📘 Domain 3: Security Architecture (18%)

🔹 3.1 Secure Network Design

🧱 Network Segmentation

- **Divides a network into smaller zones to reduce attack surfaces.**
- **Example: Public web servers in one segment, internal HR servers in another.**
- **Tools: VLANs, firewalls, routers.**

🔐 DMZ (Demilitarized Zone)

- **A semi-public zone between internal and external networks.**
- **Hosts public-facing services (e.g., web server, mail server).**
- **Separates external access from internal resources.**

🔄 East-West vs North-South Traffic

Direction	Description
North-South	Traffic between internal network and external sources
East-West	Lateral movement inside internal networks

✅ **Micro-segmentation limits East-West traffic to prevent lateral spread of malware.**

🚦 Firewalls and ACLs

Type	Description
Packet-filtering	**Simple, uses IPs/ports**
Stateful Inspection	**Tracks active sessions**
NGFW (Next-Gen)	**Adds deep packet inspection, application-layer filtering**
ACL (Access Control List)	**Rules on routers/firewalls to allow or deny traffic**

📡 VPN (Virtual Private Network)

- **Creates secure, encrypted tunnels over untrusted networks.**
- **Common Protocols:**
  - **IPSec (L2TP/IPSec) – Network-layer encryption**
  - **SSL/TLS VPN – Browser-based access**

> ⚠️ **Split tunneling allows both secure VPN and unsecured internet traffic — may be a risk!**

🌐 Proxies and Load Balancers

Component	Purpose
Proxy Server	**Hides client identity, filters requests**
Reverse Proxy	**Protects backend servers, handles incoming traffic**
Load Balancer	**Distributes traffic across multiple servers to ensure availability**

🔹 3.2 Secure Protocols

Protocol	Purpose	Secure Version
HTTP	Web traffic	HTTPS
FTP	File transfer	SFTP or FTPS
Telnet	Remote access	SSH
SNMPv1/2	Network management	SNMPv3 (uses encryption/auth)
LDAP	Directory services	LDAPS
RDP	Remote desktop	Use with TLS + network-level authentication

✅ Always use secure versions (encrypted) of common protocols.

🔹 3.3 Wireless Network Security

🔒 Encryption Standards

Standard	Encryption	Status
WEP	RC4	Obsolete (insecure)
WPA	TKIP	Weak
WPA2	AES (CCMP)	Still widely used
WPA3	SAE (Simultaneous Authentication of Equals)	Latest and strongest

🔐 Always use WPA3 if available. Avoid WEP and WPA.

📡 Wireless Security Tools

- SSID Hiding: Security through obscurity — not strong protection.
- MAC Filtering: Can be bypassed via spoofing.
- Geofencing: Limits signal range to physical locations.
- Captive Portals: Used in public Wi-Fi to force login or consent.

🔹 3.4 Secure System Design

🔧 Hardening Techniques

- Disable unused ports/services
- Change default credentials
- Apply patches and updates
- Implement least privilege
- Remove unnecessary software

🧩 Trusted Platform Module (TPM)

- Hardware chip for secure storage (e.g., encryption keys, BitLocker)

🧱 Secure Boot & UEFI

- Secure Boot: Verifies the OS is unaltered at startup
- UEFI: Modern BIOS replacement with enhanced security

🔹 3.5 Cloud Security Architecture

☁️ Cloud Models

Model	Description	Example
IaaS	Infrastructure as a Service (user manages OS, apps)	AWS EC2
PaaS	Platform as a Service (user manages apps only)	Google App Engine
SaaS	Software as a Service (everything managed)	Gmail, Dropbox

🔐 Cloud Security Best Practices

- Data encryption (in transit & at rest)
- Strong authentication (MFA)
- Secure APIs
- Shared responsibility model

> ⚠️ In IaaS, the user secures the OS. In SaaS, the provider does.

🔹 3.6 Secure Application Architecture

🧱 Key Concepts:

- Sandboxing – Isolates application processes from each other
- Containerization – Uses Docker, Kubernetes for isolated environments
- Code signing – Ensures app integrity and origin
- Input validation – Protects against injection attacks

🔹 3.7 Physical Security Controls

Control Type	Examples
Deterrent	**Signs, lighting, visible cameras**
Preventive	**Locks, fences, mantraps**
Detective	**CCTV, motion detectors, alarms**
Compensating	**Guards when tech fails**

💾 Hardware Security

- **Faraday Cage – Blocks electromagnetic signals**
- **Air Gap – Keeps systems completely disconnected from networks**

📌 Key Takeaways for Domain 3

- **Be able to design a secure network using segmentation, firewalls, DMZ, VPN.**
- **Memorize secure protocol equivalents.**
- **Understand cloud roles and shared responsibility.**
- **Know differences between WPA2 vs WPA3, and why WEP/WPA are insecure.**
- **Expect questions on hardening systems and wireless attacks.**