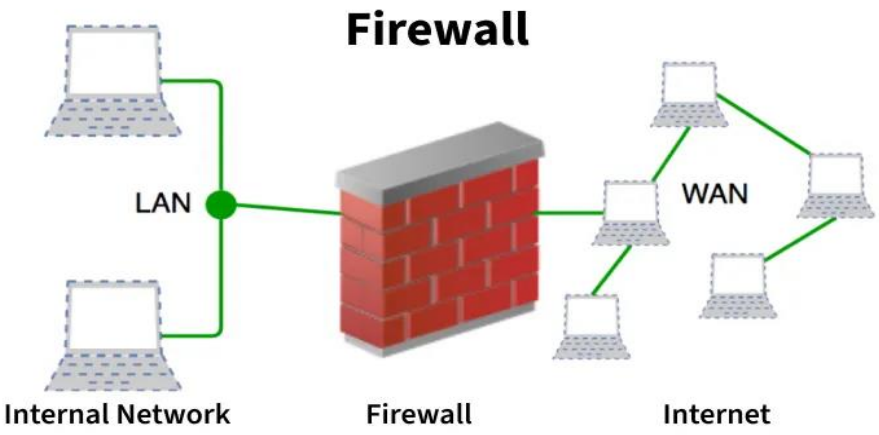
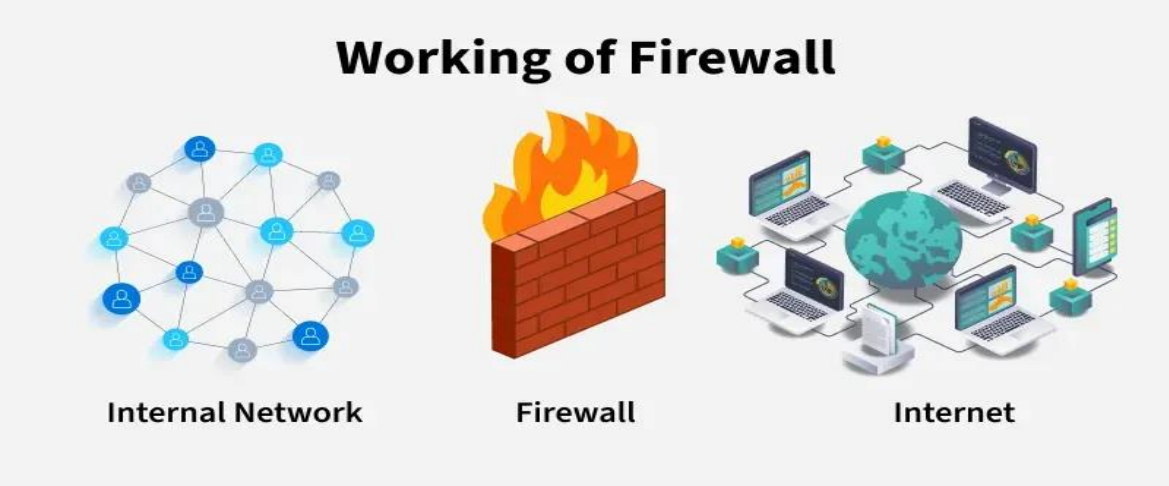
Introduction of Firewall for Security



A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and, based on a defined set of security rules, accepts, rejects, or drops that specific traffic. It acts like a security guard that helps keep your digital world safe from unwanted visitors and potential threats.



Firewall

- **Accept:** allow the traffic
- **Reject:** block the traffic but reply with an “unreachable error”
- **Drop:** block the traffic with no reply

Need For a Firewall

A firewall is essential because networks are constantly exposed to both safe and harmful traffic from the internet or other networks. Without a firewall, your systems would have no protection against unwanted access, malicious activity, or accidental data leaks.

1. Preventing Unauthorized Access

Imagine your house door is always open. Anyone passing by could walk in and take your things. A firewall is like a locked door with a guard, letting only trusted people in and keeping strangers out.

2. Blocking Malicious Traffic

Think of your email inbox. Without a spam filter, you'd get flooded with scam and spam messages. A firewall works like that spam filter it blocks harmful data before it reaches you.

3. Protecting Sensitive Information

It's like keeping your bank PIN in a safe instead of leaving it on the table where anyone can see it. A firewall ensures your personal and business data stays hidden from cybercriminals.

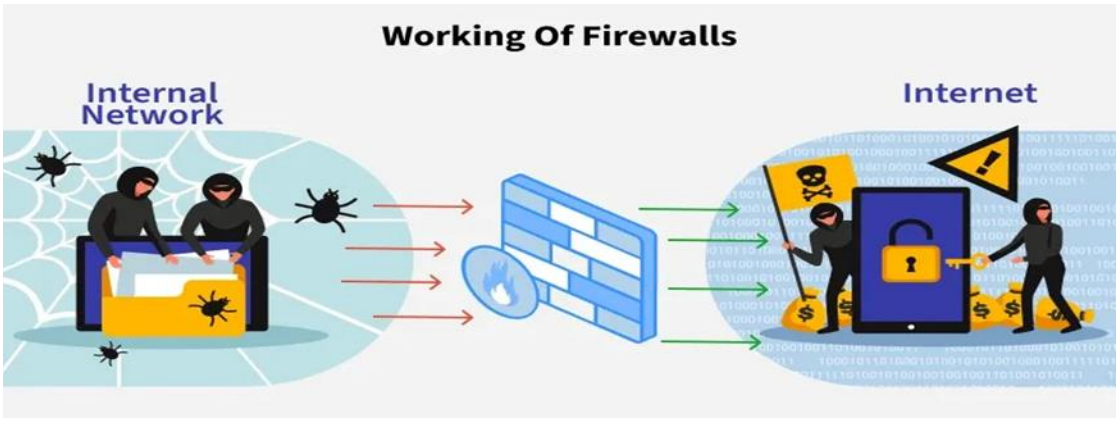
4. Preventing Cyber Attacks

If you leave your car unlocked in a parking lot, thieves can steal it. A firewall locks your network so attackers can't hijack it.

5. Controlling Network Usage

Just like parents set parental controls so kids can't visit unsafe websites, Firewalls control where your computers are allowed to connect.

Woking Of Firewall



Working of Firewalls

Firewalls can control and monitor the amount of incoming or outgoing traffic of our network. The data that comes to our network is in the forms of packets(a small unit of data), it is tough to identify whether the packet is safe for our network or not, this gives a great chance to the hackers and intruders to bombard our networks with various viruses, malware, spam, etc.

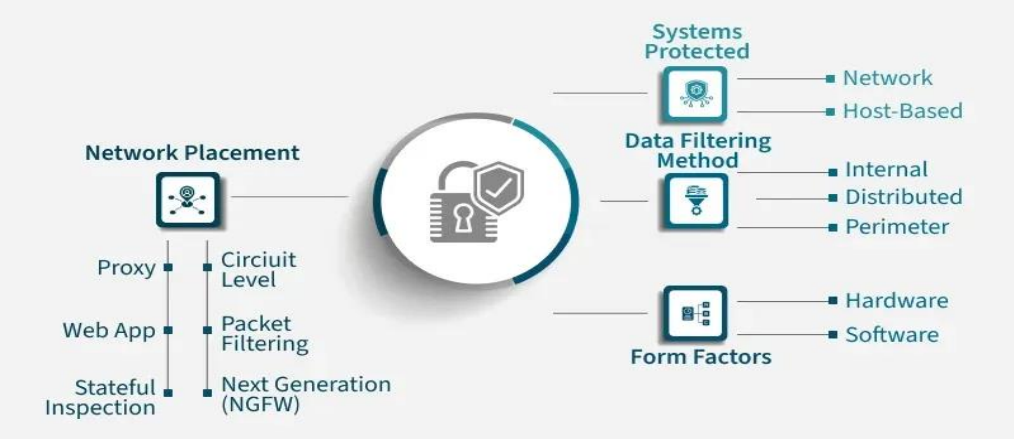
A firewall works like a security guard for your network, standing between your internal systems such as computers, servers, and devices and the outside world, like the internet or other networks. It carefully inspects all data entering or leaving to ensure only safe traffic is allowed through.

- When data tries to enter or leave your network, it passes through the firewall first.
- The firewall examines the data packets (small chunks of information) using predefined rules.
- Rules can be defined on the firewall based on the necessity and security policies of the organization.
- FIrewall allows decision making like Allow → If the packet matches safe rules. or Block → If the packet is suspicious, from a blacklisted source, or contains malicious code.
- The firewall records blocked or unusual traffic for security teams to review.
- Alerts can be sent in real time if a major threat is detected.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Types of Firewall:-

Firewalls can be categorized based on their generation.



Types of Firewalls: -

1) Network Placement

- Packet Filtering Firewall
- Stateful Inspection Firewall
- Proxy Firewall (Application Level)
- Circuit-Level Gateway
- Web Application Firewall (WAF)
- Next-Generation Firewall (NGFW)

2) Systems Protected

- Network Firewall
- Host-Based Firewall

3) Data Filtering Method

- Perimeter Firewall
- Internal Firewall
- Distributed Firewall

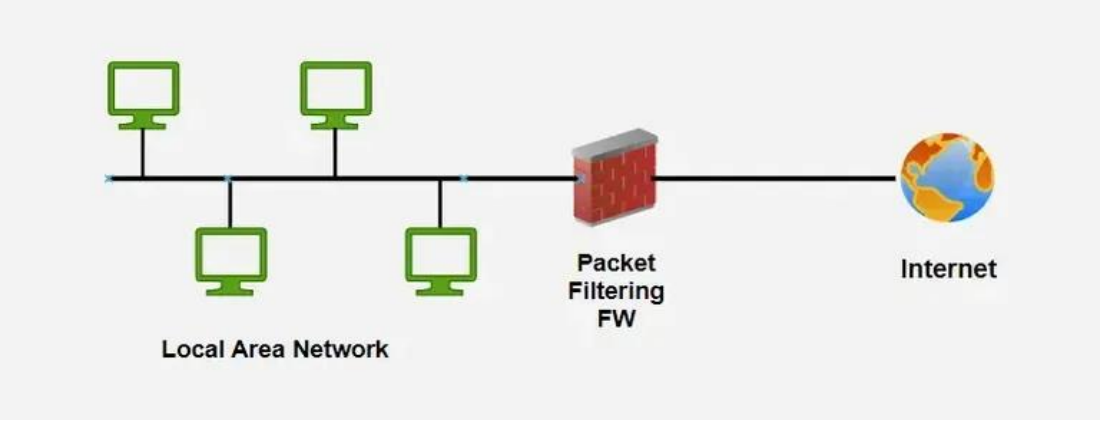
4) Form Factors

- Hardware Firewall
- Software Firewall

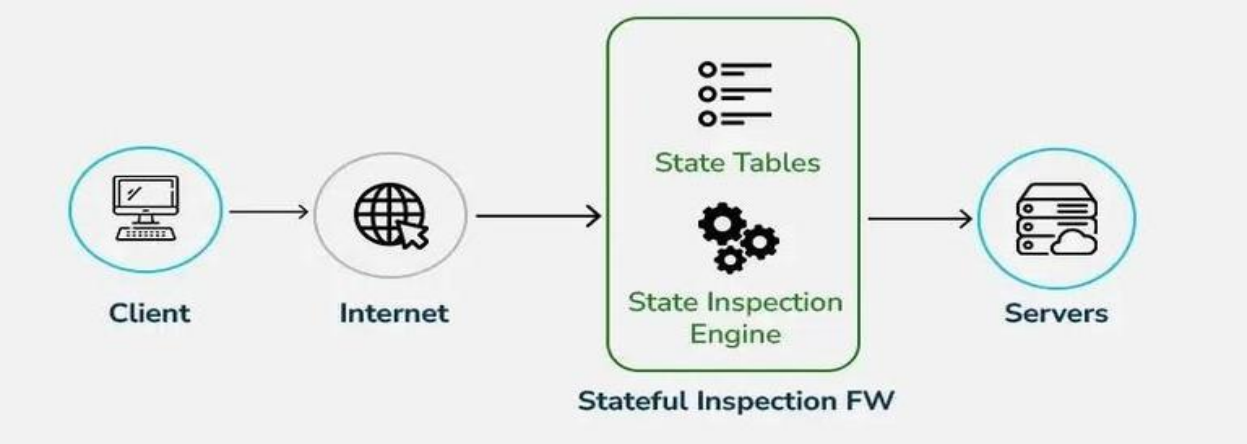
1) Network Placement

Network Security is the process of protecting networks, systems, and data from unauthorized access, attacks, and damage.

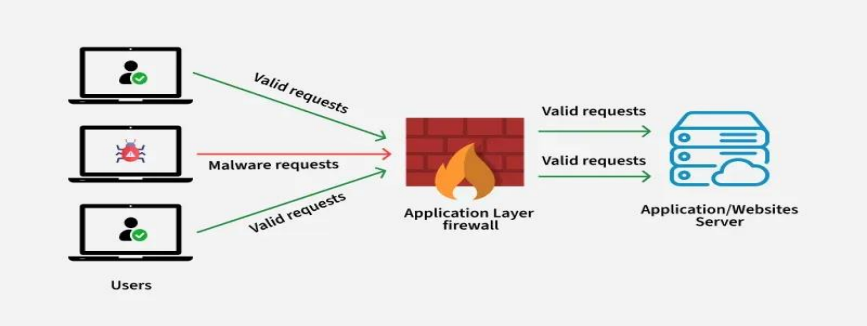
- **Packet Filtering Firewall**
  This is the most basic type. It checks packet headers—like IP address, port number, and protocol—and decides whether to allow or block them. Think of it like checking someone's ID at the gate. If the name and ID match the list, they're allowed in, no questions asked.



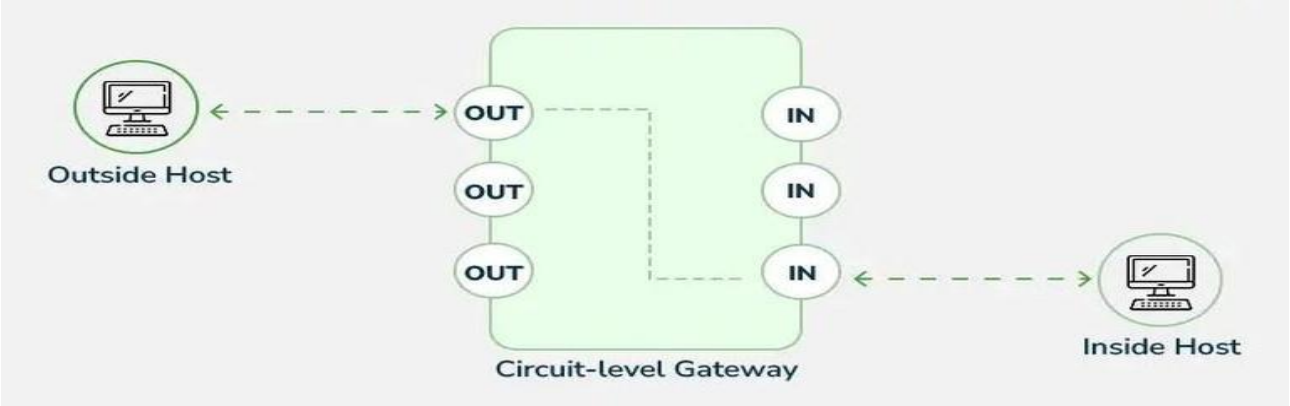
- **Stateful Inspection Firewall**
  Goes a step further. It monitors active connections and makes decisions based on the context of traffic. Imagine a hotel that remembers you checked in earlier, so it doesn't question you every time you enter.



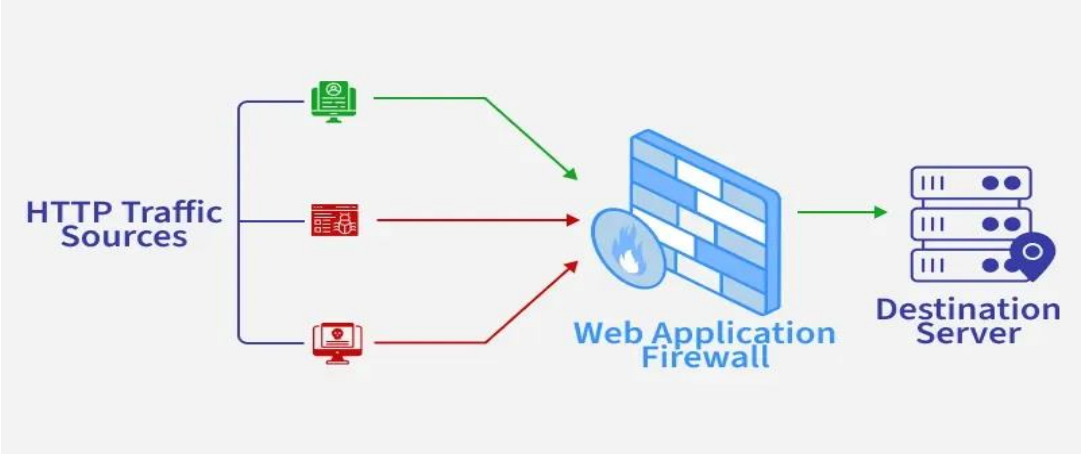
- **Proxy Firewall (Application Level)**
  This acts like a middleman between user and destination. It fetches data on your behalf while filtering dangerous content. Like asking your assistant to go to a store for you—they check the item first before handing it over.



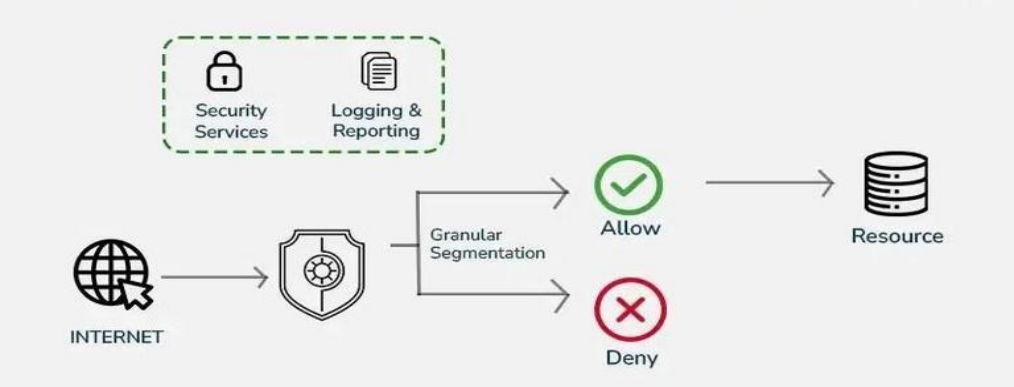
- **Circuit-Level Gateway**
  Validates if a connection is successfully established (like TCP handshake), but doesn't inspect actual data. Like confirming someone is calling from a known number without listening to the call.



- **Web Application Firewall (WAF)**
  Specifically protects websites and web apps from attacks like SQL injection or cross-site scripting. Imagine a form guard that checks what users type before it reaches your website—blocking any harmful tricks.



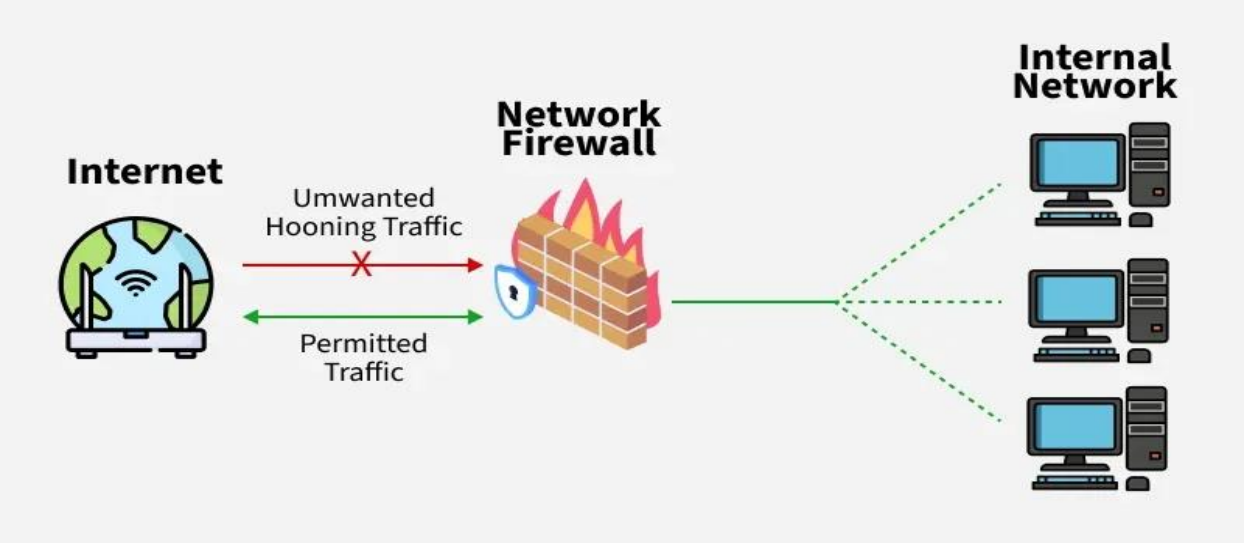
- **Next-Generation Firewall (NGFW)**
  Combines traditional firewalls with modern features like app control, intrusion prevention, malware detection, and encrypted traffic inspection. It's like a security team with surveillance cameras, ID scanners, and behavior monitoring—all working together.



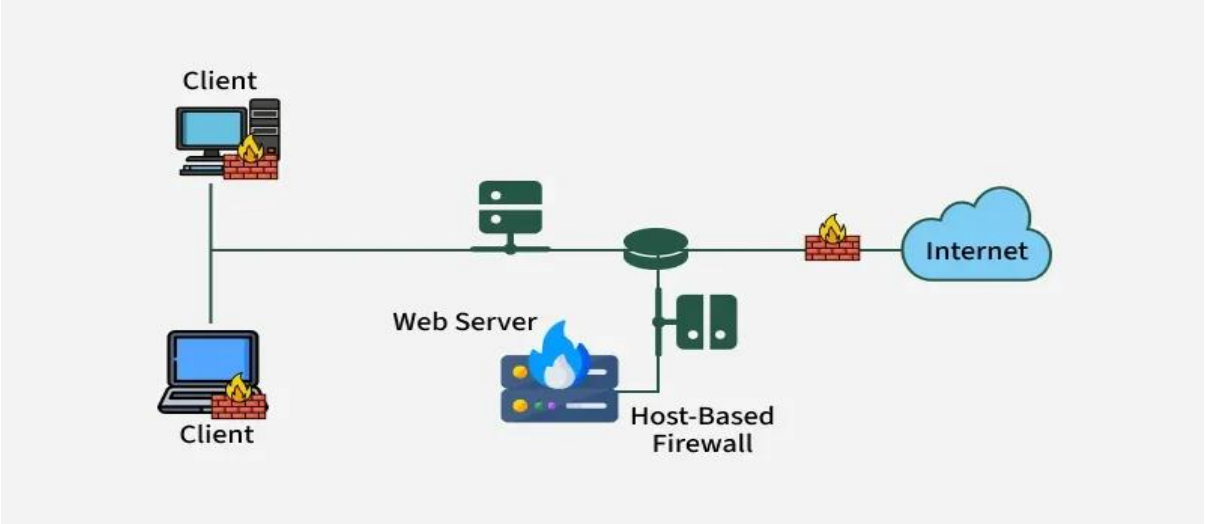
2) Network Firewall

A Network Firewall secures the perimeter, while a Host-Based Firewall protects the endpoint.

- **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.



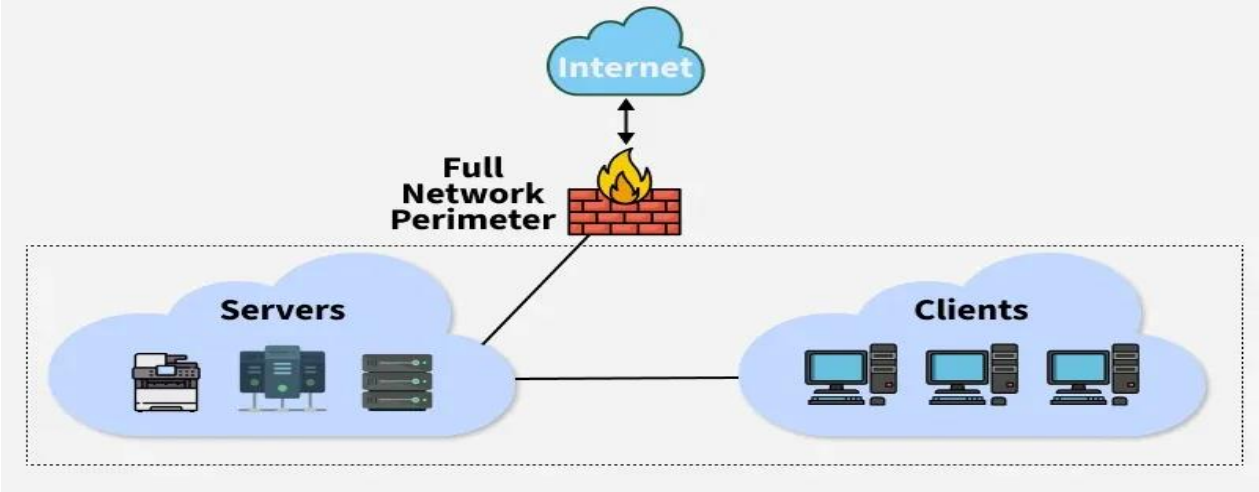
- **Host-Based Firewall**
  Installed on individual devices like laptops, servers, or mobile phones. It protects only that one system. Think of it as having a security app that watches over just your phone, not the whole office.



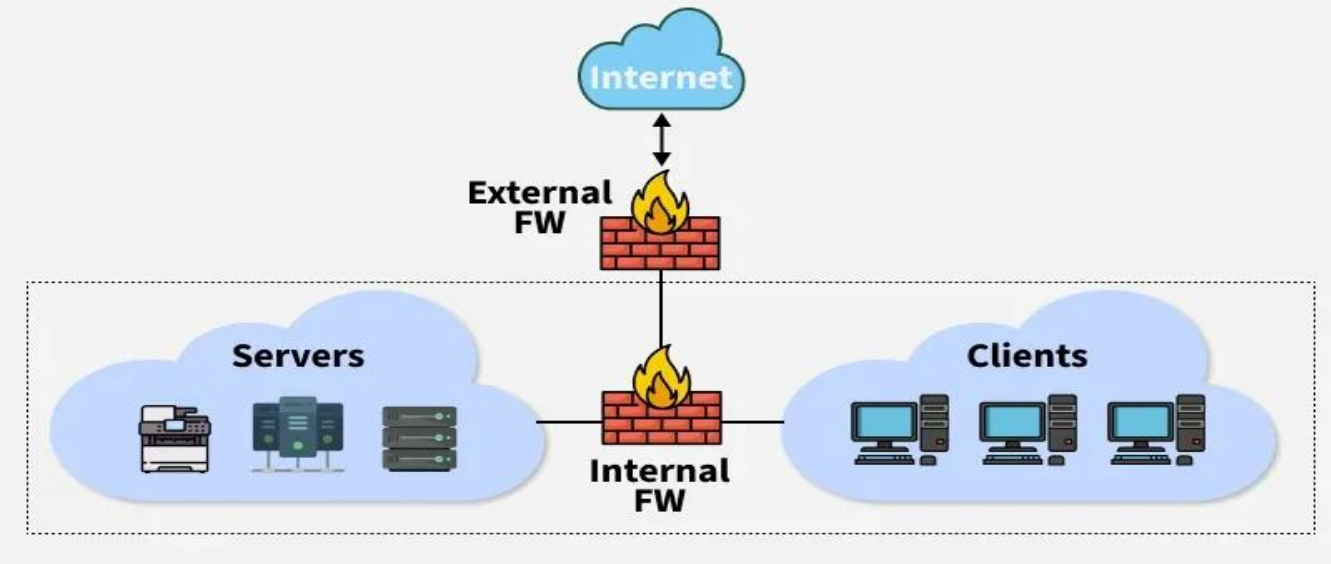
3) Data Filtering Method

All three of these firewall types work to control network access, but they differ in their placement and scope.

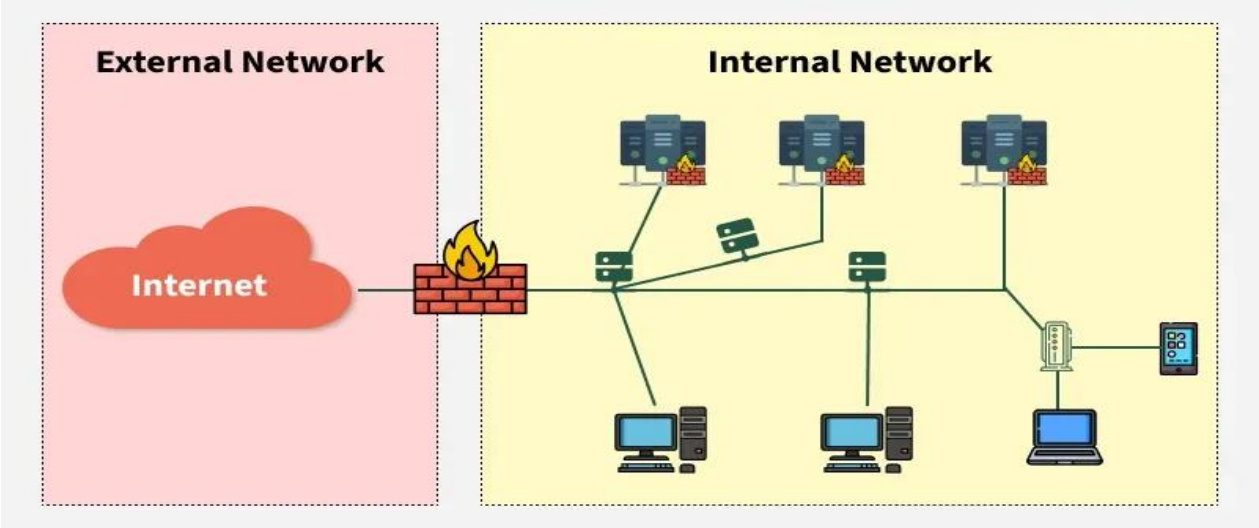
- **Perimeter Firewall**
  Sits at the edge of your network, filtering traffic coming in and out from the internet. Like a fence with a gate that controls who gets into your property.



- **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.



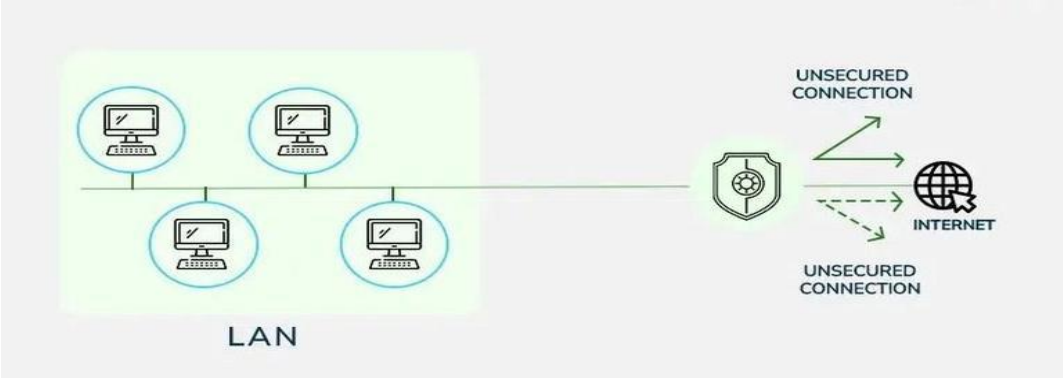
- **Distributed Firewall**
  Instead of one firewall at the edge, security rules are applied at multiple endpoints across the network. Like installing security alarms in every room of your house rather than just at the main door.



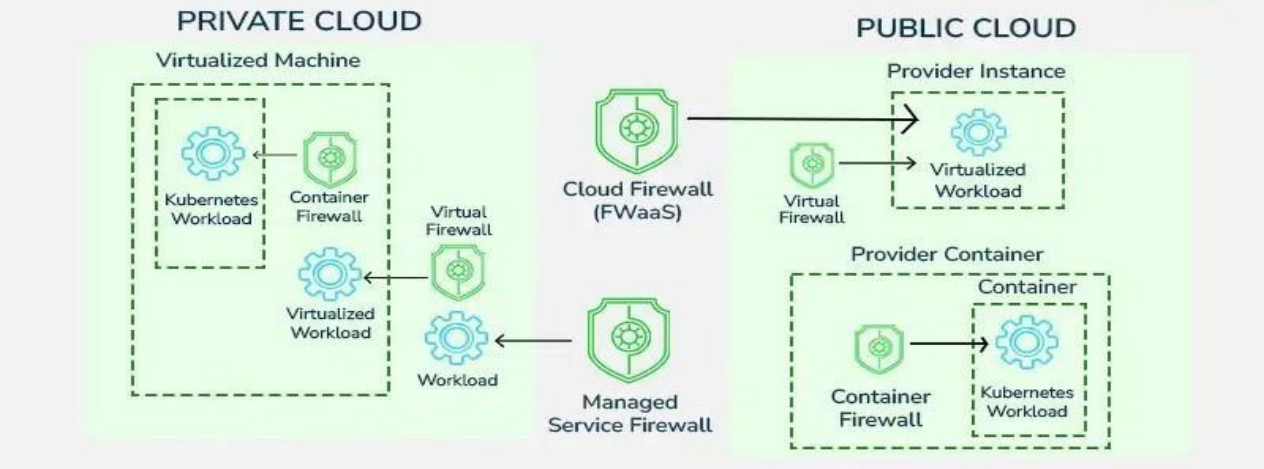
4) Form Factors

A program installed on a computer or server that protects it from network threats.

- **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.



Limitations of Network Firewall

Here are the demerits of Network Firewall

- **Cost:** Depending on the type of firewall, it can be costly, usually, the hardware firewalls are more costly than the software ones.
- **Restricts User:** Restricting users can be a disadvantage for large organizations, because of its tough security mechanism. A firewall can restrict the employees to do a certain operation even though it's a necessary operation.
- **Issues With The Speed of The Network:** Since the firewalls have to monitor every packet passing through the network, this can slow down operations needed to be performed, or it can simply lead to slowing down the network.
- **Maintenance:** Firewalls require continuous updates and maintenance with every change in the networking technology. As the development of new viruses is increasing continuously that can damage your system.

Importance of Firewalls

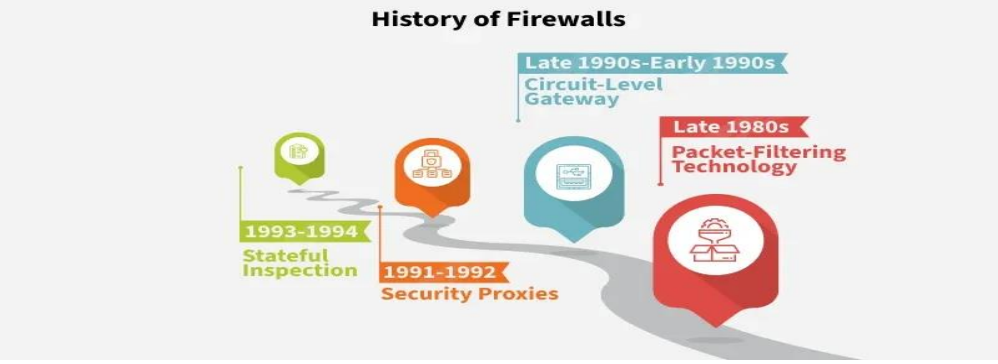
A network firewall is your first line of defense in cybersecurity. It monitors, filters, and controls data moving in and out of your network

- Networks are vulnerable to any traffic trying to access your systems, whether it's harmful or not. That's why it's crucial to check all network traffic.
- When you connect personal computers to other IT systems or the internet, it opens up many benefits like collaboration, resource sharing, and creativity. But it also exposes your network and devices to risks like hacking, identity theft, malware, and online fraud.

- Once a malicious person finds your network, they can easily access and threaten it, especially with constant internet connections.
- Using a firewall is essential for proactive protection against these risks. It helps users shield their networks from the worst dangers.

History of Firewalls

Firewalls evolved from simple packet filtering to advanced, user-friendly security systems used worldwide.



- **Late 1980s**: Jeff Mogul, Brian Reid, and Paul Vixie at Digital Equipment Corp (DEC) developed packet-filtering technology, laying the groundwork for firewalls by checking external connections before they reached internal networks.
- **Late 1980s - Early 1990s**: AT&T Bell Labs researchers, including Presotto, Sharma, and Nigam, developed the **circuit-level gateway**, a firewall that vetted ongoing connections without reauthorizing each data packet, paving the way for more efficient security.
- **1991-1992**: Marcus Ranum introduced security proxies at DEC, leading to the creation of the **Secure External Access Link (SEAL)**, the first commercially available application-layer firewall, based on earlier DEC work.
- **1993-1994**: At **Check Point**, Gil Shwed pioneered **stateful inspection technology**, filing a patent in 1993. Nir Zuk developed a graphical interface for **Firewall-1**, making firewalls accessible and widely adopted by businesses and homes

What Does Firewall Security Do?

A firewall serves as a security barrier for a network, narrowing the attack surface to a single point of contact. Instead of every device on a network being exposed to the internet, all traffic must first go through the firewall. This way, the firewall can filter and block non-permitted

traffic, whether it's coming in or going out. Additionally, firewalls help create a record of attempted connections, improving security awareness.

Firewalls regulate both inbound and outbound traffic, protecting the network from:

- **External threats** such as viruses, phishing emails, denial-of-service (DoS) attacks, and backdoors. Firewalls filter incoming traffic flows, preventing unauthorized access to sensitive data and thwarting potential malware infections.
- **Insider threats** like known bad actors or risky applications. A firewall can enforce rules and policies to restrict certain types of outgoing traffic, which helps identify suspicious activity and mitigate data exfiltration.

What Can Firewalls Protect Against?

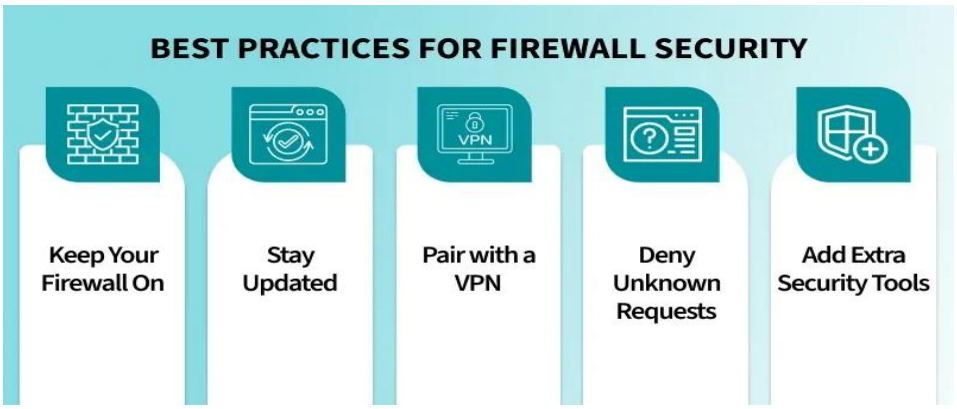
Firewalls can protect against a variety of threats by monitoring and controlling incoming and outgoing network traffic. Here are the main things they help defend against:

- **Infiltration by Malicious Actors:** Firewalls can block suspicious connections, preventing eavesdropping and advanced persistent threats (APTs).
- **Parental Controls:** Parents can use firewalls to block their children from accessing explicit web content.
- **Workplace Web Browsing Restrictions:** Employers can restrict employees from using the company network to access certain services and websites, like social media.
- **Nationally Controlled Intranet:** Governments can block access to certain web content and services that conflict with national policies or values.

By allowing network owners to set specific rules, firewalls offer customizable protection for various scenarios, enhancing overall network security.

Firewall Security Tips

To maximize your firewall’s protection, enhance its security with these best practices:



Practices For Firewall Security

Keep Your Firewall On

Never turn off your firewall just to connect to a device or network. Instead, adjust your firewall rules and add trusted devices to your allow list.

Stay Updated

Regularly update your firewall software or operating system to patch vulnerabilities and stop new security threats.

Pair with a VPN

A VPN encrypts your internet traffic, adding another layer of protection alongside your firewall. Just be sure to adjust firewall rules if there's a conflict.

Deny Unknown Requests

If you get a suspicious access request, block it immediately. Investigate later before making any permanent changes.

Add Extra Security Tools

Firewalls don't block all threats especially malicious programs you install yourself. Use trusted antivirus or anti-malware software for full coverage.