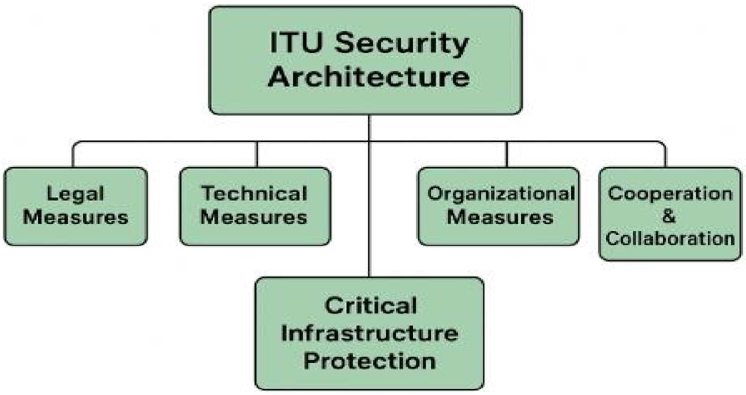
OSI MODEL (Open Systems Interconnection Model)

The OSI model is a conceptual reference framework developed by ISO to standardize how different systems communicate over a network.
It divides the communication process into **7 layers**, each with clear **functions, protocols, addresses, and security considerations**.

Why OSI is important in Network Security?

- Helps **identify where vulnerabilities** exist (e.g., ARP spoofing at Data Link layer, SQL Injection at Application layer).
- Helps **design security controls** layer-wise (firewalls, encryption, authentication, etc.).
- Provides a **structured approach** for troubleshooting attacks and network issues.


ITU Security Architecture
Legal Measures
Technical Measures
Organizational Measures
Cooperation & Collaboration
Critical Infrastructure Protection

The **International Telecommunication Union (ITU)** is a UN-specialized agency responsible for **global ICT (Information and Communication Technology)** standards and cybersecurity development.

While **ITU-T X.800** specifically deals with OSI security architecture, the broader **ITU Security Architecture** refers to **ITU's global cybersecurity framework**, which consists of **multi-level security pillars** that guide countries and organizations in building secure ICT ecosystems.

This architecture is commonly represented through **5 or 6 core components**.

1. Legal Measures: Legal measures focus on creating a **legal foundation for cybersecurity**. These laws enable nations to prevent, detect, investigate, and punish cybercrimes.

Key Elements:

- Cybercrime laws and IT-specific legislation
- Data privacy and data protection laws
- Digital evidence handling rule
- Cyber incident reporting obligations
- International legal harmonization (common definitions of cybercrime)

Objectives

- Define what constitutes cybercrime
- Support law enforcement agencies
- Enable prosecution of offenders.
- Protect users' rights and privacy

Examples

- National Cybersecurity Acts
- IT Acts (e.g., IT Act 2000 and amendments)
- Digital privacy regulations

2. Technical Measures TSBP

These are **technical controls, standards, protocols, and best practices** recommended by ITU for secure networks, devices, and services.

Key Technical Components

- Security standards for communication networks
- Cryptographic techniques
- Secure authentication and access control mechanisms
- Security in 5G, IoT, and cloud systems
- Incident detection and response tools

Important ITU Standards (other than X.800)

- **X.805** – End-to-end network security framework
- **X.1036** – Information security management guidelines
- **Y.2701** – NGN (Next Generation Networks) security
- **Y.3051** – IoT security framework

Objectives

- **Prevent** unauthorized access
- Ensure confidentiality, integrity, availability
- **Protect** telecom infrastructure
- **Improve** resilience against cyber attacks

3. Organizational Measures: These ensure that organizations adopt proper **processes, governance structures, and security policies**.OPGS

Key Elements

- National cybersecurity strategies
- Cybersecurity governance (roles, responsibilities, committees)
- Organizational security policies and SOP
- Security audits and compliance frameworks
- Adoption of ISMS (Information Security Management Systems)
- Establishment of **CERTs/CSIRTs**

Objectives

- Build systematic security operations
- Reduce risk via structured management
- Ensure accountability within organizations
- Align with global standards like ISO 27001

4. Capacity Building

ITU emphasizes strengthening human and institutional capabilities in developing and developed nations.

Key Activities

- Training programs for cybersecurity professionals
- Workshops on incident handling, forensics, secure coding
- Awareness programs for citizens
- Development of cybersecurity education curriculum
- Advisory support to governments

Objectives

- Improve technical expertise
- Promote cyber hygiene among users
- Strengthen national response capabilities
- Support developing nations in building security capacities

5. Cooperation & Collaboration

Cybersecurity is a shared global responsibility. ITU promotes cooperation at multiple levels.

Key Collaboration Areas

- International cyber threat intelligence sharing
- Cooperation between governments
- Public-private partnerships
- Emergency response coordination
- Sharing best practices and technical knowledge

Global Partners

- INTERPOL
- UNODC
- World Bank
- Regional CERTs
- Private organizations (ISPs, vendors, telecom operators)

Objectives

- Combat cross-border cybercrime
- Improve speed of incident response
- Build global trust
- Unified standardization of cybersecurity efforts

6. Critical Infrastructure Protection (CIP)

(Sometimes shown as a separate pillar, sometimes part of Technical/Organizational Measures)

Critical infrastructure includes systems essential for national security and public welfare: telecom, power grids, finance, transportation, healthcare, etc.

Key Components

- Risk assessment for critical infrastructure
- Protection of telecom and internet backbone
- Disaster recovery and business continuity planning
- Securing SCADA/ICS systems
- National-level resilience planning

Objectives

- Prevent large-scale disruption
- Ensure continuity of essential services
- Reduce national vulnerability

Why ITU Security Architecture Is Important

- Provides a **global model** for countries to build cybersecurity systems
- Standardizes national cybersecurity strategies
- Helps developing countries with resources and frameworks
- Ensures secure communication networks worldwide
- Facilitates international collaboration to handle global threats

Zero Trust Model:

The **Zero Trust Model (ZTM)** is a modern security framework based on the principle:

“Never Trust, Always Verify.”

Traditional security models trusted internal networks and used firewalls as a boundary.
But Zero Trust assumes:

- **No user, device, or application is trustworthy by default**, whether inside or outside the network.
- Every access request must be **continuously authenticated, authorized, and monitored**.

It was introduced by **Forrester Research (John Kindervag, 2010)**.

2. Why Zero Trust is needed? CRITSL

Modern networks face new problems:

1. **Cloud-based systems** – no fixed perimeter
2. **Remote employees** – work-from-home, VPN weaknesses
3. **IoT devices** – insecure & unmanaged
4. **Internal threats** – insider attacks
5. **Sophisticated cyberattacks** – ransomware, APTs
6. **Data leakage** due to misconfigurations

Zero Trust solves these by enforcing strict verification on **every user, every device, every access request. UDA**

3. Core Principles of Zero Trust Model [VELBMC]

Zero Trust is built on **five major principles**:

1. Verify explicitly

Always authenticate and authorize based on:User identity,Device health,Location,Application requesting access,Time of request &Risk level

Tools: MFA, identity providers, certificates.

2. Least Privilege Access

Give **minimum required permissions** to perform tasks.

Example:
A user who needs only database read access is not given write or admin access.

Tools: RBAC, ABAC, IAM policies.

3. Assume breach MIC

Always design the system as if an attacker is already inside.

Meaning:

- Internal network is **not trusted**.
- Micro-segmentation is used.
- Continuous monitoring is required.

4. Micro-Segmentation

- Network is divided into **small security zones**.
- Even if one zone is breached, attacker **cannot move laterally**.

Example:
Web server, application server, database server all placed in separate segments.

5. Continuous Monitoring & Logging

Logs must be checked in real-time:

- User activity
- Device behavior
- Network traffic
- Access patterns

Tools: SIEM (Security Information & Event Management), threat analytics.

Architecture / Components of Zero Trust Model

Zero Trust Architecture contains the following components:**[IPDS NPEDM]**

1. Identity Provider (IdP)

Handles authentication of users & applications.
Examples: Azure AD, Okta, Google IAM.

2. Device Security

- Ensure devices comply with policies before giving access.
- Checks include:OS version,Patch status,Antivirus &Device certificate

3. Network Segmentation / Micro-Perimeters

Divide the network into **low-risk, isolated segments**.

4. Policy Enforcement Point (PEP)

Decides whether user/device should get access.

Example:
Firewalls, secure gateways, proxy servers.

5. Policy Decision Point (PDP)

Applies Zero Trust policies and provides “allow/deny” decisions.

6. Continuous Diagnostics & Monitoring (CDM)

Monitors traffic, behavior, and anomalies.

Technologies used in Zero Trust

Zero Trust can be implemented using:

- **MFA** (Multi-Factor Authentication)
- **Identity & Access Management (IAM)**
- **Next-Gen Firewalls (NGFW)**
- **Micro-segmentation tools** (VMware NSX, Cisco ISE)

- Zero Trust Network Access (ZTNA)
- **Endpoint Detection & Response (EDR)**
- **Behavioral Analytics** (UEBA)
- TLS/SSL Encryption
- **VPN Alternatives** (Secure Access Service Edge – SASE)

Feature	Traditional Security	Zero Trust
Trust Model	**Trust inside, untrusted outside**	Trust no one
Perimeter	Strong perimeter	No fixed perimeter
Access	Once authenticated → free access	Continuous validation
Lateral Movement	Easy	Very restricted
Device Security	Low priority	High priority
Monitoring	After incident	Continuous

TMPAL DM

7. Steps to Implement Zero Trust IAM MSIMA HEM

A practical Zero Trust deployment includes these steps:

1. **Identify & classify assets** (users, devices, apps, data).
2. **Map transaction flows** (who accesses what).
3. **Create micro-segments** for isolation.
4. **Establish identity-based policies**.
5. **Enable MFA & strong authentication**.
6. **Verify device health & compliance**.
7. **Use encryption everywhere**.
8. **Monitor continuously** via logs, SIEM, and analytics.

8. Advantages of Zero Trust

- Strong protection against **insider threats**
- Prevents **lateral movement** in case of breach
- Enhances **data security**
- Supports **remote work** securely
- Reduces attack surface
- Works well with **cloud environments**
- Provides better **visibility** into network traffic

9. Limitations / Challenges of Zero Trust

- High implementation cost
- Requires redesigning network architecture
- Requires trained security teams
- Continuous monitoring can increase overhead
- Integration complexity for legacy systems
- Resistance from employees (more authentication steps)

10. Real-World Use Cases of Zero Trust GBHIT

- **Google BeyondCorp** → One of the world's first Zero Trust models.
- **Banks** → Protect financial transactions.
- **Government agencies** → Prevent espionage.
- **IT companies** → Secure cloud and hybrid infrastructure.
- **Healthcare** → Protect patient data.

Local Area Network (LAN) : connects computers within a limited area such as a college, office, building, or campus.

LAN Management refers to the **planning, configuration, monitoring, securing, and troubleshooting** of LAN resources.

Effective LAN management ensures:**PRSA MD**

- High performance
- Reliable communication
- Security & access control
- Minimal downtime

It is a crucial part of **network security administration**.

2. Objectives of LAN Management

- **Efficient resource sharing** (printers, files, servers)
- **Reliable connectivity** within the organization
- **High network performance**
- **Ensure security** of devices and data
- **Monitoring of network faults**
- **User and device management**
- **Cost-effective operation and maintenance**

3. Components of a LAN

Understanding LAN components is essential for their management.

1. Networking Devices :

Switches,Routers,Access Points & Firewalls

2. Network Media

Ethernet cables (Cat5e, Cat6),Fiber optic cables & Wireless radio frequencies

3. Protocols

Ethernet,TCP/IP,DHCP, DNSVLAN, STP

4. Servers: File servers,Authentication servers,Application servers

5. End Devices

PCs ,Laptops ,Printers & IoT devices

4. Key Functions of LAN Management CFPS UANS

1. Configuration Management

Ensures that the LAN is configured correctly and optimally.

Tasks include:

- ✓ Setting up switches and routers
- ✓ Assigning IP addresses and subnetting
- ✓ Configuring VLANs
- ✓ Setting routing protocols
- ✓ Configuring Wi-Fi SSIDs and security
- ✓ Updating firmware and software
- ✓ Maintaining configuration backups

Benefits:

- ✓ Prevents misconfigurations
- ✓ Standardizes network layout
- ✓ Improves network security

2. Fault Management DID RD

Detects, logs, and resolves network issues.

Steps include:

1. **Detection:** Using monitoring tools
2. **Isolation:** Identify root cause
3. **Diagnosis:** Using commands (ping, traceroute)
4. **Resolution:** Applying fixes
5. **Documentation:** For future reference

· **Tools:**SNMP, network monitoring systems like Nagios, SolarWinds.

3. Performance Management

Ensures that the network operates at peak efficiency

Performance metrics:BLPSR

- ✓ Bandwidth usage
- ✓ Latency
- ✓ Packet loss
- ✓ Switch and router performance

Methods:

- ✓ Load balancing
- ✓ Upgrading hardware
- ✓ (Quality of Service)

4. Security Management

Protects LAN from internal/external threats.Ensure CIA

Security tasks:

- ✓ Configure firewalls
- ✓ Enabling VLAN segmentation
- ✓ Using Access Control Lists (ACLs)
- ✓ Enabling WPA3 for Wi-Fi
- ✓ Monitoring suspicious traffic
- ✓ Applying security patches
- ✓ Enforcing authentication policies (802.1X)

5. User Management

Maintains user accounts, roles, and permissions.

Includes:

- ✓ Adding/removing users
- ✓ Enforcing password policies
- ✓ Role-based access control (RBAC)
- ✓ Multi-factor authentication (MFA)
- ✓ Managing user privileges

6. Address & Name Management

Involves management of:

DHCP (Dynamic Host Configuration Protocol)

Automatically assigns IP addresses.

DNS (Domain Name System)

Converts domain names into IP addresses.

Tasks:

- ✓ IP address allocation
- ✓ IP conflict resolution
- ✓ Managing DNS records
- ✓ DHCP scope configuration

6. Security in LAN Management

LANs are often vulnerable to internal attacks.

Major security threats:

- ✓ Unauthorized access
- ✓ MAC spoofing
- ✓ ARP poisoning
- ✓ Rogue access points
- ✓ Malware spread
- ✓ Broadcast storms

Security Techniques:

1. Port Security: Limits MAC addresses allowed on a port.

2. 802.1X Authentication: Provides secure, port-based network access.

3. VLAN Segmentation: Separates sensitive departments.

4. Firewall Rules: Filters traffic based on IP, port, protocol.

5. IDS/IPS: Detects and prevents malicious behavior.

6. Patch Management: Keeps firmware updated.

7. Disable Unused Ports: Prevents unauthorized connections.

8. Strong Wi-Fi Security:WPA3/WPA2, long passwords.

9. Endpoint Security: Antivirus, EDR, device hardening.

7. Tools Used in LAN Management

- **Simulation Tools:**Cisco Packet Tracer,GNS3
- **Monitoring Tools:**SolarWinds,PRTG,Nagios
- **Analysis Tools:**Wireshark,ManageEngine OpManager

8. Advantages of LAN Management

- Improved reliability
- Higher security
- Efficient troubleshooting
- Reduced downtime
- Faster communication
- Better device and user control

9. Challenges in LAN Management

- Increasing devices (IoT, BYOD)
- Complex VLAN configurations
- Firmware vulnerabilities
- Insider threats
- Wi-Fi interference and congestion
- High dependency on skilled administrators

Web Security: WAS

- Web Security refers to the **protection of websites, web applications, and web servers** from cyberattacks, unauthorized access, and data breaches.
- It ensures secure communication between client (browser) and server, and protects user data during transmission and storage.

•

Web Security is **essential** because:

- Most services today (banking, e-commerce, social media) run on web applications.
- Web servers are constantly exposed to the internet.
- Attackers often target websites because they contain **sensitive data**.

1. Goals of Web Security

Web Security is based on the **CIA Triad**:

1. Confidentiality

Ensure that sensitive data (passwords, financial info) is not accessed by unauthorized users.
→ **Achieved** by **HTTPS, encryption, access control**.

2. Integrity

Ensure data is not modified, tampered, or corrupted.
→ Achieved by **hashing, digital signatures, input validation**.

3. Availability

Ensure the website/web application is always available. Protected using **load balancers, DDoS protection, redundancy**.

4. Authentication

Verify user identity.
→ Achieved by **username/password, MFA, OAuth, digital certificates**.

5. Authorization

Ensures user accesses only the allowed resources.
→ Role-based access control (RBAC), session tokens.

6. Non-Repudiation

Users cannot deny their actions.
→ Achieved with **logs, digital signatures**.

Common Web Security Threats

These are the most common attacks found in web applications

1. SQL Injection (SQLi)

The attacker inserts malicious SQL into input fields to read or modify DB data.

Impact:

- Database compromise
- Leakage of sensitive information
- Deletion/modification of data

Prevention:

- Prepared statements
- ORM frameworks
- Input validation

2. Cross-Site Scripting (XSS)

Attacker injects malicious JavaScript into web pages.

3 Types:

1. Stored XSS
2. Reflected XSS
3. DOM-based XSS

Impact:

- Steal cookies
- Hijack sessions
- Deface website

Prevention:

- Input sanitization
- Output encoding
- Content Security Policy (CSP)

3. Cross-Site Request Forgery (CSRF)

Attacker tricks user into performing actions without consent (e.g., transferring money).

Example:

Malicious link forces victim to submit form unknowingly.

Prevention:

- CSRF tokens
- SameSite cookies
- Re-authentication for critical actions

4. Broken Authentication

Weak login systems allow attackers to bypass authentication.

Common issues:

- Weak passwords
- No account lockout
- Session ID exposed

Prevention:

- MFA
- Strong password policies
- Secure session management

4. Web Security Mechanisms & Controls

1. HTTPS (SSL/TLS)

Secures communication using encryption.

Provides:

- Confidentiality
- Data integrity
- Authentication (via SSL certificate)

2. Web Application Firewall (WAF)

- Filters and monitors web traffic.
- Protects against:SQLi,XSS,CSRF & Bot attacks
- Examples: **Cloudflare WAF, AWS WAF.**

3. Authentication & Authorization Controls

Techniques:

OAuth 2.0,JWT (JSON Web Tokens),MFA (Multi-Factor Authentication),Role-based access control (RBAC)

4. Secure Coding Practises

Validate input, Escape output,Avoid eval() in JavaScript,Use prepared statements,Use latest frameworks

5. Session Security

- Generate unique session IDs
- Set secure & HttpOnly cookies
- Implement session timeout

6. Database Security

- Use least privileges
- Encrypt sensitive fields
- Disable remote access
- Use database firewalls

7. Server Hardening

- Disable unused port
- Configure firewall (iptables)

- Regular patching
- Use intrusion detection systems (IDS/IPS)

6. Web Security Tools

1. Burp Suite – Security testing

2. OWASP ZAP – Penetration testing

3. Nikto – Web server vulnerability scanner

4. Nessus – Vulnerability assessment

5. Acunetix – Automated scanner

6. Wireshark – Packet analysis

7. Secure Web Development Lifecycle (SWDLC)

Secure development includes:

1. **Requirements analysis** (define security needs)
2. **Design** (secure architecture)
3. **Implementation** (secure coding)
4. **Testing** (penetration testing) **PT**
5. **Deployment** (secure configuration) **DC**
6. **Maintenance** (patching and monitoring) **MP**

8. Best Practices for Web Security

1. Use HTTPS everywhere
2. Implement WAF & IDS/IPS
3. Validate user inputs
4. Encrypt cookies and data
5. Use updated frameworks
6. Perform regular penetration testing
7. Disable unnecessary services
8. Backup data regularly

6. Sensitive Data Exposure

Occurs when data is sent/stored without encryption.

Prevention:

- HTTPS
- Encrypt databases
- Mask sensitive fields

Digital Signature : **cryptographic technique** used to verify the **authenticity, integrity**, and **non-repudiation** of a digital message, software, or document. **AIR**

It **acts** like an electronic version of a handwritten signature but is **more secure**, mathematically generated, and legally recognized.

Digital signatures use **asymmetric key cryptography** (public–private key pairs).

2. Need for Digital Signature

Digital signatures are necessary in environments like:

- ✓ Online transactions
- ✓ E-commerce
- ✓ Emails
- ✓ Software distribution
- ✓ Legal documents and e-contracts

They ensure:

- ✓ **Authenticity** → verifies sender's identity
- ✓ **Integrity** → ensures message is not modified
- ✓ **Non-repudiation** → sender cannot deny sending the message

3. Working of Digital Signature

Digital Signature creation involves two major processes:

1. **Hashing the message**
2. **Encrypting the hash using sender's private key**

Step 1: Message Hashing

- Sender applies a **hash function** (SHA-256, SHA-512 etc.) to the message.
- Produces a fixed-size **Message Digest**

Example:

Message: "Hello"Hash: AFD34A89... (256-bit)

Step 2: Signing (Encrypting Hash)

- Sender encrypts the hash with **sender's private key**.
- Output = **Digital Signature**.

Step 3: Send Message + Signature

Sender sends:Original message &Digital signature

Step 4: Verification

Receiver performs:

1. Computes hash of received message
2. Decrypts signature using **sender's public key**
3. If both hashes match → message is authentic

Message → Hash Function → Message Digest → encrypt with private key → Digital Signature

Received message → Hash Function → Hash2

Received signature → decrypt using sender's public key → Hash1

If Hash1 = Hash2 → valid

5 Properties of Digital Signature AIRUV

1. Authenticity: Only the user who owns the private key could have created the signature.

2. Integrity: Any change to the message changes the hash, making the signature invalid.

3. Non-Repudiation: Signer cannot deny sending the message.

4. Unforgeable: Without private key, signature cannot be generated.

5. Verifiable: Anyone with public key can verify.

Algorithms Used for Digital Signature RS DEC Ed

1. RSA Digital Signature

- Uses RSA public-key algorithm
- Steps: hash → encrypt digest using private key

2. DSA (Digital Signature Algorithm)

- Standard by NIST
- Used in U.S. government application

3. ECDSA (Elliptic Curve DSA)

- More secure with shorter keys
- Used in Bitcoin, TLS, and modern systems

4. EdDSA

- Uses modern elliptic curve cryptography
- Faster and **more secure**

6. Hash Functions Used

Digital signatures rely on secure hash functions:

✓ SHA-1 (old, insecure)
✓ **SHA-256 (recommended)**
✓ SHA-384
✓ SHA-512

Hash function must be

1. Collision-resistant
2. Deterministic
3. Fast

Types of Digital Signatures DS BAQ

1. Basic (Simple) Digital Signature

Only uses hashing + encryption.

2. Advanced Digital Signature

Includes additional verification features like:

✓ Identity verification
✓ Timestamping

3. Qualified Digital Signature

Provided by trusted third-party CA (Certificate Authority) and legally binding.

9. Applications of Digital Signature

1. **Emails** – signing emails in Gmail, Outlook
2. **E-commerce** – secure online transactions
3. **Banking** – NEFT/RTGS authorizations
4. **Software signing** – Windows drivers, Android apps
5. **PDF Signing** – contracts, agreements
6. **E-Governance** – Aadhaar, e-filing, digital certificates

10. Attacks on Digital Signatures

1. Key Theft:If private key is stolen → attacker can sign messages.

2. Replay Attack: Reuse a valid signature with old message.

3. Hash Collision: If hash algorithm is weak, attacker may create a colliding message.

4. Man-in-the-Middle (MITM):Attacker swaps victim's public key with attacker's public key.

11. How to Secure Digital Signatures

- Use strong hashing algorithms (SHA-256, SHA-512)
- Private key must be stored securely (HSM, smart cards)
- Use PKI-based certificates
- Use timestamps
- Regularly rotate keys
- Implement two-factor authentication

12. Advantages of Digital Signature

- High level of security
- Valid in court (legally enforceable)
- Reduces paper usage
- Fast verification
- Prevents forgery
- Ensures accountability

13. Disadvantages

- Requires technical knowledge
- If private key is lost → signatures become invalid
- Dependence on CA (Certificate Authority)
- Needs secure key storage

Digital Certificate is an electronic document issued by a trusted authority (Certificate Authority – CA) to verify the **identity** of an individual, organization, or device. **DCA**

It binds:

- ✓ A **public key**
- ✓ With the **identity** of the owner (person, server, or organization)

Digital certificates are essential for **secure communication**, **authentication**, and **data encryption** over networks (e.g., HTTPS websites).

2. Why Digital Certificates Are Needed

1. To ensure **secure communication** using SSL/TLS
2. To verify the **identity** of websites, servers, or users
3. To prevent **man-in-the-middle attacks**
4. To support **digital signatures** and **PKI (Public Key Infrastructure)**
5. To ensure the **authenticity** of public keys

Without digital certificates, anyone could impersonate a website or user.

3. Components / Fields of a Digital Certificate

A standard digital certificate (X.509 Certificate) contains:

1. **Version Number**
2. **Serial Number** (unique ID assigned by CA)
3. **Signature Algorithm** (SHA-256 with RSA, ECDSA, etc.)
4. **Issuer Name** (Certificate Authority like DigiCert, eMudhra, VeriSign)
5. **Validity Period:**Start Date & Expiry Date
6. **Subject Name:**Person/organization/server to whom certificate is issued
7. **Public Key** of the subject
8. **Extensions:**Key usage,Extended key usage,Subject alternative names (SAN)
9. **Signature of CA:**Ensures authenticity

4. How a Digital Certificate Works

Step 1: Certificate Creation

User generates a key pair:

- ✓ Private Key
- ✓ Public Key

User sends public key + identity details to CA.

Step 2: CA Verification

CA verifies the identity:

- ✓ Domain ownership
- ✓ Organizational documents
- ✓ Person's identity

Step 3: Certificate Issuance

CA signs the certificate using **CA's private key**:

Digital Certificate = {Public Key + Identity Info + CA Signature}

Step 4: Certificate Installation

Website/server installs the certificate.

Step 5: Verification by Client

When a user visits a website:

- ✓ Browser receives server's certificate
- ✓ Browser verifies CA's digital signature using **CA's public key**
- ✓ If valid → secure connection established (HTTPS)

5. Types of Digital Certificates

1. SSL/TLS Certificates

Used for securing websites (HTTPS)

- DV (Domain Validation)
- OV (Organization Validation)
- EV (Extended Validation – green bar)

2. Code Signing Certificates

Used to sign:

- Software
- Drivers
- Applications

Ensures they are not tampered with.

3. Email Signing Certificates (S/MIME)

Used to:

- Sign emails
- Encrypt email content

4. Client Certificates

Used for user authentication instead of passwords.

5. Server Certificates

Used to authenticate servers (e.g., web servers, mail servers).

6. Root Certificates

Owned by Root CAs and stored in browsers/OS.
They issue certificates to intermediate CAs.

7. Intermediate Certificates

Used by intermediate CAs to sign end-user certificates.

6. X.509 Standard

The **X.509** standard defines the structure of digital certificates.

Key elements:

- Certificate format
- Fields (subject, issuer, public key, signature)
- Validation rules
- Extensions for advanced features

It is widely used in

- ✓ SSL/TLS
- ✓ Email security
- ✓ Smart cards
- ✓ VPN authentication

7. Certificate Hierarchy / Chain of Trust

Digital certificates operate in a **hierarchical trust model:**

Root CA
↓Intermediate CA
↓End-Entity Certificate (User/Server)

Root CA

- Trusted by operating systems and browsers
- Very secure, rarely used directly

Intermediate CA

- Issues certificates to organizations
- Used to reduce risk to the root CA

End-Entity Certificate

- Installed on websites or devices

8. Certificate Revocation

A certificate may be revoked if:

1. Private key is compromised
2. Owner information changes
3. Misuse detected
4. CA suspects fraud

Two revocation mechanisms:

1. CRL – Certificate Revocation List

A list of revoked certificates published by CA.

2. OCSP – Online Certificate Status Protocol

Real-time verification if certificate is valid.

9. Verification Process of a Digital Certificate

Browser receives the server certificate and checks:

1. **Signature Verification:**Uses CA's public key to verify CA’s signature
2. **Validity Period:**Checks expiration date
3. **Revocation Status:**Uses CRL/OCSP.

4. **Chain of Trust:**Verifies intermediate and root certificates.
5. **Domain Matching**:Checks if certificate belongs to the domain visited.

If all checks pass → connection becomes **HTTPS (secure)**.

Applications of Digital Certificates

1. HTTPS (Secure web browsing)
2. Digital signatures
3. Secure email (S/MIME)
4. VPN authentication
5. Smart card authentication
6. Securing IoT devices
7. E-commerce and online banking
8. Code signing (Windows, Android, iOS)

11. Advantages

1. Strong authentication
2. Prevents impersonation
3. Enables encrypted communication
4. Supports digital signatures
5. Legally valid
6. Protects users from phishing attacks

12. Disadvantages

1. Requires trusted CA
2. Certificates can expire
3. Private key leakage can compromise entire system
4. Cost of purchasing some certificates
5. Complex management in large organizations

13. Digital Certificate Example

Example (simplified):

Version: 3Serial Number: 6F:98:77:32
Signature Algorithm: SHA256-RSAIssuer: DigiCert CAValidity:
  From: 01-01-2024
  To: 01-01-2026Subject: https://example.comPublic Key: RSA 2048-bit
Extensions: SAN = www.example.com, example.comCA Digital Signature: 3A:D9:4F:C0…

Public Key Infrastructure (PKI) is a **framework of policies, technologies, roles, and procedures** used to manage **public-key encryption and digital certificates**.

PKI **enables**:

- Secure communication
- Authentication
- Digital signatures
- Confidentialit
- Non-repudiation

PKI is the backbone of **HTTPS, SSL/TLS, e-commerce, e-governance, digital signatures, banking**, etc.

PKI is a **security architecture** that provides a set of services to support **public-key cryptography**, including:

- Key generation
- Certificate issuance
- Certificate distribution
- Key lifecycle management
- Certificate validation (CRL/OCSP)

It ensures secure communication between entities in an unsecured network.

3. Why PKI Is Needed?

✔ To authenticate users in a network
✔ To verify identity of servers in HTTPS
✔ To enable digital signatures
✔ To prevent man-in-the-middle attacks
✔ To protect sensitive data transmitted over the internet
✔ To establish trust between parties

⭑ 4. Components of a PKI

PKI involves several major components:

1. Certificate Authority (CA): The most important PKI component.

Role:

- Issues digital certificates
- Verifies identity of users, servers, devices
- Signs certificates using its private key
- Root of trust in PKI

Types of CA:

1. **Root CA** – highest authority
2. **Intermediate CA** – subordinate to Root CA
3. **Issuing CA** – issues certificates to end users

2. Registration Authority (RA)

- Works as a **verifier** for the CA
- Validates user identity before CA issues certificate
- Acts between **user and CA**

3. Certificate Repository

- Public database to store issued certificates

4. Digital Certificates

- ➢ Electronic documents binding **public key with identity**
- ➢ Issued by CA and signed with CA private key
- ➢ Follows **X.509 standard**
- ➢ Each certificate contains:

- ✓ Subject name (owner)
- ✓ Public key
- ✓ Issuer (CA)
- ✓ Serial number
- ✓ Validity period
- ✓ Signature of CA

5. Certificate Revocation List (CRL)

- ➢ List of certificates that are **revoked before expiry**
- ➢ Published by CA
- ➢ Reasons: key compromise, employee left organization, etc.

6. Online Certificate Status Protocol (OCSP)

- ➢ Real-time certificate verification
- ➢ Faster than CRL

7. Key Pairs (Public & Private Keys)

PKI uses **asymmetric cryptography**.

Functions:

- ➢ **Private key**: used for signature & decryption
- ➢ **Public key**: used for verification & encryption

Keys are usually st**ored** in:

- ✓ Hardware Security Module (HSM)
- ✓ Smart cards
- ✓ TPM chips

8. Policies and Procedures

Define:

- ➢ Who can request certificate
- ➢ How certificates are issued
- ➢ Security level of keys
- ➢ Key recovery mechanism

⭑ 5. Working of PKI (Step-by-Step)

Step 1: Key Generation: User generate public-private key pair.

tes a **Step 2: Certificate Request:**User sends Certificate Signing Request (CSR) to the CA.

Step 3: Verification:RA verifies identity of user.

Step 4: Certificate Issuance:CA signs the certificate using CA's private key.

Step 5: Distribution: Certificate is stored in repository.

Step 6: Usage

User uses certificate for:

Authentication,Digital signature & Encryption

Step 7: Expiry/Revocation

If compromised → CA puts certificate in CRL.

⭑ 6. Applications of PKI

1. **SSL/TLS Certificates** for HTTPS
2. Email security (S/MIME)
3. Code signing (Windows, Android, Apple apps)
4. VPN authentication
5. IoT security
6. Online banking & payment systems
7. E-governance (Aadhar, e-sign, digital signatures)
8. Document signing (PDF, forms)

⭑ 7. Advantages of PKI

- ✔ High security
- ✔ Scalable for large organizations
- ✔ Ensures data integrity
- ✔ Provides confidentiality
- ✔ Supports digital signatures
- ✔ Trusted communication
- ✔ Essential for modern cybersecurity

⭑ 8. Limitations of PKI

- ✘ Complex architecture
- ✘ Requires proper management
- ✘ Expensive to maintain
- ✘ Single point of trust (CA must be trusted)
- ✘ Certificate revocation overhead

SSL / TLS

SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are cryptographic protocols used to secure communication over the internet.

When you see **HTTPS**, it means SSL/TLS is active.

1.

★ 2. What SSL/TLS Provides?

1. **Confidentiality** – encryption
2. **Integrity** – message hashing
3. **Authentication** – digital certificates
4. **Secure session establishment**

★ 3. How SSL/TLS Works (Simplified)

Step 1: Client Hello

- Browser sends supported cipher suites
- Sends random number
- Requests server certificate

Step 2: Server Hello

- Server sends its **digital certificate** (X.509)
- Server selects encryption algorithm
- Sends server random number

Step 3: Certificate Verification

- Client verifies certificate using CA public key
- Checks CRL/OCSP if needed

Step 4: Key Exchange

- Client creates **session key**
- Encrypts session key using server’s public key
- Server decrypts using private key

Step 5: Secure Communication Starts

All communication is encrypted using **symmetric session key** (fast).

★ Diagram: SSL Handshake (Text-Based)

Client → Server: ClientHelloServer → Client: ServerHello + Certificate
Client: Verifies Certificate
Client → Server: Encrypted Session KeyServer: Decrypts KeyBoth: Start Encrypted Communication

★ 4. SSL vs TLS

SSL	**TLS**
Older protocol	Modern, secure
SSL 2.0, SSL 3.0 (deprecated)	TLS 1.2, TLS 1.3
Vulnerable to attacks (POODLE)	Strong ciphers, secure handshake
No support today	Used everywhere

★ 5. Cryptography Used in SSL/TLS

1. **Asymmetric Encryption:**Used in handshake
   Examples: RSA, ECC, DH
2. **Symmetric Encryption:**Used after handshake
   Examples: AES, ChaCha20
3. **Hashing:**SHA-256, SHA-384
4. **Digital Certificates:**Issued via PKI

★ 6. Benefits of SSL/TLS

✔ Secure data transmission
✔ Prevents MITM attacks
✔ Authenticates server
✔ Builds user trust
✔ Required for online transactions

★ 7. Real-Time Applications

1. HTTPS websites
2. Banking and financial services
3. Payment gateways
4. Email communication
5. VPN connections
6. Cloud services
7. E-commerce portals

1.Firewalls MFC

A **firewall** is a **security device or software** that monitors, filters, and controls **incoming and outgoing network traffic** based on predefined security rules.
It acts as a **barrier between trusted internal networks** and **untrusted external networks (like the Internet).**

Key Purpose

- Prevent unauthorized access
- Enforce security policies
- Monitor traffic
- Protect internal network resources
- Block malicious activities

Why Firewalls Are Needed

- Networks are continuously exposed to threats (malware, hackers, DoS attacks).
- Firewalls reduce attack surface by filtering unsafe traffic.
- Essential for securing enterprise systems, data centers, and cloud networks.

Functions of a Firewall

1. **Packet Filtering**
   Checks source/destination IP, port, protocol
2. **Traffic Monitoring & Logging**
   Tracks suspicious activities for auditing
3. **Access Control**
   Allows or blocks traffic based on rules.
4. **Network Address Translation (NAT)**
   Hides internal IPs from the outside world.
5. **VPN Support**
   Enables secure remote communication through encryption.
6. **Content Filtering**
   Blocks malicious URLs, unauthorized applications.

Firewall Placement

Firewalls are commonly placed:

- Between **internal network** and **Internet**
- Between **DMZ** and **private network**
- Between **different internal segments** (micro-segmentation)

Types of Firewalls:

Firewalls can be classified based on:
(i) Filtering technique
(ii) Deployment
(iii) Platform

Below are the **major types**, explained in exam-friendly

4.1 Packet-Filtering Firewall (Stateless Firewall)

Definition

Filters packets based on **header information**:

- Source & destination IP
- Source & destination port
- Protocol (TCP/UDP/ICMP)

Working

- Applies Access Control Lists (ACLs).
- Does **not inspect packet payload**.

Advantages

- Fast and simple
- Low resource usage
- Effective for basic filtering

Limitations

- Cannot track connection states
- Vulnerable to IP spoofing
- Less secure compared to modern firewalls

Use Case

Routers in small networks or initial perimeter layer.

4.2 Stateful Inspection Firewall (Dynamic Packet Filterin

Tracks the **state of active connections** and makes decisions based on:

- Packet header
- Connection state (SYN, ACK, FIN)
- Context of the session

Advantage

- More secure than packet filters
- Prevents spoofing, reduces DoS impact
- Understands TCP handshake

Limitations

- More resource usage
- Slower compared to stateless firewalls

Use Case

Enterprise networks requiring improved security and performance balance.

4.3 Application-Level Gateway (Proxy Firewall)

Definition

Works at the **Application Layer (Layer 7)** and inspects the **payload** of packets.
Acts as an intermediary between user and server.

Examples

- HTTP Proxy
- FTP Proxy
- SMTP Proxy

Advantages

- Deep packet inspection
- Hides internal network identities
- Strong filtering and content control

Limitations

- Slower due to high processing
- Supports limited applications unless configured

Use Case

Web servers, mail servers, content filtering.

4.4 Circuit-Level Gateway

Verifies **TCP handshake** (connection establishment) but does **not inspect actual data**.

Advantages

- Simple, efficient
- Hides internal networks

Limitations

- No deep inspection
- Allows malicious data within legitimate connections

Use Case

Used with proxy servers or NAT for basic connection-level security.

4.5 Next-Generation Firewall (NGFW)

A modern firewall integrating:

- ✓ Traditional packet filtering
- ✓ Stateful inspection
- ✓ **Deep Packet Inspection (DPI)**
- ✓ **Intrusion Prevention System (IPS)**
- ✓ Application awareness
- ✓ SSL/TLS inspection

Advantages

- Best security features
- Detects modern threats (malware, DDoS, zero-day attacks)
- Controls applications (e.g., block Skype, Torrent)

Limitations

- Expensive
- Requires high computing power

Use Case

Large enterprises, cloud, data centers.

4.6 Host-Based Firewalls

Definition

Firewall installed on individual devices (PCs, servers).

Advantages

- Protects individual hosts
- Customizable according to system needs
- Monitors local applications

Limitations

- Hard to manage across many systems
- Relies on end-user security

Examples

Windows Defender Firewall, Linux iptables.

4.7 Network-Based Firewalls

A dedicated hardware or virtual device deployed at network boundaries.

Advantages

- High performance
- Centralized management
- Protects entire networks

Limitations

- Cannot protect internal threat
- Expensive hardware

Examples

Cisco ASA, Palo Alto NGFW, Fortinet.

4.8 Cloud Firewalls / Firewall-as-a-Service (FWaaS)

Firewalls delivered as cloud services.

Advantages

- Scalable
- Managed by provider
- Supports distributed cloud environments

Limitations

- Internet dependency
- Subscription cost

Examples

AWS WAF, Azure Firewall, Cloudflare.

Feature	Packet Filter	Stateful	Proxy	NGFW
Layer	L3/L4	L3/L4 + session	L7	L2–L7
Examines Data	Header only	Connection state	Payload	Full payload
Security Level	Low	Medium	High	Very High
Speed	Fast	Moderate	Slow	Moderate
Use Case	Basic filtering	Business networks	Application control	Enterprise security

6. Advantages of Using Firewalls

1. Prevents unauthorized access
2. Protects against hacking attempts
3. Enforces organization policies
4. Reduces attack surface
5. Monitors traffic patterns
6. Provides logging and auditing
7. Improves network reliability and availability

7. Limitations of Firewalls

- Cannot prevent internal attacks
- Cannot protect against social engineering
- Cannot stop malware in encrypted traffic (unless DPI used)
- Misconfiguration can weaken security
- Cannot guarantee protection against zero-day exploits

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Modern networks face threats such as malware, DoS attacks, unauthorized access, and insider misuse.
To detect and prevent such attacks, organizations use **IDS** and **IPS**.

- ✓ **IDS = Detects intrusions**
- ✓ **IPS = Detects + Prevents intrusions**

Both systems play a major role in **network monitoring**, **traffic analysis**, and **security automation**.

2. Intrusion Detection System (IDS)

An **Intrusion Detection System** is a security mechanism that **monitors network or host activity**, analyzes traffic, and identifies **suspicious behavior or policy violations**.

IDS **does not block traffic**, it only alerts administrators or logs events.

2.2 Functions of IDS

- Monitors network traffic in real-time
- Detects malicious activities
- Generates alerts/logs
- Helps identify attacks like:

- ✓ DoS/DDoS
- ✓ Malware activity
- ✓ Port scanning
- ✓ Unauthorized access

- Supports forensic analysis

3. Types of IDS

3.1 Network-Based IDS (NIDS)

Monitors traffic across the **entire network** or a specific segment.

Features

- Analyzes packet flows
- Detects attacks like DDoS, scanning
- Installed at strategic locations (DMZ, gateways)

Advantages

- Covers large network
- No performance impact on hosts

Limitations

- Cannot inspect encrypted traffic
- Hard to monitor distributed networks

3.2 Host-Based IDS (HIDS)

Installed on a specific host (server/PC) to monitor **system-level events**.

Monitors:

- ✓ Logs
- ✓ File integrity
- ✓ System calls
- ✓ User activity
- ✓ Application behavior

Advantages

1. Detects insider threats
2. Can inspect encrypted traffic locally
3. Highly detailed monitoring

Limitations

1. High resource usage
2. Difficult to manage across many hosts

4. IDS Detection Techniques

4.1 Signature-Based Detection

Compares traffic against **known attack patterns**.

Pros

1. Accurate for known attacks
2. Low false positives

Cons

1. Cannot detect new (zero-day) attacks
2. Requires frequent updates

4.2 Anomaly-Based Detection

Creates a baseline of **normal behavior**, then flags deviations.

Pros

1. Detects unknown attacks
2. Useful in adaptive environments

Cons

1. High false positives 2.Requires learning period

4.3 Hybrid Detection

Uses both signature and anomaly techniques.

5. Limitations of IDS

1. Cannot prevent attacks, only alerts
2. False positives can overload admins
3. Encrypted traffic is difficult to analyze
4. IDS must be updated regularly
5. May not detect insider attacks without HIDS

6. Intrusion Prevention System (IPS)

An **Intrusion Prevention System** detects and also **actively prevents/block suspicious traffic**.

IPS is placed **in-line** with network traffic, unlike IDS which is out-of-band.

6.2 Functions of IPS

1. Monitors traffic in real-time
2. Blocks malicious packets immediately
3. Drops suspicious connections
4. Enforces security policies
5. Prevents DoS, exploits, malware

7. Types of IPS

7.1 Network-Based IPS (NIPS)

Placed at network gateways to monitor and block malicious traffic.

Blocks:

1. Malware
2. Port scans
3. SQL injection
4. DoS attacks

7.2 Host-Based IPS (HIPS)

Installed on individual systems.
It can block:

1. Unauthorized applications
2. Malicious system calls
3. Filesystem changes

7.3 Wireless IPS (WIPS)

Protects wireless networks by detecting:

1. Rogue access points
2. Fake SSIDs
3. Wireless attacks

7.4 Network Behavior Analysis (NBA IPS)

Detects abnormal network behaviors (e.g., DDoS patterns, traffic spikes).

8. IPS Detection Methods

Same as IDS:

1. Signature-based
2. Anomaly-based
3. Policy-based (rule-based)
4. Hybrid IPS

9. IDS vs IPS –

Feature	IDS	IPS
Action	Detects	Detects & Prevents
Placement	Out-of-band	In-line
Response	Alerts/logs	Blocks/drops packets
Impact	No delay	May affect performance
Use Case	Monitoring	Active protection

10. Advantages of IPS

1. Prevents attacks immediately
2. Reduces malware spread
3. Protects against zero-day attacks (anomaly IPS)
4. Automates threat response
5. Enhances overall network security

11. Limitations of IPS

1. May cause false blocking
2. Performance overhead
3. Requires continuous updates
4. Difficult to configure correctly

12. Combined IDS/IPS (IDPS)

Most modern systems combine IDS and IPS functions into **IDPS**, providing:

- Detection + Prevention
- Traffic analysis
- Logging
- Policy enforcement

Examples:

- ✓ Snort, Suricata
- ✓ Cisco FirePOWER
- ✓ Palo Alto NGFW
- ✓ Fortigate IPS

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can be deployed in two major ways:

1. **Network-Based (NIDS/NIPS)** – monitors the network
2. **Host-Based (HIDS/HIPS)** – monitors individual devices

Both help organizations detect and prevent unauthorized access, malicious activities, and policy violations.

2. Network-Based IDS/IPS (NIDS / NIPS)

A **Network-Based IDS/IPS** monitors and analyzes **network traffic** flowing through a specific network segment.

- **NIDS** detects attacks.
- **NIPS** detects and **blocks** malicious traffic in real time.

2.2 How it Works

- Deployed at **network boundaries**, gateways, or strategic points (e.g., DMZ).
- Inspects packet headers and payloads.
- Analyzes traffic patterns to detect intrusions.

2.3 Capabilities

- Detects network threats such as:DDoS attacks,Port scanning,Worm propagation,Botnet traffic & Unauthorized access attempts
- Can block or drop malicious packets (in NIPS).

2.4 Advantages

- Covers entire network segments
- No overhead on individual devices
- Detects attacks targeting multiple hosts
- Centralized monitoring

2.5 Limitations

- Cannot monitor encrypted traffic easily (HTTPS, SSH)
- Cannot detect local host-level attack
- Might miss attacks within local machines
- Large networks → overwhelming data

3. Host-Based IDS/IPS (HIDS / HIPS)

A **Host-Based IDS/IPS** is installed on a **specific host (PC, server, workstation)** to monitor internal system activity.

- **HIDS** detects malicious actions on the host.
- **HIPS** detects and **blocks** malicious behavior on the host.

3.2 What It Monitors

System logs

- File integrity changes
- Registry entries
- Running processes
- System calls
- User activities
- Application behavior

3.3 Capabilities

- Detects host-specific attacks like:

- ✓ Unauthorized file modification
- ✓ Privilege escalation
- ✓ Rootkits
- ✓ Malware execution
- ✓ Insider abuse

3.4 Advantages

- Detects attacks that NIDS cannot see
- Can analyze encrypted traffic (after decryption on host)
- Very detailed monitoring
- Useful for server protection
- Detects insider threats

3.5 Limitations

- Performance overhead on host
- Difficult to manage on large numbers of devices
- Can be disabled if host is compromised
- Requires endpoint agent installation

5. Where Each Type Is Used

Network-Based IDS/IPS Best Uses

1. Monitoring enterprise network
2. Detecting DDoS and scanning
3. Perimeter defense
4. Cloud and DMZ environments

Host-Based IDS/IPS Best Uses

- Protecting critical servers (DB, email, application servers)
- Detecting insider threats
- Monitoring system integrity
- Protecting highly sensitive endpoints

6. Combined Deployment (NIDS + HIDS + IPS)

Modern security architecture uses a **hybrid approach**:

- NIDS/NIPS → monitors network-wide threats
- HIDS/HIPS → monitors individual systems

Together, they form a complete **Intrusion Detection and Prevention System (IDPS)**.

This gives defense against:

- ✓ External attacks
- ✓ Internal threats
- ✓ Malware
- ✓ System misuse
- ✓ Network exploits

Feature	Network-Based IDS/IPS	Host-Based IDS/IPS
Location	Network perimeter / gateway	Individual hosts (PC/server)
Traffic Visibility	Monitors network traffic	Monitors internal system activities
Detection	Network attacks (DDoS, scanning)	Local attacks (file changes, malware)
Encrypted Traffic	Hard to inspect	Can inspect after decryption
Deployment	No software on hosts	Agent/software required on hosts
Performance Impact	None on hosts	Consumes host resources
Coverage	Broad (multiple devices)	Limited to one host
Response (IPS)	Blocks suspicious packets	Blocks harmful actions on host
Best For	Network-wide security	Sensitive servers, endpoints

Signature-Based vs Anomaly-Based Detection

- These two are the **primary detection techniques** used by IDS and IPS to identify attacks.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) detect malicious activity using various detection methods.

The **two most important techniques** are:

1. **Signature-Based Detection**
2. **Anomaly-Based Detection**

2. Signature-Based Detection

Signature-based detection compares incoming traffic or system events against a database of **known attack signatures**.

A **signature** = a pattern that identifies a specific attack. Examples:

- ✓ Known malware hash
- ✓ Specific sequence of bytes
- ✓ Known malicious IP address
- ✓ Snort rule pattern

If incoming data matches a stored signature → attack detected.

2.2 Working Principle

- ✓ Traffic/logs are captured.
- ✓ IDS/IPS compares them to a database of known attack signatures.
- ✓ If a match is found → alert/block.
- ✓ If no match → considered safe.

2.3 Types of Signatures

1. **Pattern-based signatures** (match exact strings)
2. **Heuristic signatures** (match behavior patterns)
3. **State-based signatures** (detect multi-step attacks)

2.4 Advantages

- **Highly accurate** for known attacks
- **Low false positives**
- Easy to understand and configure
- Fast detection

2.5 Limitations

- Cannot detect **zero-day attacks**
- Requires continuous signature updates
- Fails when attackers modify patterns
- Large signature databases slow down scanning

2.6 Use Cases

- Antivirus software
- Snort for network IDS
- Firewalls with DPI
- Web Application Firewalls (WAF)

3. Anomaly-Based Detection

Anomaly-based detection identifies deviations from **normal behavior** in network traffic, system usage, or user activities.

An IDS first learns what "normal" looks like → **Baseline**
Anything significantly different → **Anomaly** → Possible intrusion.

3.2 Working Principle

- System collects normal traffic/behavior over time.
- Builds a **baseline profile**.
- Monitors live data.
- If behavior deviates significantly → flagged as suspicious.

3.3 Types of Anomalies

1. **Statistical anomalies**
2. **Behavioral anomalies**
3. **Machine-learning-based anomalies**

3.4 Advantages

- Detects **unknown** or **zero-day attacks**
- Can discover insider threats
- Adapts to evolving environments
- Effective for detecting new malware patterns

3.5 Limitations

- **High false positives**
- Requires long learning period
- Difficult to tune
- Resource-intensive (CPU, memory)

3.6 Use Cases

- Detecting abnormal system usage
- Zero-day exploit detection
- Unusual traffic spikes (possible DDoS)
- Unauthorized access attempt
- Suspicious user behavior in enterprises

5. When to Use Which?

Use Signature-Based Detection When:

- You want stability with minimal false alarms
- You deal with known, common threats
- CPU resources are limited
- Quick detection is required

Use Anomaly-Based Detection When:

- You want to detect new/zero-day attacks
- Insider threats must be detected
- Network behavior varies often
- You can afford higher false positives

6. Hybrid (Signature + Anomaly) Detection

Modern IDS/IPS often use **both methods together** to provide balanced detection:

- Signature → detects known attacks with high accuracy
- Anomaly → detects unknown attacks

Examples:

- ✓ Suricata IDS
- ✓ Snort 3
- ✓ Palo Alto Firewalls
- ✓ Cisco FirePOWER IPS

Feature	Signature-Based Detection	Anomaly-Based Detection
Detection Basis	Known attack signatures	Deviations from normal behavior
Detects Zero-Day Attacks?	✗ No	✓ Yes
Accuracy	High for known attacks	Lower (more false positives)
Updates Required	Frequent signature updates	Baseline updates
False Positives	Low	High
False Negatives	High (misses unknown attacks)	Low
Speed	Fast	Slower; more processing
Learning Period	Not required	Required
Best For	Known, common attacks	Unknown, new, sophisticated attacks

1. Virtual Private Networks (VPN)

A **Virtual Private Network (VPN)** is a secure communication technology that creates an **encrypted tunnel** over a public network (like the Internet) so that data can be sent **privately and securely**.

VPNs ensure:

- ✓ **Confidentiality** (through encryption)
- ✓ **Integrity** (through hashing/MAC)
- ✓ **Authentication** (through certificates/keys)
- ✓ **Secure remote access** to private networks

1.2 Why VPNs Are Needed?

- Secure communication over untrusted networks
- Protect data from eavesdropping, man-in-the-middle attacks
- Enable employees to access corporate resources remotely
- Support secure branch-to-branch communication
- Reduce cost compared to leased private lines (MPLS, frame relay)

1.3 Key Features of VPN

- **Encryption** (AES, 3DES)
- **Tunneling** (encapsulating packets inside another protocol)
- **Authentication** (password, certificate, key-based)
- **Integrity check** (SHA, MD5)
- **Access control**
- **Data privacy**

2. Types of VPNs

VPNs are mainly of two types:

1. **Site-to-Site VPN**
2. **Remote Access VPN**

2.1 Site-to-Site VPN

A site-to-site VPN connects **two or more LANs (offices/branches)** over the Internet securely.

Example: Head office ↔ Branch office

How It Works

- VPN gateways (routers/firewalls) at both ends create a secure tunnel.
- Users inside the LAN do not need VPN software

Types of Site-to-Site VPN

1. **Intranet VPN** – connects different branches of same organization
2. **Extranet VPN** – connects company with partners/vendors

Advantages

- Secure communication between offices
- No need for individual user setup
- Centralized management

Limitations

- Less flexible for roaming users
- Requires VPN-capable routers/firewalls

2.2 Remote Access VPN

- A remote access VPN allows **individual users** to securely connect to a private network using a laptop, PC, or mobile device.
- Used by employees working from home or travelling.

How It Works

- User installs **VPN client software**
- Client authenticates to VPN server
- Encrypted tunnel is created

Advantages

- Ideal for remote workers
- Strong authentication
- Encrypted data transmission

Limitations

- Depends on user device configuration
- More vulnerable to malware on user's system

3. VPN Protocols

The main protocols used in VPNs are:

- **IPSec (Internet Protocol Security)**
- **SSL/TLS VPN**
- **Other protocols** (PPTP, L2TP, IKEv2, OpenVPN, WireGuard)

3.1 IPSec (Internet Protocol Security):

IPSec is a **network-layer security protocol suite** that provides **confidentiality, integrity, and authentication** for IP packets.

- Used in **site-to-site VPNs** and many remote access VPNs.

3.1.1 IPSec Components

(a) Authentication Header (AH)

- Provides **authentication and integrity**
- Does **not encrypt data**
- Protects against spoofing

(b) Encapsulating Security Payload (ESP)

- Provides **encryption, authentication, integrity**
- Most commonly used
- Protects the actual data payload

3.1.2 IPSec Modes

Tunnel Mode

- Entire IP packet is encrypted
- Used in **site-to-site VPNs**

Transport Mode

- Only payload is encrypted
- Used in host-to-host communication

3.1.3 Key Exchange: IKE (Internet Key Exchange)

Used for:

- ✓ Authentication
- ✓ Sharing encryption keys
- ✓ Negotiating security associations (SA)

3.2 SSL/TLS VPN

SSL/TLS VPN uses **web-based encryption protocols (HTTPS)** to secure communication between client and server.

Used mainly for **remote access**.

3.2.1 How SSL/TLS VPN Works

- User connects via a web browser (no software needed)
- Server authenticates client & establishes encrypted HTTPS tunnel
- Traffic passes through SSL/TLS-secured channel

3.2.2 Advantages of SSL/TLS VPN

- Works through browsers (no installation)
- Easy to deploy

- Uses port **443**, bypassing firewalls
- Good for mobile users

3.2.3 Limitations

- Suitable mostly for remote access, **not** site-to-site
- Limited access depending on configuration

4. Other VPN Protocols (Short Notes)

4.1 PPTP (Point-to-Point Tunneling Protocol)

- ✓ Oldest VPN protocol
- ✓ Fast but weak security
- ✓ Uses MS-CHAP authentication
- ✓ Not recommended today

4.2 L2TP (Layer 2 Tunneling Protocol)

- ✓ Combines **L2TP + IPSec**
- ✓ Provides strong encryption
- ✓ Used in many modern VPNs

4.3 OpenVPN

- ✓ Open-source
- ✓ Uses SSL/TLS
- ✓ Highly secure and configurable

4.4 IKEv2

- ✓ Fast, stable, good for mobile environments
- ✓ Handles network switching smoothly (WiFi to mobile data)

4.5 WireGuard (New Generation VPN)

- ✓ Very fast
- ✓ Uses modern cryptography
- ✓ Lightweight and secure

6. Advantages of VPNs

- ✓ Provides **confidentiality & integrity**
- ✓ Protects data over public network
- ✓ Enables remote access securely
- ✓ Reduces network cost
- ✓ Prevents eavesdropping
- ✓ Supports secure communication for cloud systems

7. Limitations of VPNs

- ✓ Performance overhead due to encryption
- ✓ Misconfiguration risks
- ✓ Depends on user device security
- ✓ Might be impacted by weak protocols (like PPTP)
- ✓ Requires strong key management

Feature	**IPSec VPN**	**SSL/TLS VPN**
Layer	Network Layer	Application Layer
Deployment	Site-to-site, remote access	Mostly remote access
Encryption	ESP, AH	TLS/HTTPS
Client	Needs VPN client software	Browser-based
Speed	High	Moderate
Firewall issues	May be blocked	Uses HTTPS → rarely blocked
Use Case	Corporate office-to-office	Remote/mobile users

Wireless Security

Wireless networks allow devices to communicate without physical cables using radio waves.
Compared to wired networks, wireless LANs are **more vulnerable** because signals travel through the air and can be intercepted..

What is IEEE 802.11?

IEEE 802.11 is a set of standards developed by the **Institute of Electrical and Electronics Engineers (IEEE)** for wireless LAN (WLAN) communication.

It defines:

- ✓ Wireless frequencies
- ✓ Data rates
- ✓ Modulation techniques
- ✓ Authentication and encryption methods
- ✓ MAC layer operations

The IEEE 802.11 standard forms the **foundation of Wi-Fi technology** used globally.

3. Architecture of IEEE 802.11 WLAN

A wireless LAN consists of the following components:

3.1 Basic Service Set (BSS)

A BSS is the **fundamental building block** of WLAN.

Types of BSS:

1. **Independent BSS (IBSS):**Also called **Ad-hoc network.**No access point.Devices communicate directly.Used for temporary communication (e.g., file sharing)
2. **Infrastructure BSS**:Uses an **Access Point (AP)**.Devices communicate via the AP.Most common Wi-Fi deployment

3.2 Extended Service Set (ESS)

- Multiple BSS connected via a **Distribution System (DS)** form an ESS.
- Allows roaming between APs
- Provides coverage across buildings or campuses

3.3 Access Point (AP)

An AP acts as a **central communication hub** between wired and wireless networks.

Functions:

1. Authentication
2. Association of clients
3. Signal modulation
4. Packet forwarding

4. IEEE 802.11 Physical Layer (PHY)

The PHY layer defines:

- ✓ Frequencies
- ✓ Data rates
- ✓ Modulation schemes

5. IEEE 802.11 MAC Layer

The MAC layer handles **how devices access the wireless channel.**

Key Functions:

5.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Because collisions cannot be detected in wireless networks, 802.11 uses **collision avoidance**.

Steps:

1. Listen to channel
2. If free → transmit
3. If busy → wait random backoff
4. Use ACK frames to confirm delivery

5.2 RTS/CTS Mechanism

Used to reduce collisions from hidden nodes.

- RTS: Request to Send
- CTS: Clear to Send
- AP grants permission before a device transmits.

5.3 Frame Types in 802.11

1.Management Frames

1. Beacon
2. Probe request/response
3. Authentication
4. Association

2.Control Frames

1. RTS, CTS
2. ACK

3.Data Frames

6. Security in IEEE 802.11 WLAN

Initially, Wi-Fi security was weak (WEP), but new protocols improved protection.

6.1 WEP (Wired Equivalent Privacy)

- First security protocol
- Uses RC4 encryption
- **Weak and easily breakable**
- Not recommended

6.2 WPA (Wi-Fi Protected Access)

- An improvement over WEP.

Key Features:

- ✓ TKIP encryption
- ✓ MIC (Message Integrity Check)
- ✓ Still vulnerable but better than WEP

6.3 WPA2 (802.11i Standard)

The most widely used security method.

- Encrypts using **AES-CCMP**
- Strong and secure

Modes:

- WPA2-Personal (PSK)
- WPA2-Enterprise (802.1X + RADIUS)

6.4 WPA3 (Latest Security Standard)

Modern and highly secure.

Features:

- Simultaneous Authentication of Equals (SAE)

- Protection against dictionary attacks
- Stronger encryption

7. Wireless Security Threats

1. **Eavesdropping**:Attackers capture wireless traffic
2. **Rogue Access Points**:Unauthorized AP that mimics a real network
3. **Evil Twin Attack**:Fake AP used to steal credentials
4. **Jamming**:Attacker floods network with signals
5. **MAC Spoofing**:Attacker changes MAC address to impersonate a device
6. **Man-in-the-Middle Attacks**:Attacker intercepts communication between AP and user

8. Wireless Security Best Practices

1. Use **WPA2/WPA3** encryption
2. Disable WEP
3. Strong passwords and passphrases
4. MAC filtering (limited protection)
5. Disable SSID broadcasting (minor security)
6. Enable firewall in AP
7. Use VPN when connecting to public Wi-Fi
8. Regularly upgrade firmware

Feature	WPA	WPA2	WPA3
Encryption	RC4 + TKIP	AES-CCMP	AES-GCMP, 192-bit
Authentication	PSK / 802.1X	PSK / 802.1X	SAE / 802.1X
Security Level	Medium	High	Very High
Vulnerable to	Dictionary, TKIP weakness	KRACK, weak PSK	Much fewer vulnerabilities
Public network protection	No	No	Yes (OWE)
Forward Secrecy	No	No	Yes

Protocol	Year	Security Level	Notes
WEP	1999	Weak	Based on RC4, easily crackable
WPA	2003	Medium	Temporary fix over WEP
WPA2	2004	High	Based on AES-CCMP
WPA3	2018	Very High	Latest, strongest; resistant to dictionary