19z701 - Cryptography

Firewall Characteristics and Types

22z204 - Abirami M

22z212 - Aravinth Cheran K S

22z228 - Jeevashakthi V

22z229 - Kabhinyasri S V

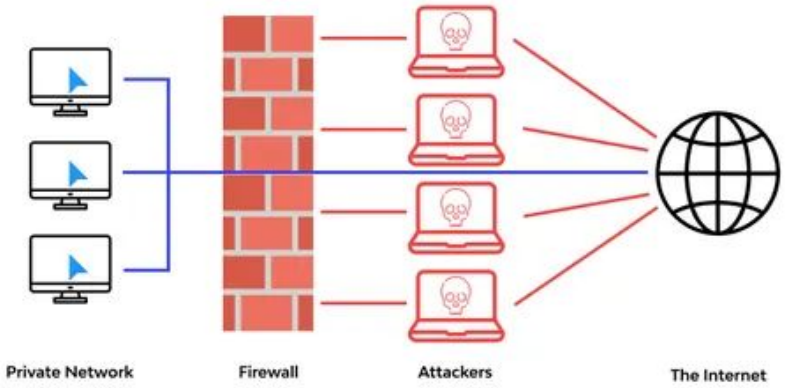
22z235 - Madhisha S

Introduction to Firewall

Jeevashakthi V - 22z228

What is a Firewall?

- A firewall is a network security system that monitors and controls data traffic.
- Acts as a barrier between a trusted internal network and an untrusted external network.
- Can be hardware, software, or both.
- Works using predefined security rules to allow or block traffic.
- Main goal: prevent unauthorized access and protect data.



Where is Firewall used?

Firewalls are used everywhere network communication happens

- In personal computers, to prevent unauthorized access.
- In organizations, to protect internal servers and data.
- In data centers, to control traffic between multiple networks.
- And even in cloud environments, as software-based firewalls or Firewall-as-a-Service (FWaaS).

Evolution of Firewall

Packet Filtering Firewall (1980s) | *First Generation*
Examined only packet headers (source/destination IP, port, protocol)
Basic rule-based filtering — no tracking of connections

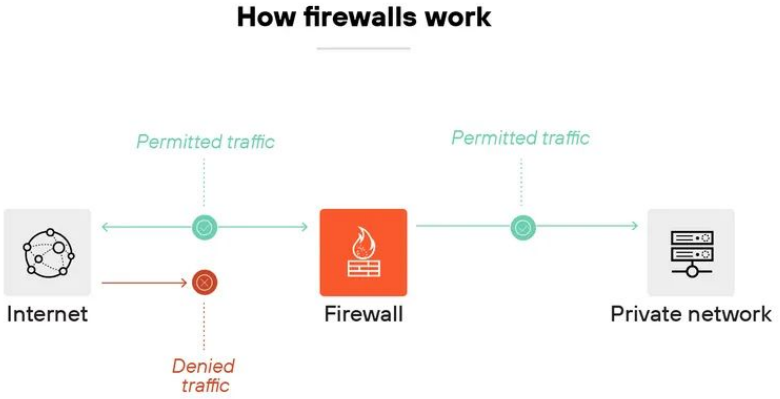
Stateful Inspection Firewall (1990s) | *Second Generation*
Tracked connection states — aware of active sessions
More secure than simple packet filters

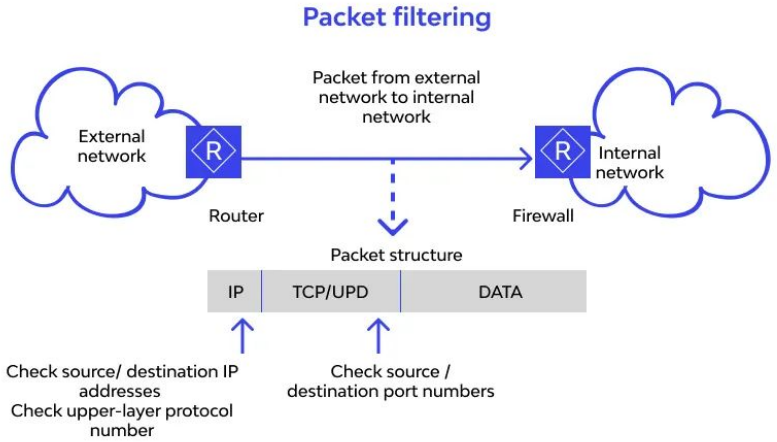
Proxy / Application Layer Firewall (2000s) | *Third Generation*
Worked at application layer — inspected actual content (HTTP, FTP, etc.)
Could block malicious payloads, not just ports

Next-Generation Firewall (Present) | *Fourth Generation*
Combines packet filtering + stateful inspection + IDS/IPS + app control Uses AI/ML for threat detection and deep packet inspection
Supports cloud and hybrid environments

How it works?

- Every message sent online is broken into packets.
- Firewall inspects each packet's:
  - Source & destination address
  - Port number
  - Protocol (HTTP, FTP, etc.)
- Compares packets with a set of security rules.
- Allows safe packets and blocks suspicious ones.
- Keeps logs of network activity for monitoring.





Characteristics of Firewall

- Kabhinyasri S V
22z229

Packet Filtering

- Examines packet **headers** (source IP, destination IP, ports, protocols).
- Allows or denies packets based on **predefined rules**.
- Simple but offers basic protection only.
- Example: Allow only packets to port 80 (HTTP).

Stateful Inspection

- Tracks **active network connections** (session-based).
- Checks if packets are part of an **existing valid session**.
- Provides **better inspection** than basic filtering.
- Example: Ongoing session packets - Website.

Logging & Auditing

- Records details of **allowed and blocked traffic**.
- Helps **detect attacks, troubleshoot**, and ensure compliance.
- Essential for **network administrators** to monitor activity.
- Example: Repeated failed login attempts - hacking.

Access Control Policies

- Define **who** can access **what** on the network.
- Rules based on:
    - IP addresses
    - Users / Devices
    - Applications or Ports
- Enforces **security policies** across the organization.
- Example: Accessing company's internal HR system

Network Address Translation (NAT)

- Hides **internal IP addresses** behind a single public IP.
- Enhances **privacy and security**.
- Prevents **direct external access** to internal devices.
- Example: Multiple computers in an office appear with common public IP

VPN Support

- Allows **secure remote access** to internal networks.
- Encrypts communication between remote users and servers.
- Ideal for **remote workers or branch offices**.
- Example: An employee working from home

Performance & Scalability

- Handles **high-speed traffic** efficiently.
- Scales for **small offices or large enterprises**.
- Uses **hardware acceleration** in advanced firewalls.
- Example: High-end firewalls from Cisco

Types of Firewall
(Data Filtering Method)

- Madhisha S
(22z235)

Packet Filtering Firewall

How it works:

- Examines packet headers (source/destination IP, port, protocol).
- Uses a rule set to decide **allow or deny**.
- Works at **Network Layer (Layer 3)** and **Transport Layer (Layer 4)**.

Pros:

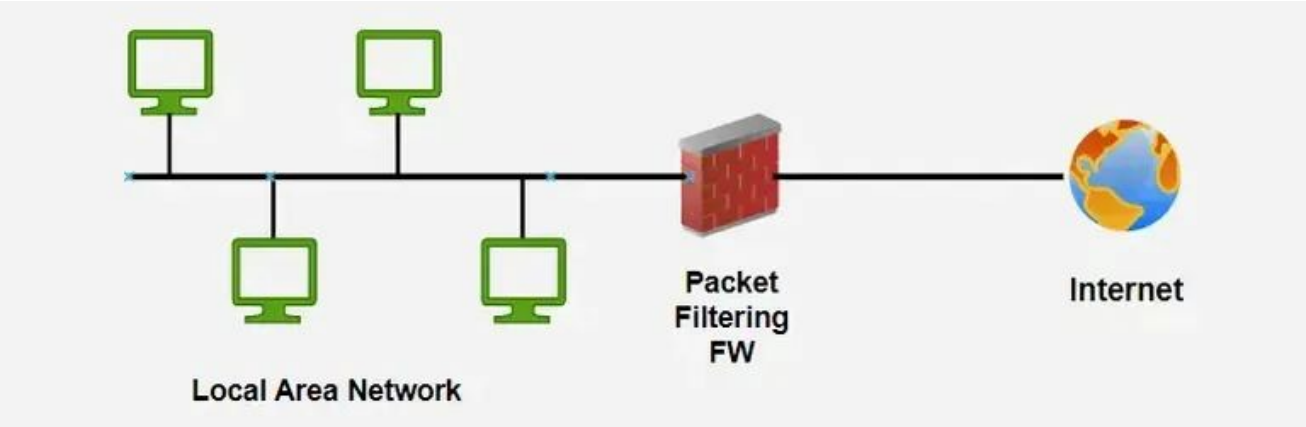
- Simple, fast, low resource usage.
- Good for small networks.

Cons:

- Doesn’t inspect payload (actual data inside packets).
- Vulnerable to spoofing attacks.

Packet Filtering Firewall

- Examines packet headers (source/destination IP, port, protocol).
- Uses a rule set to decide **allow or deny**.
- Works at **Network Layer (Layer 3)** and **Transport Layer (Layer 4)**.



Stateful Inspection Firewall

How it works:

- Tracks **state of active connections** (session info).
- Checks if a packet is part of an existing valid session.
- Works at **Network & Transport layers**.

Pros:

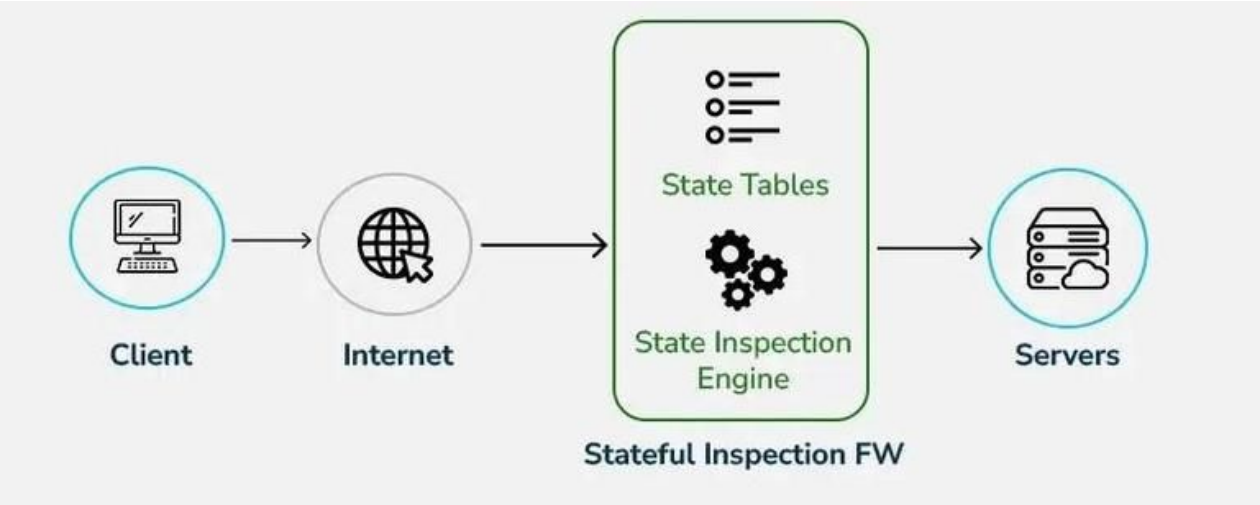
- More secure than packet filtering.
- Can block out-of-state or malicious packets.

Cons:

- Uses more resources.
- Slower than packet filtering.

Stateful Inspection Firewall

- Tracks **state of active connections** (session info).
- Checks if a packet is part of an existing valid session.
- Works at **Network & Transport layers**.



Proxy Firewall (Application-Level Gateway)

How it works:

- Acts as an **intermediary** between user and destination.
- Terminates requests and re-initiates them on behalf of the client.
- Works at **Application Layer (Layer 7)**.

Pros:

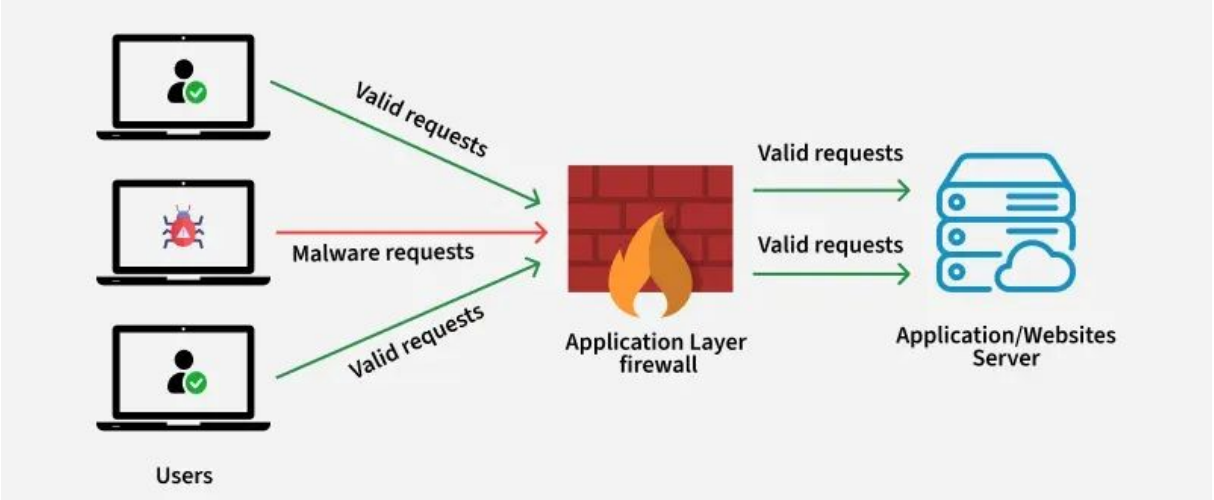
- Hides internal network.
- Performs deep inspection of application data.

Cons:

- Slower due to high processing.
- May block some legitimate applications.

Proxy Firewall (Application-Level Gateway)

- Acts as an **intermediary** between user and destination.
- Terminates requests and re-initiates them on behalf of the client.
- Works at **Application Layer (Layer 7)**.



Circuit-Level Gateway

How it works:

- Validates **TCP handshakes** and session setup.
- Ensures a legitimate connection before data exchange.
- Operates at **Session Layer (Layer 5)**.

Pros:

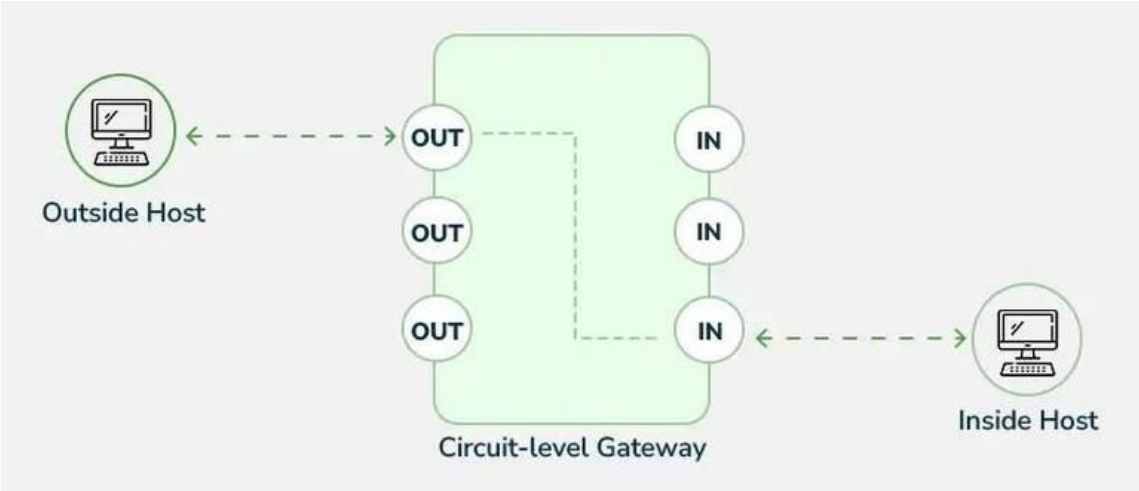
- Simple and efficient for connection validation.
- Provides anonymity (hides internal structure).

Cons:

- Doesn’t inspect the data inside packets.
- Cannot block application-level threats.

Circuit-Level Gateway

- Validates **TCP handshakes** and session setup.
- Ensures a legitimate connection before data exchange.
- Operates at **Session Layer (Layer 5)**.



Web Application Firewall (WAF)

How it works:

- Specifically filters **HTTP/HTTPS traffic**.
- Protects against **SQL injection, XSS, CSRF**, and other web attacks.
- Works at **Application Layer (Layer 7)**.

Pros:

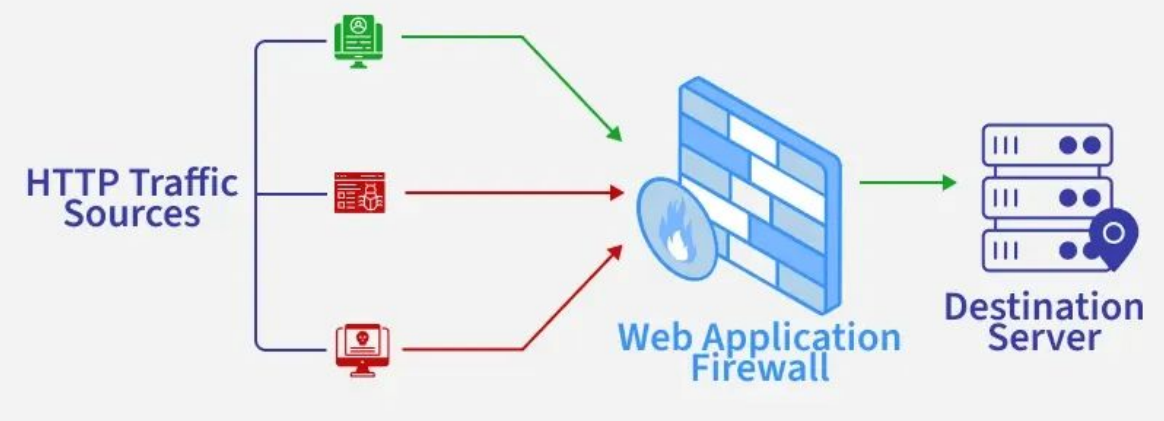
- Tailored for web apps.
- Protects servers from common web exploits.

Cons:

- Limited to web traffic only.
- Needs constant rule updates.

Web Application Firewall (WAF)

- Specifically filters **HTTP/HTTPS traffic**.
- Protects against **SQL injection, XSS, CSRF**, and other web attacks.
- Works at **Application Layer (Layer 7)**.



Next-Generation Firewall (NGFW)

How it works:

- Combines traditional firewall + IDS/IPS + deep packet inspection.
- Identifies applications, users, and threats with context awareness.
- Works across **multiple OSI layers**.

Pros:

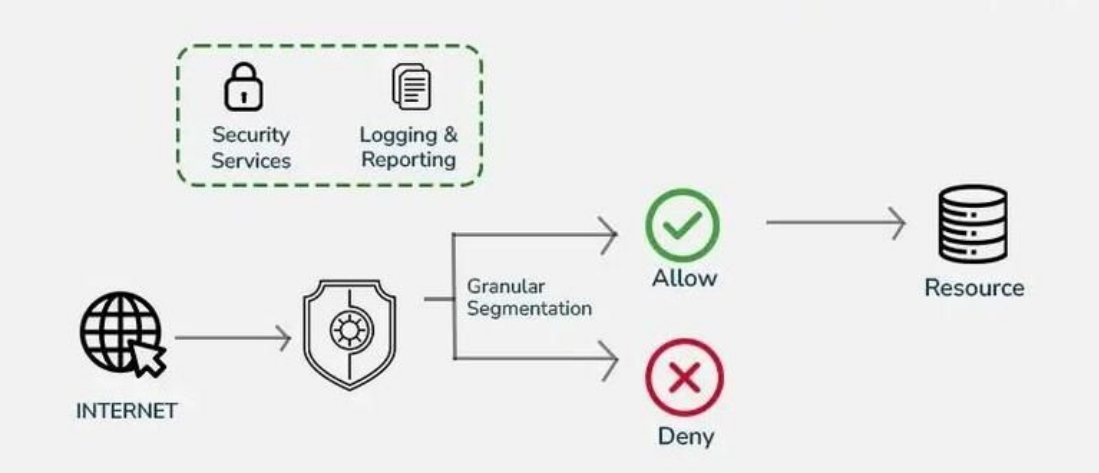
- High security, detects advanced threats.
- Application-level visibility and control.

Cons:

- Expensive.
- Complex to configure and manage.

Next-Generation Firewall (NGFW)

- Combines traditional firewall + IDS/IPS + deep packet inspection.
- Identifies applications, users, and threats with context awareness.
- Works across **multiple OSI layers**.

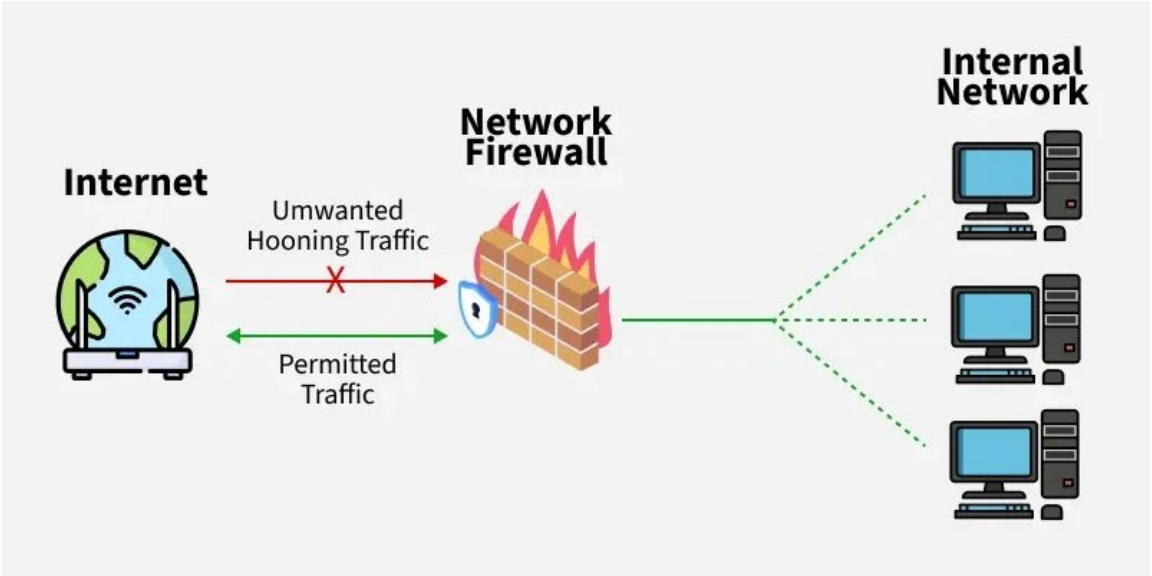


Types of Firewall (Other Types)

- Aravinth Cheran K S (22z212)

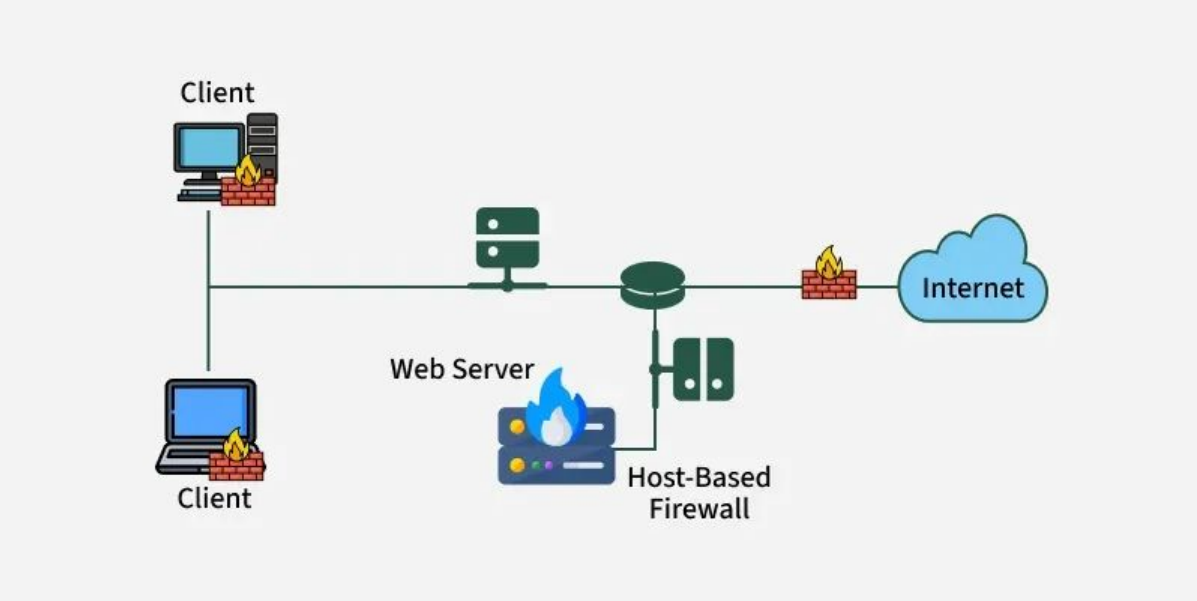
Network Firewall

Protects a whole network—usually placed at the entry/exit point between your internal systems and the internet. Picture it like a guard standing at your building's main entrance.



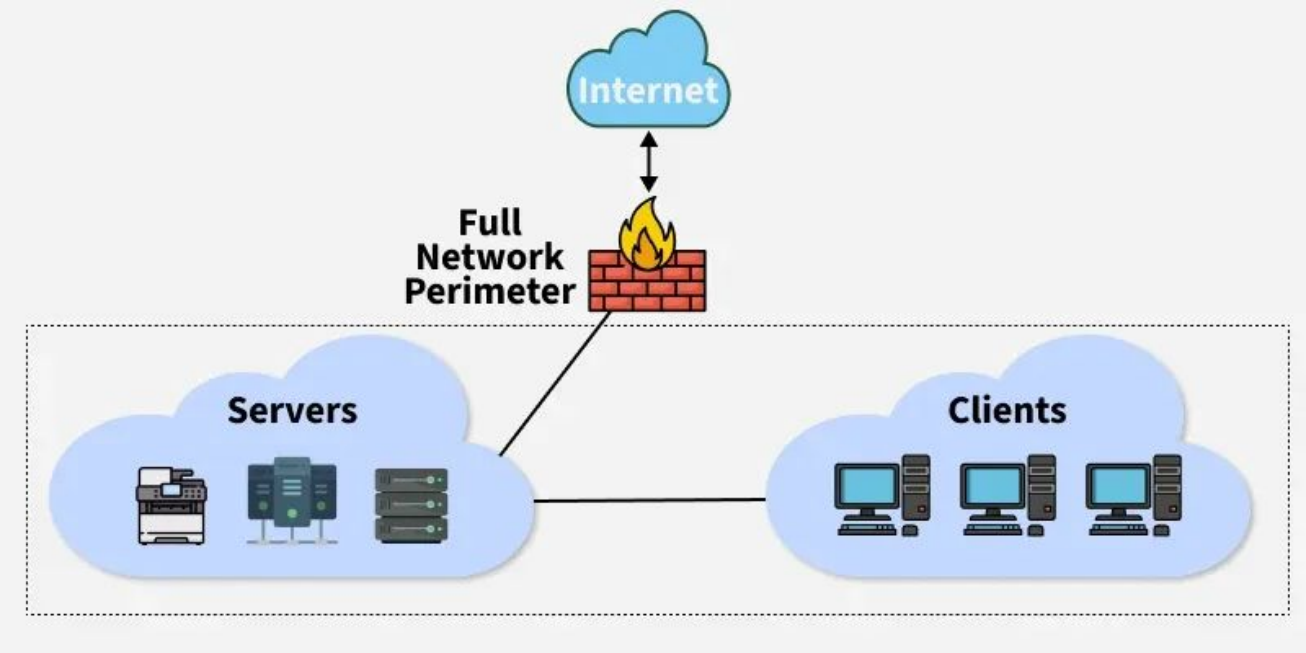
Host-Based Firewall

Installed on individual devices like laptops, servers, or mobile phones. It protects only that one system. Think of it as having a security app that watches over just your phone, not the whole office.



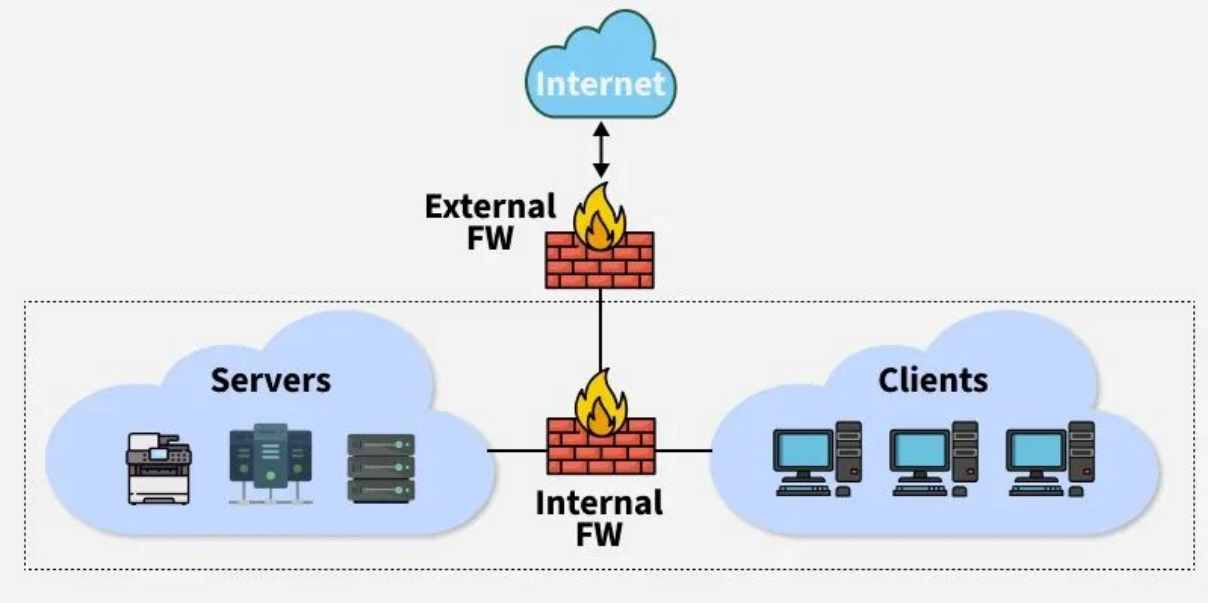
Perimeter Firewall

Sits at the edge of your network, filtering traffic coming in and out from the internet. Like a fence with a gate that controls who gets into your property.



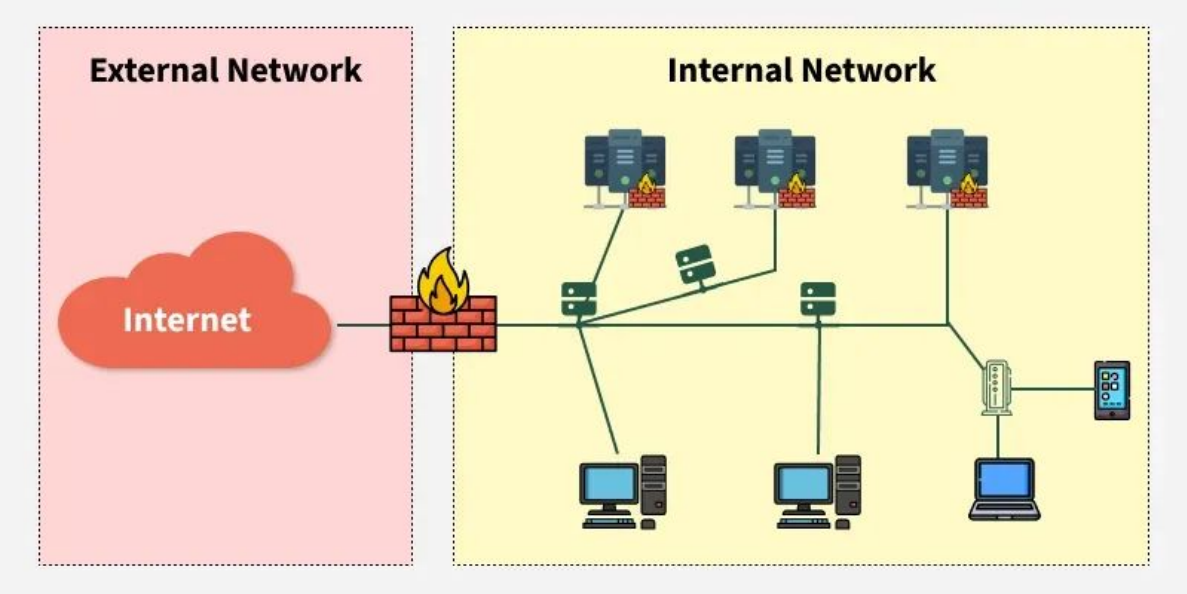
Internal Firewall

Placed between different segments inside your network, such as departments or sensitive zones. Imagine every department in a company having a door lock with access rules.



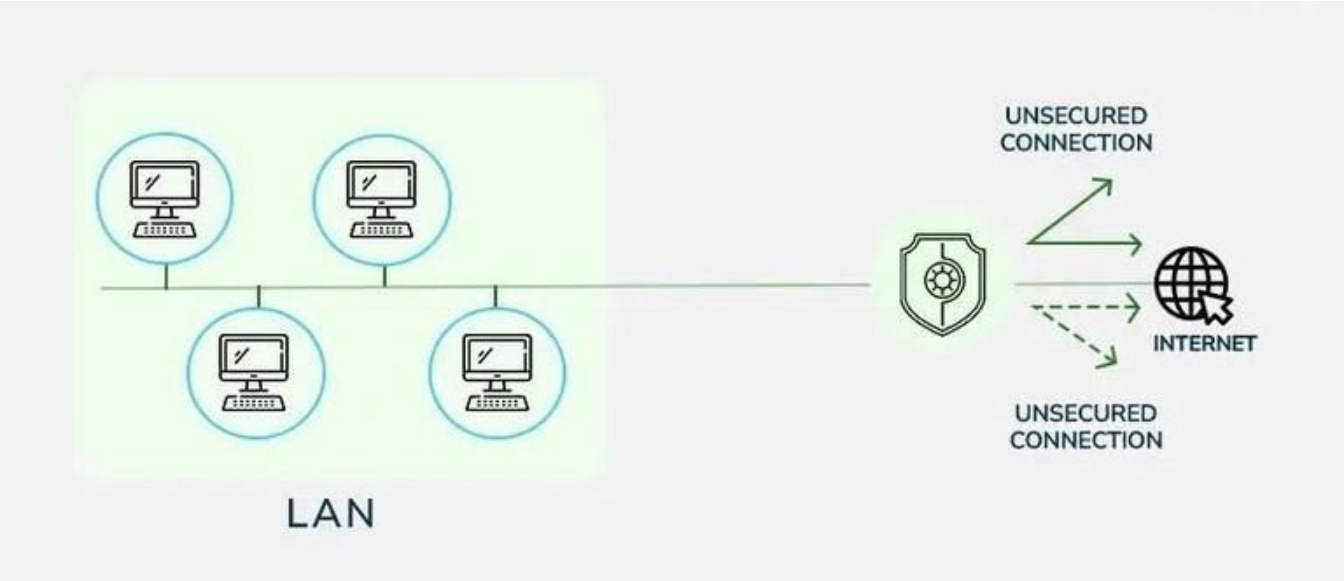
Distributed Firewall

Instead of one firewall at the edge, security rules are applied at multiple endpoints across the network. Like installing security alarms in every room of your house rather than just at the main door.



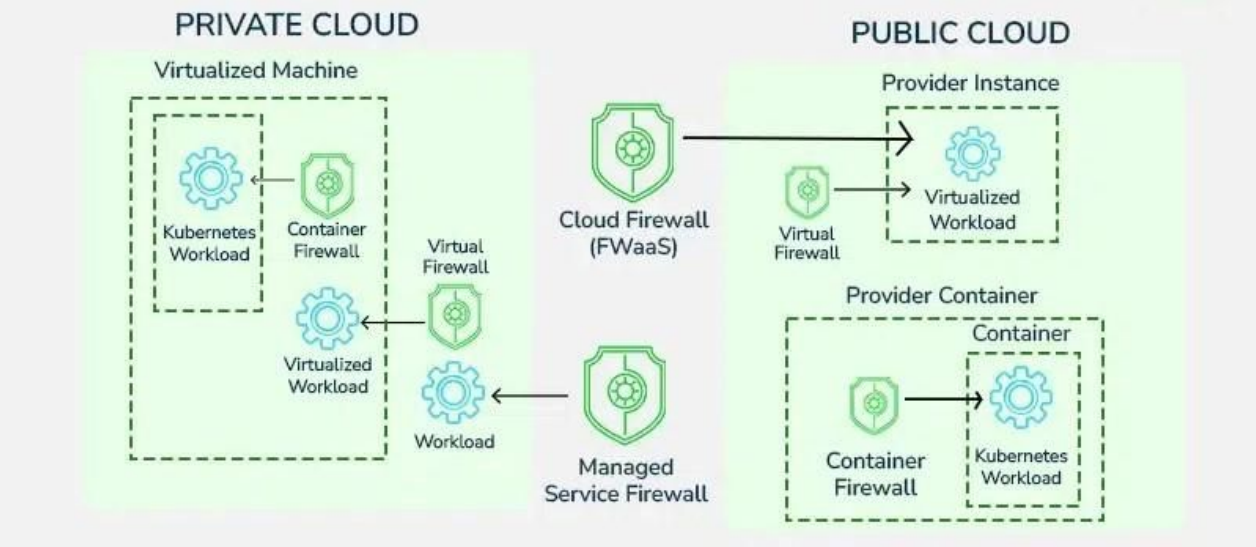
Hardware Firewall

A physical box or appliance that connects to your network. Often used in large or office environments. Think of it like a security gate at the main entrance—visible, strong, and standalone.



Software Firewall

Installed as a program on a device or server. Easier to set up and ideal for individuals or virtual setups. Like installing a firewall app on your laptop to control its own internet access.



Real World Examples

- Abirami M
22z204

Examples of Firewalls

Personal Use

Windows Defender Firewall offers built-in protection for home users, monitoring connections on personal devices. It's free and pre-installed.

Enterprise Solutions

Palo Alto NGFW and **Cisco ASA** provide advanced threat detection, deep packet inspection, and application-level control for large networks.

Cloud Platforms

AWS Network Firewall and **Azure Firewall** offer scalable, managed security for cloud infrastructure with centralized policy management.

Advantages

External Threat Defense Blocks unauthorized access, malware, and malicious traffic.

Policy Enforcement Ensures consistent security rules, reducing vulnerabilities.

Traffic Visibility Provides real-time network insights for rapid incident response.

Secure Remote Access Enables secure remote work via VPN integration.

Firewall Limitations

Insider Threats Cannot prevent actions from legitimate users. Requires user analytics and access management.

Configuration Challenges Misconfigured rules create gaps or block legitimate traffic. Regular audits and skilled administrators are key.

Performance Impact Deep inspection can cause latency during high traffic. Proper sizing and optimization are essential for network speed.

Cost Considerations Enterprise firewalls are significant investments. Balance security needs with budget.

The Bottom Line on Firewall Security

o Choose the Right Type

Different firewall solutions for different needs (personal devices to cloud).

o Align with Requirements

Select based on budget, network scale, and specific security needs.

o Implement Defense in Depth

Complement firewalls with antivirus, IDS, encryption, and awareness training.