FIREWALL

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

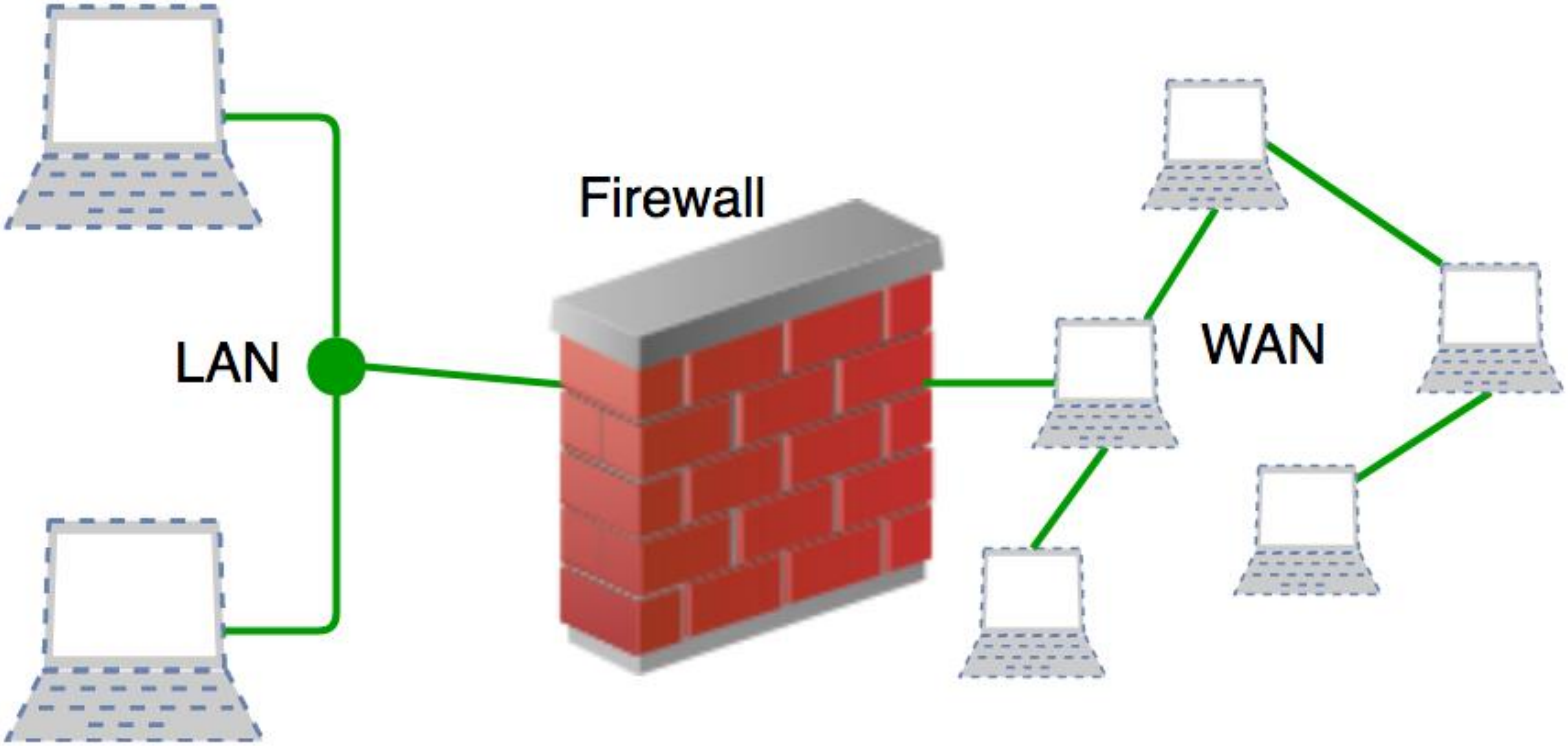
The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

What is 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 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 is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization. A firewall is essentially the wall that separates a private internal network from the open Internet at its very basic level.


Firewall
LAN
WAN

Working of Firewall

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.

Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming.
Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Functions of Firewall

- Every piece of data that enters or leaves a computer network must go via the firewall.
- If the data packets are safely routed via the firewall, all of the important data remains intact.

- A firewall logs each data packet that passes through it, enabling the user to keep track of all network activities.
- Since the data is stored safely inside the data packets, it cannot be altered.
- Every attempt for access to our operating system is examined by our firewall, which also blocks traffic from unidentified or undesired sources.

Advantages of using Firewall

- **Protection from unauthorized access:** Firewalls can be set up to restrict incoming traffic from particular IP addresses or networks, preventing hackers or other malicious actors from easily accessing a network or system. Protection from unwanted access.
- **Prevention of malware and other threats:** Malware and other threat prevention: Firewalls can be set up to block traffic linked to known malware or other security concerns, assisting in the defense against these kinds of attacks.
- **Control of network access:** By limiting access to specified individuals or groups for particular servers or applications, firewalls can be used to restrict access to particular network resources or services.
- **Monitoring of network activity:** Firewalls can be set up to record and keep track of all network activity.
- **Regulation compliance:** Many industries are bound by rules that demand the usage of firewalls or other security measures.
- **Network segmentation:** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Disadvantages of using Firewall

- **Complexity:** Setting up and keeping up a firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of users and devices.
- **Limited Visibility:** Firewalls may not be able to identify or stop security risks that operate at other levels, such as the application or endpoint level, because they can only observe and manage traffic at the network level.
- **False sense of security:** Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.
- **Limited adaptability:** Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.
- **Performance impact:** Network performance can be significantly impacted by firewalls, particularly if they are set up to analyze or manage a lot of traffic.
- **Limited scalability:** Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.
- **Limited VPN support:** Some firewalls might not allow complex VPN features like split tunneling, which could restrict the experience of a remote worker.
- **Cost:** Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.