Exam Cram Notes: Securing Enterprise Infrastructure

1. Overview

Securing enterprise infrastructure involves implementing security controls, best practices, and technologies to protect an organization's **network, systems, and data** from threats. This includes network security, endpoint protection, access control, and monitoring.

---

2. Network Security Controls

A. Network Segmentation

✅ **VLANs (Virtual Local Area Networks) –** Separate network traffic to limit lateral movement of threats.
✅ **Subnets –** Divide the network into smaller sections for better control and monitoring.
✅ **DMZ (Demilitarized Zone)** – Isolated area for public-facing services to prevent direct access to internal networks.
✅ **Air-Gapped Networks –** Physically separated networks for high-security environments (e.g., military, SCADA).

B. Network Access Controls (NAC)

✅ **802.1X Authentication –** Uses RADIUS or TACACS+ to verify users before granting network access.
✅ **MAC Address Filtering –** Restricts devices by their MAC addresses (not foolproof due to MAC spoofing).
✅ **Guest Networks** – Isolate guest users from internal resources.

C. Firewalls & Network Security Devices

✅ **Stateful Firewalls –** Track the state of network connections to allow or block traffic.
✅ **Next-Generation Firewalls (NGFWs)** – Combine deep packet inspection (DPI), intrusion prevention, and malware filtering.
✅ **Web Application Firewalls (WAFs) –** Protect web apps from attacks like SQL injection & XSS.
✅ **Intrusion Detection Systems (IDS)** – Monitor network traffic for suspicious activity (alerts only).
✅ **Intrusion Prevention Systems (IPS) –** Block detected threats automatically.
✅ **DLP (Data Loss Prevention)** – Prevents unauthorized data transfers via network, email, or USB devices.

---

3. Endpoint Security & Device Hardening

A. Endpoint Protection

✅ **Antivirus & EDR (Endpoint Detection & Response)** – Detects malware and suspicious behavior.
✅ **Host-Based Firewalls** – Control inbound and outbound connections at the endpoint level.
✅ **Application Whitelisting** – Only allows pre-approved applications to run.
✅ **Patch Management** – Regular updates for OS, software, and firmware to fix vulnerabilities.

B. Hardening Systems & Devices

✅ **Disable Unnecessary Services & Ports** – Reduces attack surface.
✅ **Secure Configurations** – Use security baselines (CIS Benchmarks, NIST guidelines).
✅ **Remove Default Credentials** – Change default usernames and passwords.
✅ **Enable Full-Disk Encryption (BitLocker, FileVault)** – Protects data at rest.

---

4. Secure Remote Access

A. Virtual Private Network (VPN) Security

✅ **IPSec VPN** – Uses encryption (ESP) and authentication (IKE) for secure communication.
✅ **SSL/TLS VPN** – Browser-based secure access, often used for remote users.
✅ **Split Tunneling vs. Full Tunneling** – Full tunneling routes all traffic through the VPN, while split tunneling allows direct internet access.

B. Remote Access Controls

✅ **Zero Trust Architecture (ZTA)** – "Never trust, always verify"; continuously authenticates users & devices.
✅ **RDP (Remote Desktop Protocol) Security** – Disable when not needed; use strong authentication (MFA).
✅ **Cloud Access Security Broker (CASB)** – Monitors and secures cloud-based applications.
✅ **Geolocation & Conditional Access** – Restrict access based on user location and risk level.

---

5. Securing Wireless Networks

✅ **WPA3 (Wi-Fi Protected Access 3)** – Strongest encryption for wireless security.
✅ **Disable WPS (Wi-Fi Protected Setup)** – Prevents brute-force PIN attacks.
✅ **MAC Address Randomization** – Protects against tracking and sniffing.
✅ **Hidden SSIDs (Limited Benefit)** – Security through obscurity is not a strong defense.
✅ **Enterprise Authentication (802.1X + RADIUS)** – Ensures only authorized users can access Wi-Fi.

---

6. Logging, Monitoring, & Incident Response

A. Security Information and Event Management (SIEM)

✅ **Collects & Analyzes Logs** – Centralized monitoring of security events.
✅ **Correlates Data** – Identifies suspicious patterns in logs.
✅ **Automated Alerts & Incident Response** – Detects threats in real-time.

B. Network & Host Monitoring

✅ **NetFlow Analysis** – Monitors network traffic patterns.
✅ **File Integrity Monitoring (FIM)** – Detects unauthorized file changes.
✅ **Honeypots & Deception Technology** – Lures attackers to fake systems for analysis.

---

7. Redundancy & Resiliency in Enterprise Infrastructure

A. High Availability & Fault Tolerance

✅ **Load Balancers** – Distributes traffic to prevent server overload.
✅ **Clustering** – Multiple systems working together for redundancy.
✅ **RAID (Redundant Array of Independent Disks)** – Protects against disk failures.

B. Backup & Disaster Recovery

✅ **Offsite & Cloud Backups** – Protects against ransomware and hardware failures.
✅ **Cold, Warm, Hot Sites** – Different levels of disaster recovery readiness.
✅ **RTO & RPO (Recovery Time Objective & Recovery Point Objective)** – Defines recovery speed & data loss tolerance.

---

8. Key Exam Takeaways

✅ **Network segmentation (VLANs, subnets, DMZ) reduces attack surfaces.**
✅ **NAC (802.1X) and firewalls prevent unauthorized access.**
✅ **Patch management, EDR, and system hardening protect endpoints.**
✅ **Zero Trust & VPNs enhance secure remote access.**
✅ **SIEM, NetFlow, and honeypots improve monitoring & threat detection.**
✅ **Redundancy (RAID, load balancers) and backups ensure business continuity.**