STUDENT HANDOUT · WEEK 9

Secure Enterprise Infrastructure

SY0-701 objectives 3.2. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

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.

KEY IDEAS

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	Fail-closed
Traffic keeps flowing without inspection	Traffic stops until the device recovers

Favors availability over security	Favors confidentiality and integrity
Fits a guest Wi-Fi content filter	Fits a perimeter firewall or IPS on records
Risk: attacks pass while it is down	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

Type	What it inspects	Best fit
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

IPSec and TLS both build tunnels

IPSec	TLS
Works at layer 3 and protects all IP traffic	Works above transport, usually on TCP 443
AH gives integrity; ESP adds encryption	Passes most firewalls and proxies easily
Tunnel mode wraps the whole original packet	Common for remote access VPNs and HTTPS
IKE negotiates keys and security associations	Clientless portals run in a web browser
Common for site-to-site VPNs	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 1: 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.

#	Prompt	Your answer
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	

EXERCISE 2: 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.

#	Prompt	Your answer
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 QUESTIONS

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?

KEY TAKEAWAYS

- **Placement is policy.** Put controls where traffic between zones has to pass through them.
- **Choose the failure mode.** Fail closed protects data; fail open protects uptime. Decide on purpose.
- **Pick firewalls by layer.** Layer 4 sees ports; layer 7, NGFW, and WAF see the application.
- **Tunnels protect the path.** IPSec for sites, TLS for users, SASE for users who are everywhere.

LAB 9: FIREWALL RULES AND SEGMENTATION WITH UFW

60 MINUTES

You need two Linux VMs from Lab 1 (Ubuntu or Debian) on a VirtualBox internal network or VMware host-only network with no route to any other network. Scan and firewall only your own lab VMs; never run these scans against a network you do not own.

Steps

1. While both VMs still have internet access, install the tools: sudo apt install nginx openssh-server on the VM that will be records, and sudo apt install nmap on the one that will be staff. Then put both VMs on the internal network labnet. Name one records and the other staff. Give them static addresses from the console: on records sudo ip addr add 192.168.56.10/24 dev enp0s8, on staff sudo ip addr add 192.168.56.20/24 dev enp0s8 (check the interface name with ip a). Confirm with ping.
2. On records, confirm the web server and SSH are running: systemctl status nginx ssh. On staff, take a baseline: nmap -sT -p 22,80,443,5432 192.168.56.10. Save the output.
3. Write the rule plan before typing anything: default deny inbound, allow outbound, allow TCP 80 from 192.168.56.0/24, allow TCP 22 only from 192.168.56.20, log denied traffic. Note which rule is the implicit deny.
4. Apply it on records from the VM console: sudo ufw default deny incoming, sudo ufw default allow outgoing, sudo ufw allow from 192.168.56.20 to any port 22 proto tcp, sudo ufw allow from 192.168.56.0/24 to any port 80 proto tcp, sudo ufw logging on, sudo ufw enable. Check with sudo ufw status numbered.
5. Test from staff: rerun the Nmap scan, then curl http://192.168.56.10 and ssh <user>@192.168.56.10. Record which ports are open, closed, or filtered.
6. Test segmentation: on staff, add a second address with sudo ip addr add 192.168.56.30/24 dev enp0s8 and try SSH from it with ssh -b 192.168.56.30 <user>@192.168.56.10. It should fail while web access still works.
7. Read the evidence on records: sudo grep 'UFW BLOCK' /var/log/ufw.log | tail -n 20 (or sudo journalctl -k | grep UFW). Match three log lines to the tests that caused them.
8. See a failure mode: run sudo ufw disable, rescan from staff, and note what is now reachable. Then sudo ufw enable and rescan to confirm the rules are back.
9. Optional extension: build the same default-deny policy with iptables (sudo iptables -L -n -v to view it), or route between two internal networks through a pfSense VM and write the rules there.

Hand in

A short report with your rule plan table, the ufw status numbered output, before-and-after Nmap results, three matched log lines, and a one-page diagram of the Lakeside Family Clinic zones showing where a firewall like this one would sit.

Questions to answer in your report

1. Which rule acts as the implicit deny in your configuration, and what would the scan show without it?
2. Is a host firewall like ufw inline or tap, and active or passive? Explain.
3. When you disabled ufw, did the host fail open or closed? Which would Lakeside want for its records server, and what does that choice cost?
4. What could a layer 7 firewall or WAF catch on port 80 that your rules cannot?
5. How would you extend this design to keep the guest Wi-Fi zone from reaching the clinical zone?