Firewall

It is a network security device for monitoring traffic and considered as the first line of defence. It works on certain security rules and blocks the traffic from untrusted sources based on these rules.

It inspects each data packet transferred through and mitigates threat.

Why Firewall is required?

There are multiple types of attacks which can be used to access unprotected computers.Firewall prevents against these attacks:

Remote login
When someone is able to connect to your computer control it remotely have access to system files.

Application backdoors
Some programs contain bugs that provide a hidden access,that provides some level of control of the program.

SMTP session hijack
It is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send junk e-mail.

Denial of service

The hacker sends a request to the server to connect to it.When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request.

By repeating this cycle , a hacker causes the server to eventually crash.

Viruses

A virus is a small program that can copy itself to other computers. This way it can spread quickly from one system to the next.

Working of a firewall

To understand working of firewall , one should know about few terms.

Packet: Packet is a unit of data formatted in such a manner that it can be easily carried along the network path.

Firewall Rule: It consists of various firewall services, which specify the type of traffic and the ports that can be used.
eg : For example, a rule called Web browsing has a service called HTTP,which uses the TCP and port number 80.

Protocol: protocol is the pre-defined way in which someone wants to use a service.

It acts as a **virtual borderline** between the incoming traffic and the outgoing traffic.It scans all the “packets” passing through it.

Firewall then takes appropriate actions based on some predefined security rules to distinguish between valid and malicious packets.

Rules can be set on the basis of information contained inside each packet.
Various **types of firewall protocol** are :

IP(Internet Protocol)
Delivery system for information over Internet.

TCP(Transmission Control Protocol)
Used to break and rebuild information that travels over Internet

HTTP(Hyper Text Transfer Protocol)
Used for Web pages

FTP(File Transfer Protocol)
Used for downloading and uploading files

UDP(User Datagram Protocol)
Used for information that requires no response

ICMP(Internet Control Message Protocol)
Used by a router to exchange information with other routers

SMTP(Simple Mail Transport Protocol)
Used to send text-based information or E-mail

Telnet
Used to perform commands on a computer located remotely

Types of firewall

There are various types of firewall which are as follows:

1. Network Level

As the name suggests, it works at the network level and inspects packet headers .
When a packet passes through the firewall ,following things are checked :

- a) Source Address
- b) Destination Addresss
- c) Protocol
- d) Port Number

The packet is dropped if it does not comply with the set of firewall rules. It mainly works on network layer of OSI model.
It examines each packet independently.
Although it is quite effective,but because of its characteristic of processing packets in isolation, it is vulnerable to IP Spoofing.

2. Circuit Level

It works as a session layer of Open Systems Interconnection Model(OSI Model). It provides connection security to User Datagram Protocol (UDP) and Transmission Control Protocol(TCP).
It determines the legitimacy of the message by the method of handshake.

3. Application Level

It is application specific and blocks the packets based on the content & not on the basis of IP Addresses.
It examines the payload of a packet and distinguishes it among the valid or malicious request.

4. Stateful Multilayer

It is combination of above three types . They filter packets at the network layer,determine legitimacy at application layer and provide direct connection between the host and the client.