

Introduction to Network Security

Introduction to Network Security

Key concepts, goals, and foundational components

1. What Is Network Security?

- **Definition** – The practice of protecting the integrity, confidentiality, and availability of data and resources as they travel across or reside within a computer network.
 - **Why It Matters** – Networks are the backbone of modern organizations; a breach can lead to data loss, financial damage, reputational harm, and legal penalties.
-

2. Core Objectives (CIA Triad)

Objective	What It Means	Typical Controls
Confidentiality	Prevent unauthorized access to data	Encryption, access control lists, VPNs
Integrity	Ensure data is accurate and unaltered	Checksums, digital signatures, hashing
Availability	Keep services reachable when needed	Redundancy, load balancing, DDoS mitigation

3. Main Threat Categories

Threat Type	Description	Example
Passive attacks	Eavesdrop or monitor traffic without altering it	Packet sniffing, traffic analysis
Active attacks	Interfere with, modify, or destroy data	Man-in-the-middle, injection, ransomware
Internal threats	Originating from trusted insiders (employees, contractors)	Credential abuse, accidental misconfiguration
External threats	Actors outside the organization	Hackers, nation-state actors, botnets

Introduction to Network Security

4. Fundamental Security Controls

4.1 Perimeter Defenses

- **Firewalls** – Packet filtering, stateful inspection, next-generation firewalls (NGFW) with application awareness.
- **Intrusion Detection/Prevention Systems (IDS/IPS)** – Signature-based and anomaly-based detection of malicious traffic.

4.2 Network Segmentation

- **VLANs & Subnets** – Logical separation of traffic.
- **DMZ (Demilitarized Zone)** – Isolates public-facing services from internal assets.
- **Zero-Trust Architecture** – Verify every request, regardless of location.

4.3 Secure Communication

- **VPNs (IPsec, SSL/TLS)** – Encrypt traffic over untrusted networks.
- **TLS/SSL** – Protect web, email, and other application protocols.
- **SSH** – Secure remote command-line access.

4.4 Endpoint Protection

- **Antivirus/Anti-malware** – Detect known threats.
- **Host-based firewalls** – Enforce local traffic policies.
- **Patch management** – Keep OS and applications up-to-date.

4.5 Authentication & Authorization

- **Password policies** – Complexity, rotation, lockout.
- **Multi-Factor Authentication (MFA)** – Something you know + something you have/are.
- **Role-Based Access Control (RBAC)** – Grant permissions based on job function.

4.6 Monitoring & Logging

- **Security Information and Event Management (SIEM)** – Collect, correlate, and alert on log data.

Introduction to Network Security

- **NetFlow / sFlow** – Traffic analysis metadata.
 - **Regular audits** – Verify compliance and detect drift.
-

5. Common Network Security Protocols

Protocol	Purpose	Typical Use
IPsec	Secure IP layer (confidentiality, integrity)	Site-to-site VPNs
TLS/SSL	Secure application layer	HTTPS, FTPS, SMTPS
SSH	Secure remote administration	Server management, file transfer (S