SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

Firewall Design Principles

Firewall:
A **firewall** is a security device (hardware or software) that controls the flow of network traffic between two or more networks based on predetermined security rules.

Design Principles:

1. **All Traffic Must Pass Through the Firewall:**
   - No direct access between internal and external networks is allowed.
   - All communication must be mediated and filtered by the firewall.
2. **Only Authorized Traffic is Allowed:**
   - Traffic that meets the defined security policies is permitted.
   - Unauthorized traffic is blocked or dropped.
3. **The Firewall Itself Must Be Secured:**
   - The firewall should be immune to security breaches.
   - Minimal software and services are installed to reduce vulnerabilities.
4. **Policy-Based Control:**
   - Firewall decisions are based on a clear, well-defined security policy.
   - Policies specify what services are allowed (e.g., HTTP, HTTPS, VPN) and to whom.
5. **Least Privilege Principle:**
   - Only essential network services and permissions are allowed.
   - Deny by default; only allow explicitly permitted traffic.
6. **Logging and Auditing:**
   - Maintain logs of traffic for monitoring, analysis, and troubleshooting.
   - Helps in detecting and responding to attacks.
7. **Fail-Safe Defaults:**
   - In case of failure or error, the firewall should default to a secure state (block traffic).

Types of Firewalls

There are **several types** of firewalls based on their method of operation:

1. Packet-Filtering Firewall

- **Function:** Inspects individual packets and makes decisions based on source/destination IP address, port number, and protocol.
- **Characteristics:**
  - Fast and efficient.
  - Basic filtering without inspecting packet payloads.
  - Works at the **Network Layer** (OSI Layer 3).
- **Weakness:** Limited protection against attacks using legitimate ports.

Example: Early routers with basic access control lists (ACLs).

2. Stateful Inspection Firewall

- **Function:** Tracks the **state** of active connections and makes decisions based on connection state and context.
- **Characteristics:**
  - Maintains a state table (record of connections).
  - Provides better security than packet filters.
  - Works at **Network and Transport Layers** (OSI Layer 3 and 4).
- **Strength:** Can identify and block spoofed packets and unauthorized traffic.

Example: Cisco ASA.

3. Application-Level Gateway (Proxy Firewall)

- **Function:** Acts as an intermediary between users and services, inspecting application-layer traffic.
- **Characteristics:**
  - Works at the **Application Layer** (OSI Layer 7).
  - Can enforce strict security policies (e.g., allow only specific commands in FTP).
  - Slower due to detailed inspection.
- **Strength:** Excellent for filtering based on user authentication and application-specific commands.

Example: Squid Proxy Server.

4. Circuit-Level Gateway

- **Function:** Monitors TCP handshakes and session establishment between trusted clients and untrusted hosts.
- **Characteristics:**
  - Works at **Session Layer** (OSI Layer 5).
  - Does not inspect packet content.
- **Use:** Mainly used to hide the details of a private network.

Example: SOCKS proxy.

5. Next-Generation Firewall (NGFW)

- **Function:** Combines traditional firewall features with advanced features like:
  - Deep packet inspection (DPI)
  - Intrusion Prevention Systems (IPS)
  - Application awareness and control
  - Malware detection and sandboxing
- **Characteristics:**
  - Works across multiple OSI layers.
  - Identifies and blocks sophisticated attacks.
- **Strength:** Comprehensive protection against modern threats.

Example: Palo Alto Networks NGFW.