Firewall

A firewall is a specialized version of a router, which guards a corporate network by standing between the network and the outside world. It decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further.

A firewall is a combination of hardware and software that isolates an organization's internal network from the Internet at large, allowing specific connections to pass and blocking others.

Firewalls can be hardware, software or a combination of both. They can be categorized as :

1. **Host – based**: They run on the host they are protecting and are usually software implementation.
2. **Network - based:** They protect the local network from external untrusted traffic and are usually hardware (or a hybrid) implementation.

We need a firewall as it can enforce security policy. It protects all your personal information. There is a focus for security decision as it stops hackers from accessing your computer. It limits your exposure as it blocks “pop-up” ads and certain cookies. It can log Internet activity effectively thus determining which programs can access the internet.

Some characteristics of a good firewall implementation:

1. All traffic from inside to outside and vice-versa must pass through the firewall. All access to the local network must be physically blocked and access only via the firewall must be permitted.
2. Only authorized traffic, as defined by the local security policy, should be allowed to pass through.
3. The firewall itself must be strong enough, to render attacks on it useless.

Types of firewalls

There are 2 types of firewalls:

i) Packet Filters **ii) Application Gateways**

i) **Packet Filters:** applies a set of rules to each packet and based on the outcomes, decides to either forward or discard the packets.

It performs the following functions:

i) It receives each packet as it arrives.

ii) It passes the packet through a set of rules, based on the contents of the IP and transports header fields of the packet. If there is a match with one of the set of rules, it decides whether to accept or reject it based on the rule.

iii) If there is no match with any rule, the packet filter takes the default action (Discard/Accept all packets).

However there exists some security issues using a packet filter:

IP address spoofing

An intruder outside the corporate network can attempt to send a packet towards the internal corporate network, with the source IP address set equal to one of the IP addresses of the internal users. This attack can be defeated by discarding all the packets that arrive at the incoming side of the firewall with the source address equal to one of the internal addresses.

Source routing attacks

An attacker can specify the route that a packet should take as it moves along the Internet. The attacker hopes that by specifying this option, the packet filter can be fooled to bypass its normal checks. Discarding all packets that use this option can thwart such an attack.

Tiny fragment attacks

Most of the devices send data in IP packets of a specific size through various physical networks. These networks have a pre-defined maximum frame size also called the **Maximum Transmission Unit (MTU)**. If the size of the IP packet is greater than the maximum size allowed by the network, then the IP packets needs to be fragmented. An attacker might exploit this characteristic of TCP/IP protocol suite and intentionally create and send the fragments of original IP packet.

The attacker feels that the packet filter can be fooled, so that after fragmentation, it checks only the first fragment and not the remaining fragments. This attack can be foiled by discarding all the packets where the protocol type is TCP and the packet is fragmented.

Dynamic/Stateful packet filter

It is a type of packet filter. It allows examination of packets based on the current state of the network. It adapts itself to the current exchange of information, unlike the normal packet filters, which have routing rules hard coded.

ii) Application Gateways:

Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source and is thus known as an “application-level gateway”. Also called as a **proxy server** as it acts like a proxy (deputy/substitute)

Limitations of firewall

I. Insider’s Intrusion

A firewall is designed to thwart only outside attacks. If an inside user attacks the internal network in some way, the firewall cannot prevent such an attack.

II. Direct Internet Traffic

A firewall must be configured very carefully. It is effective only if it is the only entry-exit point of an organization’s network. If, instead the firewall is one of the entry-exit points, a user can bypass the firewall and exchange information with the internet via the other entry-exit points. This can lead to attacks on the internal network through those points.

III. Virus Attacks

A firewall cannot protect the internal network from virus threats. This is because a firewall cannot be expected to scan every file or packet for possible virus contents. Therefore, a separate virus detection and removal mechanism is required for preventing virus attacks.