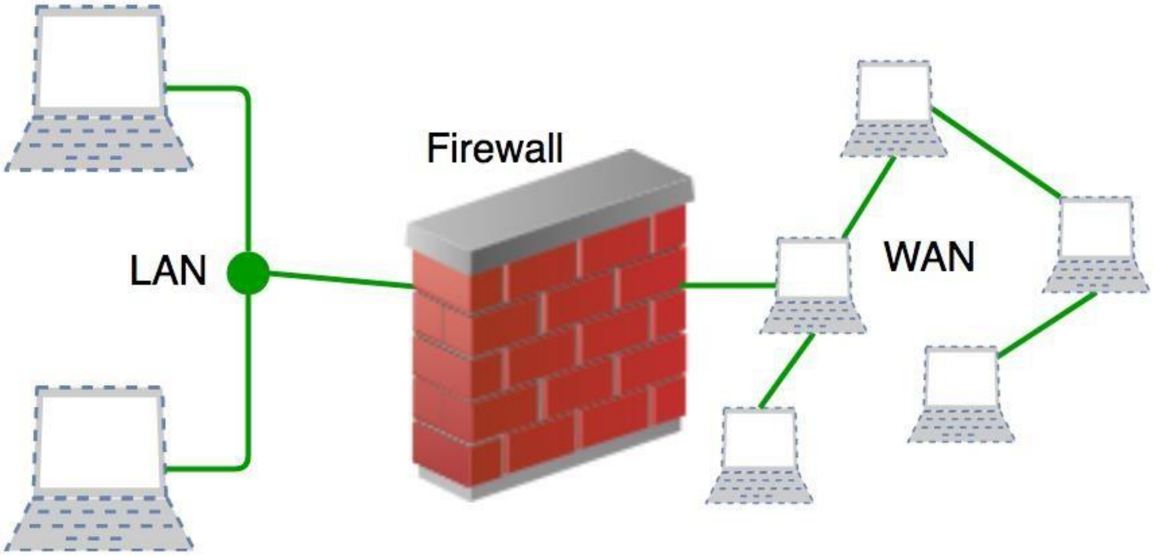
Introduction of Firewall in Computer Network

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 network, such as the Internet.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.
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.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. 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.

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.

Firewall Design Principles

A **Firewall** is a hardware or software to prevent a private computer or a network of computers from unauthorized access, it acts as a filter to avoid unauthorized users from accessing private computers and networks. It is a vital component of network security. It is the first line of defense for network security. It filters network packets and stops malware from entering the user’s computer or network by blocking access and preventing the user from being infected.

Characteristics of Firewall

1. **Physical Barrier:** A firewall does not allow any external traffic to enter a system or a network without its allowance. A firewall creates a choke point for all the external data trying to enter the system or network and hence can easily block access if needed.
2. **Multi-Purpose:** A firewall has many functions other than security purposes. It configures domain names and Internet Protocol (IP) addresses. It also acts as a network address translator. It can act as a

meter for internet usage.

3. **Flexible Security Policies:** Different local systems or networks need different security policies. A firewall can be modified according to the requirement of the user by changing its security policies.
4. **Security Platform:** It provides a platform from which any alert to the issue related to security or fixing issues can be accessed. All the queries related to security can be kept under check from one place in a system or network.
5. **Access Handler:** Determines which traffic needs to flow first according to priority or can change for a particular network or system. specific action requests may be initiated and allowed to flow through the firewall.

Need and Importance of Firewall Design Principles

1. **Different Requirements:** Every local network or system has its threats and requirements which needs different structure and devices. All this can only be identified while designing a firewall. Accessing the current security outline of a company can help to create a better firewall design.
2. **Outlining Policies:** Once a firewall is being designed, a system or network doesn't need to be secure. Some new threats can arise and if we have proper paperwork of policies then the security system can be modified again and the network will become more secure.
3. **Identifying Requirements:** While designing a firewall data related to threats, devices needed to be integrated, Missing resources, and updating security devices. All the information collected is combined to get the best results. Even if one of these things is misidentified leads to security issues.
4. **Setting Restrictions:** Every user has limitations to access different level of data or modify it and it needed to be identified and taken action accordingly. After retrieving and processing data, priority is set to people, devices, and applications.
5. **Identify Deployment Location:** Every firewall has its strengths and to get the most use out of it, we need to deploy each of them at the right place in a system or network. In the case of a packet filter firewall, it needs to be deployed at the edge of your network in between the internal network and web server to get the most out of it.

Firewall Design Principles

1. Developing Security Policy

Security policy is a very essential part of firewall design. Security policy is designed according to the requirement of the company or client to know which kind of traffic is allowed to pass. Without a proper security policy, it is impossible to restrict or allow a specific user or worker in a company network or anywhere else. A properly developed security policy also knows what to do in case of a security breach. Without it, there is an increase in risk as there will not be a proper implementation of security solutions.

2. Simple Solution Design

If the design of the solution is complex. then it will be difficult to implement it. If the solution is easy. then it will be easier to implement it. A simple design is easier to maintain. we can make upgrades in the simple design according to the new possible threats leaving it with an efficient but more simple structure. The problem that comes with complex designs is a configuration error that opens a path for external attacks.

3. Choosing the Right Device

Every network security device has its purpose and its way of implementation. if we use the wrong device for the wrong problem, the network becomes vulnerable. if the outdated device is used for a designing firewall, it exposes the network to risk and is almost useless. Firstly the designing part must be done then the product requirements must be found out, if the product is already available then it is tried to fit in a design that makes security weak.

4. Layered Defense

A network defense must be multiple-layered in the modern world because if the security is broken, the network will be exposed to external attacks. Multilayer security design can be set to deal with different levels of threat. It gives an edge to the security design and finally neutralizes the attack on the system.

5. Consider Internal Threats

While giving a lot of attention to safeguarding the network or device from external attacks. The security becomes weak in case of internal attacks and most of the attacks are done internally as it is easy to access and designed weakly. Different levels can be set in network security while designing internal security. Filtering can be added to keep track of the traffic moving from lowerlevel security to higher level.

Advantages of Firewall:

1. **Blocks infected files:** While surfing the internet we encounter many unknown threats. Any friendly-looking file might have malware in it. The firewall neutralizes this kind of threat by blocking file access to the system.
2. **Stop unwanted visitors:** A firewall does not allow a cracker to break into the system through a network. A strong firewall detects the threat and then stops the possible loophole that can be used to penetrate through security into the system.
3. **Safeguard the IP address:** A network-based firewall like an internet connection firewall(ICF). Keeps track of the internet activities done on a network or a system and keeps the IP address hidden so that it can not be used to access sensitive information against the user.
4. **Prevents Email spamming:** In this too many emails are sent to the same address leading to the server crashing. A good firewall blocks the spammer source and prevents the server from crashing.
5. **Stops Spyware:** If a bug is implanted in a network or system it tracks all the data flowing and later uses it for the wrong purpose. A firewall keeps track

of all the users accessing the system or network and if spyware is detected it disables it.

Limitations:

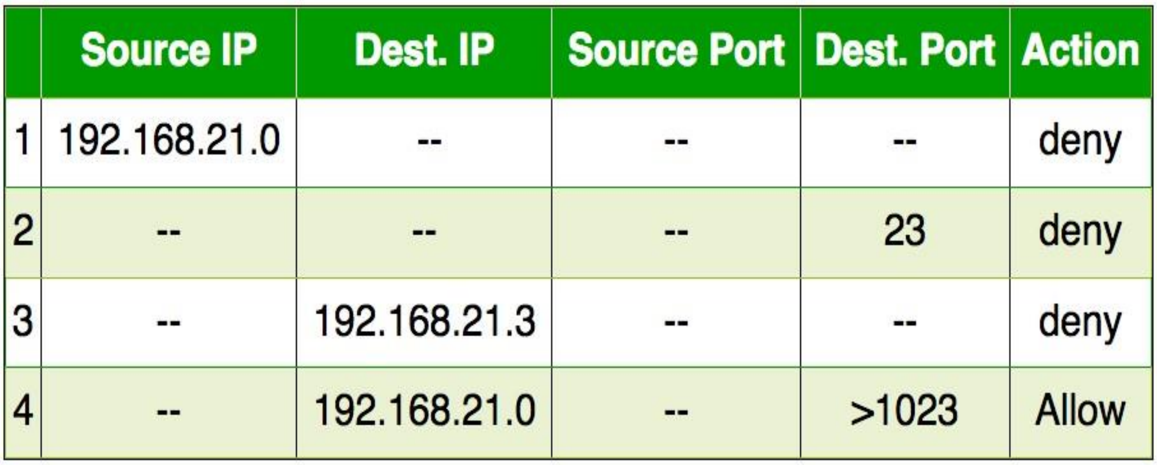
1. **Internal loose ends:** A firewall can not be deployed everywhere when it comes to internal attacks. Sometimes an attacker bypasses the firewall through a telephone lane that crosses paths with a data lane that carries the data packets or an employee who unwittingly cooperates with an external attacker.
2. **Infected Files:** In the modern world, we come across various kinds of files through emails or the internet. Most of the files are executable under the parameter of an operating system. It becomes impossible for the firewall to keep a track of all the files flowing through the system.
3. **Effective Cost:** As the requirements of a network or a system increase according to the level of threat increases. The cost of devices used to build the firewall increases. Even the maintenance cost of the firewall also increases. Making the overall cost of the firewall quite expensive.
4. **User Restriction:** Restrictions and rules implemented through a firewall make a network secure but they can make work less effective when it comes to a large organization or a company. Even making a slight change in data can require a permit from a person of higher authority making work slow. The overall productivity drops because of all of this.
5. **System Performance:** A software-based firewall consumes a lot of resources of a system. Using the RAM and consuming the power supply leaves very less resources for the rest of the functions or programs. The performance of a system can experience a drop. On the other hand hardware firewall does not affect the performance of a system much, because its very less dependent on the system resources.

Generation of Firewall

Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).
   Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:



	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

   1. Incoming packets from network 192.168.21.0 are blocked.
   2. Incoming packets destined for internal TELNET server (port 23) are blocked.
   3. Incoming packets destined for host 192.168.21.3 are blocked.
   4. All well-known services to the network 192.168.21.0 are allowed.

2. **Second Generation- Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.
3. **Third Generation- Application Layer Firewall :** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.
   Note: Application layer firewalls can also be used as Network Address Translator(NAT).
4. **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Types of Firewall

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

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 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. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.

Types of Network Firewall :

1. **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.

2. **Stateful Inspection Firewalls –**

   It is also a type of packet filtering which 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.

3. **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.

4. **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.

5. **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.

6. **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.

7. **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.

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

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.

How to prevent network?

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. This way, the network remains safe and secure.

Advantages of Network Firewall :

1. **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.

2. **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.

3. **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.

4. **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.

5. Increase privacy –

By protecting the network and providing better security, we get a network that can be trusted.

Disadvantages of Network Firewall :

1. **Cost –**
   Depending on the type of firewall, it can be costly, usually, the hardware firewalls are more costly than the software ones.

2. **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.

3. **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.

4. **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.