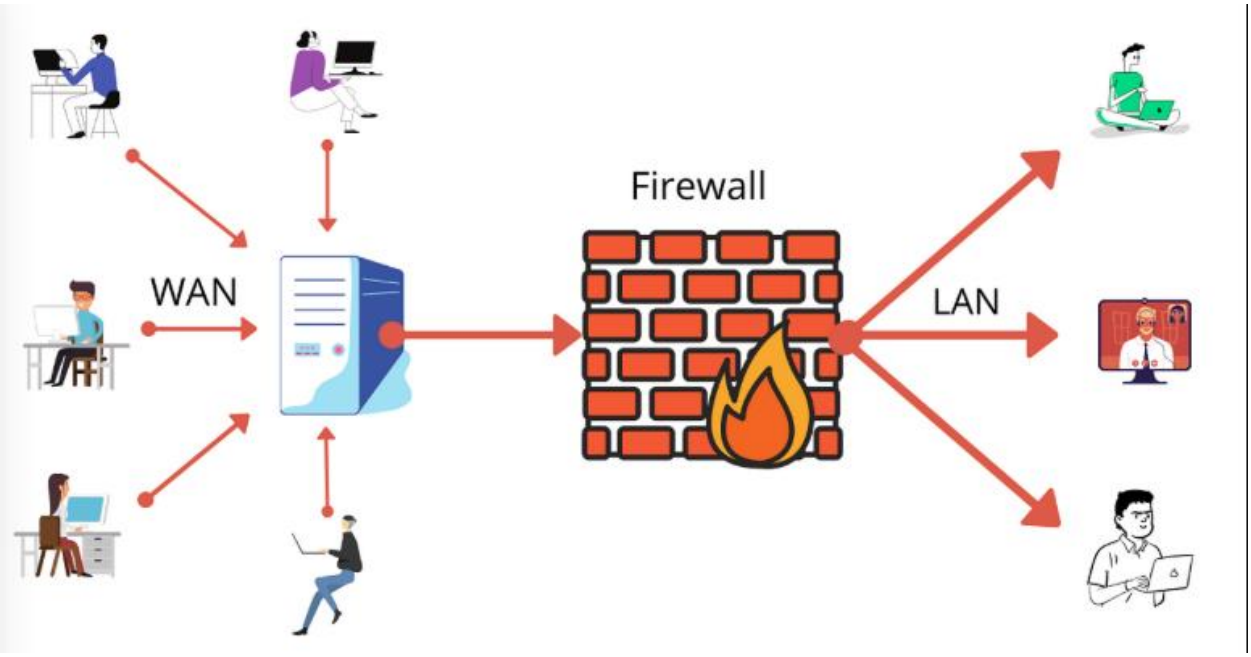
FIREWALL FUNDAMENTALS

What is a Firewall?

A firewall is a network security device or software that monitors, filters, and controls incoming and outgoing network traffic based on defined security rules. It acts as a traffic inspection barrier between trusted internal networks and untrusted external networks (e.g., the internet).

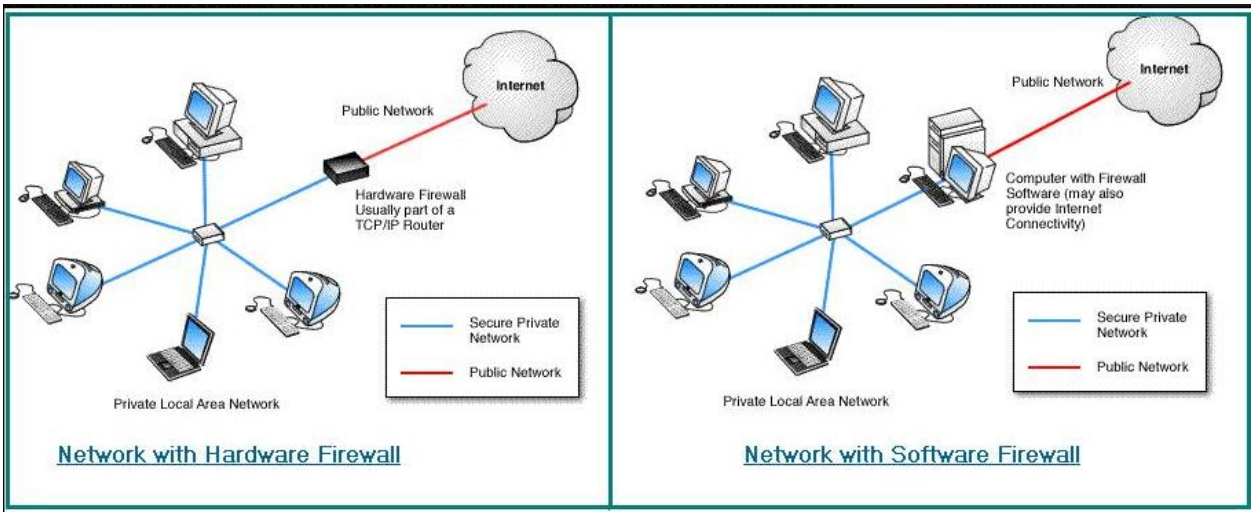


Firewalls can perform:

- Access Control (based on IP, ports, services)
- Traffic Logging
- Intrusion Detection/Prevention
- Application-Level Filtering
- Stateful Packet Inspection

Modern enterprise firewalls often integrate deep inspection capabilities and threat intelligence, especially in Next-Gen Firewalls (NGFWs).

💻 Hardware Firewall vs Software Firewall



Aspect	Hardware Firewall	Software Firewall
Location	Dedicated device on network perimeter	Installed on individual systems (OS-level)
Resource Usage	Independent resources	Consumes host resources (CPU/RAM)
Scalability	More scalable for large traffic volumes	Limited by host hardware
Central Management	Easier to manage policies at scale	Requires endpoint-level management
Examples	Cisco ASA, FortiGate, Palo Alto, Sophos XG	Windows Firewall, iptables (Linux), pfSense

🔰 Types of Firewalls

1. Personal Firewall

How it works:

- Installed on individual endpoints (laptops, desktops, servers).

- Filters inbound and outbound traffic specific to that host.
- Often includes per-application rules and alerts for unknown connections.

Features:

- Blocks unauthorized outbound traffic (malware C2)
- Controls internet access per application
- Integrated with OS (Windows Firewall, macOS Application Firewall)

Example:

- Windows Defender Firewall
- ZoneAlarm
- Comodo Personal Firewall

Use Case:

- Endpoint protection for users
- Laptops used in public networks
- Devices not behind a network firewall (remote users)

2. Network Firewall

How it works:

- Designed to protect entire network segments, not just individual devices.
- Can be deployed at:
  - Perimeter (internet-facing)
  - Internal segmentation (between departments/VLANs)
- Can be physical or virtual depending on environment.

Features:

- Can route and filter traffic

- Integrated with VPNs, IPS, QoS
- Can be HA (high availability) for redundancy

Example:

- Cisco ASA/FTD
- Palo Alto NGFW
- FortiGate
- pfSense

Use Case:

- Enterprise perimeter security
- Internal segmentation
- Cloud VPC/Subnet firewalling

3. Packet Filtering Firewall

How it works:

- Examines packet headers at OSI Layer 3 (Network) and Layer 4 (Transport).
- Makes filtering decisions based on static rules like:
  - Source IP
  - Destination IP
  - Source/destination port
  - Protocol type (TCP, UDP, ICMP)

Key Limitation:
Stateless—doesn't remember past packets or session information. Every packet is treated in isolation.

Example:

- A rule allowing traffic only from IP 192.168.1.0/24 to port 443 (HTTPS)
- Cisco ACLs or iptables with basic rules

Use Case:

- Basic perimeter filtering for small networks, routers, or internal segmentation where performance is prioritized over deep inspection

4. Proxy Firewall (Application Gateway)

How it works:

- Works at OSI Layer 7 (Application Layer).
- Acts as a middleman—the client connects to the proxy, and the proxy connects to the destination.
- Inspects full application data (e.g., HTTP requests, SMTP content).

Features:

- Anonymizes user IPs
- Can filter or block specific web content
- Can cache or rewrite requests
- Detects application-specific threats

Example:

- Squid Proxy for web traffic
- Bluecoat, Microsoft TMG (legacy)

Use Case:

- Secure web gateways
- Email and web filtering (DLP)
- Anonymous browsing or hiding internal IPs from outside

5. Stateful Inspection Firewall

How it works:

- Also called dynamic packet filtering.
- Tracks the state and context of connections:
  - Connection initiation
  - Established session
  - Termination
- Only allows packets that are part of a valid, established connection.

Example:

- Cisco ASA firewalls
- Check Point Stateful Inspection engine

Use Case:

- Enterprise networks, branch offices
- Between internal VLANs to inspect east-west traffic
- Anywhere you need more security than basic stateless filtering

6. Unified Threat Management (UTM)

How it works:
An all-in-one appliance combining several security features:

- Firewall
- Antivirus/Anti-malware
- Intrusion Prevention System (IPS)
- VPN (IPSec, SSL)
- Web content filtering
- Anti-spam

Benefits:

- Easy to deploy and manage
- Cost-effective
- Ideal for SMBs needing centralized security

Example:

- Sophos XG Firewall
- WatchGuard UTM
- Fortinet UTM mode

Use Case:

- Small to medium-sized businesses (SMBs) with limited IT staff
- Branch office security

7. Next-Generation Firewall (NGFW)

How it works:

- Combines traditional firewall functions with advanced threat detection.
- Can inspect:
  - Application signatures (Layer 7 awareness)
  - Malware and exploits (IPS/IDS)
  - Encrypted traffic (SSL inspection)
  - User identity (via integration with Active Directory)

Features:

- Deep Packet Inspection (DPI)
- Application Control (e.g., block Facebook but allow WhatsApp)
- User-based policies, not just IPs
- Threat intelligence feed integration

Example:

- Palo Alto Networks Firewalls
- Fortinet FortiGate NGFW
- Cisco Firepower
- Check Point R80+

Use Case:

- Large enterprises and data centers
- Zero Trust Network Access (ZTNA)
- East-west inspection in internal networks

🔥 FIREWALL DEPLOYMENT MODELS

1. Zone-Based Firewall

- Logical grouping of interfaces into zones (e.g., LAN, WAN, DMZ).
- Traffic between zones is explicitly controlled via security policies.
- More scalable and manageable than interface-based rules.

Example: Cisco Zone-Based Policy Firewall (ZPF)

2. Virtual Firewall

- Runs as a VM instance, usually within virtualization platforms.
- Enables firewalling between virtual machines or tenants.
- Supports microsegmentation in cloud or hybrid environments.

Platforms: VMware NSX, Cisco FTDv, Palo Alto VM-Series

3. Cloud Firewall (FWaaS)

- Firewall-as-a-Service, fully managed in the cloud.
- Secures cloud workloads or remote users via policy-based control.
- Deployed in public cloud environments (AWS, Azure, GCP).

Features:

- Global scalability
- Zero-touch maintenance
- Centralized logging

Examples: Azure Firewall, AWS Network Firewall, Zscaler

4. Transparent Firewall

- Also called Layer 2 firewall or stealth firewall.
- Doesn’t require IP addressing or routing — passes traffic like a switch.
- Ideal for insertion into existing networks with minimal disruption.

Use Case: Inline inspection with no IP address reconfiguration