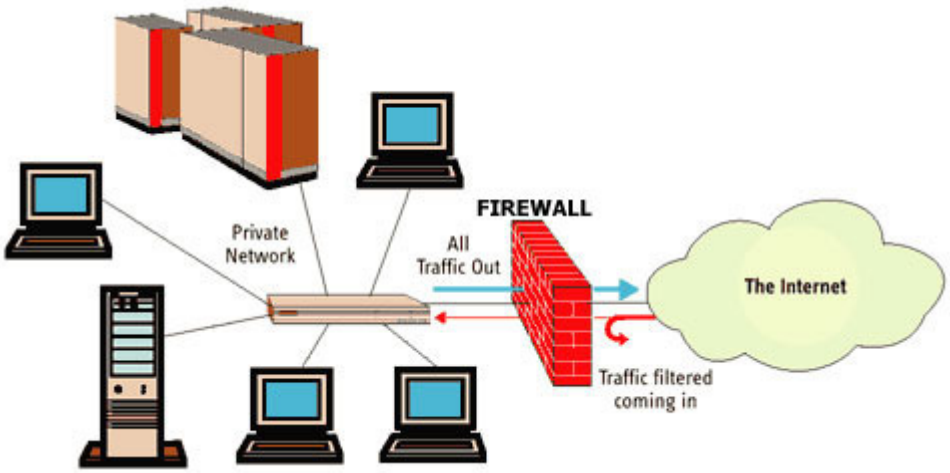
Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet (the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.



A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

- **Accept :** allow the traffic.
- **Reject :** block the traffic but reply with an “unreachable error”.
- **Drop :** block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

How Firewall Works:-

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.
From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing

traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.
Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Types of Firewall:-

Firewalls are generally of two types:-

1.*Host-based*

2. *Network-based.*

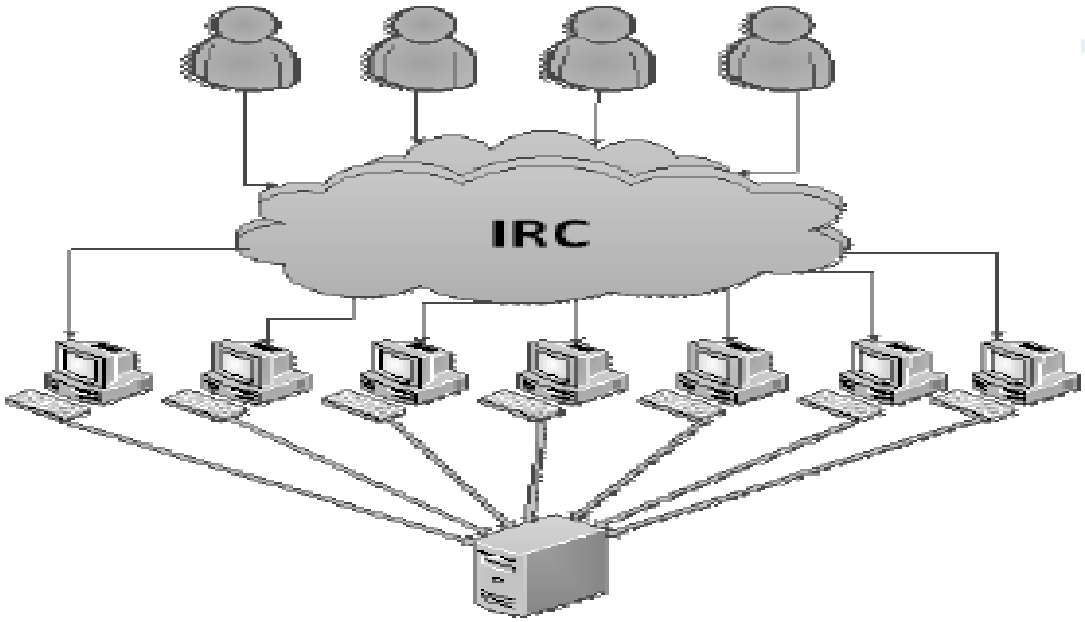
1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Internet Relay Chat(IRC) or Chating

IRC stands for "Internet Relay Chat." IRC is a service that allows people to chat with each other online. It operates on a client/server model where individuals use a client program to connect to an IRC server. Popular IRC clients include mIRC for Windows and Textual for OS X. Several web-based clients are also available, including KiwiIRC and Mibbit.
In order to join an IRC conversation, we must choose a username and a channel. Our username, also called a handle, can be whatever we want. It may include letters and numbers, but not spaces. A channel is a specific chat group within an IRC network where users can talk to each other. Some networks publish lists of available channels, while others require we to manually enter channel names in order to join them. Channels always begin with a hashtag followed by a name that represents their intended chat topic, such as "#teenchat," "#politics," or "#sports". Some IRC

channels require a password while others are open to the public.
When we join a channel, the chat window will begin displayig messages people are typing. we can join the conversation by typing our own messages. While channel members can type whatever they want, popular channels are often moderated. That means human operators or automated bots may kick people out of the channel and even ban users who post offensive remarks or spam the channel with repeated messages.
While IRC was designed as a public chat service, it supports other features such as private messaging and file transfers. For example, we can use an IRC command (which typically begins with a forward slash "/") to request a private chat session with another user. Then we can use another IRC command to send the user a file from your local system.



NOTE: IRC was a popular way for users to connect online before social media became prevalent in the early 2000s. Today, many people still use IRC, but social media sites and apps are much more popular.