COMPTIA SECURITY+ SY0-701 · WEEK 9

Secure Enterprise Infrastructure



Objective 3.2 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Place security devices by zone and explain how placement shrinks the attack surface.
2. Choose fail-open or fail-closed for a device and defend the choice.
3. Distinguish active from passive and inline from tap or monitor deployments.
4. Explain what a jump server, proxy, IDS, IPS, load balancer, and sensor each do.
5. Describe how 802.1X and EAP control access to a switch port or Wi-Fi network.
6. Compare layer 4, layer 7, NGFW, WAF, and UTM firewalls and pick one for a need.
7. Select a VPN, TLS, IPSec, SD-WAN, or SASE design for a remote access scenario.

AGENDA

4 min	Why infrastructure design is a security control
10 min	Placement, zones, attack surface, connectivity
6 min	Failure modes: fail-open and fail-closed
6 min	Device attributes: active, passive, inline, tap
10 min	Network appliances
8 min	Port security: 802.1X and EAP
10 min	Firewall types
10 min	Exercise 1: place it and pick it
8 min	Tunneling with IPSec and TLS
8 min	Remote access, SD-WAN, and SASE
8 min	Exercise 2: selecting effective controls
2 min	Wrap-up

Four questions before you place a device

Device placement

Put controls where traffic between zones must pass.

Firewall between LAN and internet

Security zones

Group systems by trust level and the data they hold.

Guest, staff, clinical, DMZ

Attack surface

Every open port, service, and account is a way in.

Close ports nobody uses

Connectivity

Know every link: ISP, VPN, wireless, cloud, vendor.

Vendor remote support line

When a device fails, what happens to traffic

Fail-open

- Traffic keeps flowing without inspection
- Favors availability over security
- Fits a guest Wi-Fi content filter
- Risk: attacks pass while it is down

Fail-closed

- Traffic stops until the device recovers
- Favors confidentiality and integrity
- Fits a perimeter firewall or IPS on records
- Risk: an outage stops the business

Active or passive, inline or on a tap

Attribute	What it means	Example
Active	Takes action: blocks, drops, or resets	IPS dropping an exploit
Passive	Watches and reports; never blocks	IDS raising an alert
Inline	All traffic flows through the device	Firewall between switch and router
Tap or monitor	Gets a copy of traffic from a tap or SPAN	IDS sensor on a SPAN port

Five appliances and the job each does

Jump server

Hardened host admins pass through to reach servers.

Bastion host into the server VLAN

Proxy server

Makes requests for clients; filters and caches.

Forward and reverse proxies

IDS and IPS

Detect, or detect and block, by signature or anomaly.

Snort, Suricata

Load balancer

Spreads requests across servers; skips dead ones.

Two portal servers, one address

Sensors

Collect traffic or events for an IDS or SIEM.

Network sensor on a SPAN port

How 802.1X opens a port

1

Connect

Device plugs in; port passes only EAP traffic.

2

Request ID

Switch or access point asks for an identity.

3

Relay

Authenticator relays EAP messages to RADIUS.

4

Verify

Server checks the certificate or credentials.

5

Open the port

On success the port opens, often to a set VLAN.

Match the firewall to what it can see

Type	What it inspects	Best fit
Layer 4	IP addresses, ports, protocol, state	Fast filtering between zones
Layer 7	Application data such as URLs and commands	Blocking an app whatever port it uses
NGFW	Layer 7 plus app and user ID, built-in IPS	Main enterprise firewall
WAF	HTTP and HTTPS sent to a web app	SQL injection and XSS before a portal
UTM	Firewall, IPS, antivirus, filtering in one	Small office with one appliance

Place it and pick it



10

MINUTES · SMALL GROUPS

For each Lakeside need, name the device or firewall type, the zone where it goes, and whether it fails open or closed.

1. Stop SQL injection against the patient portal
2. Let the IT contractor manage servers without exposing RDP
3. Watch clinical VLAN traffic with no risk of blocking it
4. Keep non-clinic laptops off the wired jacks in exam rooms
5. Keep the portal up if one of its two web servers fails
6. Filter and log staff web browsing
7. One affordable box for a two-person satellite office

IPSec and TLS both build tunnels

IPSec

- Works at layer 3 and protects all IP traffic
- AH gives integrity; ESP adds encryption
- Tunnel mode wraps the whole original packet
- IKE negotiates keys and security associations
- Common for site-to-site VPNs

TLS

- Works above transport, usually on TCP 443
- Passes most firewalls and proxies easily
- Common for remote access VPNs and HTTPS
- Clientless portals run in a web browser
- Allow TLS 1.2 and 1.3 only; retire older ones

From VPN to SASE



Remote access VPN

Encrypted tunnel from one user's device to the network.

Clinician working from home



Site-to-site VPN

Gateways join two networks over the internet.

Clinic to satellite office



SD-WAN

Software steers each app over the best link between sites.

Broadband plus LTE backup



SASE

Cloud service joining SD-WAN with security at the edge.

SWG, CASB, ZTNA, FWaaS

EXERCISE 2 · CHOOSE CONTROLS

Pick the control that fits the risk



8

MINUTES · PAIRS

For each risk, choose the most effective control from this week and give one reason it beats the next-best option.

1. Staff phones on clinic Wi-Fi can reach the records server
2. The billing vendor needs one server for two hours a month
3. A second site opens with only one broadband line
4. Twelve staff now work from home three days a week
5. The IDS raised 400 alerts last week and nobody read them
6. A lobby printer shares a VLAN with the EHR server

REVIEW

Five questions: write your answers first

1. What is the difference between fail-open and fail-closed?
2. An IDS receives traffic from a SPAN port. Is it active or passive, inline or tap/monitor?
3. Name the three roles in 802.1X and the protocol that carries the exchange.
4. What can a WAF detect that a layer 4 firewall cannot?
5. What does SASE combine?

TAKEAWAYS

Four things to take with you

01

Placement is policy

Put controls where traffic between zones has to pass through them.

02

Choose the failure mode

Fail closed protects data; fail open protects uptime. Decide on purpose.

03

Pick firewalls by layer

Layer 4 sees ports; layer 7, NGFW, and WAF see the application.

04

Tunnels protect the path

IPSec for sites, TLS for users, SASE for users who are everywhere.

NEXT Lab 9: Firewall rules and segmentation with ufw