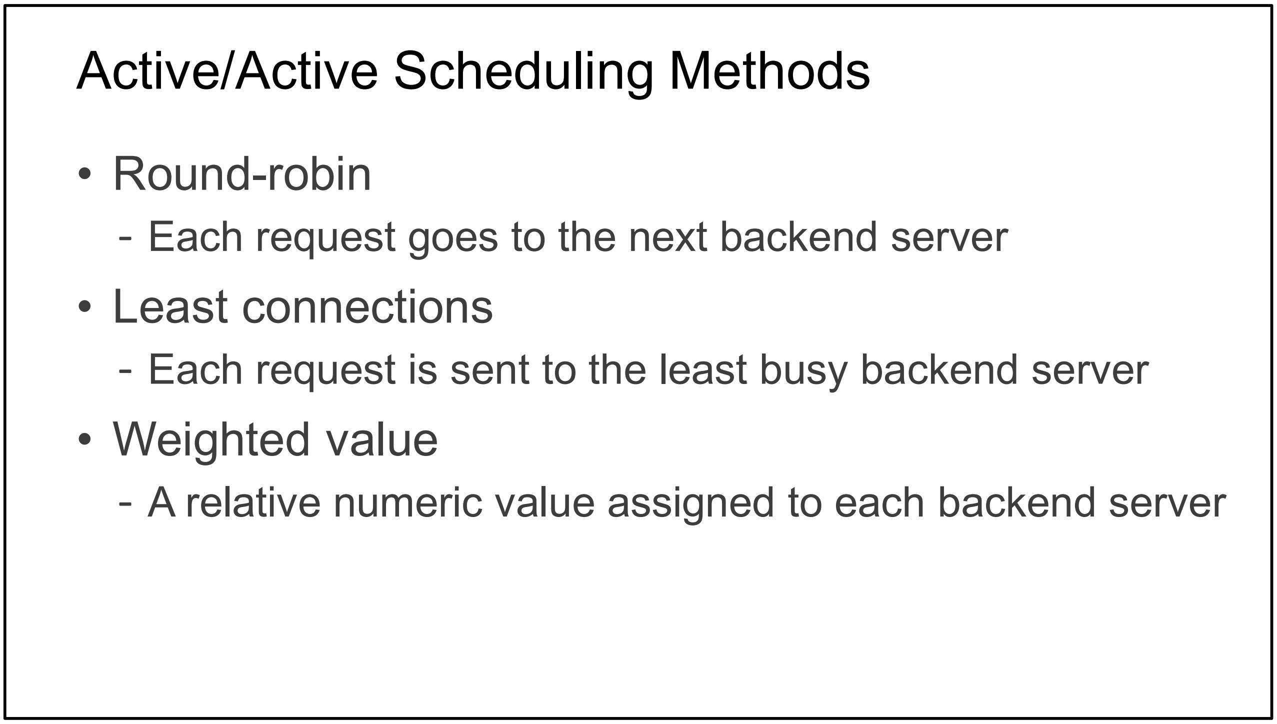


Load Balancing (LB)

- Increases service availability
- Improves service performance
- Multiple backend servers provide the same service
  - Horizontally auto-scaled
    - Scaling out: Add servers
    - Scaling in: Remove servers
- Session persistence
  - Clients remain connected to same backend server

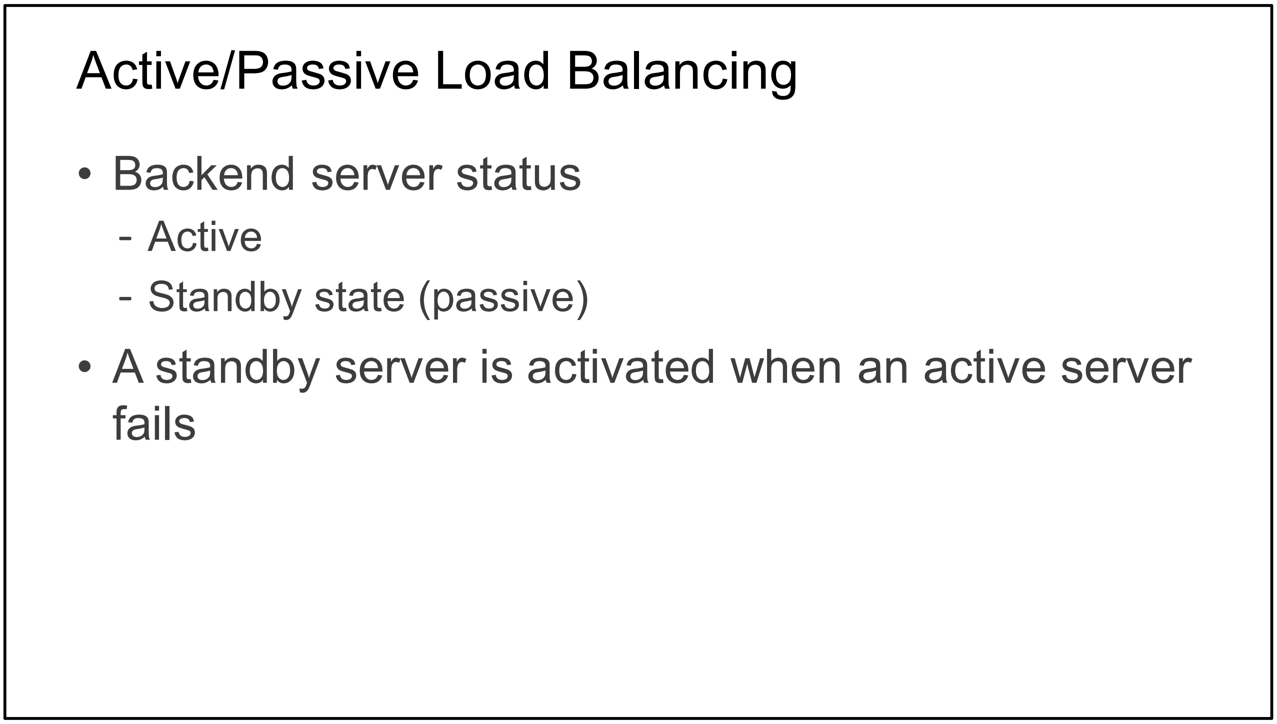


Network Load Balancing



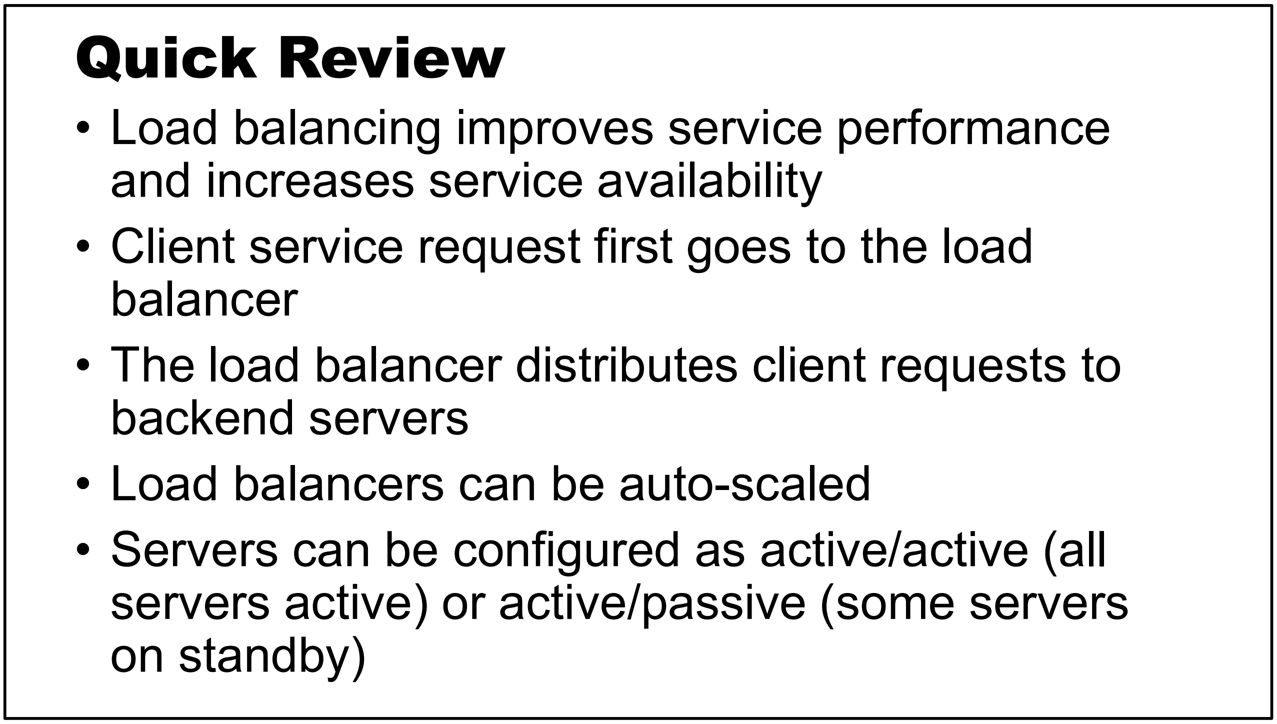
Active/Active Scheduling Methods

- Round-robin
  - Each request goes to the next backend server
- Least connections
  - Each request is sent to the least busy backend server
- Weighted value
  - A relative numeric value assigned to each backend server



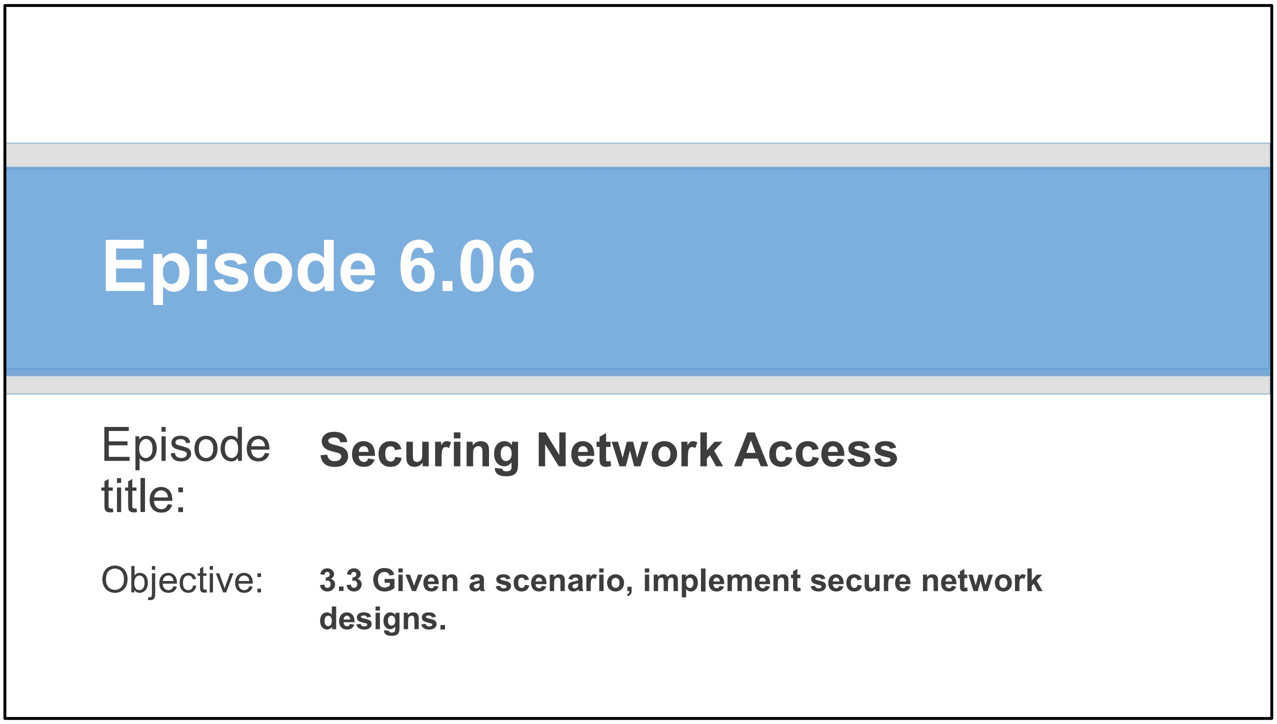
Active/Passive Load Balancing

- Backend server status
  - Active
  - Standby state (passive)
- A standby server is activated when an active server fails



Quick Review

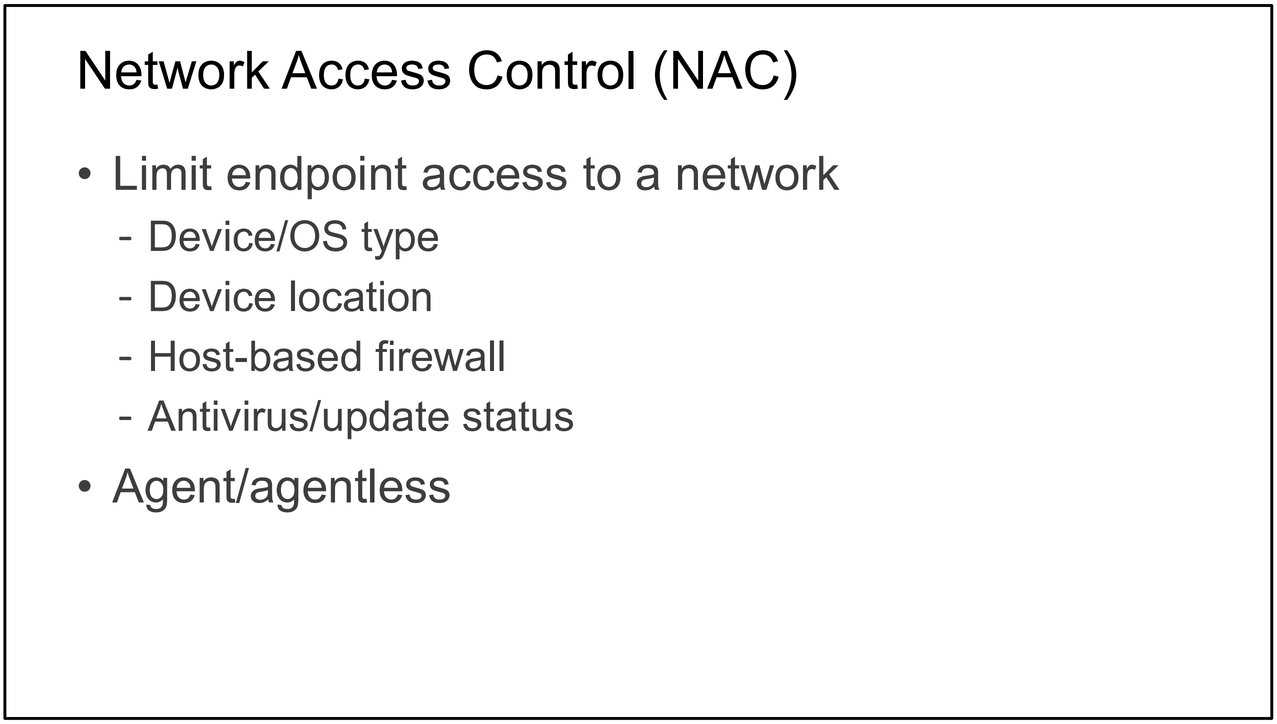
- Load balancing improves service performance and increases service availability
- Client service request first goes to the load balancer
- The load balancer distributes client requests to backend servers
- Load balancers can be auto-scaled
- Servers can be configured as active/active (all servers active) or active/passive (some servers on standby)



Episode 6.06

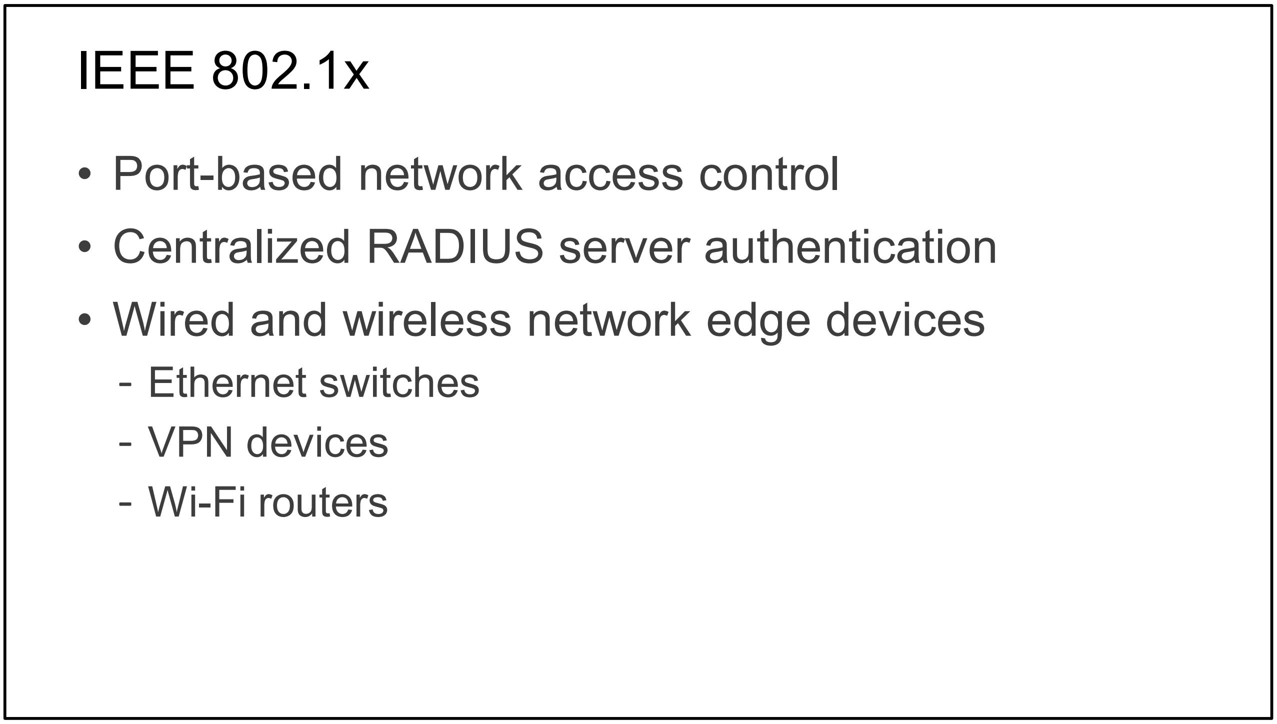
Episode title: **Securing Network Access**

Objective: **3.3 Given a scenario, implement secure network designs.**



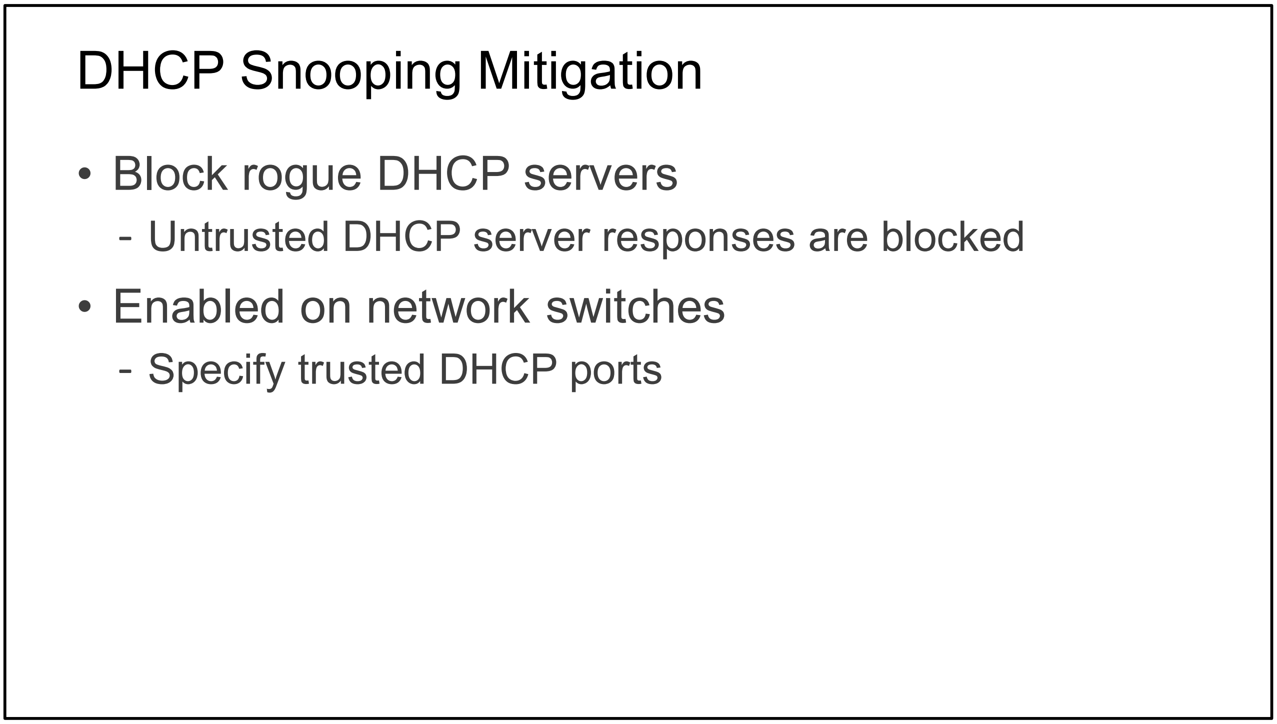
Network Access Control (NAC)

- Limit endpoint access to a network
  - Device/OS type
  - Device location
  - Host-based firewall
  - Antivirus/update status
- Agent/agentless



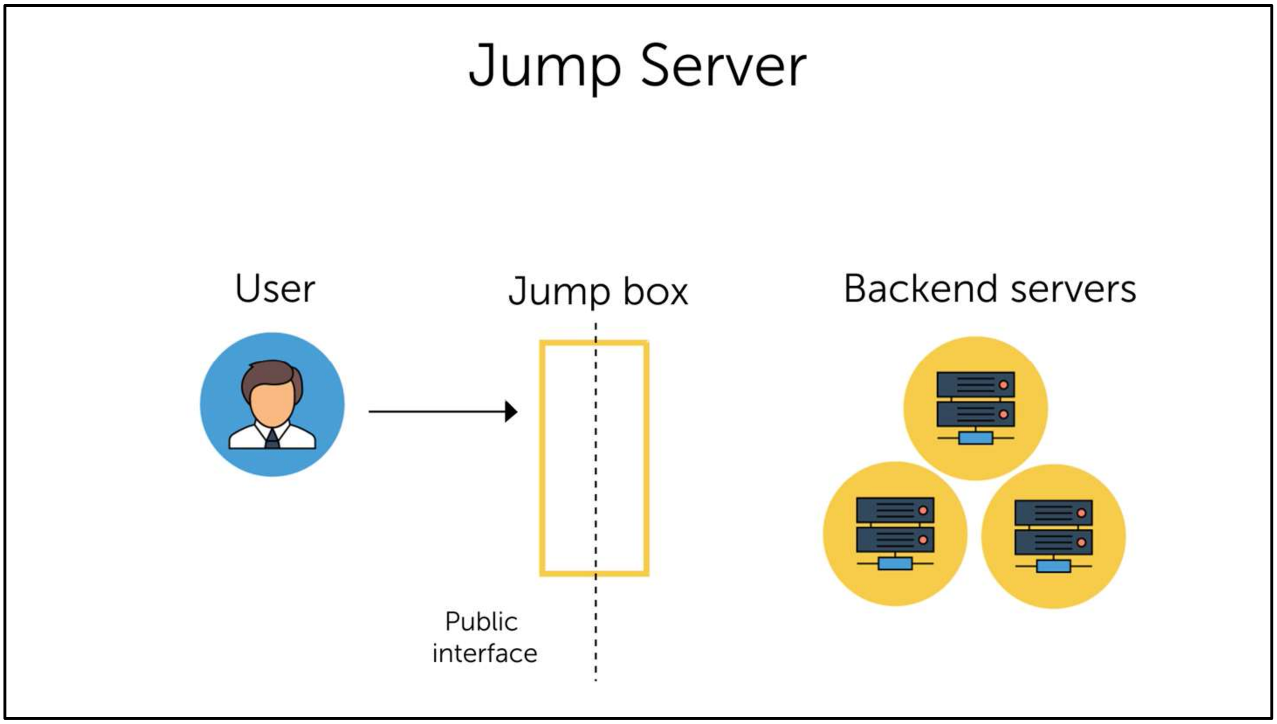
IEEE 802.1x

- Port-based network access control
- Centralized RADIUS server authentication
- Wired and wireless network edge devices
  - Ethernet switches
  - VPN devices
  - Wi-Fi routers



DHCP Snooping Mitigation

- Block rogue DHCP servers
  - Untrusted DHCP server responses are blocked
- Enabled on network switches
  - Specify trusted DHCP ports



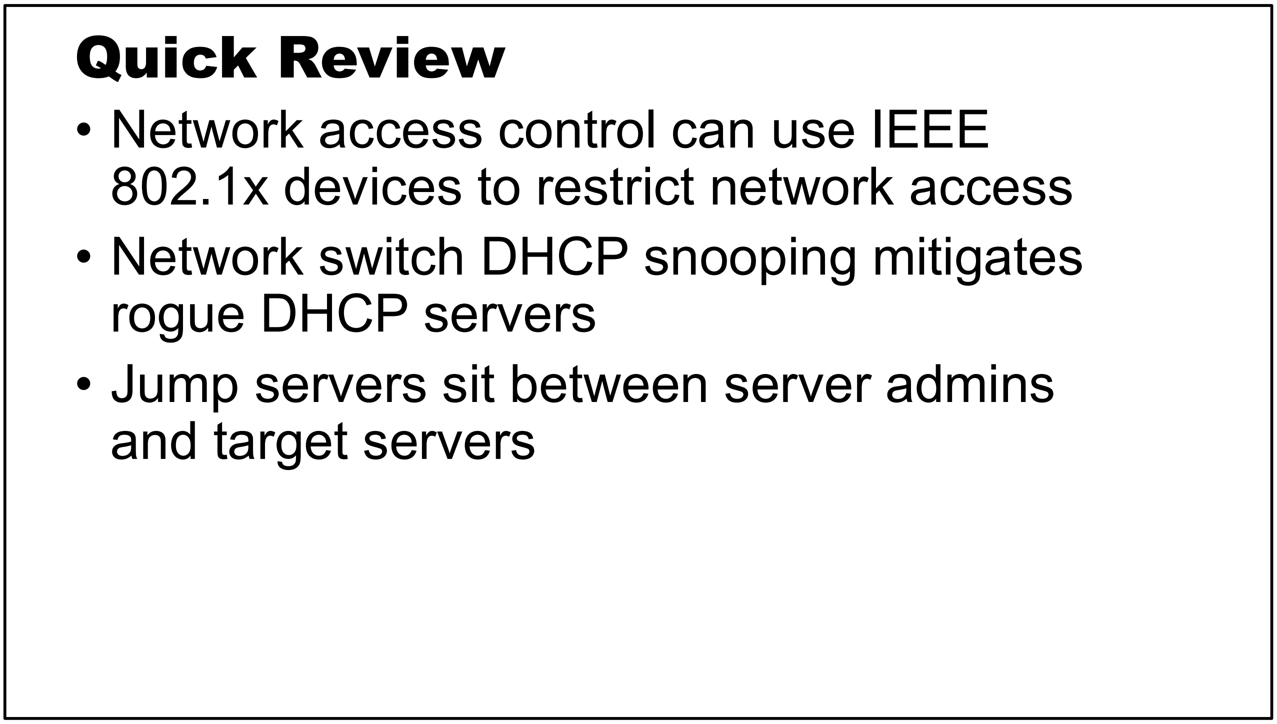
Jump Server

User

Jump box

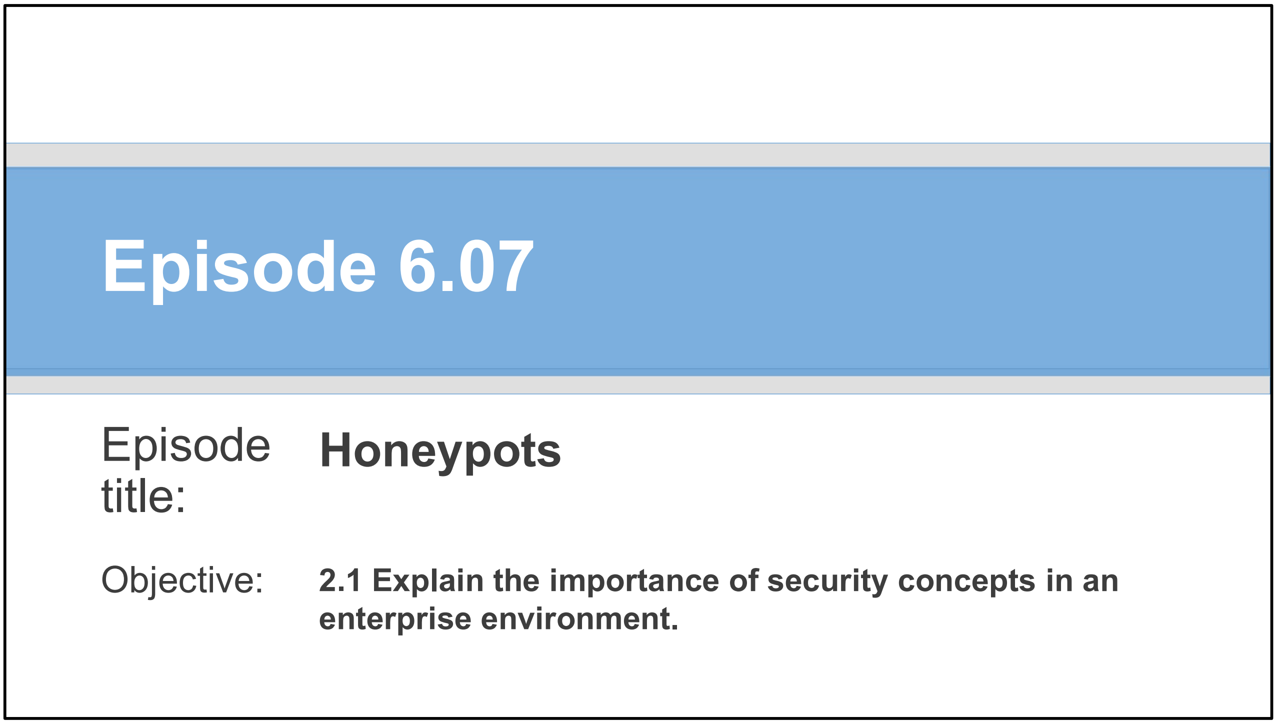
Backend servers

Public interface



Quick Review

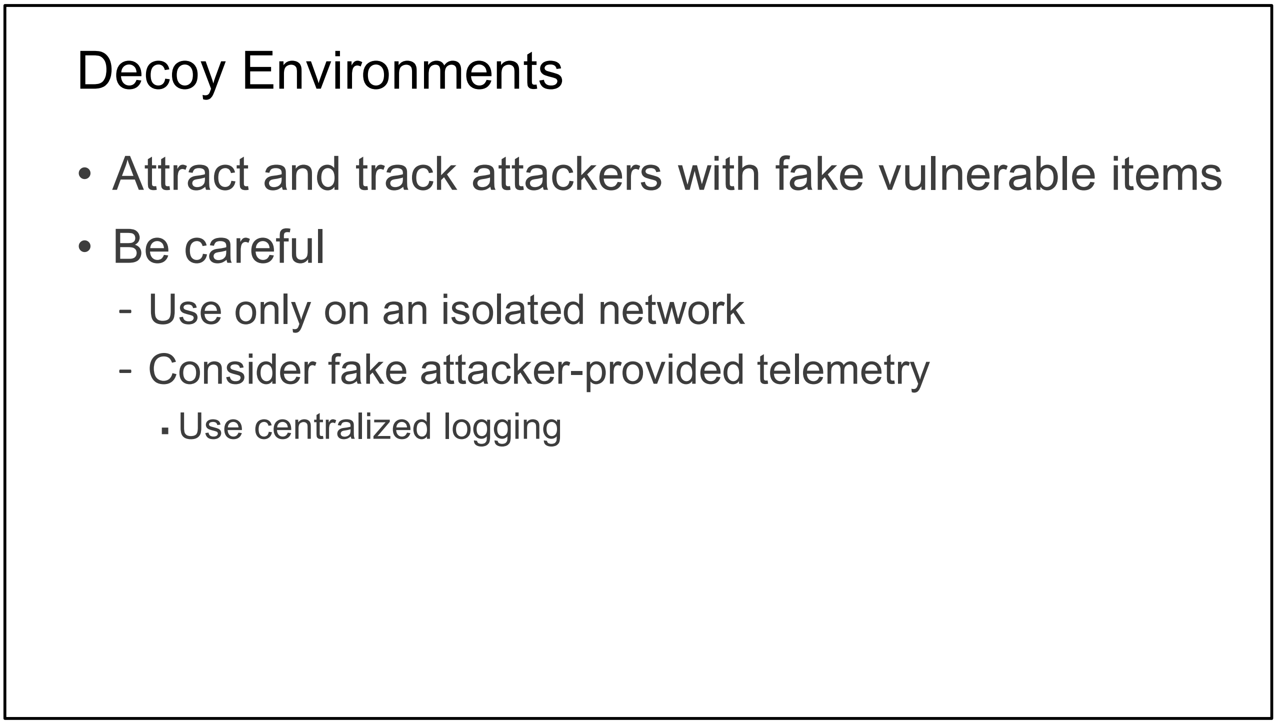
- Network access control can use IEEE 802.1x devices to restrict network access
- Network switch DHCP snooping mitigates rogue DHCP servers
- Jump servers sit between server admins and target servers



Episode 6.07

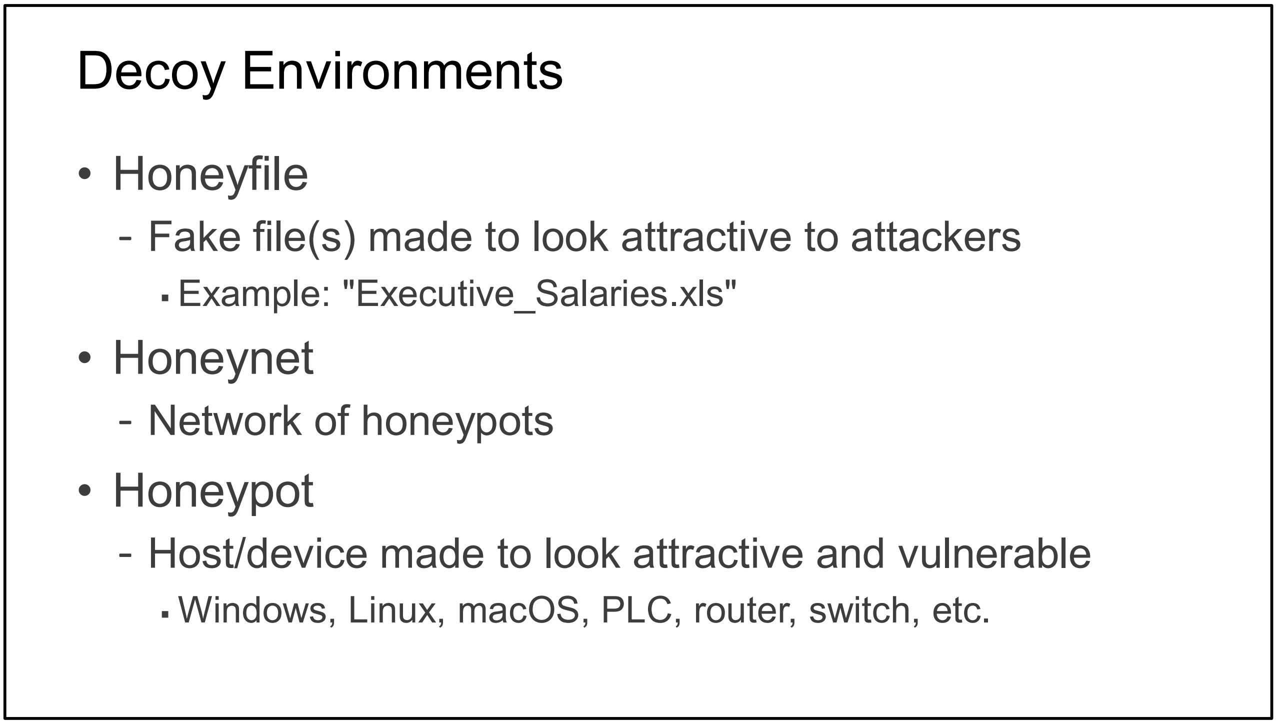
Episode title: **Honeypots**

Objective: **2.1 Explain the importance of security concepts in an enterprise environment.**



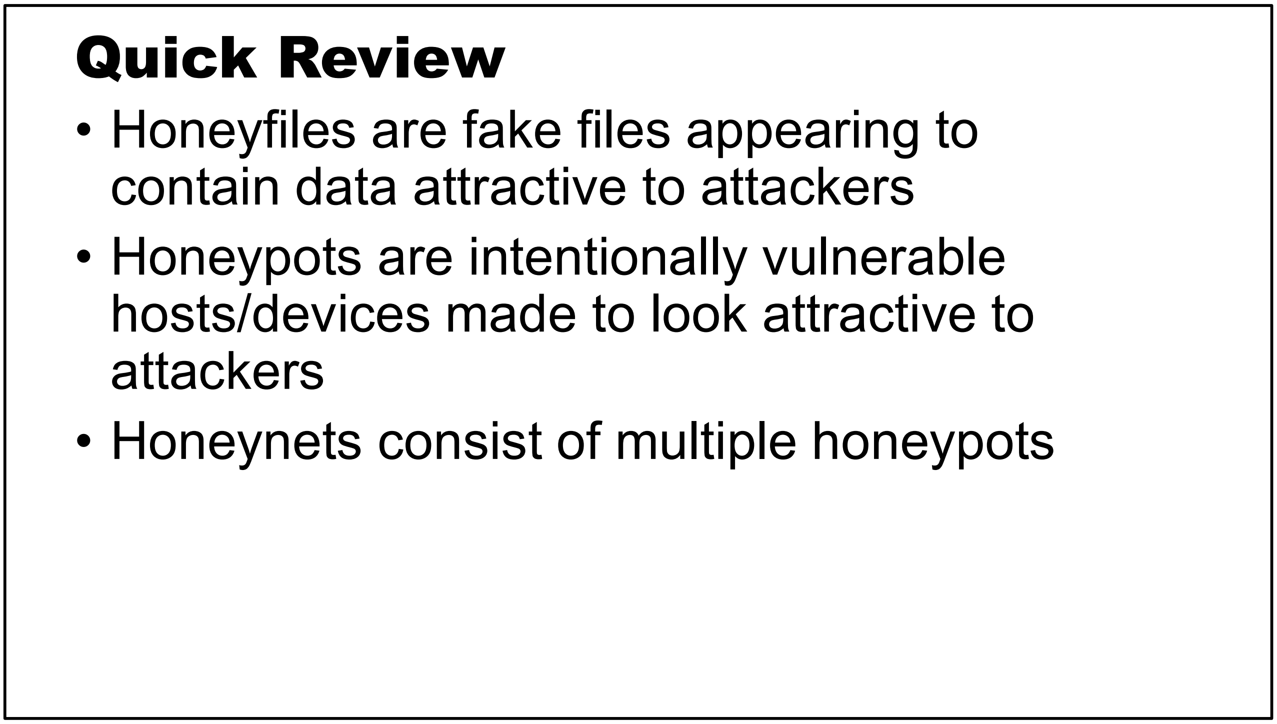
Decoy Environments

- Attract and track attackers with fake vulnerable items
- Be careful
  - Use only on an isolated network
  - Consider fake attacker-provided telemetry
    - Use centralized logging



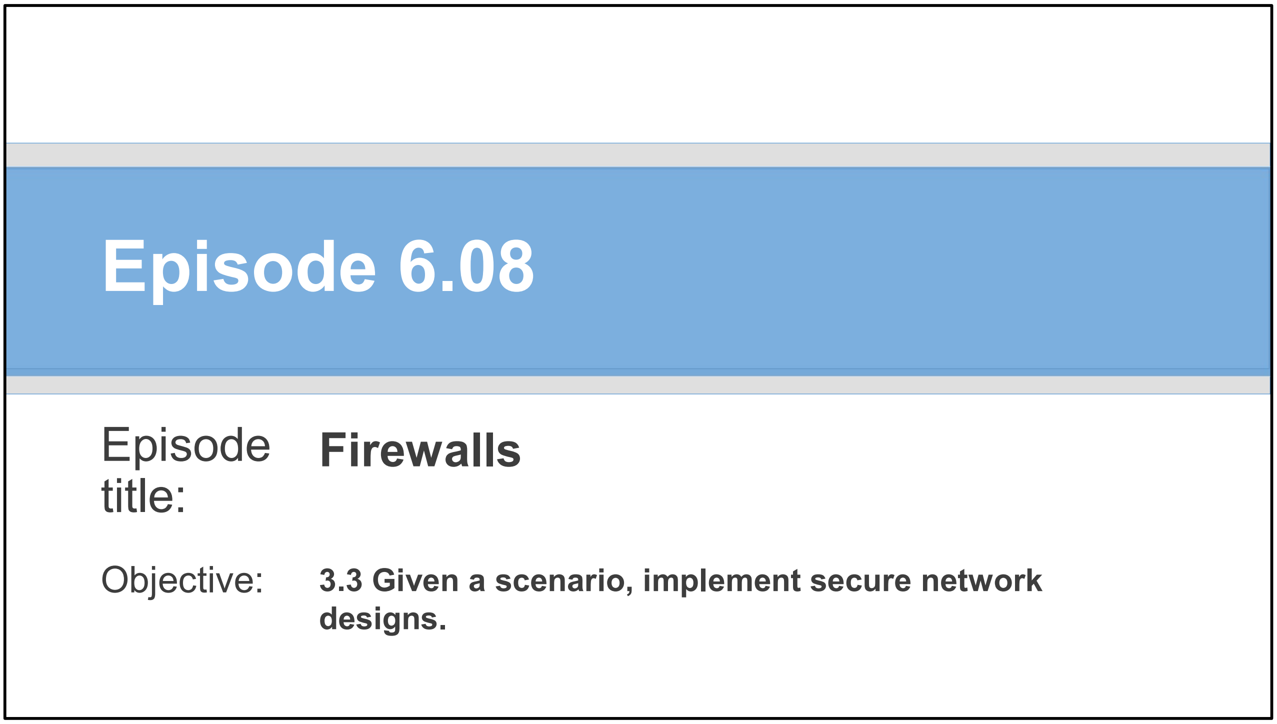
Decoy Environments

- Honeyfile
  - Fake file(s) made to look attractive to attackers
    - Example: "Executive_Salaries.xls"
- Honeynet
  - Network of honeypots
- Honeypot
  - Host/device made to look attractive and vulnerable
    - Windows, Linux, macOS, PLC, router, switch, etc.



Quick Review

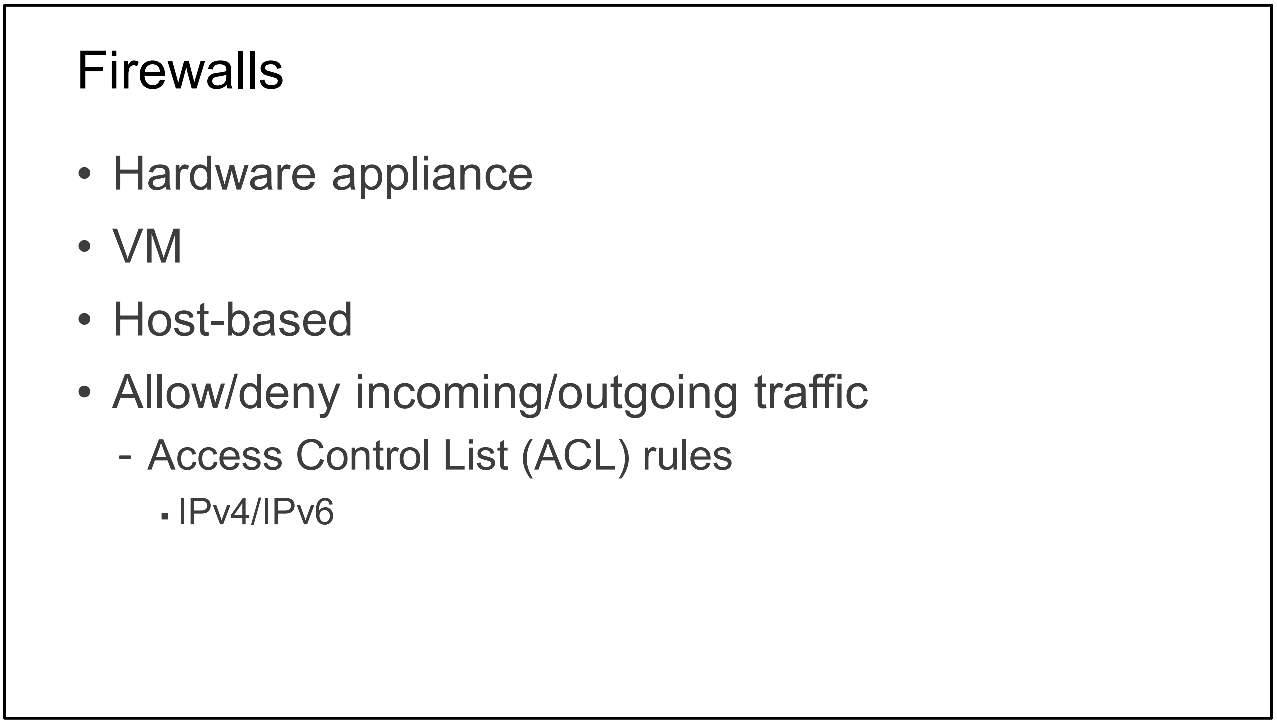
- Honeyfiles are fake files appearing to contain data attractive to attackers
- Honeypots are intentionally vulnerable hosts/devices made to look attractive to attackers
- Honeynets consist of multiple honeypots



Episode 6.08

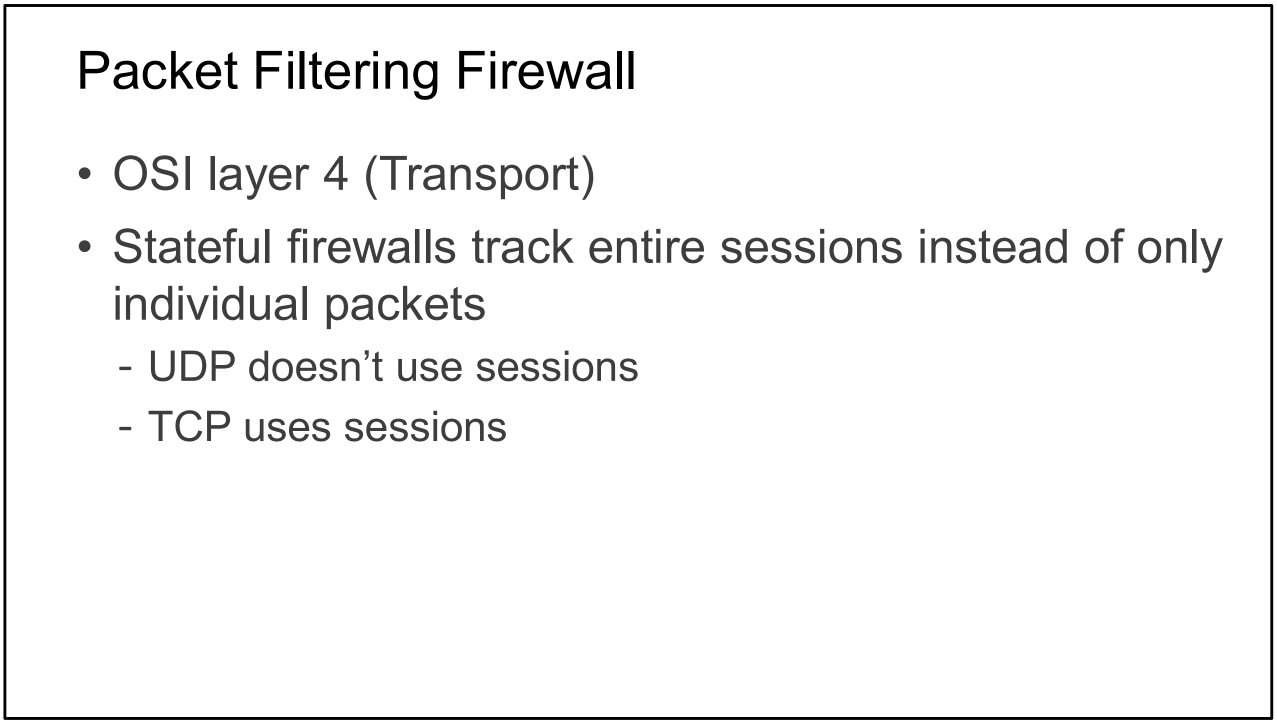
Episode title: **Firewalls**

Objective: **3.3 Given a scenario, implement secure network designs.**



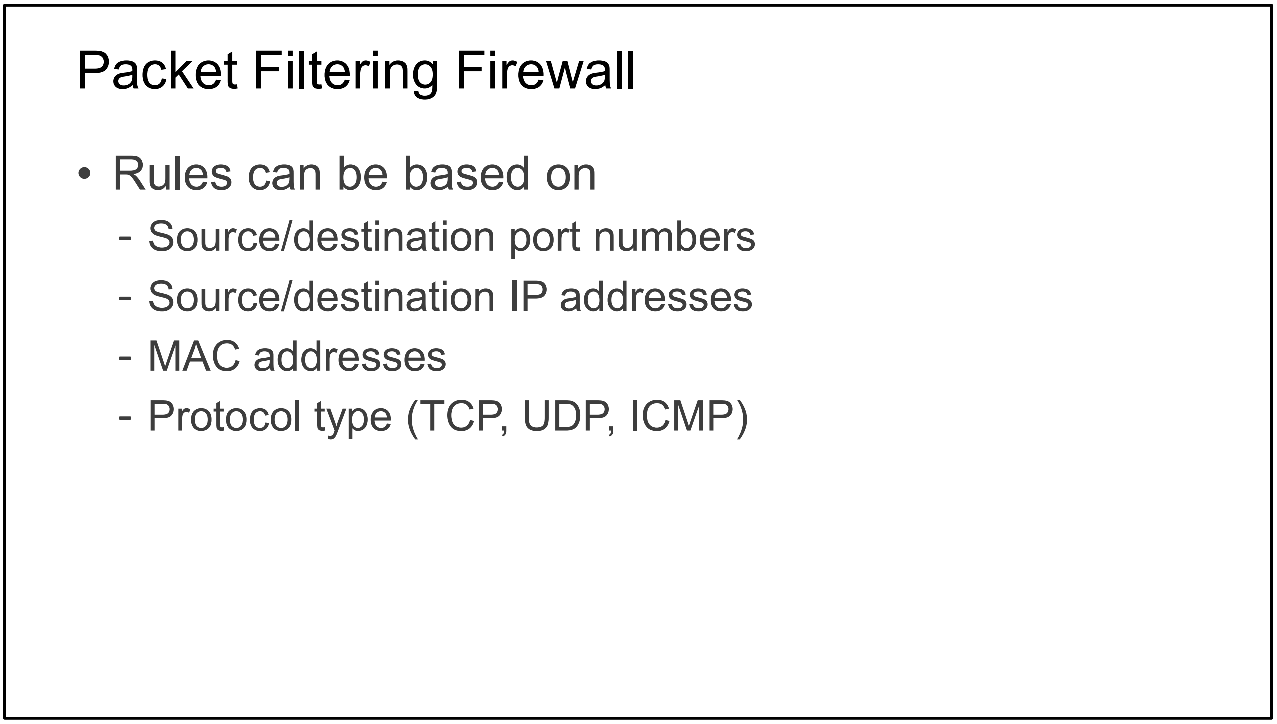
Firewalls

- Hardware appliance
- VM
- Host-based
- Allow/deny incoming/outgoing traffic
  - Access Control List (ACL) rules
    - IPv4/IPv6



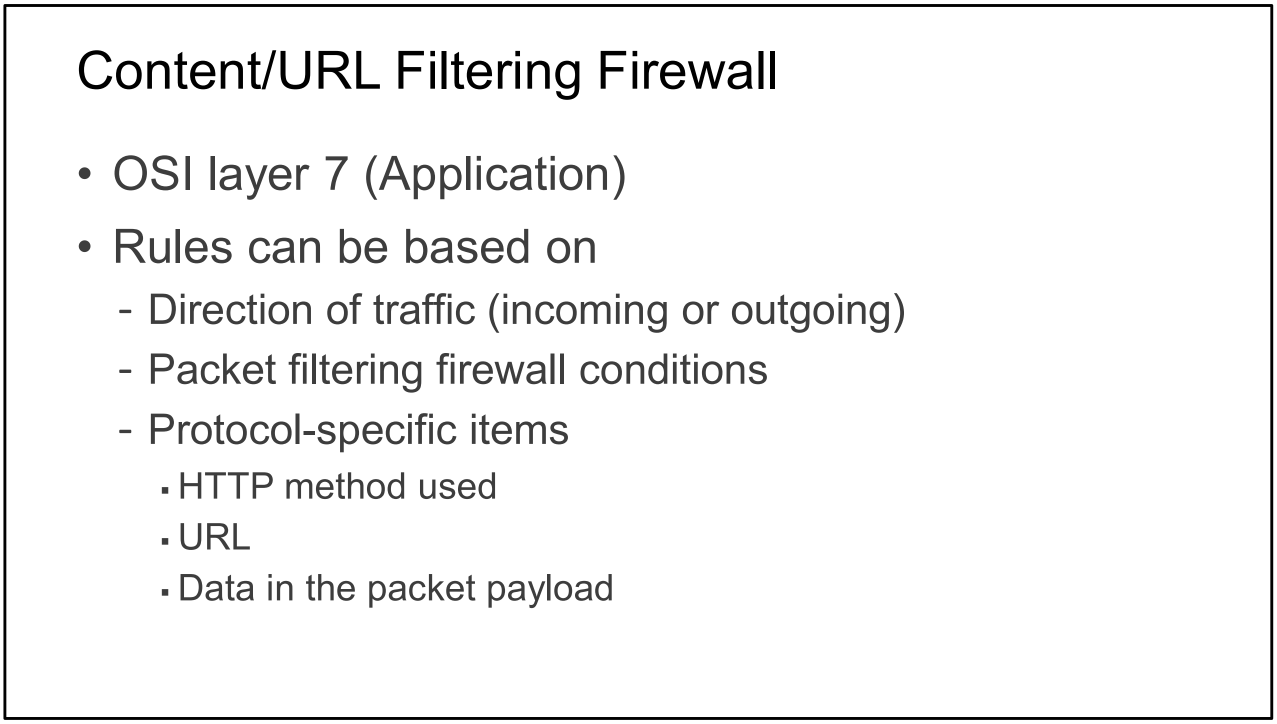
Packet Filtering Firewall

- OSI layer 4 (Transport)
- Stateful firewalls track entire sessions instead of only individual packets
  - UDP doesn’t use sessions
  - TCP uses sessions



Packet Filtering Firewall

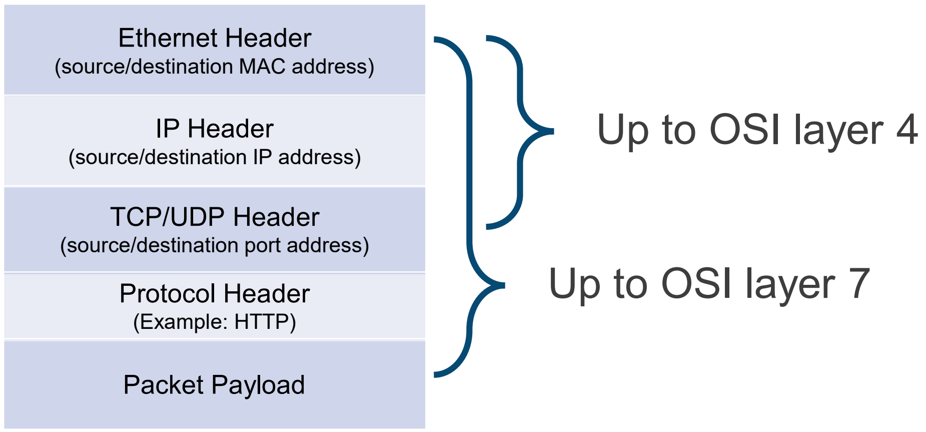
- Rules can be based on
  - Source/destination port numbers
  - Source/destination IP addresses
  - MAC addresses
  - Protocol type (TCP, UDP, ICMP)



Content/URL Filtering Firewall

- OSI layer 7 (Application)
- Rules can be based on
  - Direction of traffic (incoming or outgoing)
  - Packet filtering firewall conditions
  - Protocol-specific items
    - HTTP method used
    - URL
    - Data in the packet payload

Example Packet



Ethernet Header
(source/destination MAC address)

IP Header
(source/destination IP address)

TCP/UDP Header
(source/destination port address)

Protocol Header
(Example: HTTP)

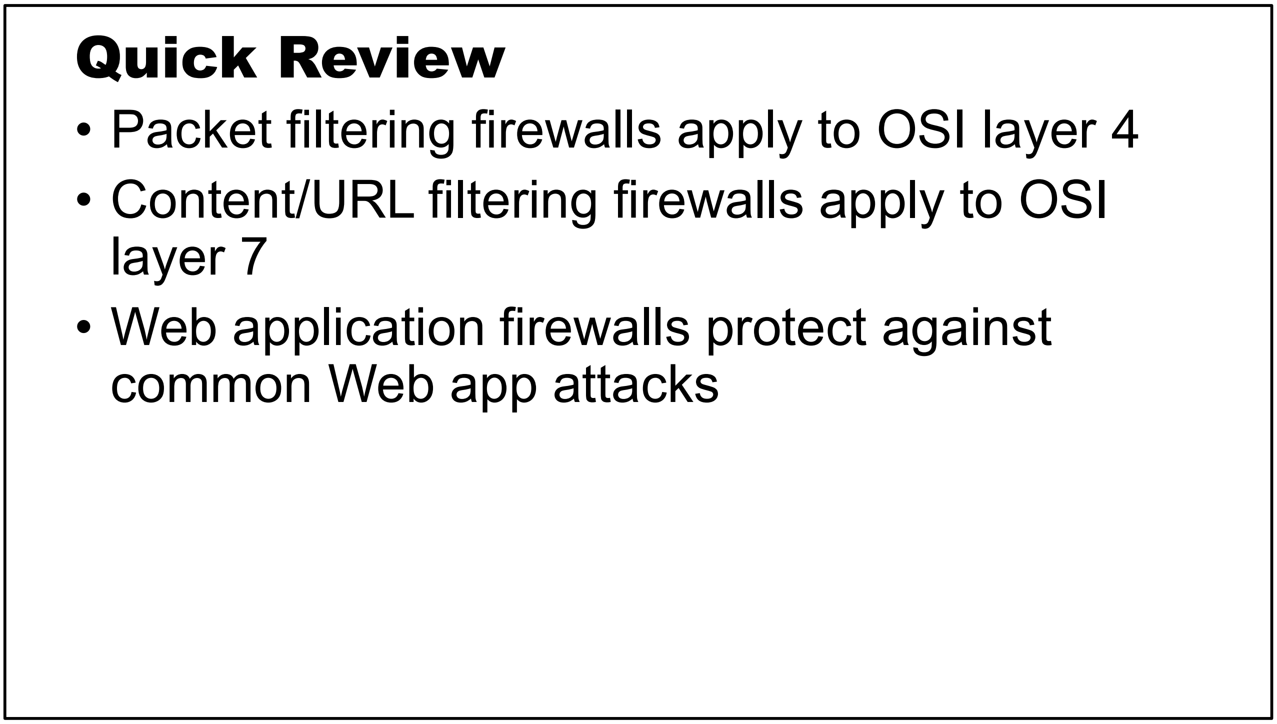
Packet Payload

Up to OSI layer 4

Up to OSI layer 7

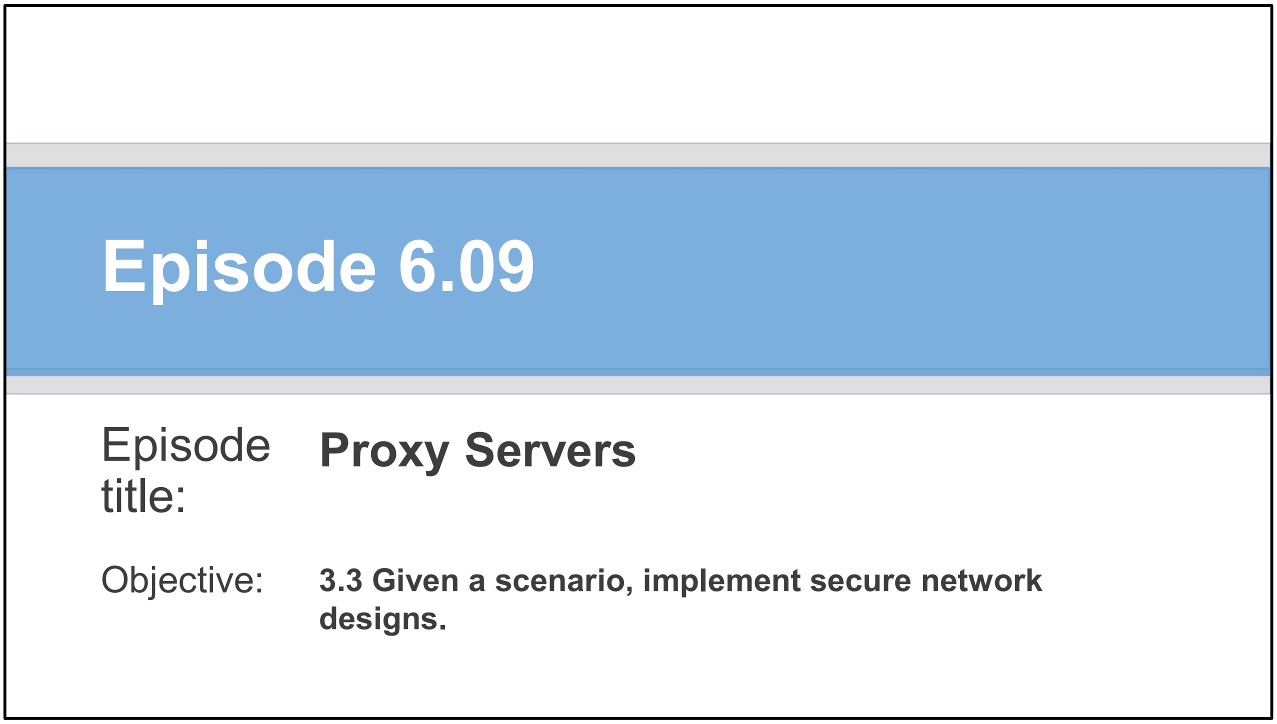
Web Application Firewall (WAF)

- OSI layer 7 (Application)
- Protects against Web app attacks
  - Cross-site scripting (XSS)
  - Cryptographic downgrades
  - Directory traversal
  - SQL injection



Quick Review

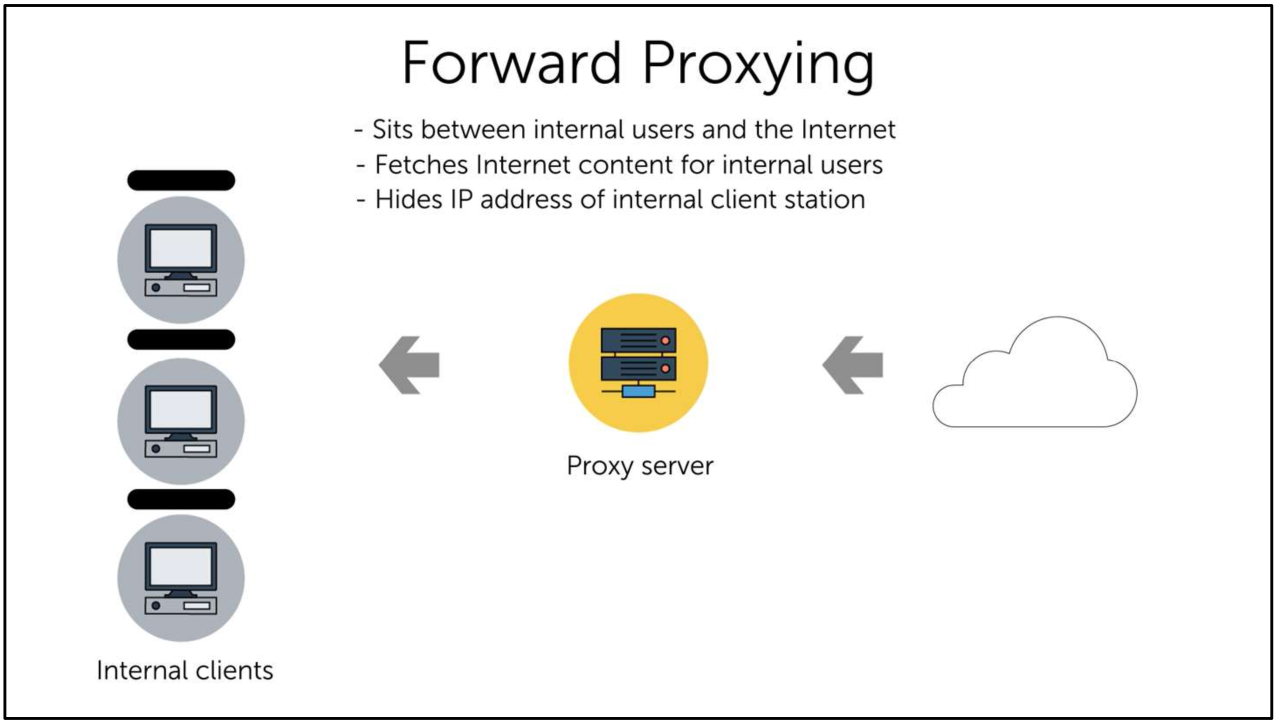
- Packet filtering firewalls apply to OSI layer 4
- Content/URL filtering firewalls apply to OSI layer 7
- Web application firewalls protect against common Web app attacks



Episode 6.09

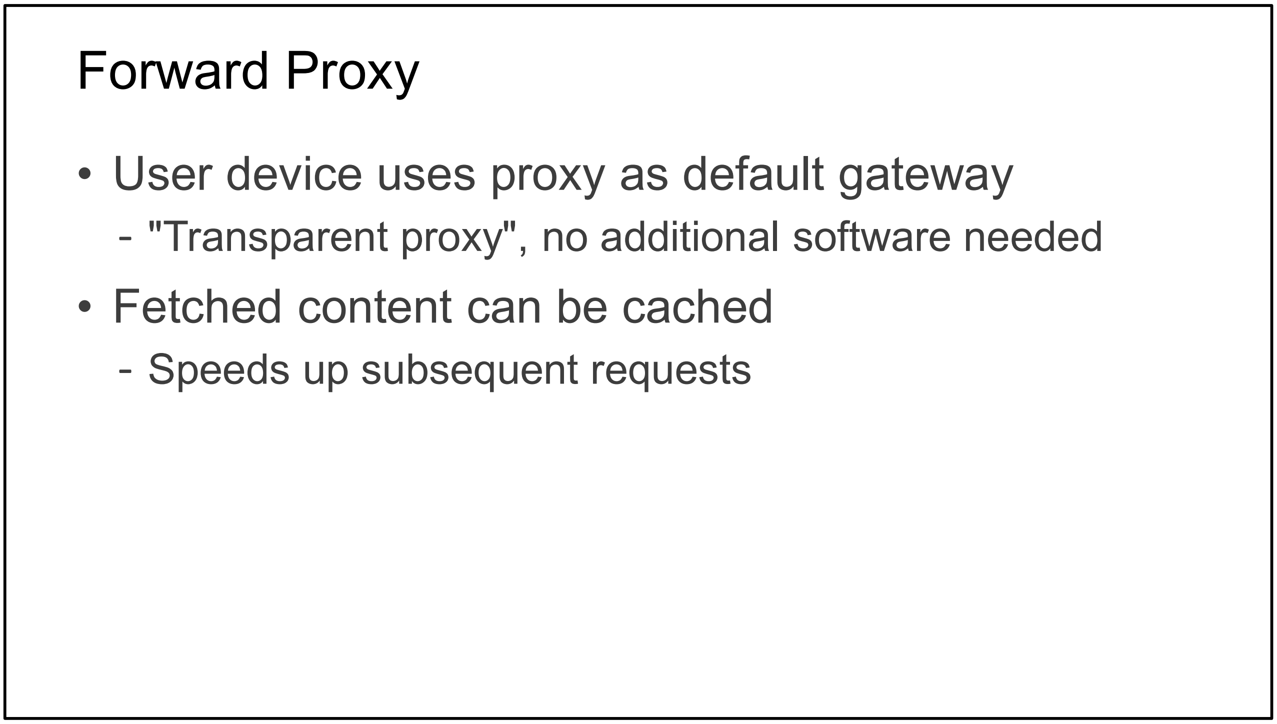
Episode title: **Proxy Servers**

Objective: **3.3 Given a scenario, implement secure network designs.**



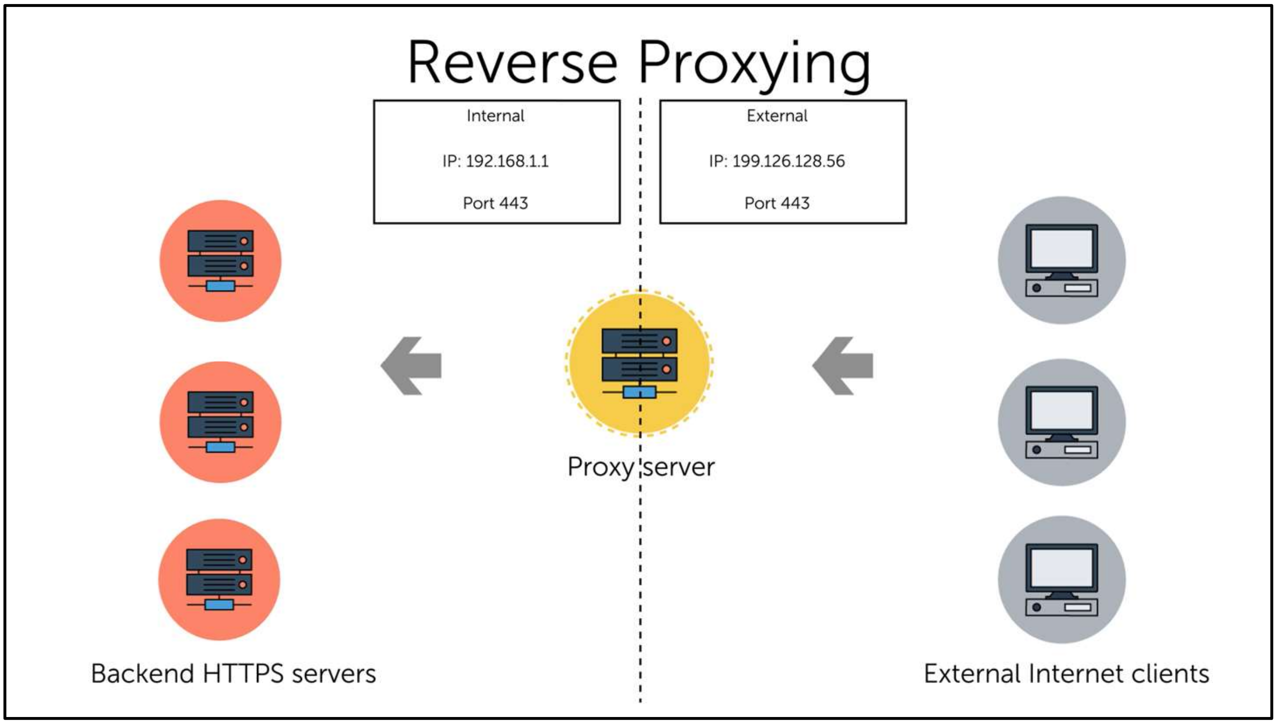
Forward Proxying

- Sits between internal users and the Internet
- Fetches Internet content for internal users
- Hides IP address of internal client station



Forward Proxy

- User device uses proxy as default gateway
  - "Transparent proxy", no additional software needed
- Fetched content can be cached
  - Speeds up subsequent requests



Reverse Proxying

Internal

IP: 192.168.1.1

Port 443

External

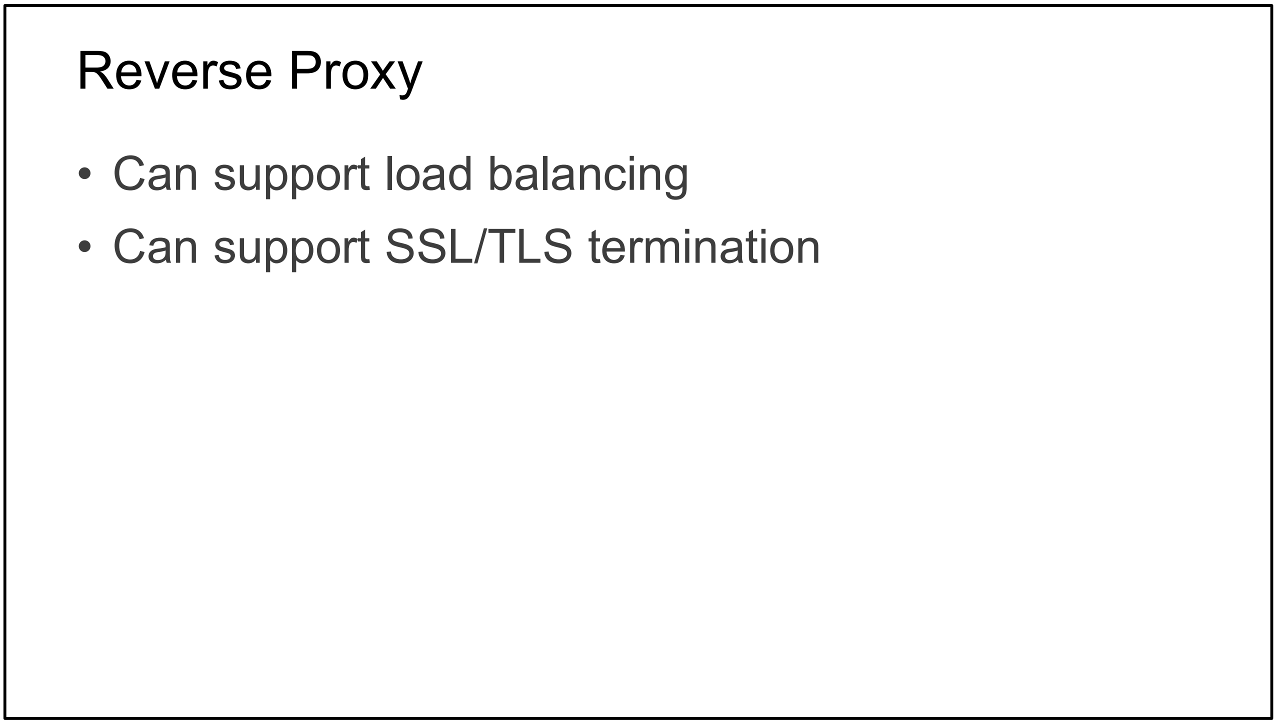
IP: 199.126.128.56

Port 443

Proxy server

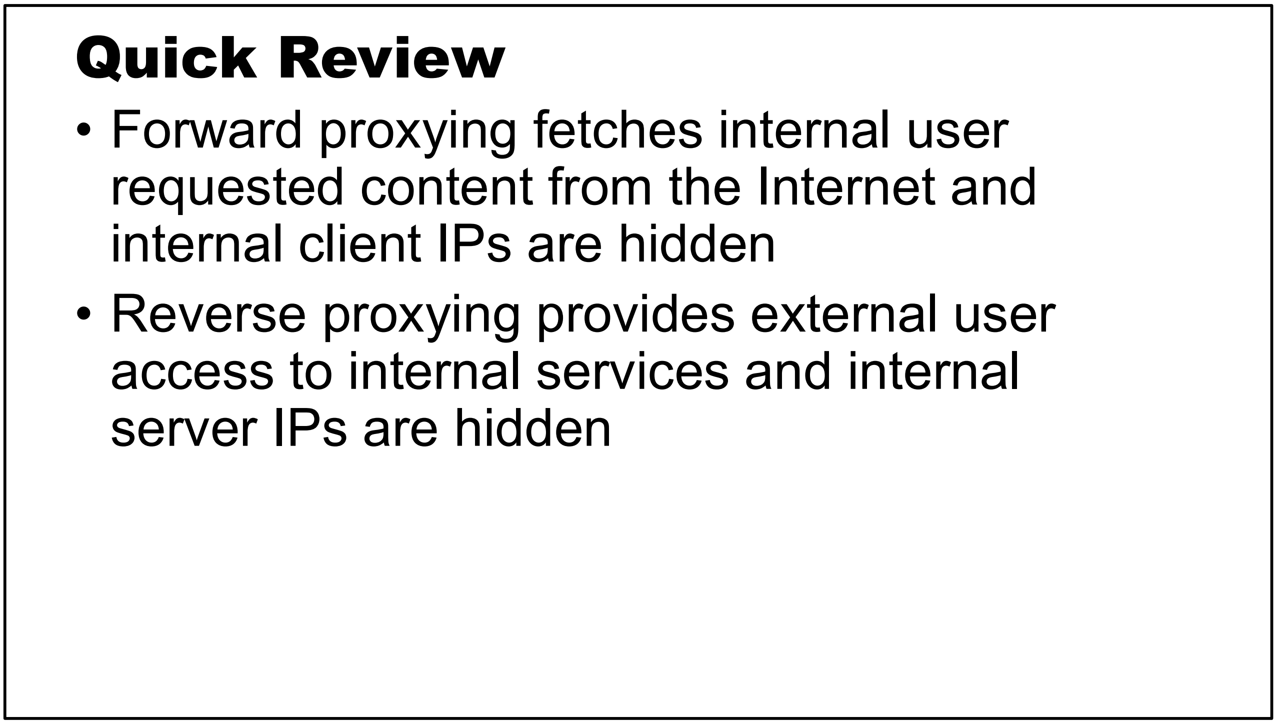
Backend HTTPS servers

External Internet clients



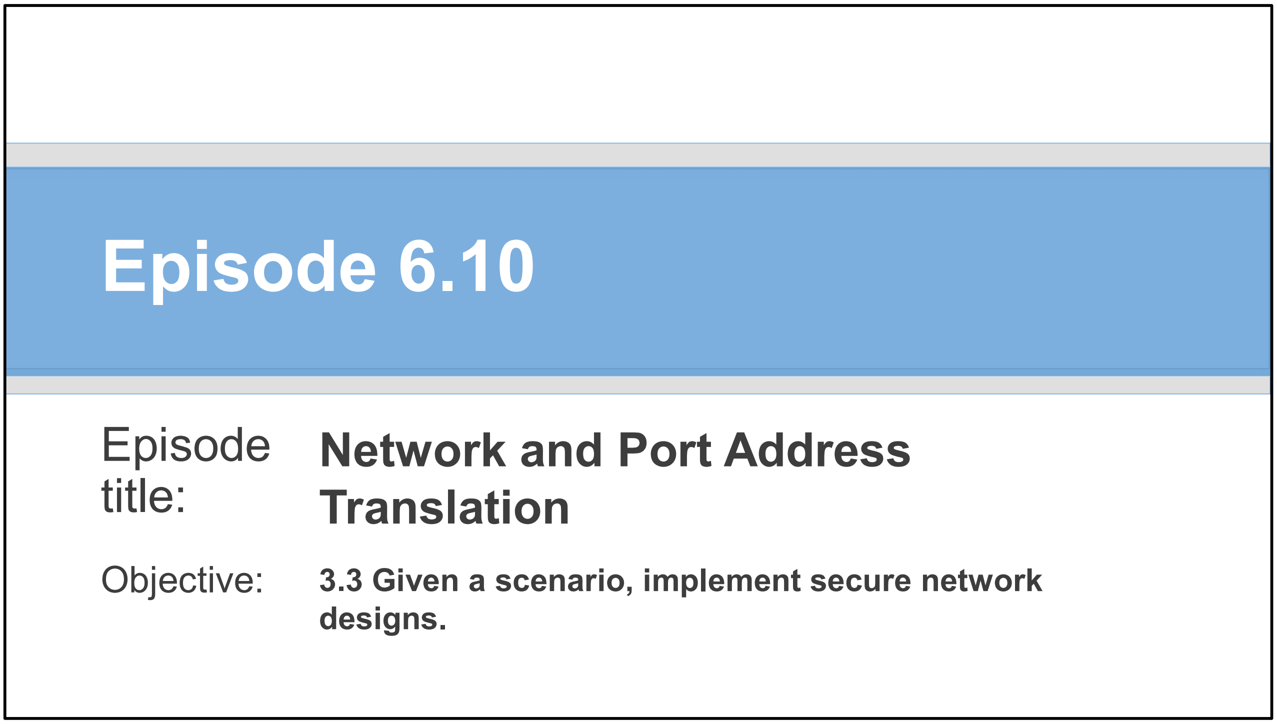
Reverse Proxy

- Can support load balancing
- Can support SSL/TLS termination



Quick Review

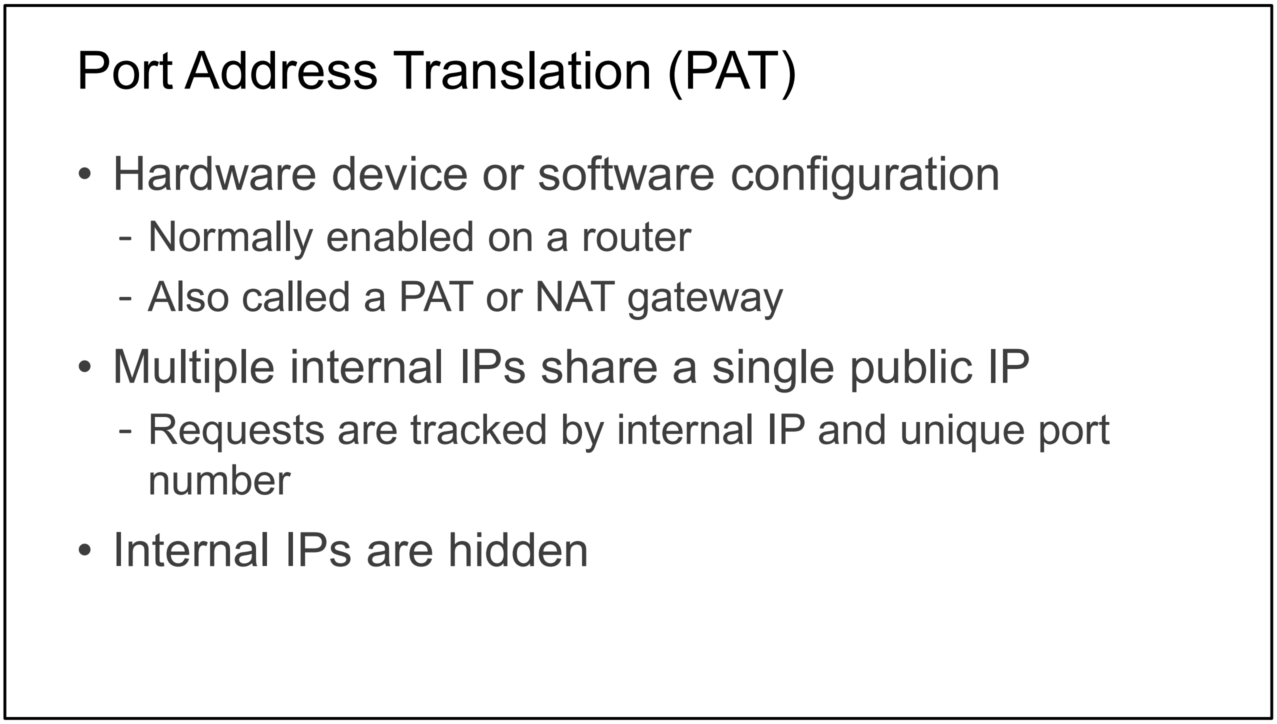
- Forward proxying fetches internal user requested content from the Internet and internal client IPs are hidden
- Reverse proxying provides external user access to internal services and internal server IPs are hidden



Episode 6.10

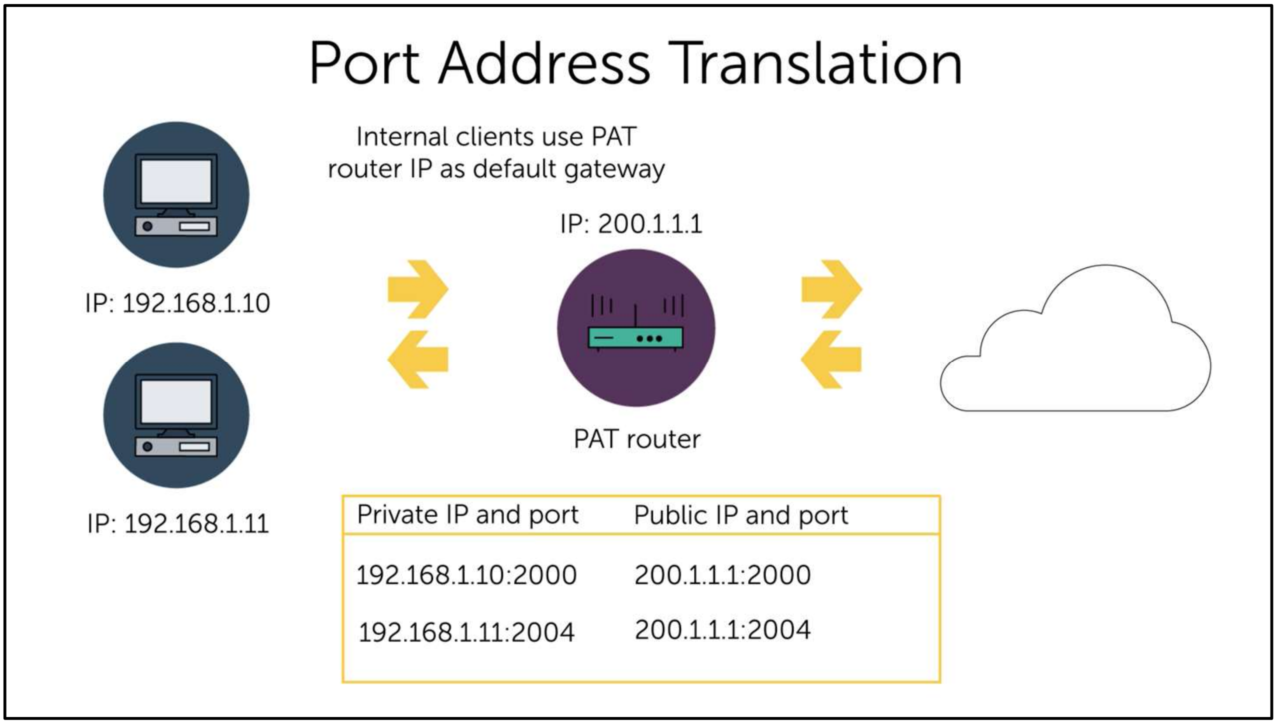
Episode title: **Network and Port Address Translation**

Objective: **3.3 Given a scenario, implement secure network designs.**



Port Address Translation (PAT)

- Hardware device or software configuration
  - Normally enabled on a router
  - Also called a PAT or NAT gateway
- Multiple internal IPs share a single public IP
  - Requests are tracked by internal IP and unique port number
- Internal IPs are hidden



Port Address Translation

Internal clients use PAT router IP as default gateway

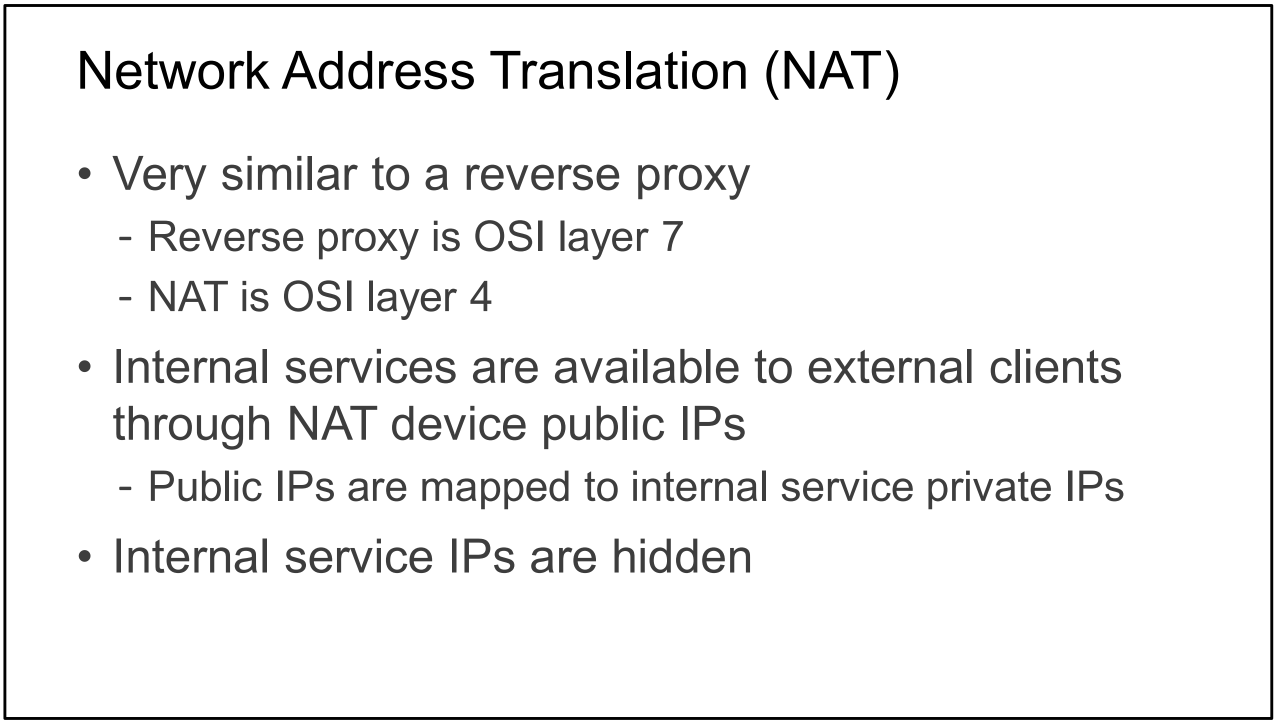
IP: 192.168.1.10

IP: 192.168.1.11

IP: 200.1.1.1

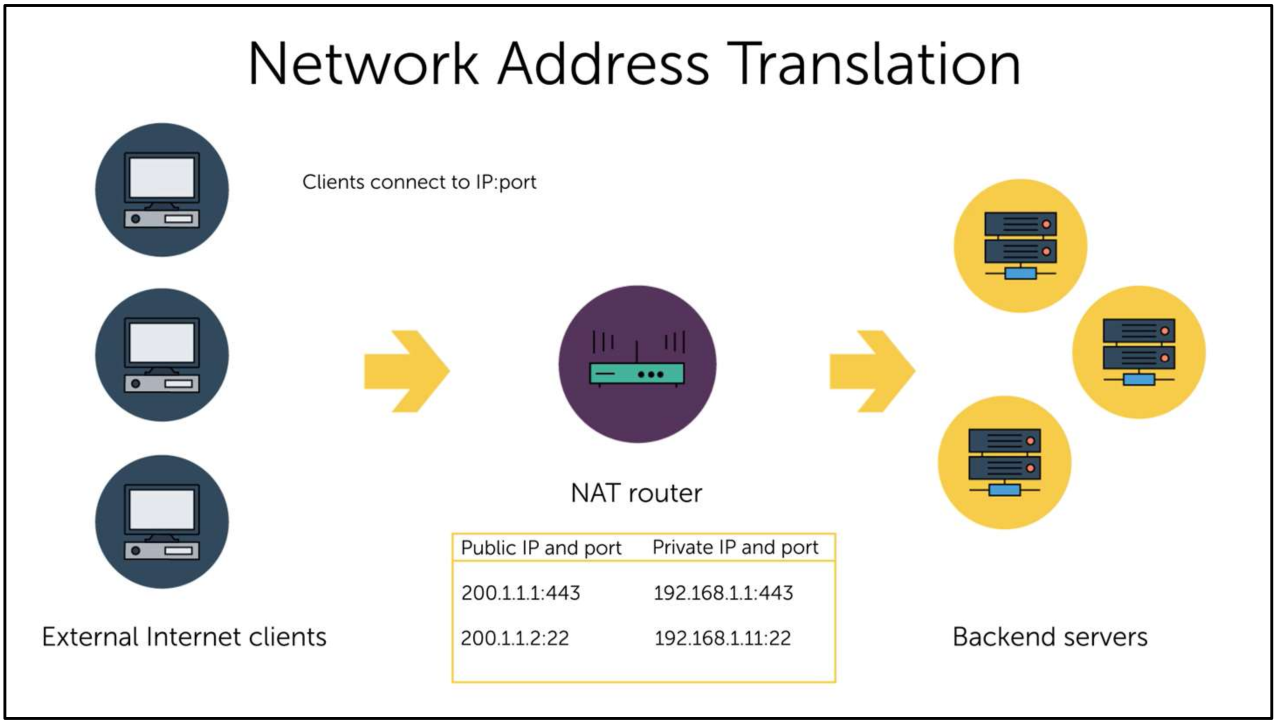
PAT router

Private IP and port	Public IP and port
192.168.1.10:2000	200.1.1.1:2000
192.168.1.11:2004	200.1.1.1:2004



Network Address Translation (NAT)

- Very similar to a reverse proxy
  - Reverse proxy is OSI layer 7
  - NAT is OSI layer 4
- Internal services are available to external clients through NAT device public IPs
  - Public IPs are mapped to internal service private IPs
- Internal service IPs are hidden



Network Address Translation

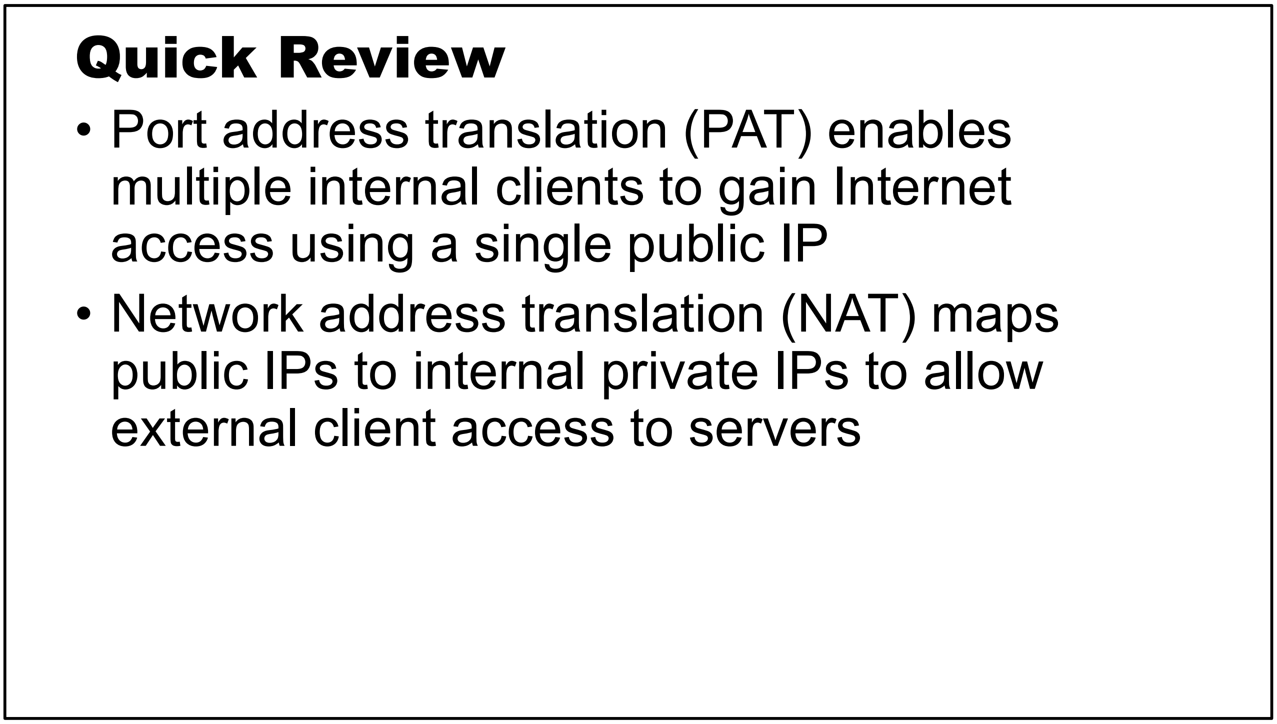
Clients connect to IP:port

External Internet clients

NAT router

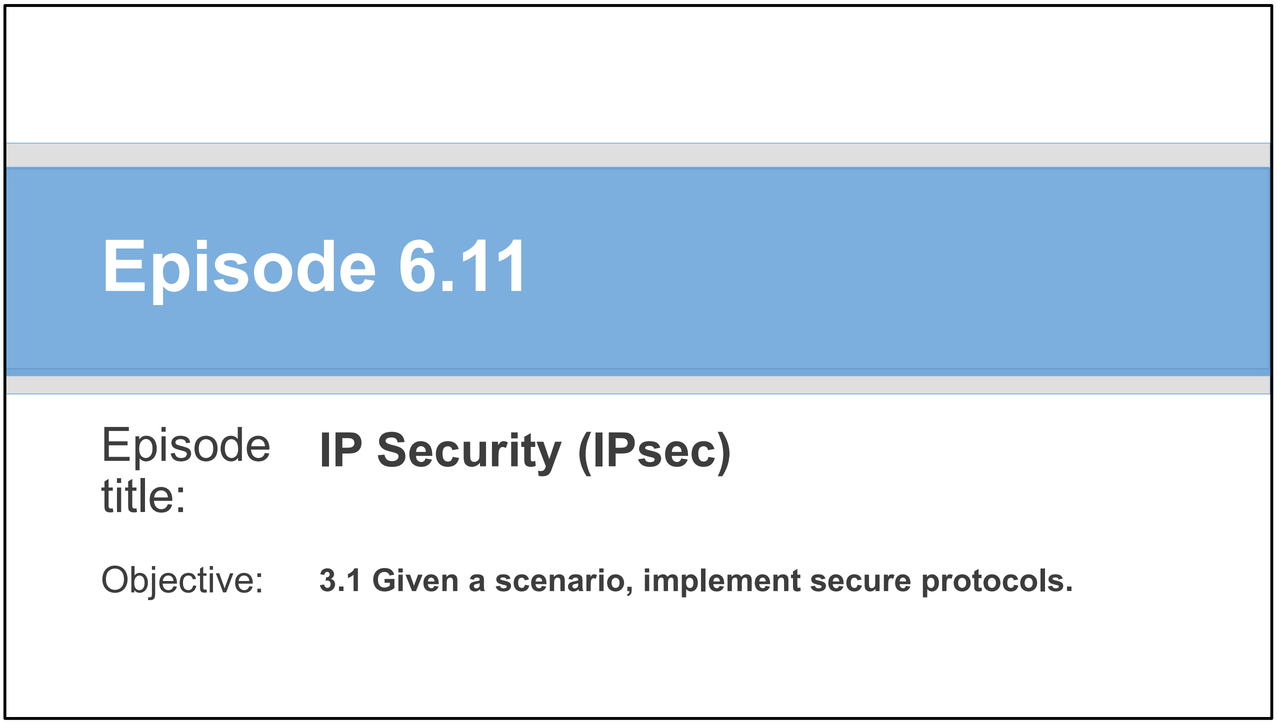
Backend servers

Public IP and port	Private IP and port
200.1.1.1:443	192.168.1.1:443
200.1.1.2:22	192.168.1.11:22



Quick Review

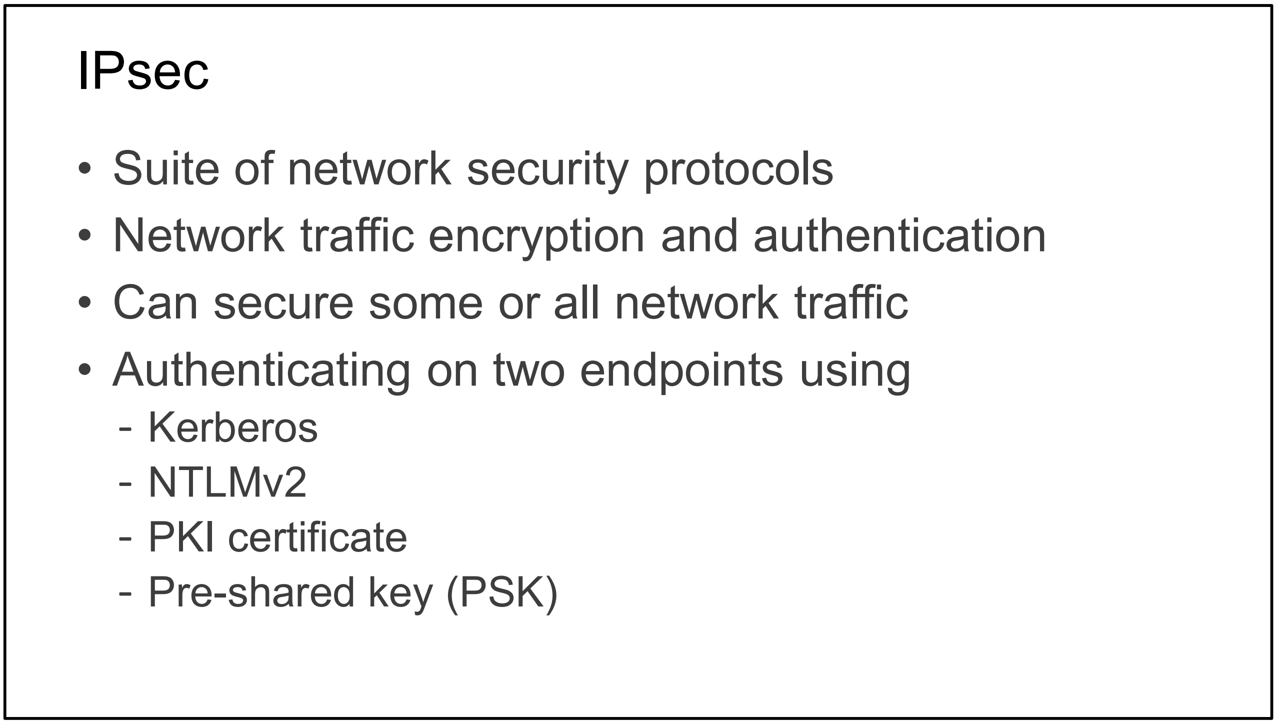
- Port address translation (PAT) enables multiple internal clients to gain Internet access using a single public IP
- Network address translation (NAT) maps public IPs to internal private IPs to allow external client access to servers



Episode 6.11

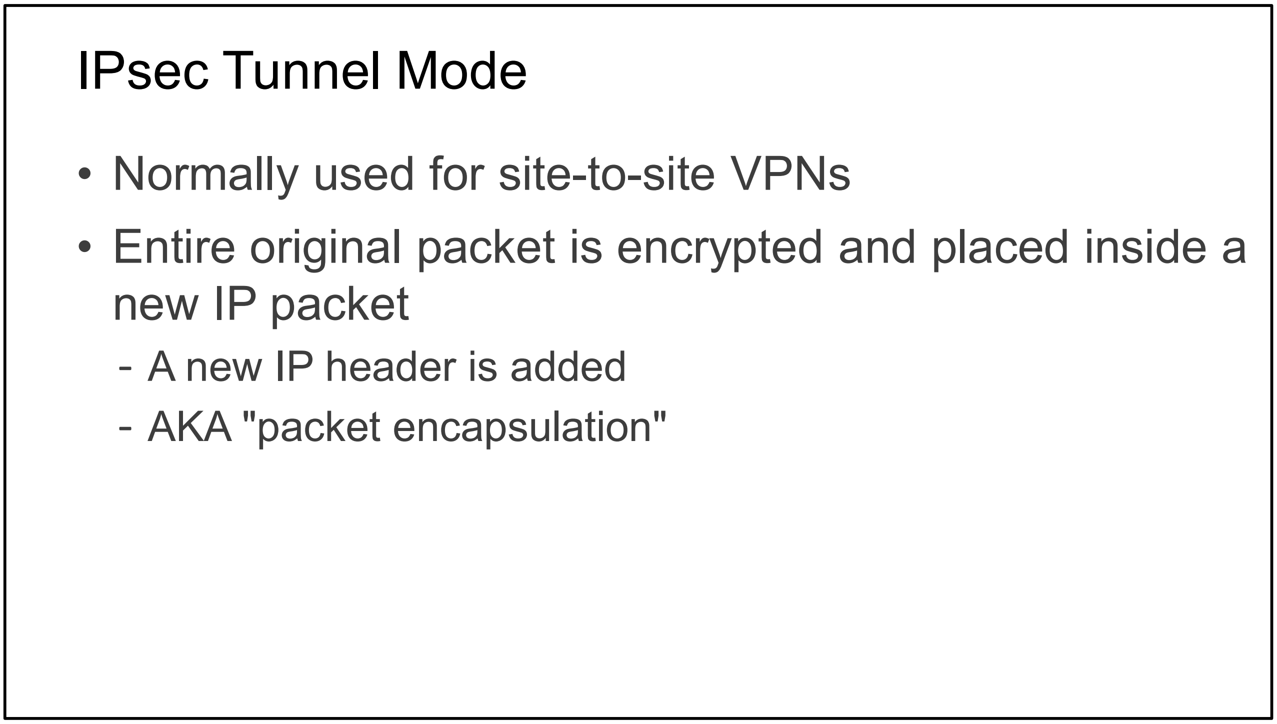
Episode title: **IP Security (IPsec)**

Objective: **3.1 Given a scenario, implement secure protocols.**



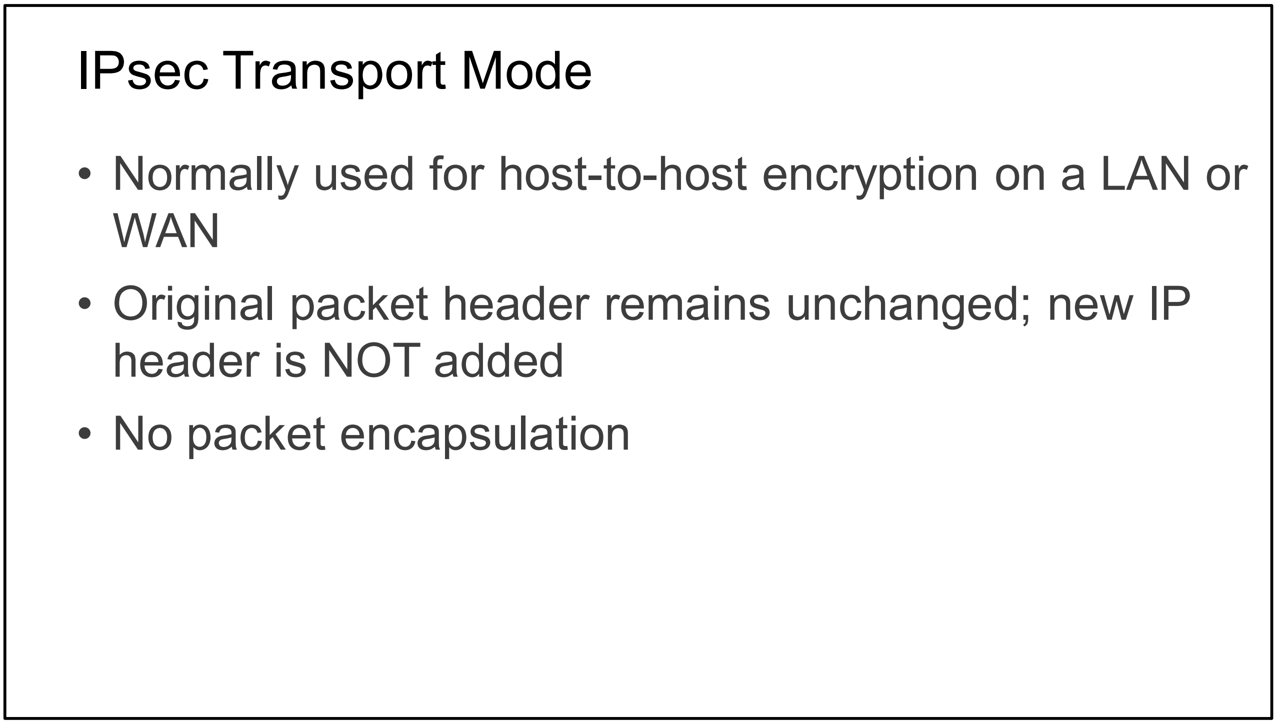
IPsec

- Suite of network security protocols
- Network traffic encryption and authentication
- Can secure some or all network traffic
- Authenticating on two endpoints using
  - Kerberos
  - NTLMv2
  - PKI certificate
  - Pre-shared key (PSK)



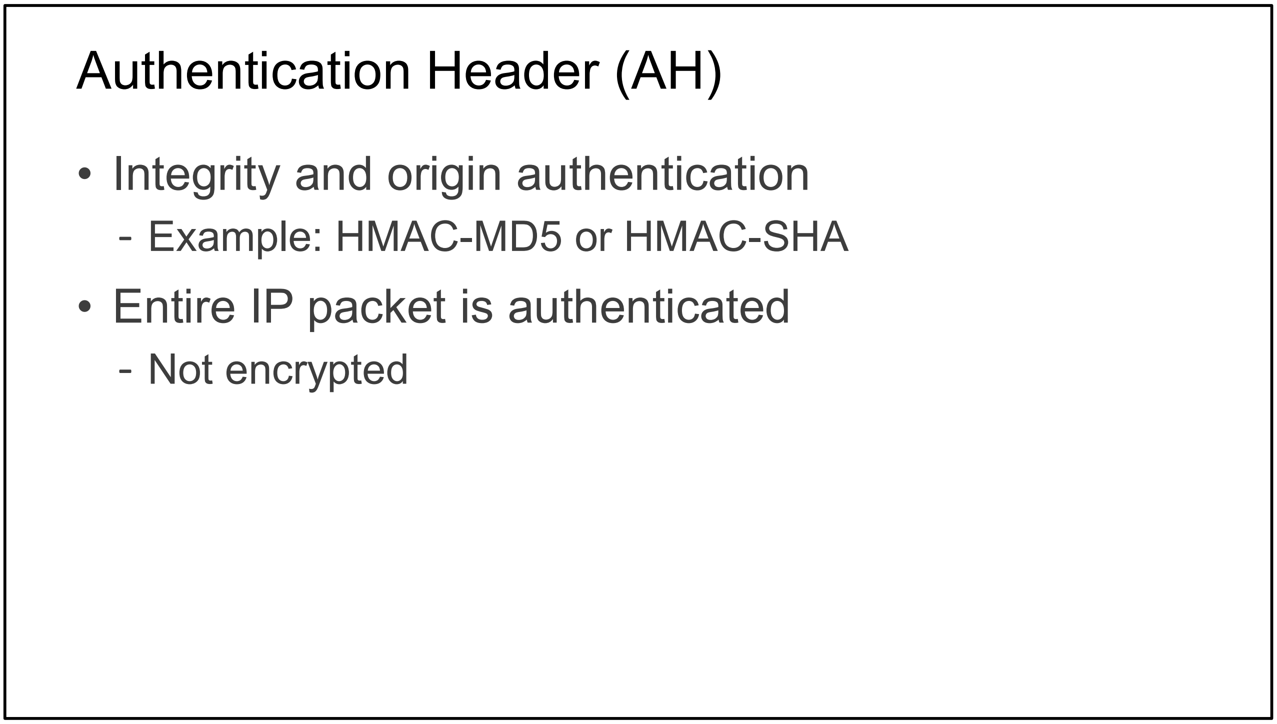
IPsec Tunnel Mode

- Normally used for site-to-site VPNs
- Entire original packet is encrypted and placed inside a new IP packet
  - A new IP header is added
  - AKA "packet encapsulation"



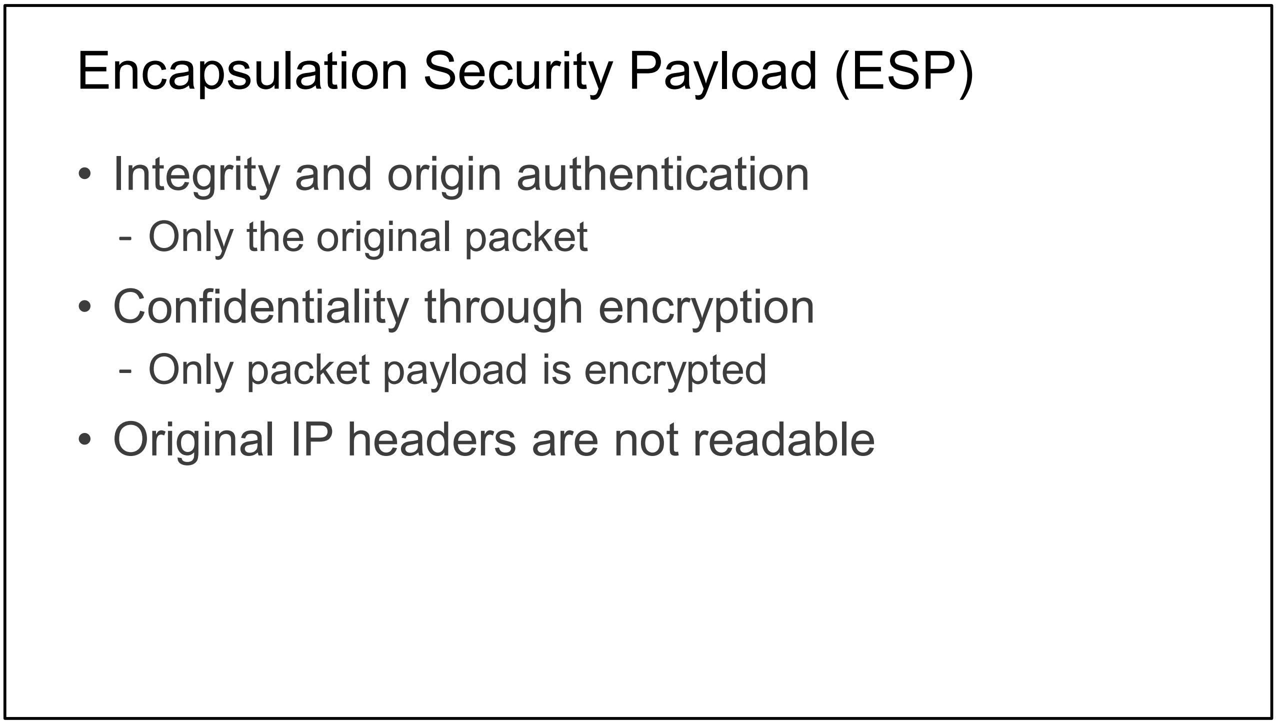
IPsec Transport Mode

- Normally used for host-to-host encryption on a LAN or WAN
- Original packet header remains unchanged; new IP header is NOT added
- No packet encapsulation



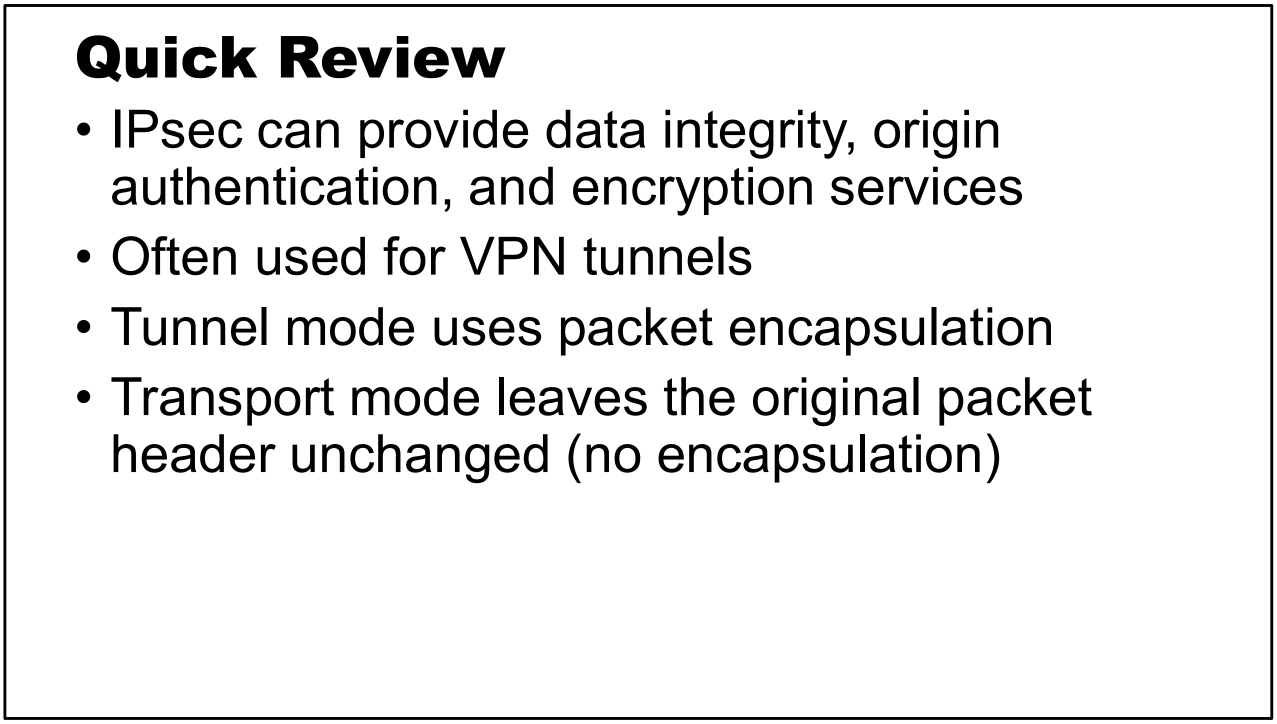
Authentication Header (AH)

- Integrity and origin authentication
  - Example: HMAC-MD5 or HMAC-SHA
- Entire IP packet is authenticated
  - Not encrypted



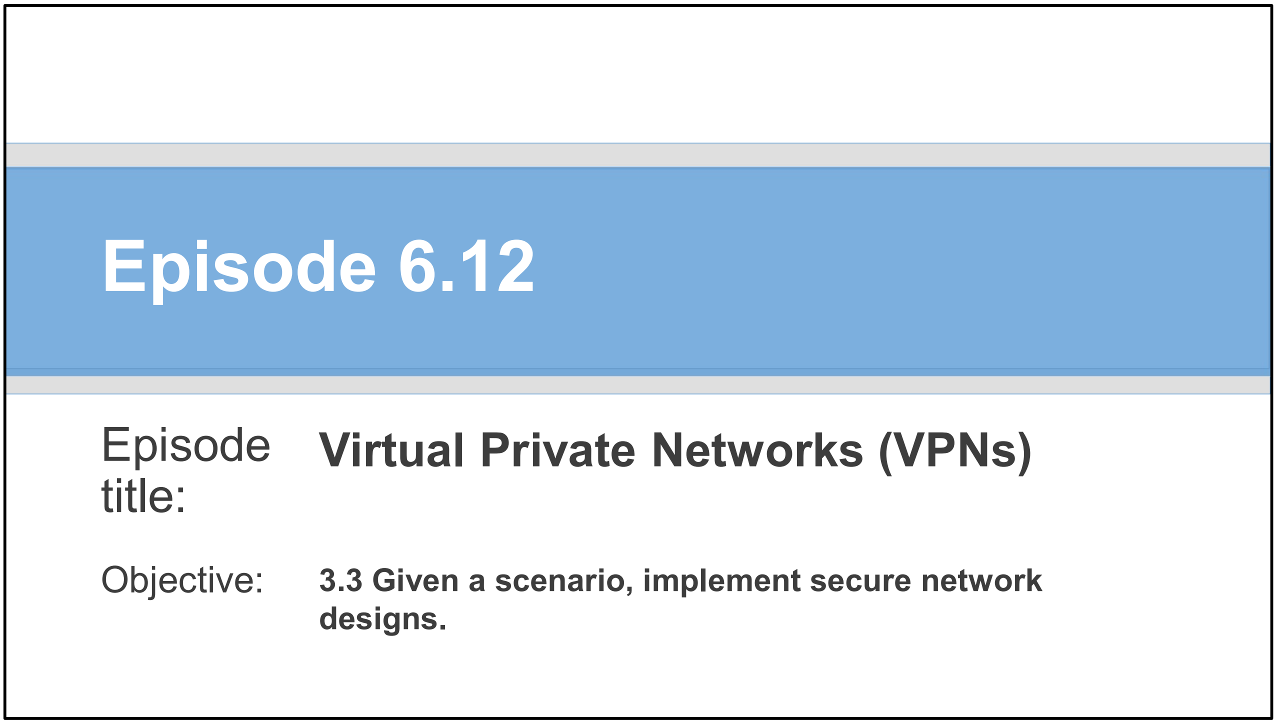
Encapsulation Security Payload (ESP)

- Integrity and origin authentication
  - Only the original packet
- Confidentiality through encryption
  - Only packet payload is encrypted
- Original IP headers are not readable



Quick Review

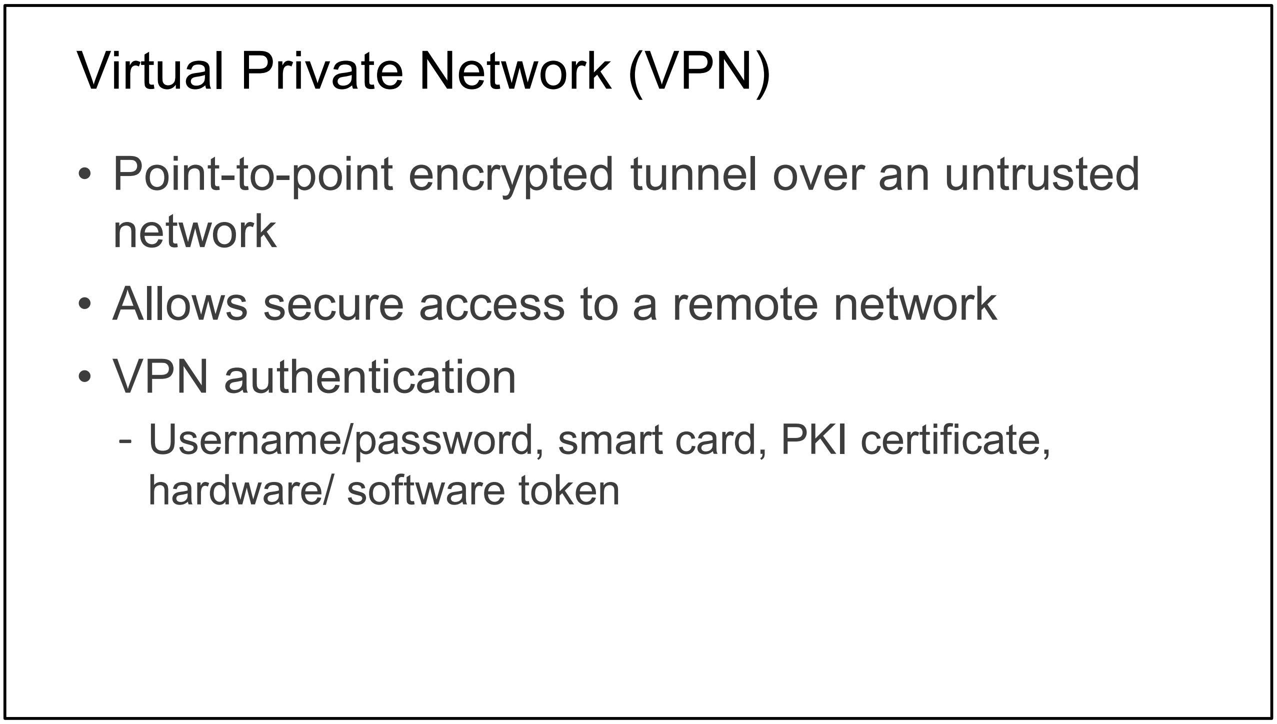
- IPsec can provide data integrity, origin authentication, and encryption services
- Often used for VPN tunnels
- Tunnel mode uses packet encapsulation
- Transport mode leaves the original packet header unchanged (no encapsulation)



Episode 6.12

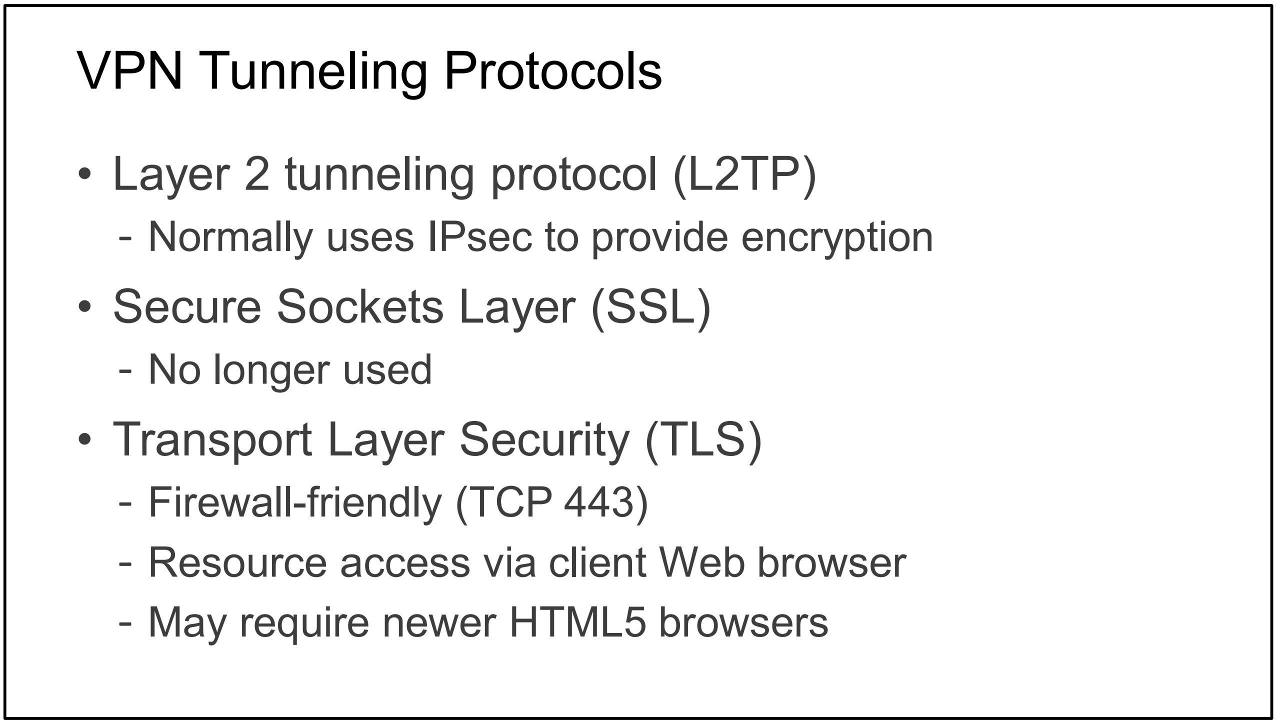
Episode title: **Virtual Private Networks (VPNs)**

Objective: **3.3 Given a scenario, implement secure network designs.**



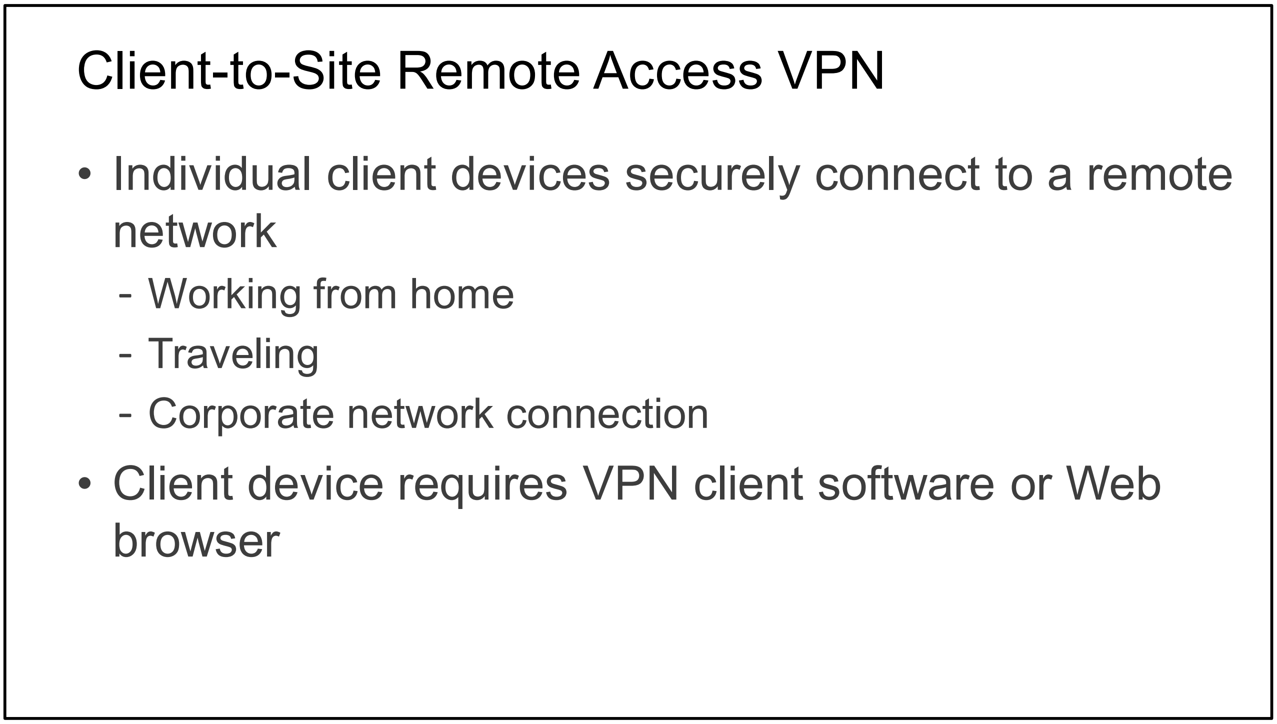
Virtual Private Network (VPN)

- Point-to-point encrypted tunnel over an untrusted network
- Allows secure access to a remote network
- VPN authentication
  - Username/password, smart card, PKI certificate, hardware/ software token



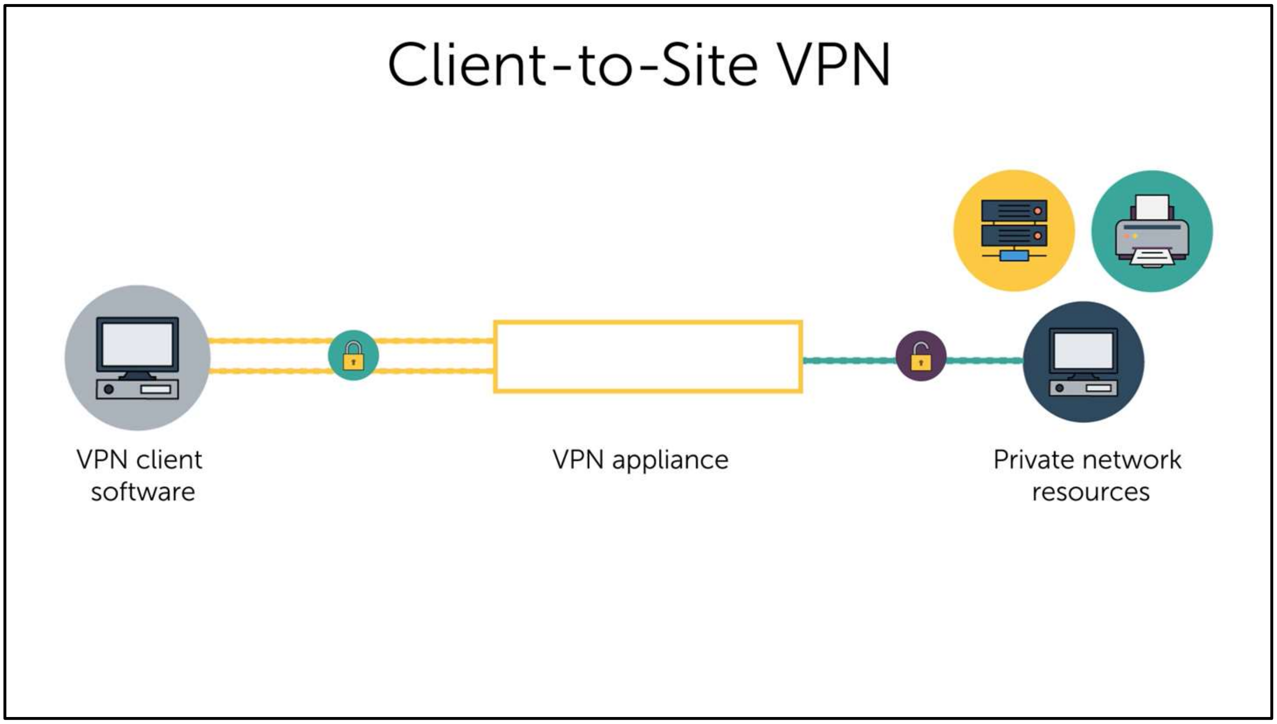
VPN Tunneling Protocols

- Layer 2 tunneling protocol (L2TP)
  - Normally uses IPsec to provide encryption
- Secure Sockets Layer (SSL)
  - No longer used
- Transport Layer Security (TLS)
  - Firewall-friendly (TCP 443)
  - Resource access via client Web browser
  - May require newer HTML5 browsers



Client-to-Site Remote Access VPN

- Individual client devices securely connect to a remote network
  - Working from home
  - Traveling
  - Corporate network connection
- Client device requires VPN client software or Web browser

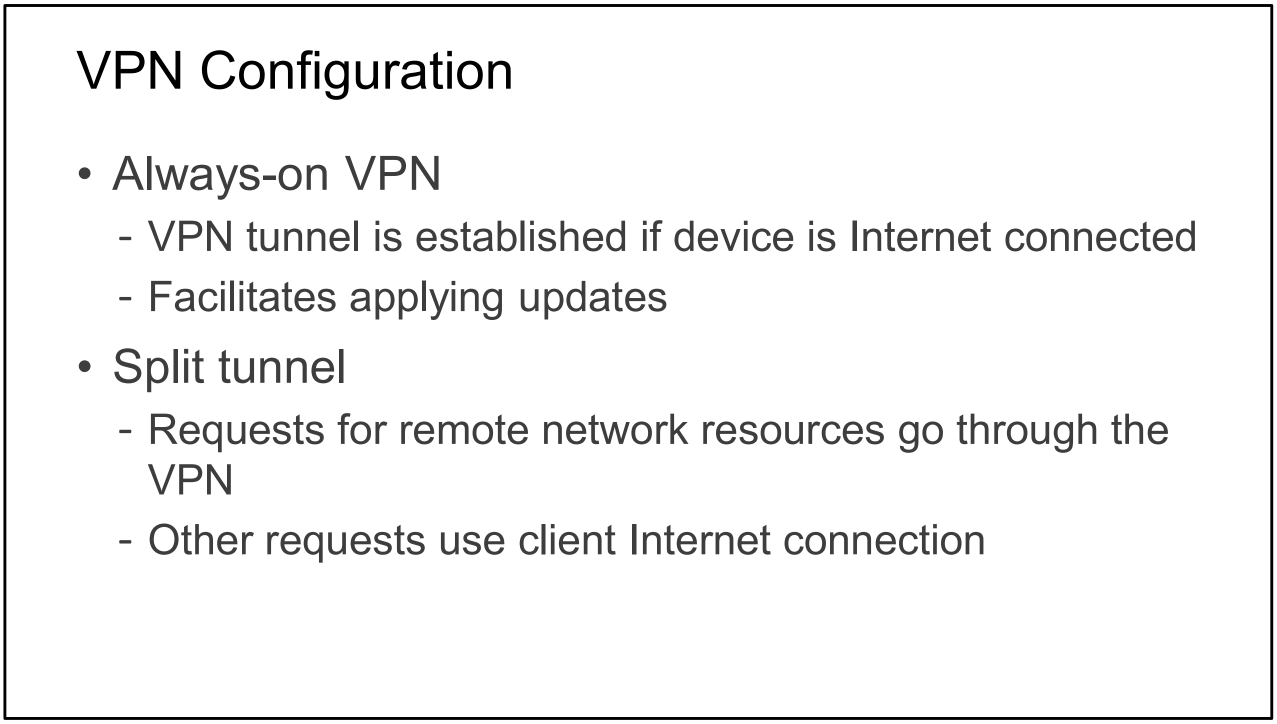


Client-to-Site VPN

VPN client software

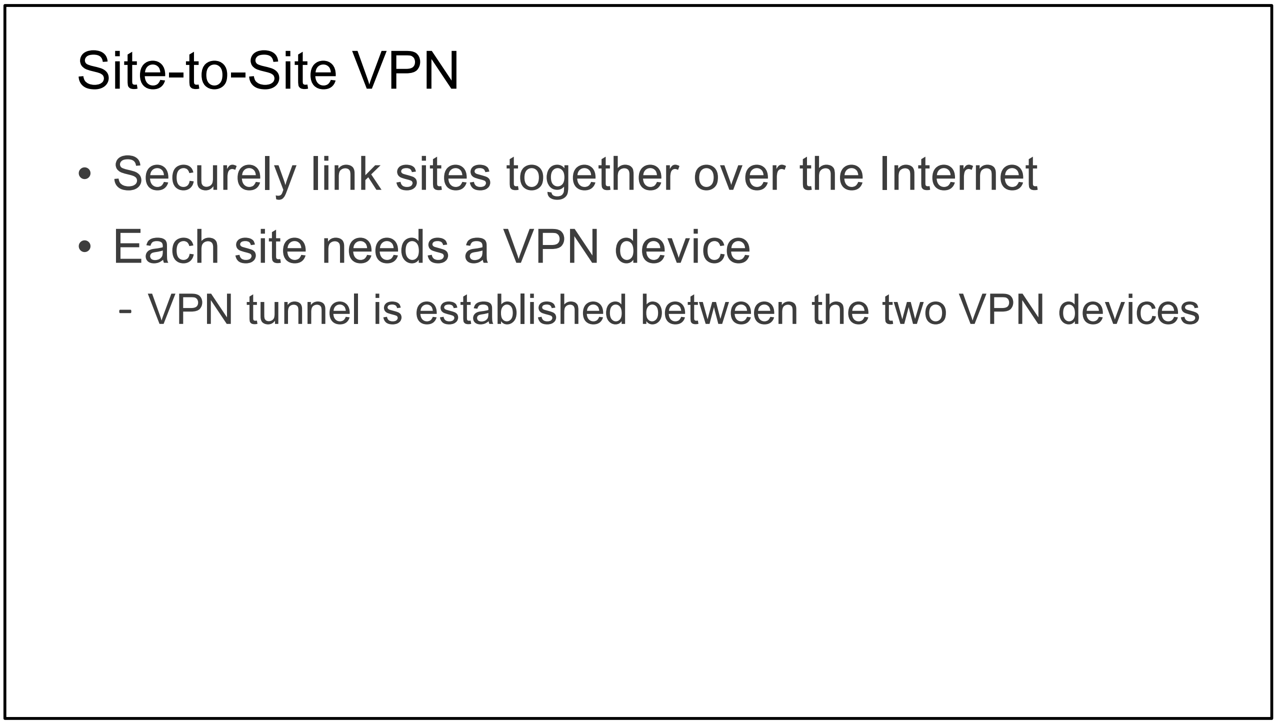
VPN appliance

Private network resources



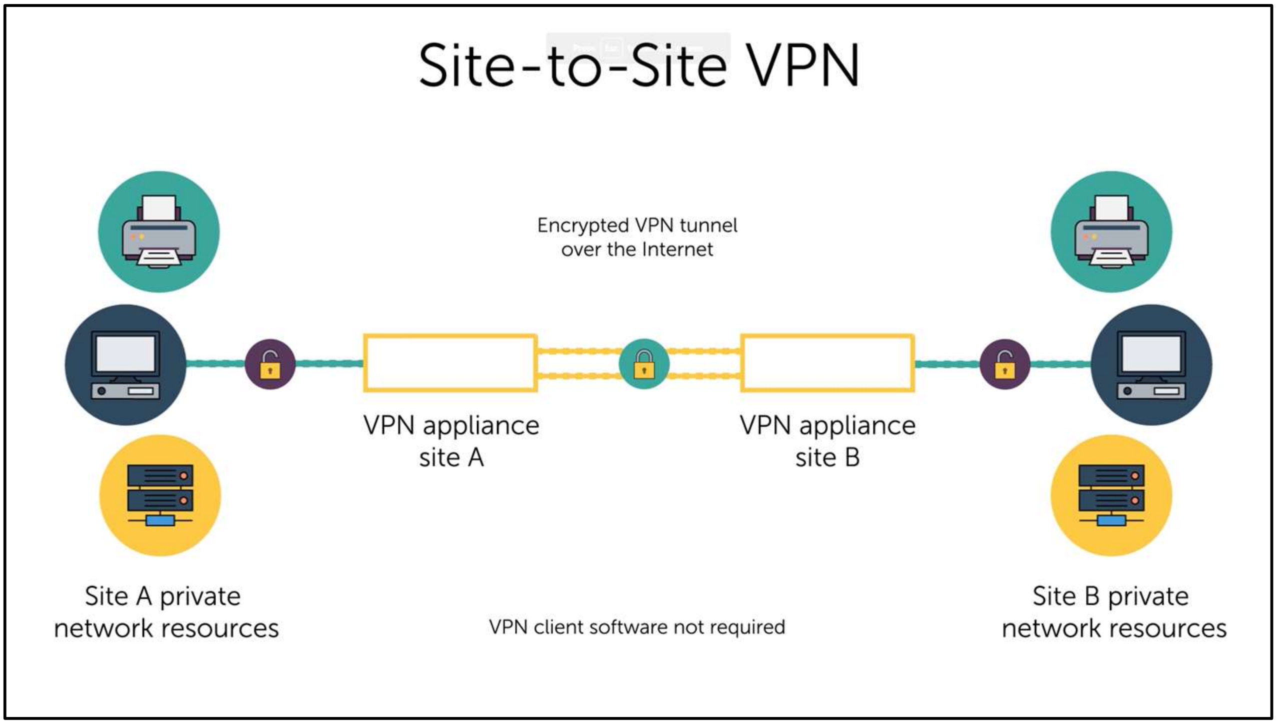
VPN Configuration

- Always-on VPN
  - VPN tunnel is established if device is Internet connected
  - Facilitates applying updates
- Split tunnel
  - Requests for remote network resources go through the VPN
  - Other requests use client Internet connection



Site-to-Site VPN

- Securely link sites together over the Internet
- Each site needs a VPN device
  - VPN tunnel is established between the two VPN devices



Site-to-Site VPN

Encrypted VPN tunnel over the Internet

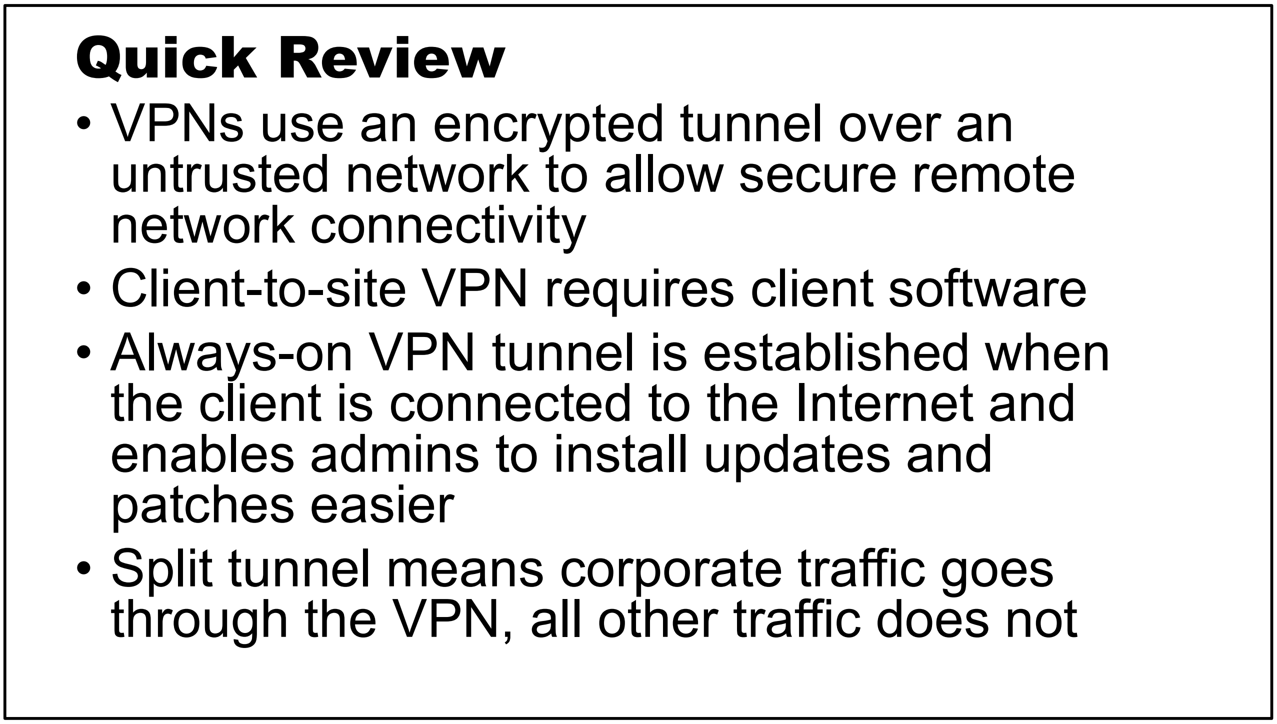
VPN appliance site A

VPN appliance site B

Site A private network resources

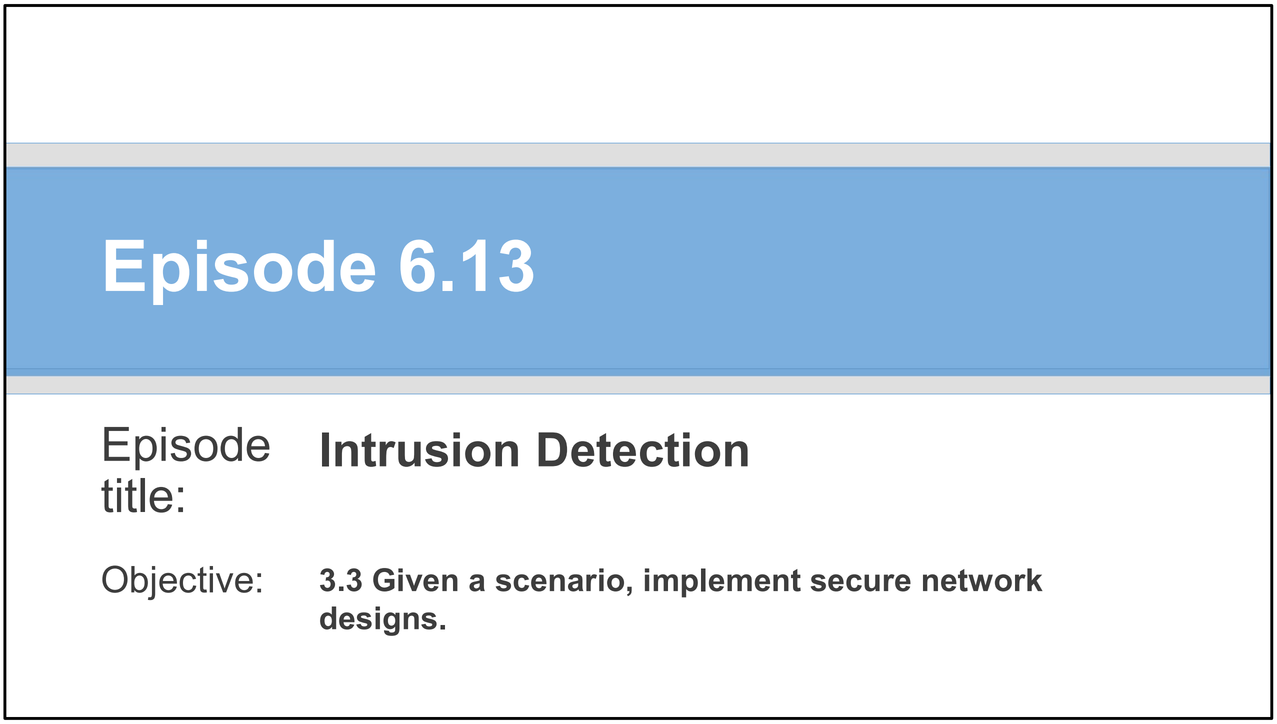
Site B private network resources

VPN client software not required



Quick Review

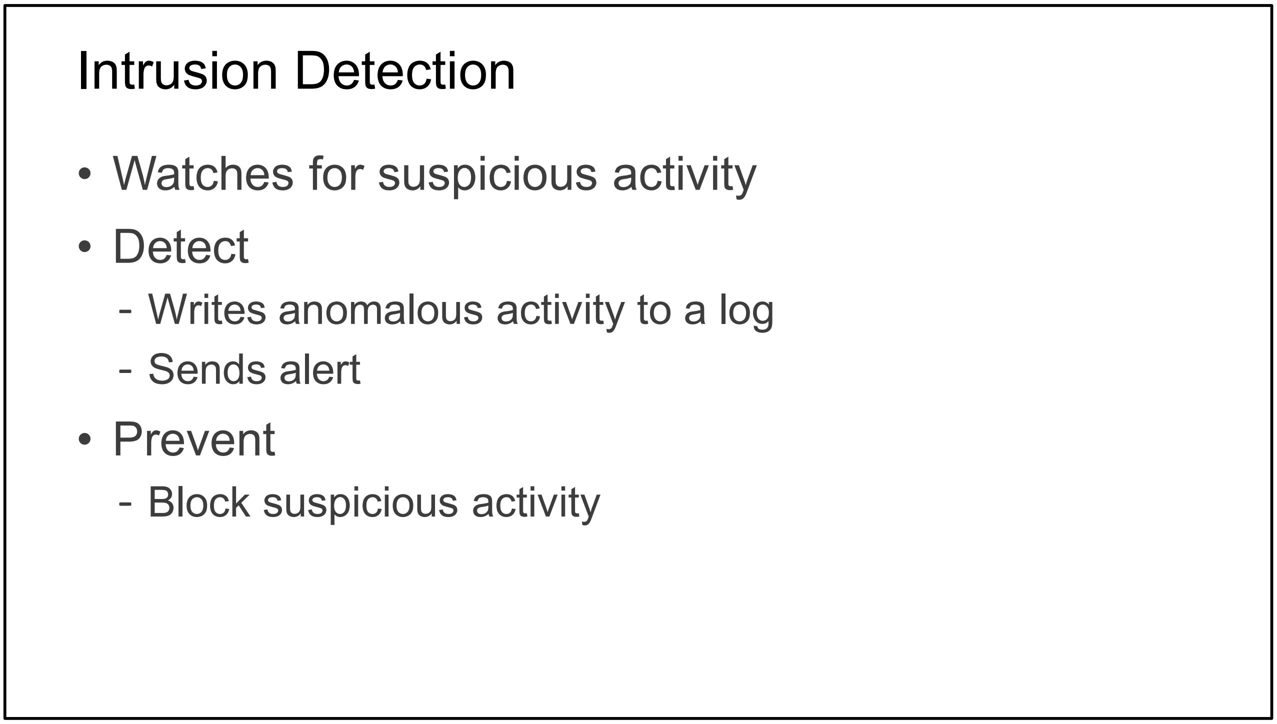
- VPNs use an encrypted tunnel over an untrusted network to allow secure remote network connectivity
- Client-to-site VPN requires client software
- Always-on VPN tunnel is established when the client is connected to the Internet and enables admins to install updates and patches easier
- Split tunnel means corporate traffic goes through the VPN, all other traffic does not



Episode 6.13

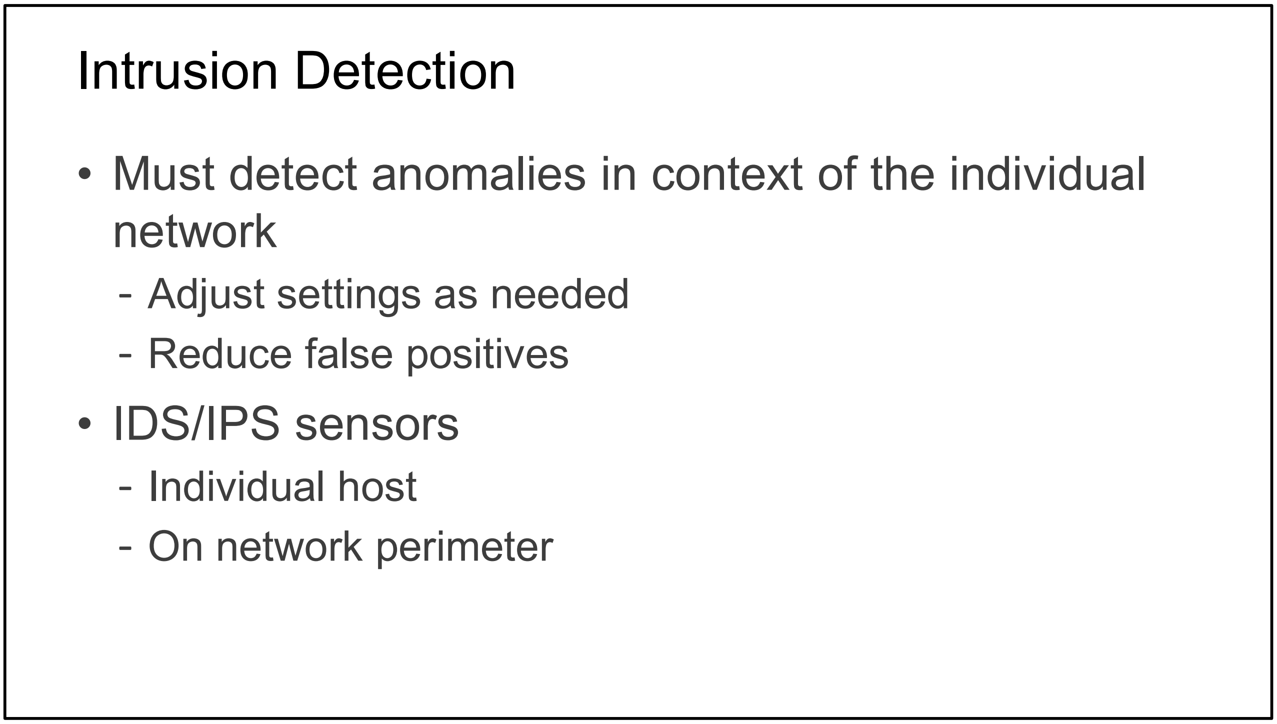
Episode title: **Intrusion Detection**

Objective: **3.3 Given a scenario, implement secure network designs.**



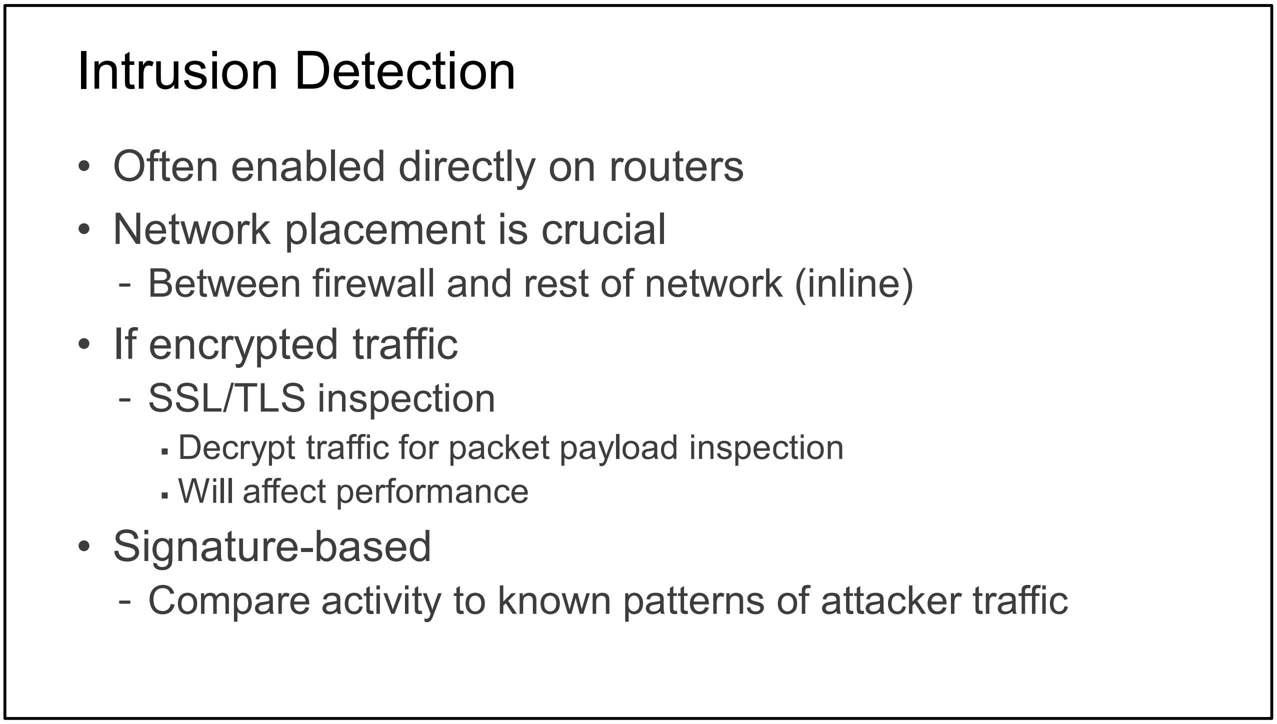
Intrusion Detection

- Watches for suspicious activity
- Detect
  - Writes anomalous activity to a log
  - Sends alert
- Prevent
  - Block suspicious activity



Intrusion Detection

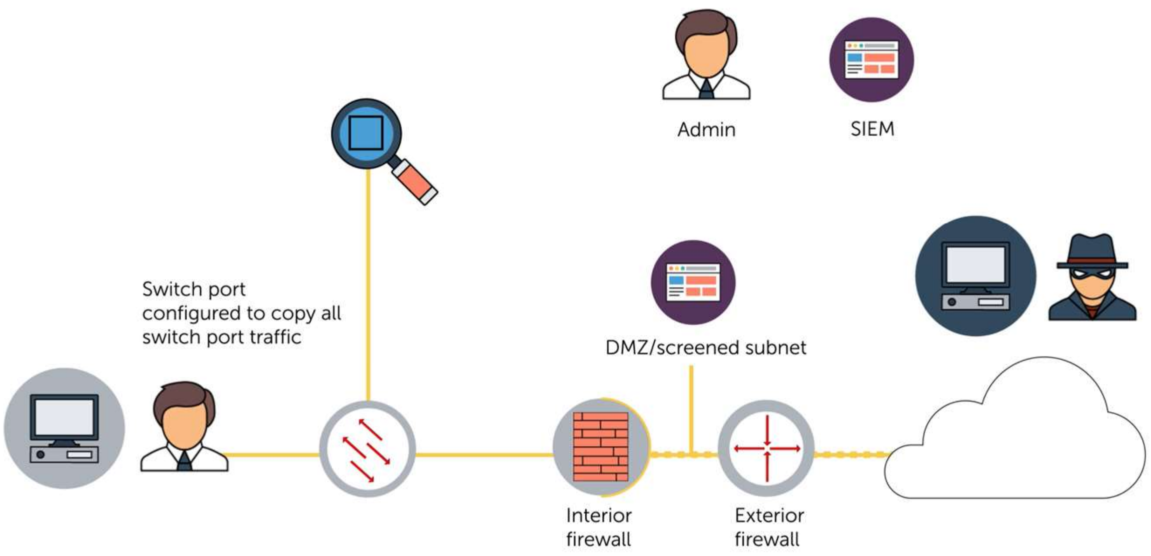
- Must detect anomalies in context of the individual network
  - Adjust settings as needed
  - Reduce false positives
- IDS/IPS sensors
  - Individual host
  - On network perimeter



Intrusion Detection

- Often enabled directly on routers
- Network placement is crucial
  - Between firewall and rest of network (inline)
- If encrypted traffic
  - SSL/TLS inspection
    - Decrypt traffic for packet payload inspection
    - Will affect performance
- Signature-based
  - Compare activity to known patterns of attacker traffic

Network Intrusion Detection



Admin

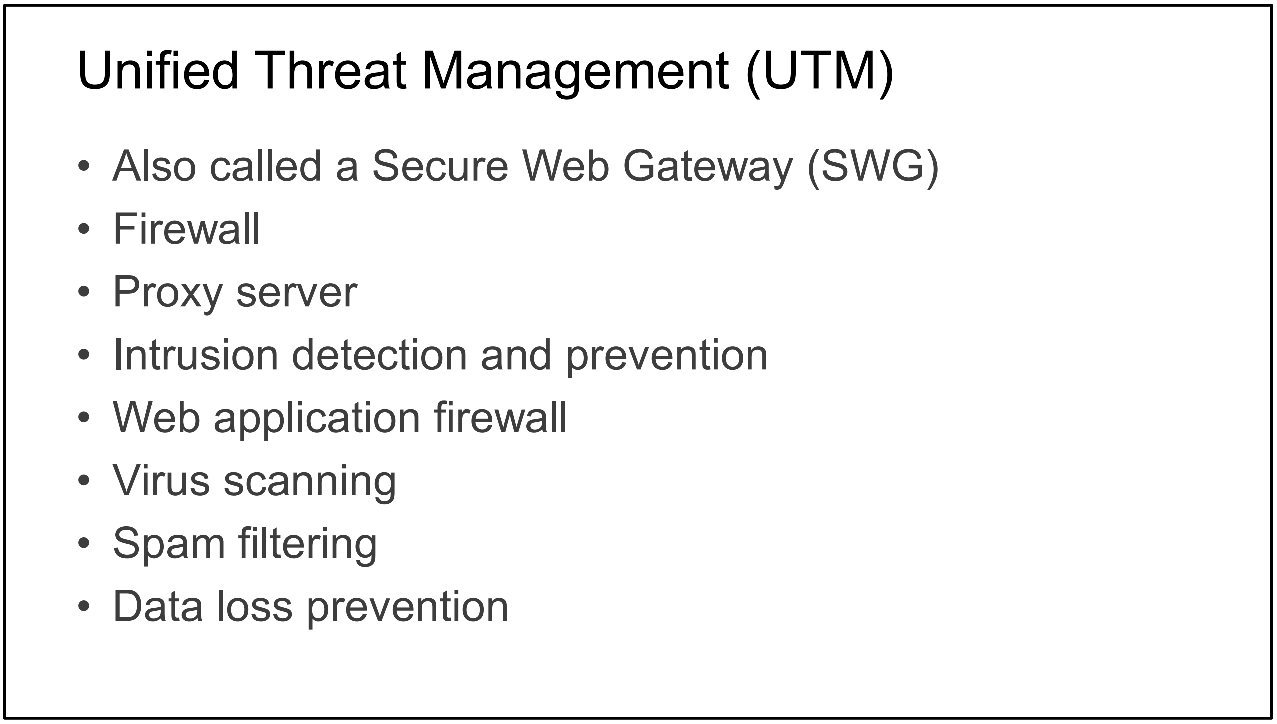
SIEM

Switch port configured to copy all switch port traffic

DMZ/screened subnet

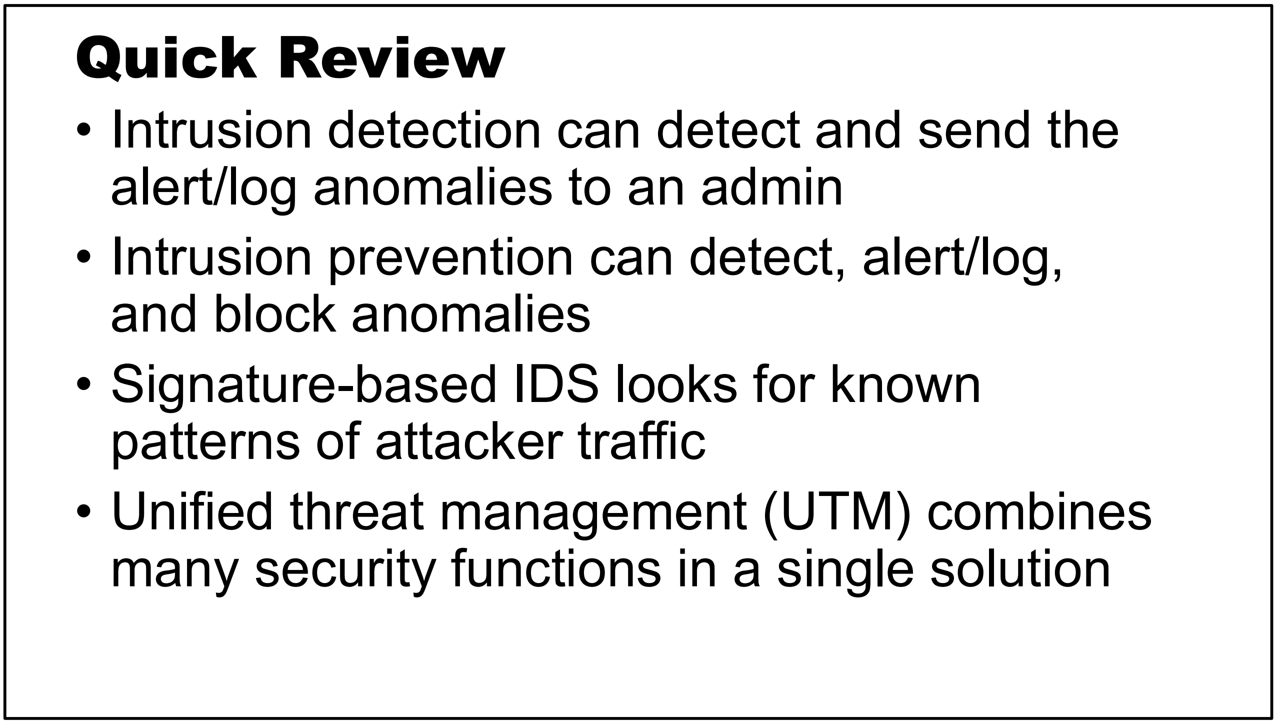
Interior firewall

Exterior firewall



Unified Threat Management (UTM)

- Also called a Secure Web Gateway (SWG)
- Firewall
- Proxy server
- Intrusion detection and prevention
- Web application firewall
- Virus scanning
- Spam filtering
- Data loss prevention



Quick Review

- Intrusion detection can detect and send the alert/log anomalies to an admin
- Intrusion prevention can detect, alert/log, and block anomalies
- Signature-based IDS looks for known patterns of attacker traffic
- Unified threat management (UTM) combines many security functions in a single solution