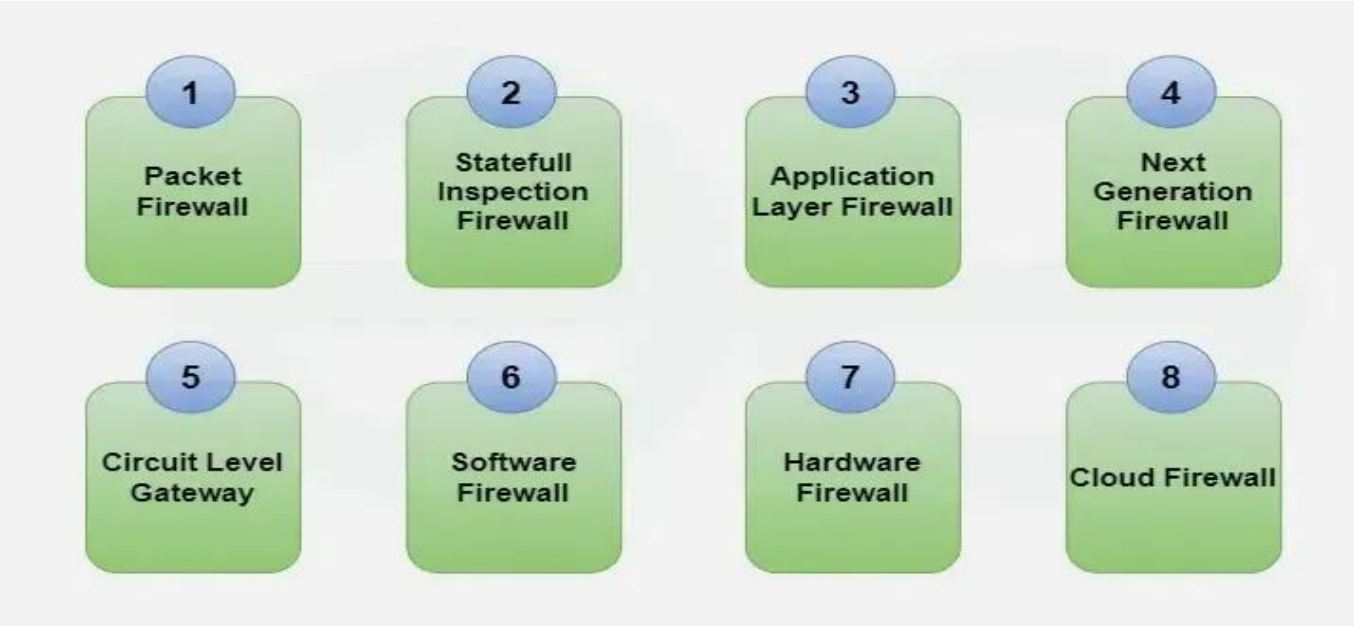
Types of Network Firewall

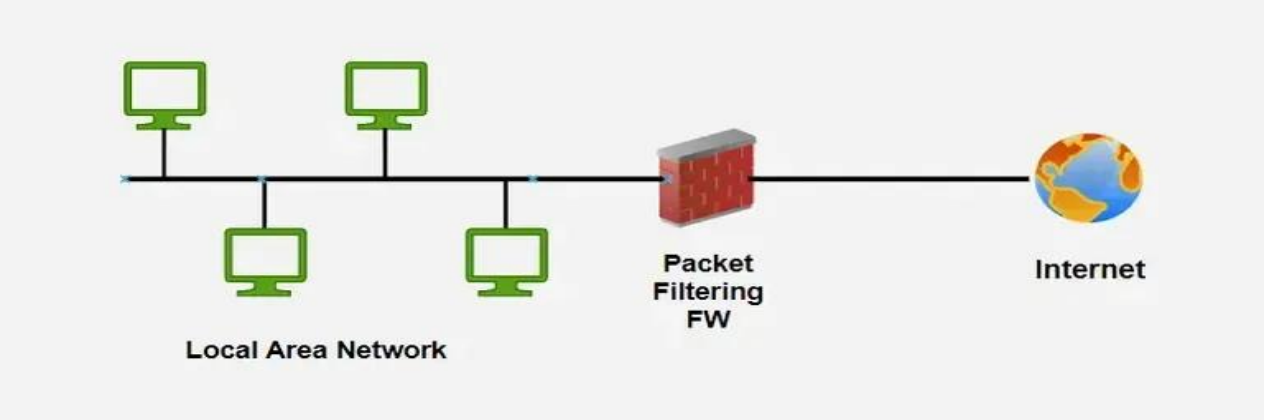
Network Firewalls are the devices that are used to prevent private networks from unauthorized access. A Firewall is a security solution for the computers or devices that are connected to a network, they can be either in the form of hardware as well as in form of software. It monitors and controls the incoming and outgoing traffic (the amount of data moving across a computer network at any given time).

The major purpose of the network firewall is to protect an inner network by separating it from the outer network. An inner Network can be simply called a network created inside an organization and a network that is not in the range of an inner network can be considered an Outer Network.



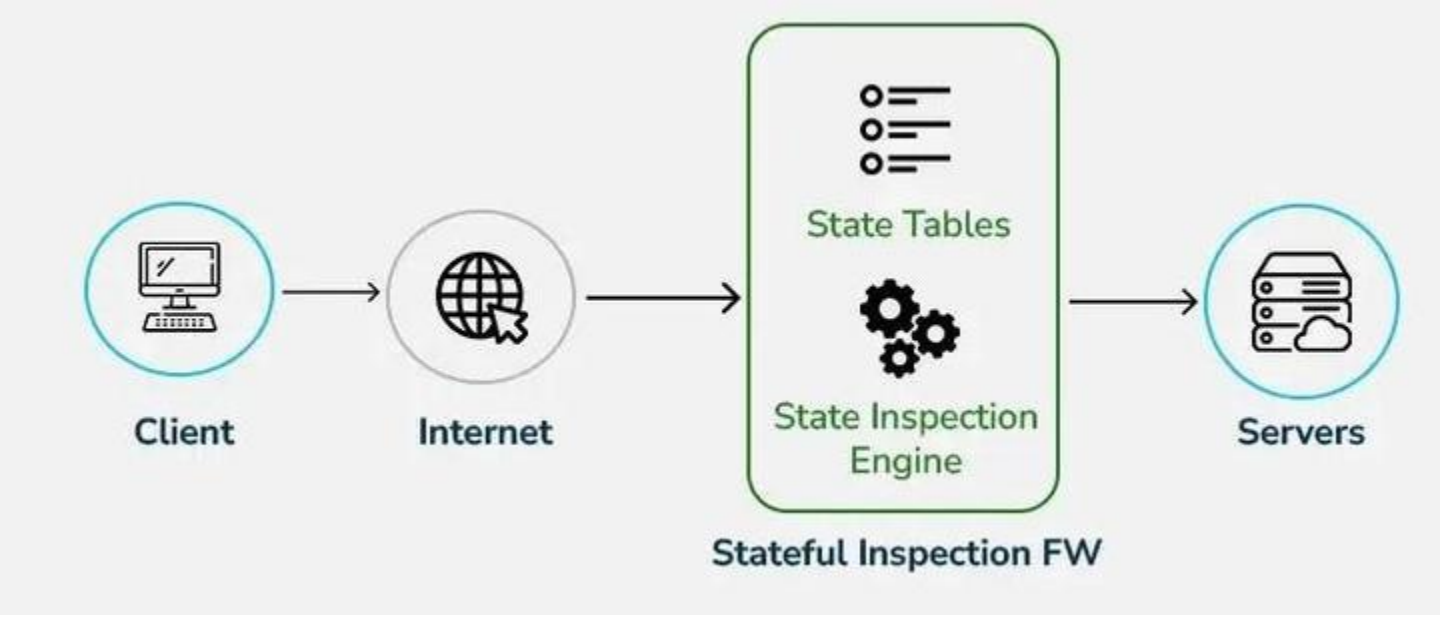
Packet Filters

It is a technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols, and ports. This firewall is also known as a static firewall.



Stateful Inspection Firewalls

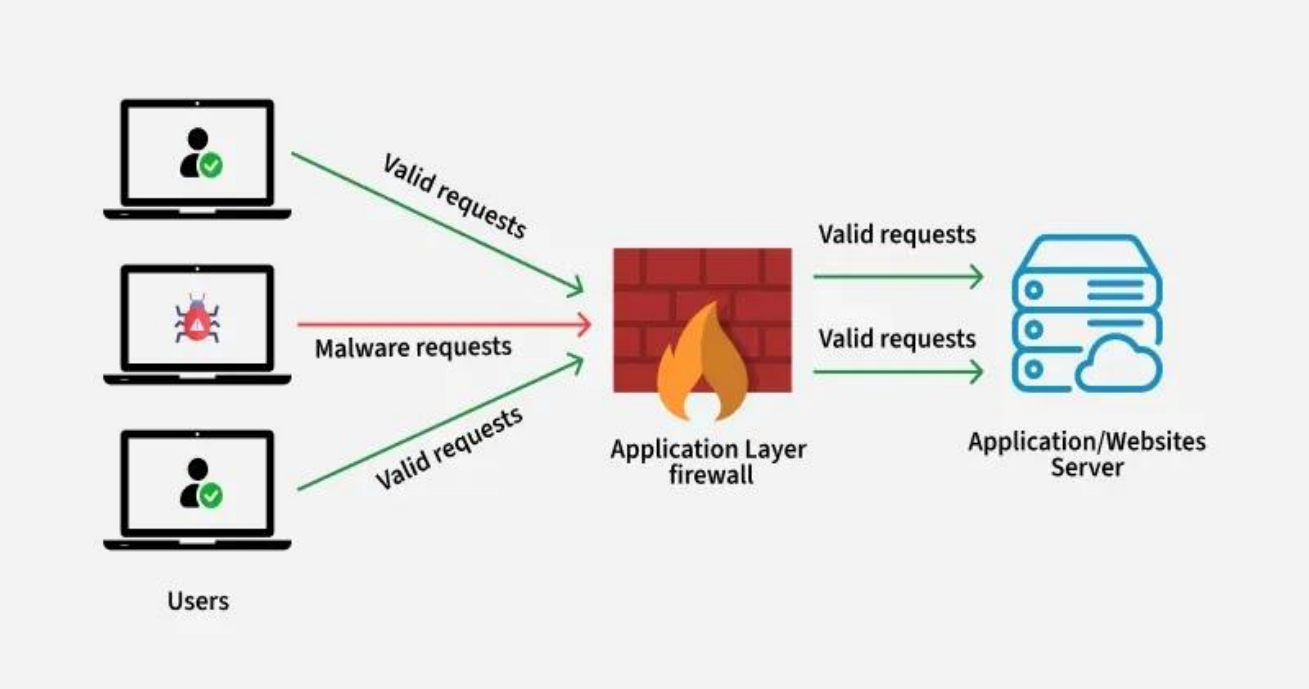
It is also a type of packet filtering that is used to control how data packets move through a firewall. It is also called dynamic packet filtering. These firewalls can inspect that if the packet belongs to a particular session or not. It only permits communication if and only if, the session is perfectly established between two endpoints else it will block the communication.



Stateful Inspection Firewalls

Application Layer Firewalls

These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

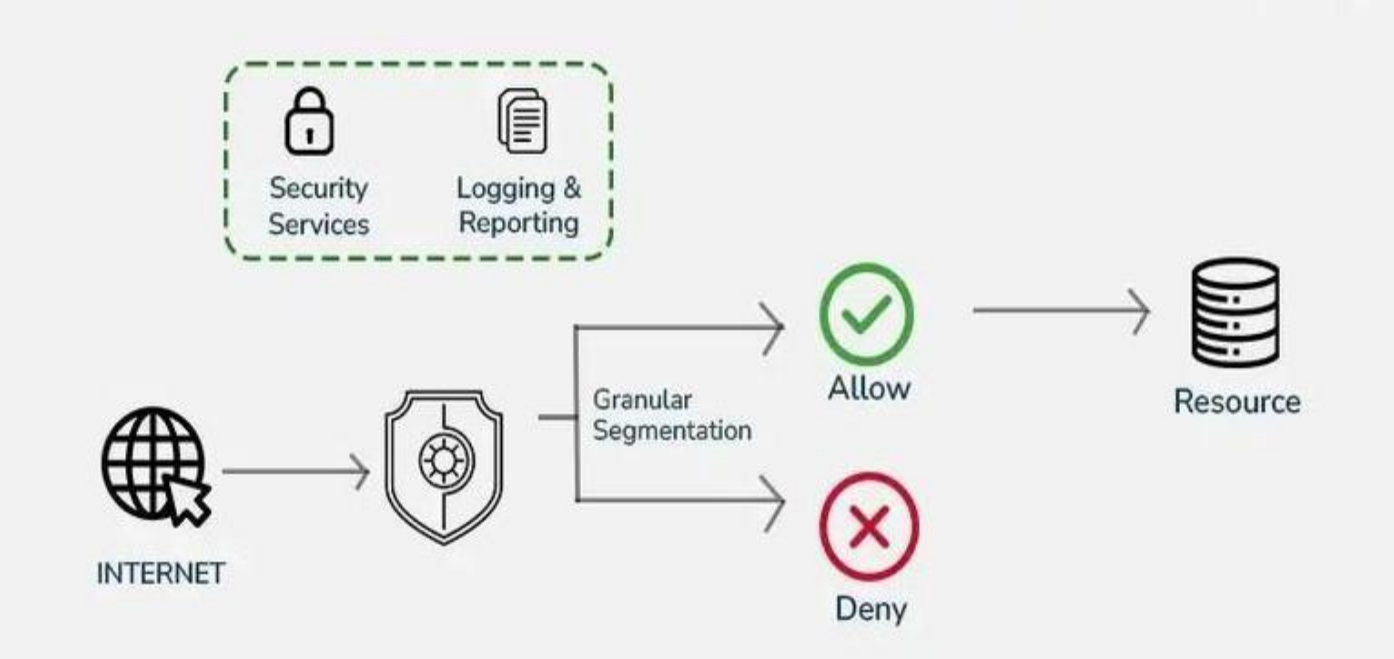


Application Layer Firewall

Next-generation Firewalls

These firewalls are called intelligent firewalls. These firewalls can perform all the tasks that are performed by the other types of firewalls that we learned previously but on top of that, it includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

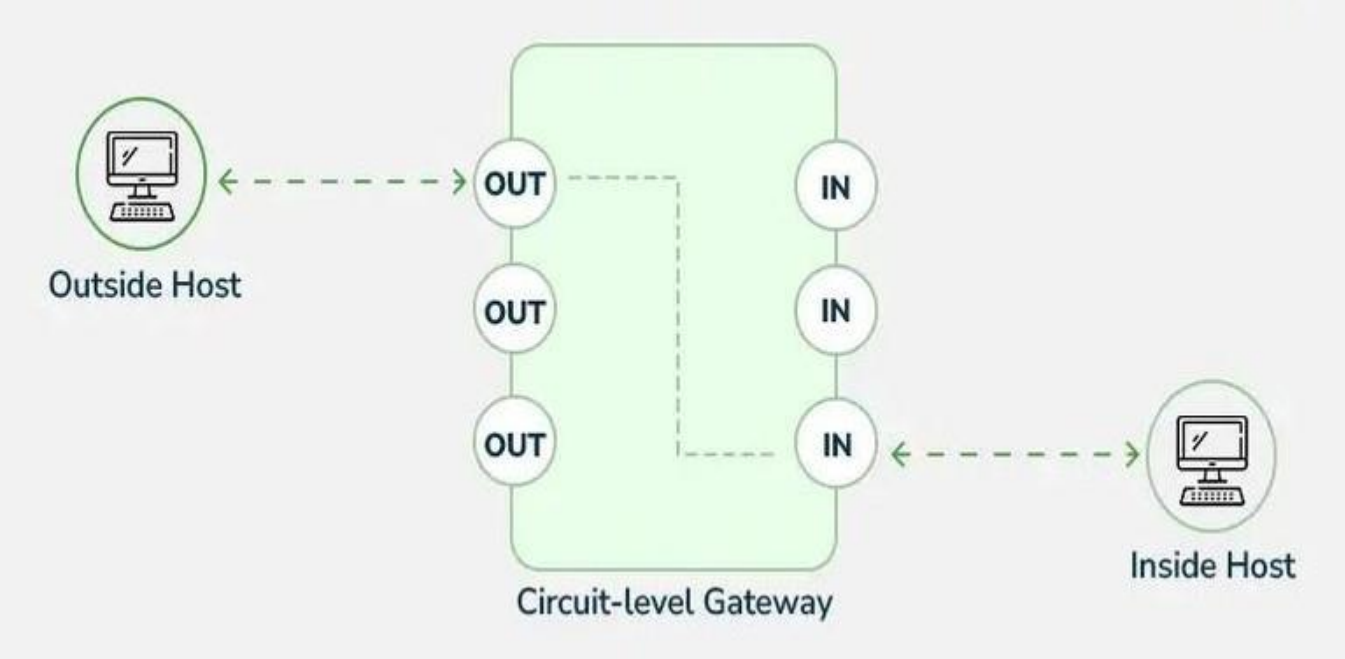
Read about Differences between Traditional Firewall and Next Generation Firewall



Next-generation Firewalls

Circuit-level Gateways

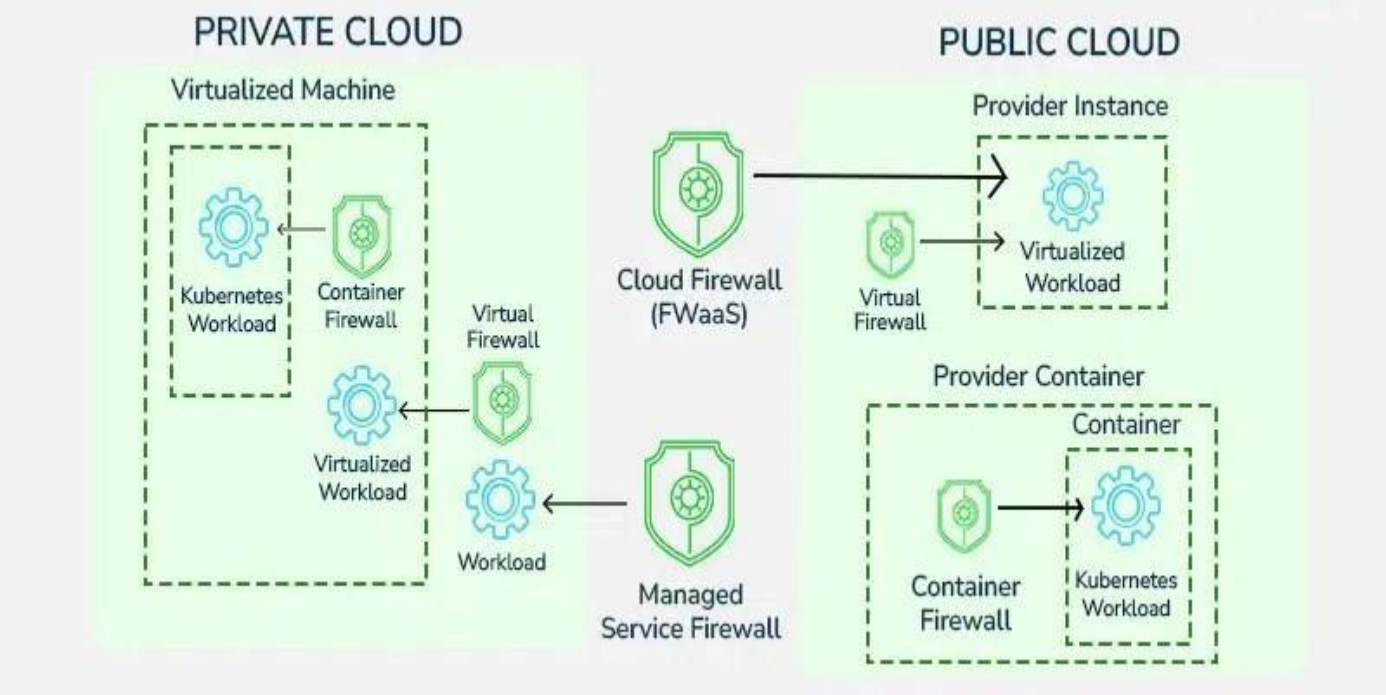
A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer.



Circuit-level Gateways

Software Firewall

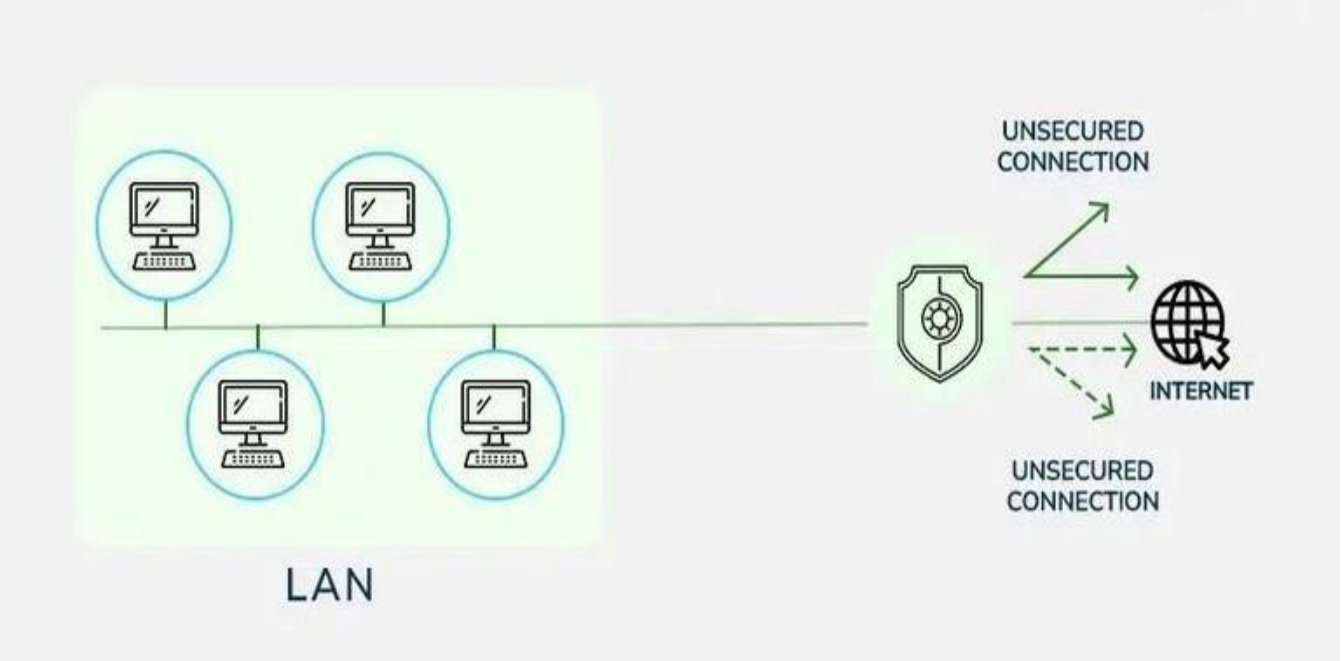
The software firewall is a type of computer software that runs on our computers. It protects our system from any external attacks such as unauthorized access, malicious attacks, etc. by notifying us about the danger that can occur if we open a particular mail or if we try to open a website that is not secure.



Software Firewall

Hardware Firewall

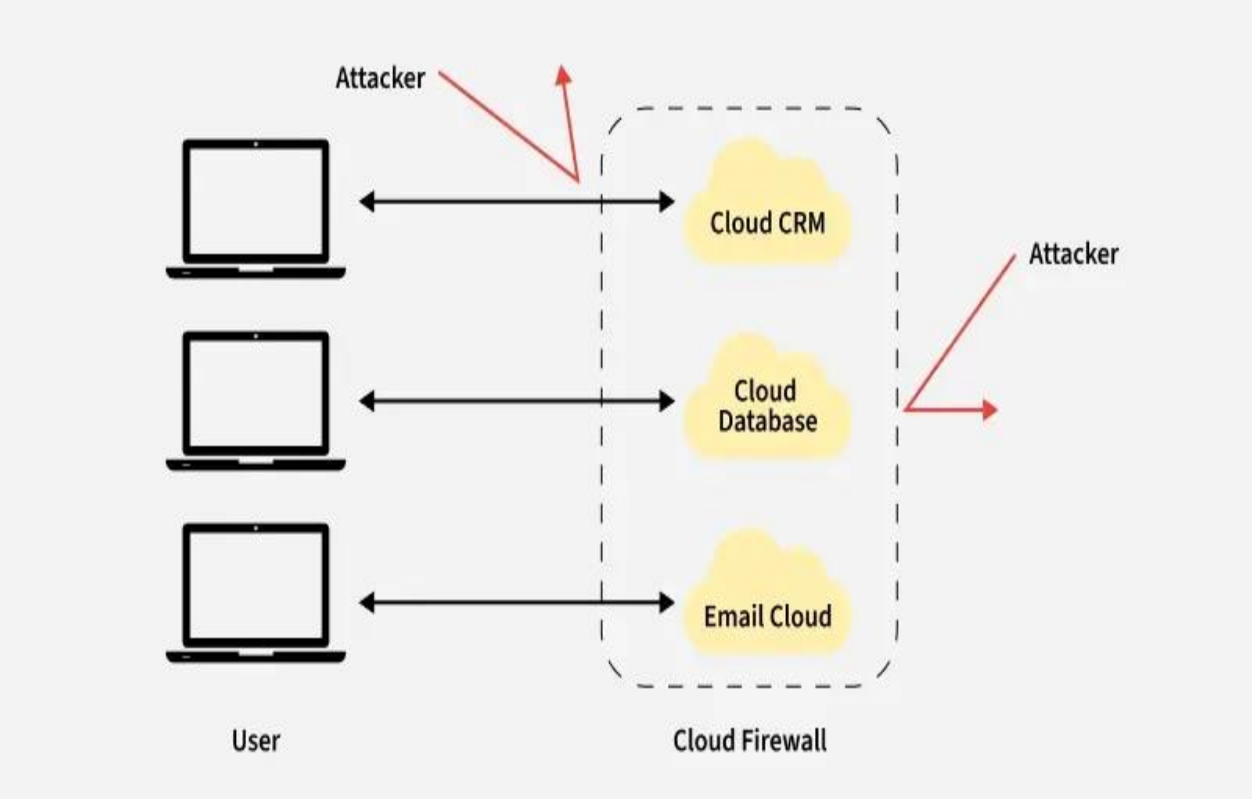
A hardware firewall is a physical appliance that is deployed to enforce a network boundary. All network links crossing this boundary pass-through this firewall, which enables it to perform an inspection of both inbound and outbound network traffic and enforce access controls and other security policies.



Hardware Firewall

Cloud Firewall

These are software-based, cloud-deployed network devices. This cloud-based firewall protects a private network from any unwanted access. Unlike traditional firewalls, a cloud firewall filters data at the cloud level.



Cloud Firewall

Hardware Firewall vs Software Firewall

A hardware firewall is a separate physical device placed between a network and its connected devices. It monitors and controls incoming and outgoing network traffic based on set security rules. In contrast, a software firewall runs on a server or virtual machine. It operates on a security-focused operating system, typically using standard hardware resources.

Both hardware and software firewalls are important for network security. The choice between them depends on specific needs and deployment contexts.

Read more about Difference between Hardware and Software 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.

Capabilities of Modern Firewalls

Since they were first created, firewalls have been a key part of network security. As technology has advanced, so have the capabilities and methods of deploying firewalls.

With these advancements, many different types of firewalls have emerged, making the options sometimes confusing. Different firewalls serve different purposes, and one way to differentiate them is by looking at what they protect, their form, where they are placed in the network, and how they filter data.

Organizations might need various types of firewalls to ensure effective network security. It's also important to remember that a single firewall product can include multiple types of firewall functions.

How to Prevent Network Traffic?

A network firewall applies a certain set of rules on the incoming and outgoing network traffic to examine whether they align with those rules or not.

- If it matches then the traffic will be allowed to pass through your network.
- If it doesn't match- then the firewall will block the traffic.

Which Firewall Architecture is best?

There is no as such best firewall architecture. The choice of firewall architecture for any network depends upon its use cases, requirements, budgets etc. In our network if we are having threat at Application layer then Application layer firewall can be best. If we are having threat at session layer then circuit level gateways can be best.

Read about Firewall Design Principles.

Advantages

- **Monitors Network Traffic** : A network firewall monitors and analyzes traffic by inspecting whether the traffic or packets passing through our network is safe for our network or not. By doing so, it keeps our network away from any malicious content that can harm our network.
- **Halt Hacking:** In a society where everyone is connected to technology, it becomes more important to keep firewalls in our network and use the internet safely.
- **Stops Viruses** : Viruses can come from anywhere, such as from an insecure website, from a spam message or any threat, so it becomes more important to have a strong

defense system (i.e. firewall in this case), a virus attack can easily shut off a whole network. In such a situation, a firewall plays a vital role.

- **Better Security:** If it is about monitoring and analyzing the network from time to time and establishing a malware-free, virus-free, spam-free environment so network firewall will provide better security to our network.

- **Increase Privacy:** By protecting the network and providing better security, we get a network that can be trusted.

Disadvantages

- **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** N**etwork:** 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.