4

DOMAIN

TOPIC FOUR

Network Security

24% of the exam · 9 lessons

The largest domain, and the most technical; models, ports, threats, cloud, design

AT A GLANCE

The largest domain on the exam

24%

of the exam — the biggest single share

9

lessons in this topic

~105

minutes

Why this one is different

- Domains 1 to 3 were concepts; this is concrete technical detail
- Port numbers, layer numbers and protocol names must be recalled exactly
- No amount of reasoning recovers a forgotten port number

So the method changes again

- Flashcards from day one — ports, layers, protocol pairs
- Ten minutes of drilling beats an hour of reading here
- Concepts still matter: cloud responsibility and segmentation reward understanding

LESSON MAP

The nine lessons

1. **Networking fundamentals**
   What a network is, the OSI and TCP/IP models, and devices by layer
2. **Addressing and Wi-Fi**
   IPv4 and IPv6, MAC addresses, NAT, DHCP, DNS, wireless security
3. **Ports and protocols**
   Well-known ports, insecure-to-secure pairs, the TCP handshake
4. **Threats and attacks**
   Malware, denial of service, on-path, spoofing, social engineering
5. **Detection and prevention**
   Firewalls, IDS versus IPS, antimalware, SIEM, scanning
6. **Data centres and redundancy**
   Power, HVAC, fire suppression, redundancy, MOU and MOA
7. **Cloud**
   Characteristics, service models, deployment models, MSP, SLA
8. **Secure network design**
   Defence in depth, zero trust, NAC, DMZ, VLANs, microsegmentation, VPN
9. **Consolidation**
   Drills for the memorisation set, plus scenario practice

Lessons 3 and 7 carry the most reliably tested content: the port pairs and the cloud responsibility split.

4.1

LESSON

Networking Fundamentals

OBJECTIVE

Describe what a network does, recite both reference models, and place common devices and protocols at the right layer.

- What a network is, and why the models exist
- The seven OSI layers and the four TCP/IP layers
- How the two models map onto each other
- Devices by layer: hub, switch, router, firewall

LESSON 4.1

Why there are reference models at all

A network moves data between devices that were never designed together.
The models are the agreement that makes that possible.

- Each layer does one job and hands off to the next
- A layer can be replaced without rewriting the others — copper to fibre changes layer 1 only
- Troubleshooting works by layer: no link light is layer 1, no IP address is layer 3
- The exam uses layer numbers as shorthand, so the numbering has to be automatic

LESSON 4.1 — THE MODELS

Seven layers, and four

Seven layers on the left, four on the right. Know both, and know how they map.

	OSI MODEL		TCP/IP MODEL
7	**Application**	HTTP, DNS, SMTP, FTP	**Application**
6	**Presentation**	Encoding, encryption, TLS	
5	**Session**	Session setup and teardown	
4	**Transport**	TCP, UDP · ports	**Transport**
3	**Network**	IP, ICMP · routers	**Internet**
2	**Data Link**	MAC, Ethernet · switches	**Network Access**
1	**Physical**	Cables, radio · hubs	

Mnemonic bottom-up: Please Do Not Throw Sausage Pizza Away.

LESSON 4.1 — LAYERS

What each OSI layer actually does

7 Application	The protocols users and programs interact with — HTTP, DNS, SMTP, FTP.
6 Presentation	Translation, encoding, compression and encryption. TLS is commonly placed here.
5 Session	Establishing, managing and tearing down conversations between hosts.
4 Transport	End-to-end delivery. TCP and UDP live here, and so do PORT NUMBERS.
3 Network	Logical addressing and routing between networks. IP and ICMP; routers operate here.
2 Data Link	Local delivery on a single network segment. MAC addresses, Ethernet; switches operate here.
1 Physical	The actual signalling — cable, fibre, radio. Hubs and repeaters operate here.

Ports at layer 4 and IP at layer 3 are the two placements the exam checks most often.

LESSON 4.1 — DEVICES

Devices by layer

Hub — layer 1

- Repeats every frame to every port
- No intelligence, no filtering
- A security problem: every host sees all traffic. Obsolete for good reason

Switch — layer 2

- Forwards by MAC address
- Sends traffic only to the intended port
- Supports VLANs, which is why segmentation is possible

Router — layer 3

- Forwards between networks by IP address
- Makes path decisions
- The boundary device between networks

Firewall — layer 3/4+

- Permits or blocks by rule
- Next-generation firewalls inspect up to layer 7
- Filters; it does not route as its main job

Why the hub matters historically: it is the reason network sniffing was once trivial on any LAN.

4.2

LESSON

Addressing and Wi-Fi

OBJECTIVE

Distinguish IPv4 from IPv6, explain what MAC addresses, NAT, DHCP and DNS do, and compare wireless security protocols.

- IPv4 and IPv6 formats and address sizes
- MAC addressing, and how it differs from IP
- NAT, DHCP and DNS — what each one solves
- WEP, WPA, WPA2, WPA3 and open networks

LESSON 4.2 — IP

IPv4 and IPv6

IPv4

- 32 bits, written as four decimal octets: 192.168.1.10
- About 4.3 billion addresses — exhausted, hence NAT
- Private ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Loopback 127.0.0.1

IPv6

- 128 bits, written as eight hexadecimal groups
- 2001:0db8:85a3::8a2e:0370:7334 — double colon compresses zeros
- Address space large enough that NAT is unnecessary
- Loopback ::1

MAC addresses are different

- 48 bits, burned into the network interface, used for LOCAL delivery at layer 2. IP is logical and routable; MAC is physical and local. Both are used on every local transmission

Three services that make addressing usable

NAT	Network Address Translation. Many private internal addresses share one public address. Conserves IPv4 space and incidentally hides internal addressing, though it is not a security control in itself.
DHCP	Assigns IP configuration automatically when a device joins. Ports 67 and 68. A rogue DHCP server is an attack — it can point victims at an attacker's gateway or DNS.
DNS	Resolves names to addresses. Port 53. Poisoning DNS is an integrity attack that redirects users to attacker-controlled hosts while the address bar still looks right.
ARP	Maps IP addresses to MAC addresses on the local segment. ARP spoofing enables on-path attacks inside a LAN.

NAT is not a firewall. It is a commonly tested misconception.

Wireless security, oldest to newest

The progression

- WEP — broken. Crackable in minutes. Never acceptable
- WPA — an interim fix, also now weak
- WPA2 — the long-standing baseline, using AES
- WPA3 — current, with stronger key exchange and protection for open networks

Other wireless facts

- SSID is the network name; hiding it is not a security control
- MAC filtering is trivially bypassed by spoofing
- Open networks provide no encryption — anything unencrypted above is readable
- An evil twin is a rogue access point imitating a legitimate SSID
- Guest wireless should be segmented from the corporate network

4.3

LESSON

Ports and Protocols

OBJECTIVE

Recall common ports, name the secure counterpart of an insecure protocol, and describe the TCP handshake.

- Port ranges and what they mean
- TCP versus UDP
- The insecure-to-secure protocol pairs
- SYN, SYN-ACK, ACK — and the attack that abuses it

Two transport protocols, different bargains

TCP

- Connection-oriented — a handshake first
- Reliable: acknowledges, retransmits, orders packets
- Slower and heavier
- Used where correctness matters: web, email, file transfer

UDP

- Connectionless — just send
- No acknowledgement, no retransmission, no ordering
- Fast and light
- Used where timeliness beats completeness: DNS lookups, VoIP, streaming, DHCP

Port ranges

- Well-known 0–1023 · registered 1024–49151 · dynamic or ephemeral 49152–65535. A service listening on a well-known port is doing something standard

LESSON 4.3 — THE PAIRS

Learn these as pairs

Learn these as PAIRS. The exam asks for the secure counterpart.

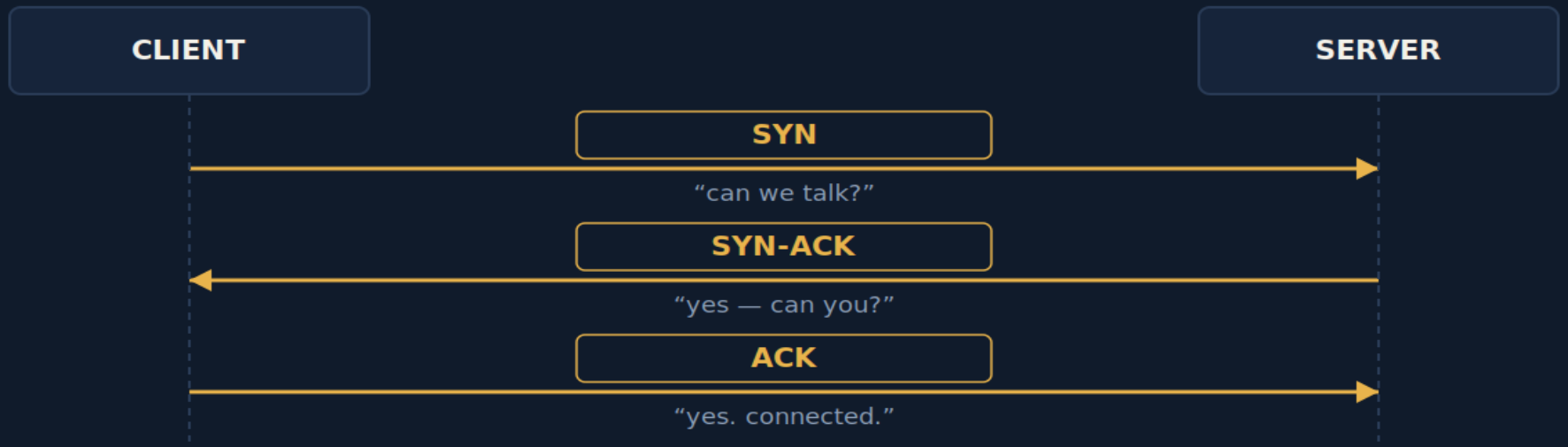
INSECURE		SECURE COUNTERPART	
FTP	20 / 21	SFTP / FTPS	22 / 989-990
Telnet	23	SSH	22
SMTP	25	SMTPS	465 / 587
DNS	53	DNS over TLS	853
HTTP	80	HTTPS	443
POP3	110	POP3S	995
IMAP	143	IMAPS	993
LDAP	389	LDAPS	636
SNMP v1/2	161 / 162	SNMP v3	161 / 162

Also: RDP 3389 · SMB 445 · DHCP 67/68 · Kerberos 88. Ranges: well-known 0–1023, registered 1024–49151, dynamic 49152–65535.

LESSON 4.3 — THE HANDSHAKE

Three packets, and one attack

Three packets to open a TCP connection. One attack abuses the middle step.



SYN flood

The attacker sends SYN and never sends the final ACK.
The server holds half-open connections until it exhausts resources — a denial-of-service attack.

4.4

LESSON

Threats and Attacks

OBJECTIVE

Identify types of network threat and attack from a description, and distinguish the malware families.

- The malware families and how they differ
- Denial of service and distributed denial of service
- On-path, spoofing, sniffing and replay
- Social engineering and the human attack surface

LESSON 4.4 — MALWARE

The malware families

Virus	Attaches to a file or program and needs a user action to spread. Requires a host.
Worm	Self-propagating — spreads across a network with no user action. The distinction from a virus is examinable.
Trojan	Disguised as something legitimate. The user installs it willingly, believing it is useful.
Ransomware	Encrypts data and demands payment. Primarily an availability attack; a breach only if data is also taken.
Rootkit	Hides its own presence, often at a deep system level, to maintain persistent access.
Spyware	Covertly gathers information — keystrokes, browsing, credentials.
Logic bomb	Dormant code that triggers on a condition — a date, or a user record disappearing from payroll.

Virus needs a host and a user; a worm needs neither. That single line answers most malware questions.

Attacks against the network itself

DoS	One source overwhelms a target so legitimate users cannot reach it. An availability attack.
DDoS	The same, from many sources at once — usually a botnet. Far harder to filter because the traffic looks distributed and ordinary.
On-path (MITM)	The attacker positions between two parties, able to read and alter traffic. Enabled by ARP spoofing, rogue access points or DNS poisoning.
Spoofing	Falsifying a source — IP, MAC, email sender, caller ID — to appear as someone else.
Sniffing	Passive capture of traffic. Effective against anything unencrypted, which is why the insecure protocols matter.
Replay	Capturing valid traffic and resending it to repeat an action. Countered by timestamps, sequence numbers and nonces.
Side-channel	Inferring secrets from physical characteristics — timing, power draw, electromagnetic emission — rather than by breaking the algorithm.

Also: zero-day (no patch exists), APT (a persistent, resourced intruder), botnet (the compromised fleet used to launch DDoS).

Social engineering is a network threat

The delivery methods

- Phishing — mass email
- Spear phishing — targeted at an individual
- Whaling — targeted at an executive
- Vishing — by voice call
- Smishing — by SMS
- Pretexting — inventing a scenario to justify the request

Why it works

- Urgency and authority short-circuit judgement
- It bypasses every technical control at once
- One credential can be worth more than any exploit
- It scales cheaply — cost per attempt is near zero

What actually helps

- Awareness training, repeated and measured (Domain 5)
- Multi-factor authentication, so a stolen password is insufficient
- Verification procedures for payment and access changes
- A culture where challenging a request is safe

Phishing is the most common initial access route in real incidents, which is why it appears across three domains.

4.5

LESSON

Detection and Prevention

OBJECTIVE

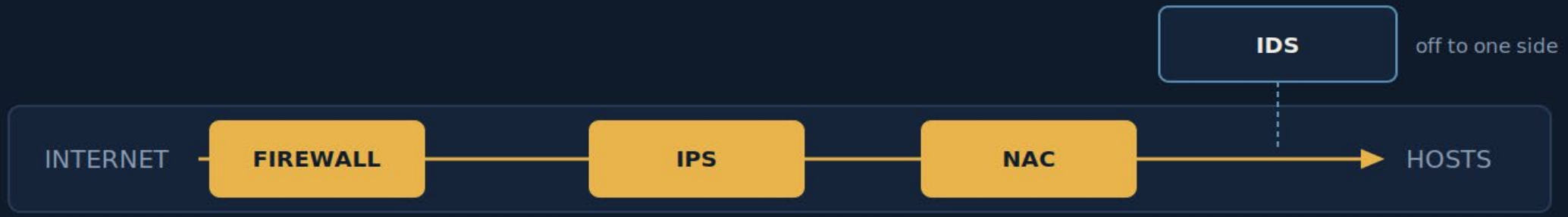
Describe the common tools used to identify and prevent threats, and state precisely what distinguishes an IDS from an IPS.

- Firewall types, from packet-filtering to next-generation
- IDS versus IPS — the tested distinction
- Host-based versus network-based, signature versus anomaly
- Antimalware, scanning, SIEM and honeypots

LESSON 4.5

Where each tool sits

Where each tool sits, and what it actually does.



FIREWALL

Allows or blocks by rule
Packet-filtering, stateful, proxy, WAF, next-gen
PREVENTS

IDS

Watches and alerts
Host-based or network-based
Signature or anomaly
DETECTS ONLY

IPS

Watches and blocks
Sits in the traffic path
False positives break real traffic — PREVENTS

SIEM

Collects and correlates logs
Across many systems
Finds patterns no single device can see

The tested distinction: IDS detects and alerts. IPS detects and blocks. That is the whole difference.

Firewall types, simplest to most capable

Packet-filtering	Decides per packet on source, destination, port and protocol. Fast, stateless, and blind to context.
Stateful inspection	Tracks connection state, so it can tell a legitimate reply from an unsolicited packet. The practical baseline.
Proxy	Terminates the connection and makes its own on the client's behalf. Can inspect content; adds latency.
WAF	Web application firewall. Inspects HTTP specifically for application attacks such as injection and cross-site scripting.
Next-generation	Stateful inspection plus application awareness, user identity and integrated threat intelligence.

A firewall enforces a rule set. It cannot stop an attack that arrives over a permitted port in permitted traffic.

LESSON 4.5 — DETECTION

Two axes to classify detection

Where it sits

- HIDS — host-based: watches one system, sees encrypted traffic after decryption and local file changes
- NIDS — network-based: watches a segment, sees traffic between hosts but not inside encryption

How it decides

- Signature-based: matches known patterns. Accurate on known threats, blind to novel ones
- Anomaly or behaviour-based: flags deviation from a learned baseline. Can catch novel attacks; produces more false positives

Why the combination matters

- A signature-based NIDS is blind to a zero-day inside TLS. This is exactly the gap host-based and anomaly-based tools are deployed to cover

LESSON 4.5 — OTHER TOOLS

The rest of the toolkit

Antimalware

- Signature and behaviour detection on endpoints
- Requires current definitions
- Scheduled and on-access scanning

Scanning

- Vulnerability scans find known weaknesses
- Port scans reveal what is listening
- Penetration testing goes further — authorised exploitation

SIEM

- Aggregates and correlates logs from many sources
- Finds patterns no single device can see
- Only as good as the logs it receives

Honeypot

- A deliberately exposed decoy
- Any interaction with it is suspicious by definition
- A honeynet is a network of them

Note the pattern: none of these is preventive on its own. They inform decisions and shorten detection time.

4.6

LESSON

Data Centres and Redundancy

OBJECTIVE

Identify common data centre terminology and explain how redundancy is achieved at each level.

- Power, cooling and environmental control
- Fire detection and suppression
- Redundancy: components, systems, sites
- MOU and MOA

What a data centre has to solve

Power

- UPS — bridges seconds to minutes
- Generator — bridges hours to days
- Dual feeds from separate substations

- A UPS without a generator only buys time to shut down cleanly

Cooling and environment

- HVAC to hold temperature and humidity
- Hot and cold aisle containment
- Humidity matters both ways: too low causes static, too high causes condensation

- Cooling failure takes a room offline as surely as power loss

Fire

- Detection: smoke, heat, flame sensors
- Suppression: wet pipe, dry pipe, pre-action, deluge
- Clean agent or gas systems suppress without water damage

- Pre-action needs two triggers — reduces accidental discharge

Life safety outranks equipment. Fire suppression design must permit people to leave first.

Redundancy at four levels

Component	RAID for disks, dual power supplies, teamed network interfaces. Survives one part failing.
System	Clustering and failover — a second server takes over. Often described as N+1: one spare beyond what is needed.
Connectivity	Two internet providers, ideally with physically separate cable routes. Two providers on one duct is one point of failure.
Site	A second facility, geographically separated. The hot, warm and cold sites from Domain 2.

The recurring principle: redundancy only helps if the redundant part does not share the failure. Correlated risk again.

MOU and MOA

The two terms

- MOU — Memorandum of Understanding. A statement of intent to cooperate. Broad, and typically not legally binding
- MOA — Memorandum of Agreement. More specific, setting out responsibilities and often obligations. Closer to a contract

Where they appear

- Shared facility arrangements
- Mutual aid between organisations
- Reciprocal recovery sites (Domain 2)
- Data-sharing between partners or agencies
- Compare with an SLA, which commits to measurable service levels and is contractual

4.7

LESSON

Cloud

OBJECTIVE

Recognise cloud service terminology, state who is responsible for what under each service model, and distinguish the deployment models.

- The five defining characteristics
- IaaS, PaaS and SaaS, and the responsibility split
- Public, private, hybrid and community
- MSP and SLA

LESSON 4.7 — CHARACTERISTICS

Five characteristics that define cloud

1. **On-demand self-service** — You provision resources yourself, without a human on the provider's side.
2. **Broad network access** — Reachable over the network from standard devices.
3. **Resource pooling** — Multi-tenancy — your workloads share physical infrastructure with other customers.
4. **Rapid elasticity** — Capacity scales up and down quickly, in principle automatically.
5. **Measured service** — Usage is metered and billed accordingly — the pay-for-what-you-use model.

Resource pooling is the one with security consequences: multi-tenancy means isolation is the provider's job and your risk.

Who is responsible for what

Who patches the operating system? The answer changes with the service model.

	On-premises	IaaS	PaaS	SaaS
Data & access	YOU	YOU	YOU	YOU
Application	YOU	YOU	YOU	PROVIDER
Runtime / middleware	YOU	YOU	YOU	PROVIDER
Operating system	YOU	YOU	PROVIDER	PROVIDER
Virtualisation	YOU	PROVIDER	PROVIDER	PROVIDER
Servers & storage	YOU	PROVIDER	PROVIDER	PROVIDER
Networking & facility	YOU	PROVIDER	PROVIDER	PROVIDER

The higher the service model, the less you manage — and the less you control.

Data and access are ALWAYS yours. No service model transfers responsibility for who you let in.

Data and access are always yours. No service model transfers responsibility for who you let in.

Four deployment models

The four

- Public — shared infrastructure, any customer. Cheapest, least control
- Private — dedicated to one organisation, on-premises or hosted. Most control, most cost
- Hybrid — a deliberate combination, often sensitive workloads private and burst capacity public
- Community — shared by organisations with common requirements, such as a group of health providers

Two more terms

- MSP — Managed Service Provider. A third party operating part of your IT. You retain accountability; they take operational responsibility
- SLA — Service-Level Agreement. Commits to measurable levels: uptime, response times, restoration times. This is where cloud promises become enforceable
- An SLA without penalties is a statement of intent

LESSON 4.7 — THE PRINCIPLE

Cloud moves responsibility, not accountability

You can outsource the operation.
You cannot outsource being answerable for it.

- A provider breach is still your breach as far as your customers and regulator are concerned
- This is the same point as transference in Domain 1 — the whole risk never moves
- Which is why due diligence, contract terms and SLAs matter as security controls
- And why data classification (Domain 5) has to happen before you decide what may go to cloud

4.8

LESSON

Secure Network Design

OBJECTIVE

Identify secure network design terminology and choose an appropriate design control for a described requirement.

- Defence in depth applied to networks
- Zero trust, and what it replaces
- Network access control
- DMZ, VLANs, microsegmentation, IoT separation, VPN

LESSON 4.8 — SEGMENTATION

Limit how far an intruder can move

Segmentation limits how far an intruder can move once inside.

A firewall between every zone. Traffic is filtered at each boundary, not just at the edge.

VLAN	Logical separation on shared switches — groups devices regardless of location
DMZ / screened subnet	Hosts that must be reachable from the internet, isolated from the LAN
Microsegmentation	Per-workload isolation — each server its own zone
IoT / OT segmentation	Cameras, sensors and industrial kit on their own network; they cannot be patched like servers
VPN	An encrypted tunnel across an untrusted network — extends the boundary, does not remove it

Two mental models

Two mental models. The second assumes the first has already failed.

- Verify explicitly — every request, every time
- Assume breach — design as if an attacker is already inside
- Least privilege — the smallest access that works
- Microsegmentation — contain what a compromise can reach

LESSON 4.8 — NAC

Network Access Control

What it does

- Decides whether a device may join the network at all
- Authenticates the device, commonly with 802.1X
- Checks posture: patch level, antimalware present, configuration compliant
- Places the device in an appropriate segment based on the result

Why organisations deploy it

- Contractor and personal devices arriving on the network
- Guest access that must not reach internal systems
- Quarantining non-compliant devices instead of refusing them outright
- It is the control that answers "an unknown laptop was plugged into a meeting-room port"

LESSON 4.8 — THE TERMS

Design terminology to recall precisely

DMZ	Also screened subnet. A segment for hosts that must be reachable from the internet, isolated so a compromise there does not reach the internal network.
VLAN	Logical segmentation on shared switching. Groups devices by function rather than physical location.
Microsegmentation	Isolation at the individual workload level — each server effectively its own zone. The practical mechanism behind zero trust.
VPN	An encrypted tunnel across an untrusted network. Extends the trusted boundary; it does not remove the need for controls inside it.
IoT / OT segmentation	Cameras, sensors and industrial equipment on their own network, because they often cannot be patched, hardened or monitored like servers.

A VPN protects data in transit. It does nothing about what the connected device does once inside.

4.9

LESSON

Consolidation

OBJECTIVE

Recall the port pairs and layer numbers cold, and select an appropriate control for a described network requirement.

- Port and layer drills
- Threat identification drill
- Control selection drill
- The memorisation set and common traps

LESSON 4.9 — DRILL 1

Port and layer recall

Telnet, and its secure replacement

23 → SSH on 22

HTTP, and its secure counterpart

80 → HTTPS on 443

IMAP, and its secure counterpart

143 → IMAPS on 993

LDAP, and its secure counterpart

389 → LDAPS on 636

Which OSI layer has port numbers?

Layer 4 — Transport

Which OSI layer do routers work at?

Layer 3 — Network

Which OSI layer do switches work at?

Layer 2 — Data Link

DNS, RDP and SMB port numbers

53, 3389, 445

Cover the amber answers. These must be instant — no reasoning recovers a forgotten port number.

LESSON 4.9 — DRILL 2

Name the threat

Spreads across the network with no user action

Worm

Attacker reads and alters traffic between two parties

On-path / man-in-the-middle

Disguised as legitimate software the user installs

Trojan

Valid captured traffic is sent again to repeat an action

Replay attack

Dormant code triggered by a future condition

Logic bomb

Half-open connections exhaust the server

SYN flood

Thousands of sources flood a site at once

DDoS — usually a botnet

Secrets inferred from timing or power draw

Side-channel attack

LESSON 4.9 — DRILL 3

Choose the design control

Web servers must be internet-reachable safely

DMZ / screened subnet

Cameras cannot be patched or hardened

IoT segmentation on a separate network

Unknown laptop plugged into a meeting room port

NAC with posture checking

One compromised server reaches every other

Microsegmentation

Finance traffic must not mix with general staff

VLAN segmentation

Remote work made the perimeter meaningless

Zero trust architecture

Staff need office access from home

VPN — plus MFA

Need to know an intrusion happened, not block it

IDS — detects and alerts only

Note the last one. If a question says detect but not block, IPS is the wrong answer.

LESSON 4.9 — MEMORISE

Produce these, don't just recognise them

Numbers

- OSI 7 layers, in order, both directions
- TCP/IP 4 layers and the mapping
- IPv4 = 32 bits, IPv6 = 128 bits
- MAC = 48 bits
- Ranges: 0–1023, 1024–49151, 49152–65535
- Port pairs: 23/22, 80/443, 25/465, 110/995, 143/993, 389/636, 21/22, 53, 445, 3389

Distinctions

- IDS detects · IPS blocks
- Virus needs a host · worm does not
- DoS one source · DDoS many
- TCP reliable · UDP fast
- HIDS one host · NIDS a segment
- Signature known · anomaly novel
- MOU intent · MOA agreement · SLA measurable

Cloud and design

- Five characteristics: self-service, broad access, pooling, elasticity, measured
- IaaS you patch the OS · PaaS and SaaS the provider does
- Data and access always yours
- Public, private, hybrid, community
- DMZ, VLAN, microsegmentation, VPN, NAC, zero trust

Three flashcard decks, not one. Numbers need daily drilling; distinctions need a single clear sentence each.

COMMON TRAPS

Where marks get lost

IPS when it says detect

- If the requirement is to know about it, not stop it, the answer is IDS
- Read the verb in the question

NAT as security

- NAT conserves addresses and obscures internal addressing
- It is not a firewall and not an access control

Hiding the SSID

- Not a security control — trivially discovered
- Same for MAC filtering, which spoofing defeats

Cloud transfers risk

- It transfers operation, not accountability
- Data and access responsibility never moves

And: assuming a VPN secures the endpoint. It secures the tunnel. A compromised laptop on a VPN is a compromised laptop inside your network.

Next: Domain 5

Security Operations

18% of the exam. Data security and encryption, system hardening, configuration management, security policies, and awareness training.

Before you move on: can you give the secure counterpart and port for Telnet, HTTP, IMAP and LDAP without hesitating, and say in one sentence what separates an IDS from an IPS?