Firewall is a hardware or software device designed to permit or deny the access of data through a computer network in order to protect the resources of a private network from users and other networks. Eg : if an organization with intranet allows its workers only to have access to its wider internet then there will a need of installing a firewall in order to prevent outsiders from accessing its own private data resources and for controlling its own users who have access to its network.

A firewall also prevents confidential information being sent out from your computer without permission. This could be passwords, bank details or other personal information

A firewall is a layer of security that designates what traffic is allowed and isn't allowed to enter your computer. Generally, they let good traffic through, while keeping hackers out. For better security and protection it is necessary to have a firewall up-to-date along with the updated antivirus and Operating system .

The main function of firewall is to protect computers on the “inside” network from computers on the “outside”, usually the **Internet**.The main characteristics of the firewall protection include the following:

Different protection levels based on the location of the computer

When your PC connects to a network, the firewall applies a security level in accordance with the type of network. If you want to change the security level assigned initially, you can do this at any time through the firewall settings.

Protection of wireless networks (Wi-Fi)

This blocks intrusion attempts launched through wireless networks (Wi-Fi). When an intruder attempts to access, a pop-up warning is displayed that allows you to immediately block the attack.

Access to the network and the Internet

It specifies which programs installed on your computer can access the network or the Internet.

Protection against intruders

It prevents hacker attacks that try to access your computer to carry out certain actions.

Blocks

The firewall can block the access of the programs that you specify should not be able to access the local network or the Internet. It also blocks access from other computers that try to connect to programs installed on your computer.

Definition of rules

This defines rules that you can use to specify which connections you want to allow and the ports and zones through which the connection can be established.

There are two type of firewalls;-

Hardware Firewalls.

Software Firewalls

Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

Hardware firewalls can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.

Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.