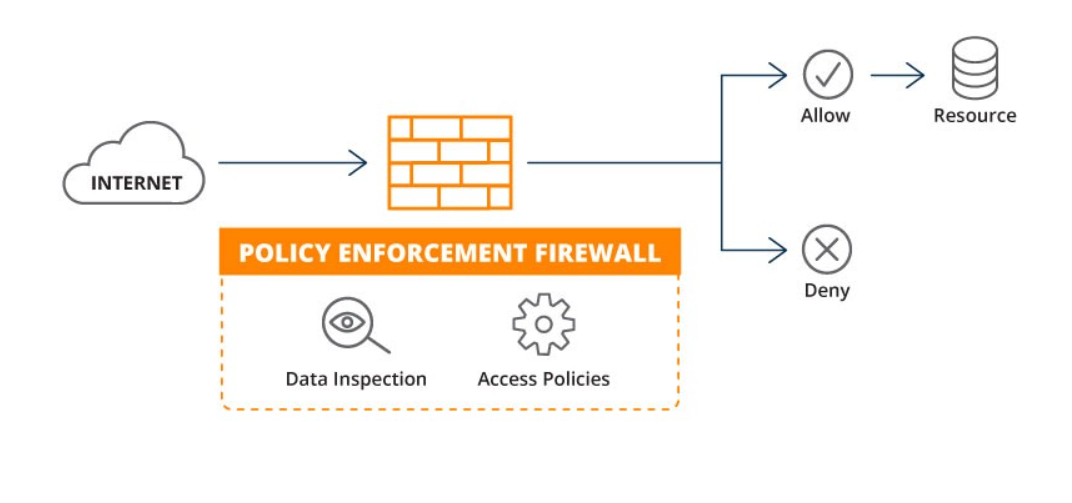
**FIREWALL**

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 it accepts, rejects or drops that specific traffic. Accept: allow the traffic, reject : block the traffic but reply with an “unreachable error”, Drop : block the traffic with no reply. A firewall establishes a barrier between secured internal networks and outside untrusted networks, such as the Internet.

Before firewalls, network security was performed through Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP addresses. But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the firewall was introduced. Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a firewall.



Types of **FIREWALL**:

* Web Application Firewall (WAF): Protects individual web applications, analyzing HTTP traffic and blocking malicious requests.
* Network Firewall: Protects the entire network infrastructure, examining all network traffic and filtering based on protocols, ports, and IP addresses.
* Cloud-based Firewall: Deployed in the cloud, provides scalable protection, offloading the burden from on-premises infrastructure.

**Web Application Firewall:**

A web application firewall is a type of firewall designated to protect web applications. It continuously inspects HTTP traffic to detect and block malicious traffic and web application attacks. This can include access violations, API manipulations, advanced HTTP DDoS attacks, cookie poisoning, and many more.

A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors. By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine’s identity by using an intermediary, a WAF is a type of reverse-proxy that protects the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe. Just as a proxy server acts as an intermediary to protect the identity of a client, a WAF operates in similar fashion but in the reverse—called a reverse proxy—acting as an intermediary that protects the web app server from a potentially malicious client.

Types of Web Application Firewalls:

1. Proxy-based WAF:

Analyzes and filters incoming HTTP traffic before it reaches the web server.

1. Packet Inspection WAF:

Examines packets at the network layer to detect and prevent attacks.

1. API Security WAF:

Specifically designed to protect APIs (Application Programming Interfaces) from security threats.

**Network Firewall:**

Network firewalls are designed to limit the flow of traffic between networks. They are often employed between a secure private network and a network with a different security posture, such as the Internet. A Network Firewall is a security device used to prevent or limit illegal access to private networks by using policies defining the only traffic allowed on the network; any other traffic seeking to connect is blocked.

Network firewalls are located at the network’s front line, serving as a communications link between internal and external networks. Network firewalls can also be placed throughout a secure private network to reduce the risk of cyberattacks and prevent unauthorized access to sensitive resources.

A network firewall is hardware or software that restricts and permits the flow of traffic between networks. Network firewalls help prevent cyberattacks by enforcing policies that block unauthorized traffic from accessing a secure network.

Network firewalls monitor and control incoming and outgoing network traffic based on predefined rules, safeguarding networks from unauthorized access and cyber threats. They prevent unauthorized access, protect against malicious activities, and enforce security policies. Network firewalls use packet filtering, stateful inspection, and other techniques to secure communication channels. They are essential for creating a barrier between trusted internal networks and untrusted external networks, such as the internet. Deployed at network perimeters, they play a critical role in securing data and systems.

The main types of network firewalls:

1. Packet Filtering Firewalls:

Make decisions based on attributes such as source and destination IP addresses, port numbers, and protocol types.

1. Stateful Inspection Firewalls:

Keep track of the state of active connections and make decisions based on the context of the traffic.

1. Proxy Firewalls (Application Layer Firewalls):

Operate at the application layer (Layer 7) of the OSI model.

1. Circuit-Level Gateways:

Monitor TCP handshakes to determine whether to permit or deny traffic.

1. Generation Firewalls (NGFW):

Combine traditional firewall capabilities with additional features such as intrusion prevention, deep packet inspection, and application-layer filtering.

1. Proxy Servers:

Handle requests and responses on behalf of clients, which can enhance security and privacy.

1. Hardware Firewalls:

Dedicated physical devices designed to provide network security.

1. Software Firewalls:

Run as software applications on general-purpose operating systems.

**Cloud-based Firewall:**

A cloud firewall is deployed in the cloud, forming these cloud Firewalls form a virtual barrier to prevent malicious network traffic in the cloud, they function as same as traditional firewalls, but the only difference is that the cloud firewall is hosted in a cloud platform.

Cloud firewalls act as a security product that acts as a shield and protects from unauthorized network traffic. This protection is provided to different cloud components like Cloud CRM, Cloud Database, and Email Cloud.

Cloud firewalls are designed in such a way that they can block cyberattacks directed against virtual cloud workspaces and provide 24/7 security to cloud components. We can assume these are the same as security guards that guard banks and these Virtual Workspaces .

Cloud firewalls safeguard cloud-based infrastructure by controlling incoming and outgoing traffic. They protect against unauthorized access, DDoS attacks, and secure data in the cloud. Cloud firewalls are scalable and adaptable to dynamic cloud environments, providing a crucial layer of defense for cloud-based applications and services. They help enforce security policies, monitor traffic, and contribute to compliance with regulatory standards. Integration with cloud platforms allows for centralized management and enhanced visibility across distributed cloud resources.

Types Of Cloud Firewall :

Cloud Firewalls are broadly distributed into two types namely :

1. Next-Generation Firewalls(NGFW) and
2. SaaS Firewalls

These are explained as following below.

1. Next-Generation Firewalls (NGFW) :

These are Cloud Firewall Service that are intended to be deployed in a data center with the aim of protecting the organization's servers in Infrastructure-As-a-Service or Platform-as-a-Service Model. In these models, the cloud firewall software is deployed and guards network traffic in cloud operations.

2. SaaS Firewalls :

These types of firewalls are configured in such a way that their main job is to secure the virtual network of the virtual space, just like traditional firewalls but the only difference being hosted in the cloud.