Introduction of Firewall in Computer Network

Last Updated : 28 Jun, 2024

In the world of computer networks, a firewall acts like a security guard. Its job is to watch over the flow of information between your computer or network and the internet. It's designed to block unauthorized access while allowing safe data to pass through.

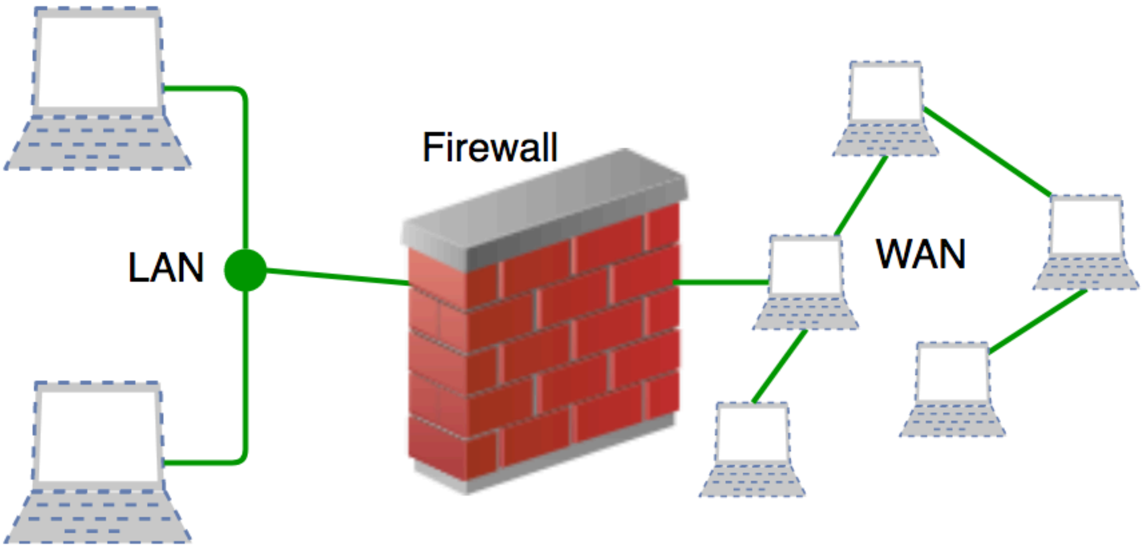
Essentially, a firewall helps keep your digital world safe from unwanted visitors and potential threats, making it an essential part of today's connected environment. It monitors both incoming and outgoing traffic using a predefined set of security to detect and prevent threats.

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.



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.

Working of Firewall

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 Human Resources 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 Human Resource 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.

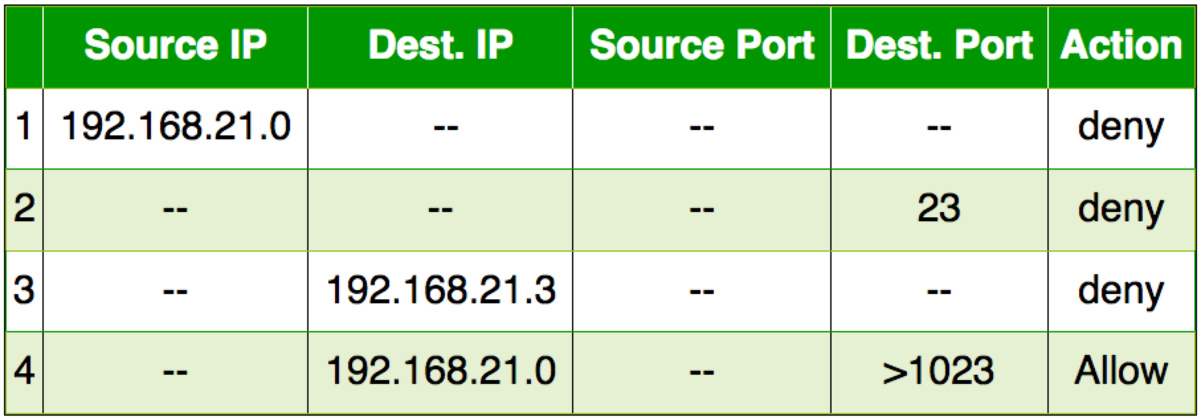
Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. 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.

Types of Firewall

Firewalls can be categorized based on their generation.

1. Packet Filtering Firewall

Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets 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 that decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be filtered according to the 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

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

2. 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. Software Firewall

A software firewall is any firewall that is set up locally or on a cloud server. When it comes to controlling the inflow and outflow of data packets and limiting the number of networks that can be linked to a single device, they may be the most advantageous. But the problem with software firewall is they are time-consuming.

4. Hardware Firewall

They also go by the name “firewalls based on physical appliances.” It guarantees that the malicious data is halted before it reaches the network endpoint that is in danger.

5. 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.

6. Next Generation Firewalls (NGFW)

NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

7. Proxy Service Firewall

This kind of firewall filters communications at the application layer, and protects the network. A proxy firewall acts as a gateway between two networks for a particular application.

8. Circuit Level Gateway Firewall

This works as the Sessions layer of the OSI Model’s . This allows for the simultaneous setup of two Transmission Control Protocol (TCP) connections. It can effortlessly allow data packets to flow without using quite a lot of computing power. These firewalls are ineffective because they do not inspect data packets; if malware is found in a data packet, they will permit it to pass provided that TCP connections are established properly.

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.

Who Invented Firewalls?

The firewall keeps changing and getting better because different people have been working on it since the late 1980s to the mid-90s. Each person added new parts and improved versions of the firewall before it became what we use in modern times. This means the firewall is always evolving to become more effective and secure.

Jeff Mogul, Paul Vixie, and Brian Reid

In the late 1980s, Mogul, Reid, and Vixie worked at Digital Equipment Corp (DEC) on packet-filtering technology. This tech became important for future firewalls. They started the idea of checking external connections before they reach computers on an internal network. Some people think this packet filter was the first firewall, but it was really a part of the technology that later became true firewall systems.

Kshitiji Nigam, William Cheswick, David Presotto, Steven Bellovin, and Janardan Sharma

In the late 1980s to early 1990s, researchers at AT&T Bell Labs worked on a new type of firewall called the circuit-level gateway. Unlike earlier methods, this firewall didn’t need to reauthorize connections for each data packet but instead vetted and allowed ongoing connections. From 1989 to 1990, Presotto, Sharma, and Nigam developed this technology, and in 1991, Cheswick and Bellovin continued to advance firewall technology based on their work.

Marcus Ranum

From 1991 to 1992, Ranum introduced security proxies at DEC, which became a crucial part of the first application-layer firewall product. Known as the Secure External Access Link (SEAL) product, it was based on earlier work by Reid, Vixie, and Mogul at DEC. SEAL marked the first commercially available firewall, pioneering the way for enhanced network security through application-level protection.

Gil Shwed and Nir Zuk

From 1993 to 1994, at Check Point, Gil Shwed and developer Nir Zuk made major contributions to creating the first widely-used and easy-to-use firewall product called Firewall-1. Gil Shwed pioneered stateful inspection technology, filing a U.S. patent in 1993. Following this, Nir Zuk developed a user-friendly graphical interface for Firewall-1 in 1994. These innovations were pivotal in making firewalls accessible and popular among businesses and homes, shaping their adoption for years to come.

Importance of Firewalls

So, what does a firewall do and why is it important? Without protection, 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.

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.

What Can Firewalls Protect 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.

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.

Conclusion

In conclusion, firewalls play a crucial role in safeguarding computers and networks. By monitoring and controlling incoming and outgoing data, they help prevent unauthorized access and protect against cyber threats. Using a firewall is a smart way to enhance security and ensure a safer online experience for users and organizations alike.

Important Question on Firewall

Question: A packet filtering firewall can [ISRO CS 2013]

(A) Deny certain users from accessing a service

(B) Block worms and viruses from entering the network

(C) Disallow some files from being accessed through FTP

(D) Block some hosts from accessing the network

Answer: Option (D)