Firewalls

To ensure the **confidentiality and integrity** of valuable information of a corporate network from the outside attacks, we must have some robust mechanism. This is where the **Firewall** comes into picture. It can be compared with a security guard standing at the entrance of a minister's home. He keeps an eye on everyone and physically checks every person who wishes to enter the house. It won't allow a person to enter if he/she is carrying a harmful object like a knife, gun etc. Similarly, even if the person doesn't possess any banned object but appears suspicious, the guard can still prevent that person's entry. **The firewall acts as a guard**. It guards a corporate network acting as a shield between the inside network and the outside world. All the traffic in either direction must pass through the firewall. It then decides whether the traffic is allowed to flow or not.

A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet.

Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons. The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

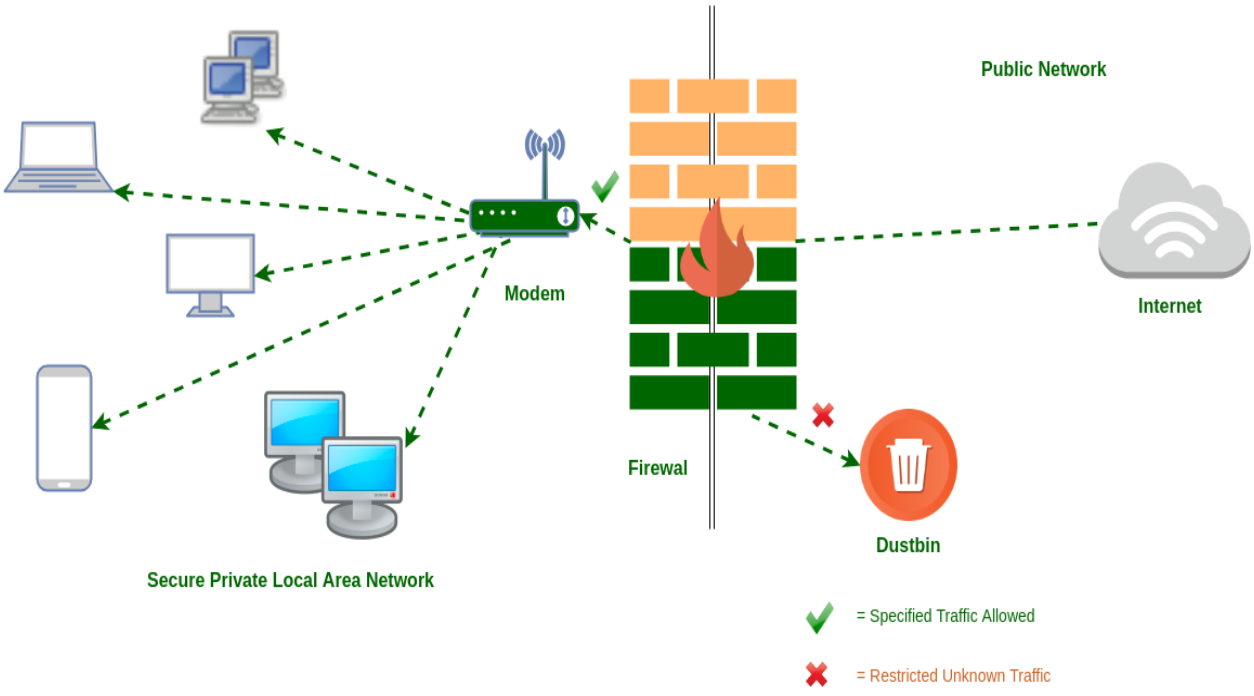

Figure 1 Firewall

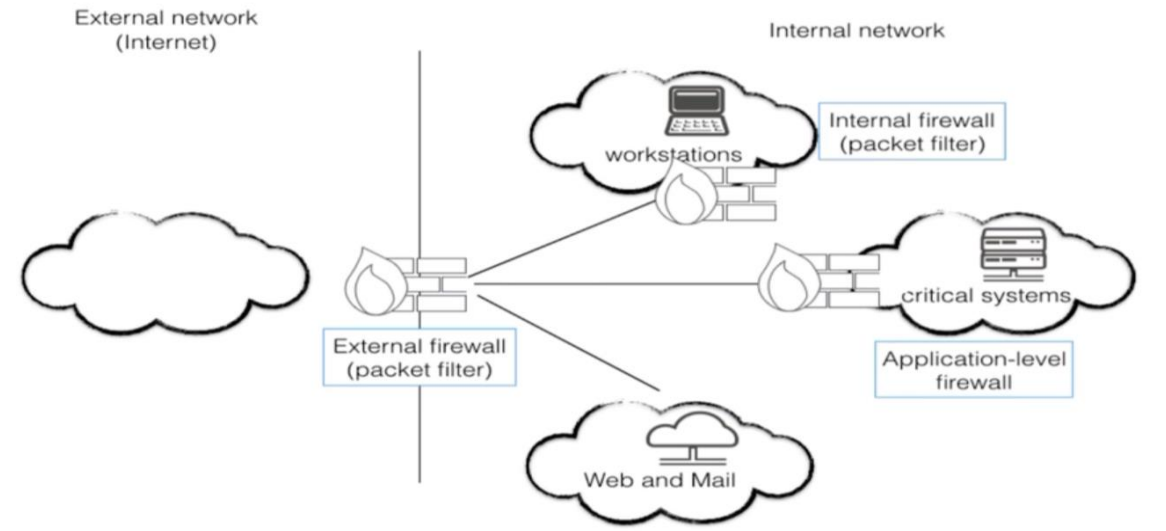

Figure 2 Placement of firewall

Types of Firewalls:

Figure given below illustrates the different types of Firewalls which is compared to OSI model

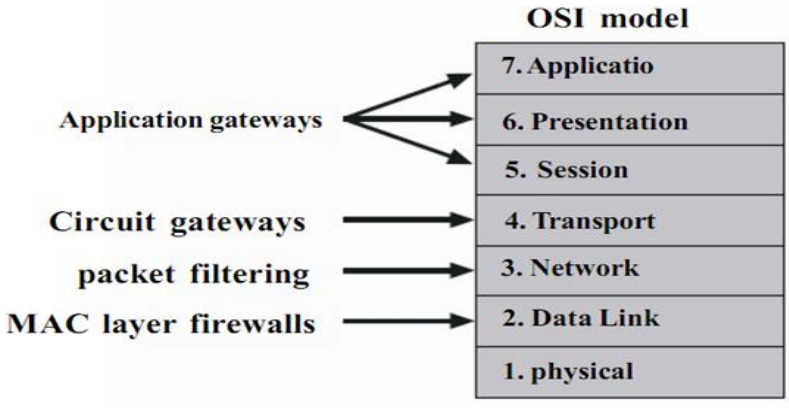

Figure 3 Types of firewalls

Firewalls can be further categorized as:

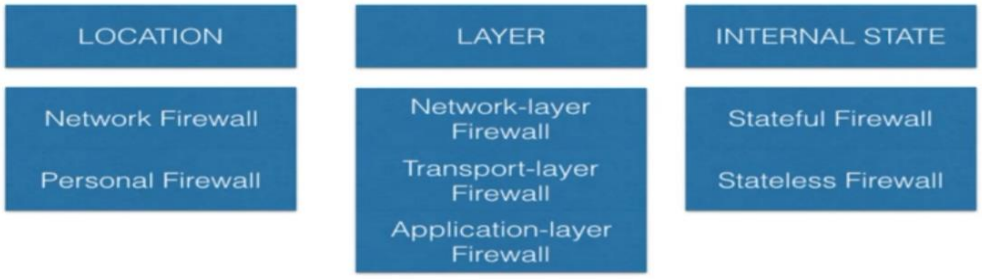

Figure 4 categories of firewalls

1. **Packet Filters –**
   It works in the **network layer** of the OSI Model. It is stateless filtering i.e. it applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
   For example, a rule could specify to block all incoming traffic from a certain IP address (as shown in figure below) or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to 'discard all packets' or to 'accept all packets'.

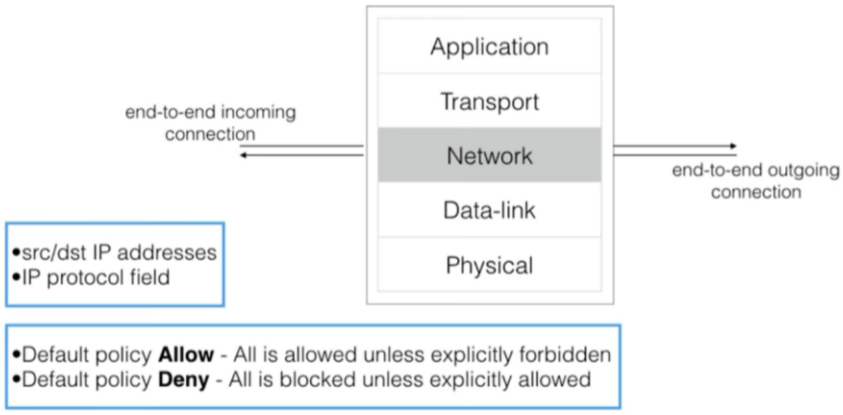

Figure 5 Concept of network level firewall

	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

Figure 6 Packet Filtering

Rules for packet filtering in the above figure: -

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.

Security threats to Packet Filters:

1. **IP address Spoofing:**
   In this kind of attack, an intruder from the outside tries to send a packet towards the

internal corporate network with the source IP address set equal to one of the IP address of internal users.

Prevention:

Firewall can defeat this attack if it discards all the packets that arrive at the incoming side of the firewall, with source IP equal to one of the internal IPs.

2. **Source Routing Attacks:**
   In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.
   Prevention:
   Firewall can defeat this attack if it discards all the packets that use the option of source routing as path addressing.
3. **Tiny Fragment Attacks:**
   Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet needs to be fragmented, so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attacker intentionally creates fragments of the original packet and send it to fool the firewall.
   Prevention:
   Firewall can defeat this attack if it discards all the packets which use the TCP protocol and is fragmented. *Dynamic Packet Filters* allow incoming TCP packets only if they are responses to the outgoing TCP packets.

2. **Application Gateways –**

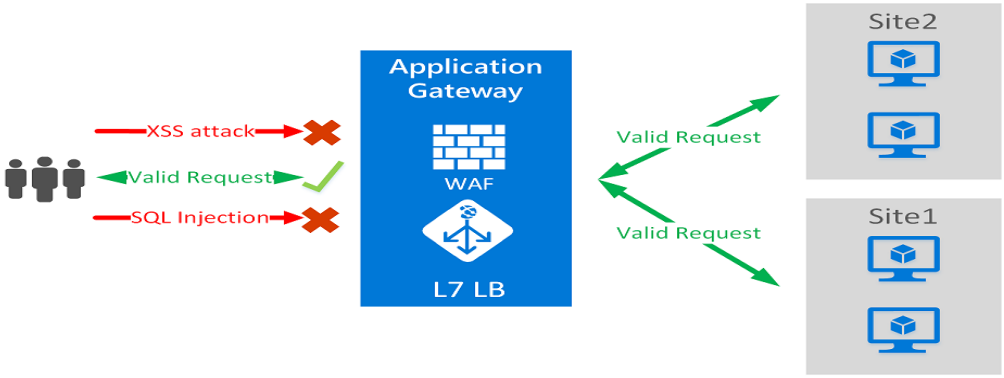

Figure 7 application Gateway firewall

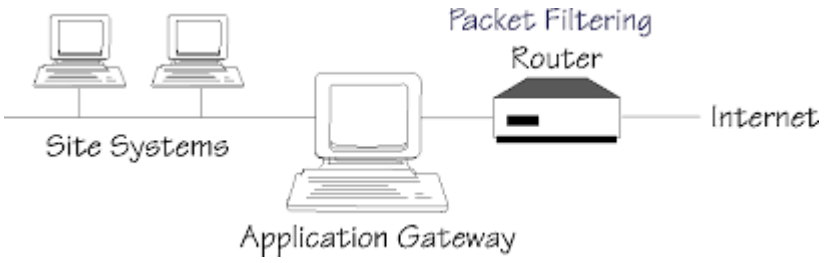

Figure 8 Placement of application Gateway

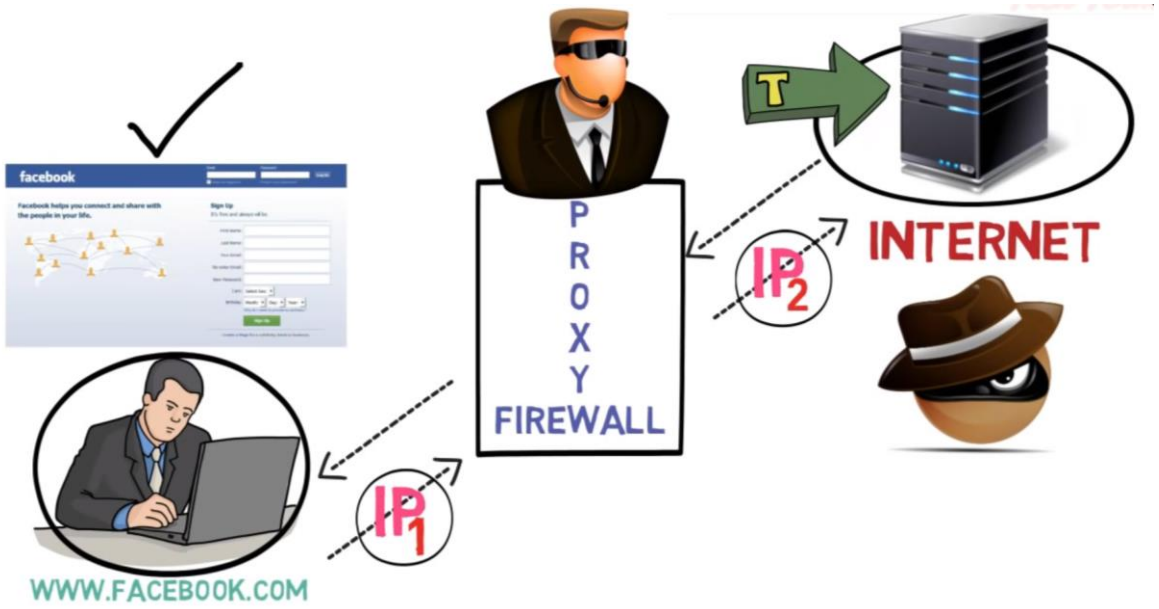

Figure 9 Application gateway/proxy firewall

The application level firewall is installed on a dedicated computer; also called as a proxy server. These servers can store the recently accessed pages in their cache and called as cache servers. As proxy server is placed in unsecured area of the network (for example DMZ), it is exposed to higher levels of risk from unreliable networks. Additional filtering routers can be implemented behind proxy server, further protecting internal systems. The disadvantage is they are characteristically restricted to a single application, as they work at application layer. It works as follows:

1. **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
2. **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
3. **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

3. **Stateful Inspection Firewalls –**

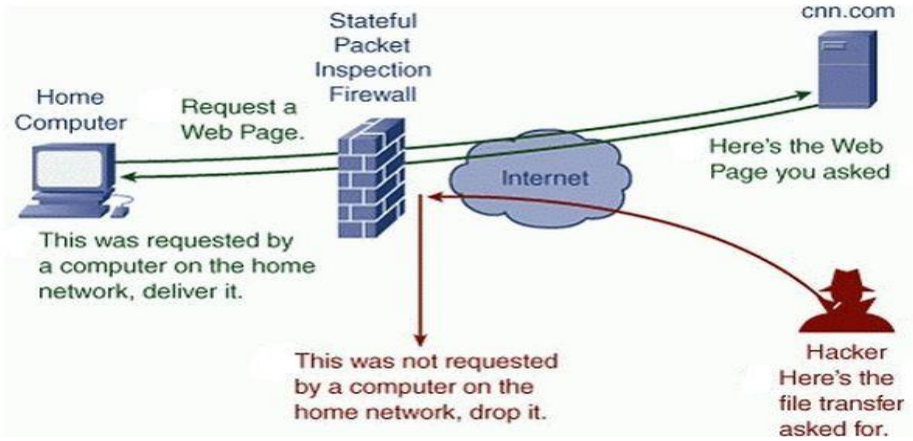

Figure 10 Stateful inspection

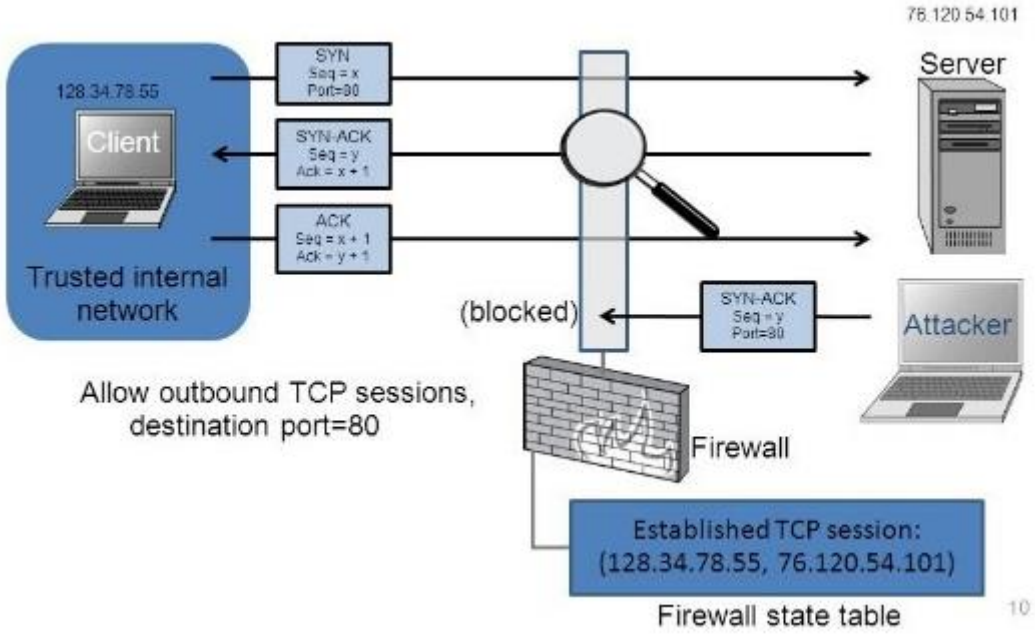

Figure 11 example of Stateful Inspection

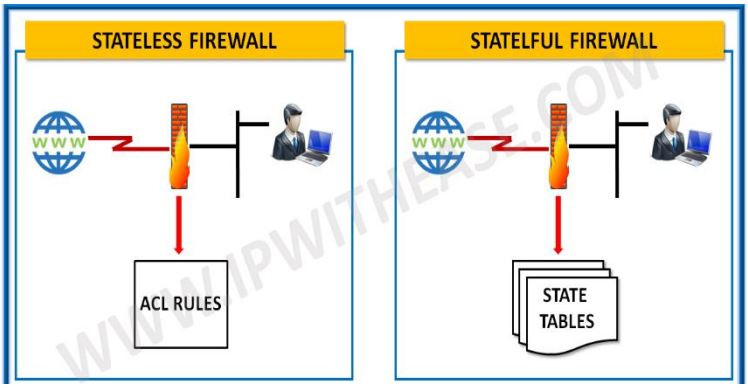

Figure 12 Difference between Packet Filtering (Stateless) and Stateful firewall

It is also known as ‘Dynamic Packet Filters’. It keeps track of the state of active connections and uses this information to decide which packets to allow through it, i.e., it adapts itself to the current exchange of information, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.

4. **Circuit-Level Gateways –**

It works at the "shim-layer" between the application layer and the transport layer of the TCP/IP stack. It is the advanced variation of Application Gateway.

A *circuit level gateway* only examines the address and port information contained in data it receives, not the content, an *application level gateway* is more in-depth. A firewall using this method runs proxy applications to view common types of data (like HTTP for web-pages, FTP, SMTP or POP3 for email, etc.) before it is allowed through the firewall.
It does not permit an end to end TCP connection. It acts as a virtual connection between the remote host and the internal users by creating a new TCP connection between itself and the remote host as show in figure below: -

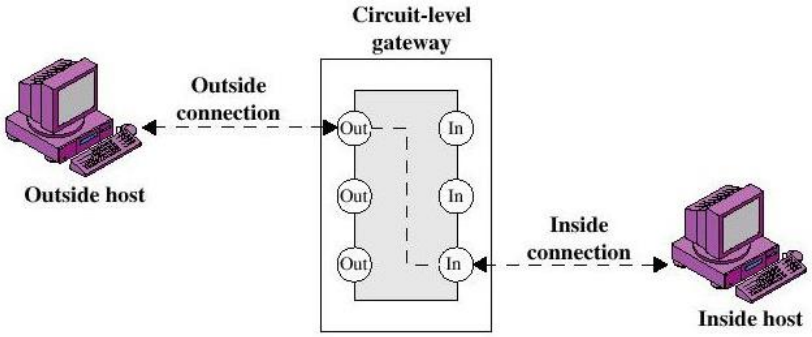

Figure 13 Circuit level gateways

It relays TCP segments from one connection to the other without examining the contents. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world. Its security function determines which connections will be allowed. It is used where internal users are trusted for all outbound services. But it has to combined with proxy firewall for inbound services.

As an example of how circuit level gateways work, say computer A is in a network protected by a circuit level gateway firewall, and wants to view a web page on computer B which is outside the firewall. Computer A sends the request for the web page to computer B, which is intercepted and recorded by the firewall before being passed on. Computer B receives the request, which as far as it is concerned came from the address of the firewall, and starts sending the web-page data back across the Internet. When it reaches the firewall, it is compared to computer A's request to see if the IP address and the port match up, then the data is either allowed or dropped.

5. **MAC Layer Firewalls**: - MAC layer firewalls which is designed to operate at media access control layer of OSI network model. This gives the ability to consider specific host computer's identity in the filtering decisions of it. The MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets which can be sent to each host; all other traffic is blocked.

6. **Hybrid Firewalls**: -
   Hybrid Firewalls combine elements of other types of firewalls; that is, elements of packet filtering and proxy services, or of packet filtering and circuit gateways. On the other hand, it may consist of 2 separate firewall devices; each is a separate firewall system, but is connected to work in tandem. Without replacing the existing firewalls completely, an organization can make a security improvement, from this approach.