***What is a firewall?***

A firewall is like a mother who acts as a guard to all the enemies. So, a firewall is a fence between your computer or your internal network and outside world.

At the minimum level, the firewall will filter the incoming packets based on parameters such as packet size, the source of the packet, the protocol and the destination port. Without surprise, both Unix and Linux have built in firewalls in Operating System.

Every firewall has advantages and disadvantages and can be of many types. Classifying them into 4 basic categories:

1.The first most basic type is ***PACKET FILTERING FIREWALL*** also called SCREENING FIREWALL:

As the name suggests, it has everything to with the packet incoming. The packet is examined carefully and only the packets that match the criteria you set are allowed to enter. That is based on rule allow or deny. The criteria used can be packet size, protocol used, source IP address or anything you specify. It is very easy to configure and inexpensive.

DISADVANTAGE OF SCREENING FIREWALL is that:

A. They do not compare or examine the packet to previous packet as there is no record of packets therefore if 500 packets come from same host in short time then also it would not notice, leading to problem of a ping flood.

B. There is also no user authentication as it only looks as the header of packet and not at its content.

2.Moving on, we have ***STATEFUL PACKET INSPECTION(SPI***) that most home routers use.

It examines each packet then deny access or permit not only on examination of current packet but also with the data derived from previous packets in conversations. It is therefore less suspectable to ping floods.

MAJOR ADVANTAGES OF SPI ARE:

1. It will tell if the packet is a part of abnormally large streams of packets from a particular IP address.
2. It also looks at actual contents of packet, allowing some highly advanced filtering capabilities.
3. Tell packet has source IP address that appears to come from firewall clearly indicating IP spoofing in progress.

3. On third we have ***APPLICATION GATEWAY*** also known as APPLICATION PROXY:

It is a program that runs on a firewall. In this the client application and the server side application to which it is trying to connect are examined rather than looking at the port and the protocol the packet is using.

There is a proxy server with which the client negotiates in order to gain access to destination service. That is, the proxy server establishes connection with destination behind the firewall and acts on behalf of the client thus protecting and hiding individual computer on network behind firewall.

In simple words, this type of firewall creates two connections:

One connection is between the client and the proxy and another is between the proxy and the destination.

Each supported client program requires a unique program to accept client application data. This sort of firewall allows individual user authentication which makes them quite effective at blocking unwanted data.

Pointing out the DISADVANTAGES:

1. The process of authenticating client application uses lots of memory and CPU time.
2. It is suspectable to various flooding attacks because:
3. Additional time to negotiate authenticating a request since both user and the client needs to be authenticated.
4. Also, because once the connection is made, packets are not checked.

However, the second vulnerability is somewhat mitigated because of user login method is secure (passwords, encrypted transmission, etc)

4.The last category of our is ***CIRCUIT LEVEL GATEWAY***:

This is similar to application gateways but it more secure. Here, authenticating the user is the first step since logon ID and passwords are checked. Each individual either by username or IP address has to verified first. After connection is established, the firewall passes bytes between the systems. There is a virtual circuit between the client and the proxy server that makes it more secure than other firewalls.

Internet requests go through this circuit to proxy server and then the proxy delivers those requests to internet after changing the IP addresses and only the external users can see IP of the proxy.

***----------------THANK YOU--------------***