How FIREWALL helps to secure PC?

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

At their most basic, firewalls work like a filter between your computer/network and the Internet. You can program what you want to get out and what you want to get in. Everything else is not allowed. There are several different methods firewalls use to filter out information, and some are used in combination. These methods work at different layers of a network, which determines how specific the filtering options can be.

How do Firewalls protect Businesses

- Large corporations often have very complex firewalls in place to protect their extensive networks.
- On the outbound side, firewalls can be configured to prevent employees from sending certain types of emails or transmitting sensitive data outside of the network.
- On the inbound side, firewalls can be programmed to prevent access to certain websites (like social networking sites).
- Additionally, firewalls can prevent outside computers from accessing computers inside the network.
- A company might choose to designate a single computer on the network for file sharing and all other computers could be restricted.
- There is no limit to the variety of configurations that are possible when using firewalls.
- Extensive configurations typically need to be handle and maintained by highly trained IT specialists, however.

The need of Firewalls for Personal Use

For home use, firewalls work much more simply. The main goal of a personal firewall is to protect your personal computer and private network from malicious mischief. Malware, malicious software, is the primary threat to your home computer. Viruses are often the first type of malware that comes to mind. A virus can be transmitted to your computer through email or over the Internet and can quickly cause a lot of damage to your files.

Other malware includes Trojan horse programs and spyware. These malicious programs are usually designed to acquire your personal information for the purposes of identity theft of some kind. There are two ways a firewall can prevent this from happening. It can allow all traffic to pass through except data that meets a predetermined set of criteria, or it can prohibit all traffic unless it meets a predetermined set of criteria.

How does FIREWALL works?

It is important to note that successfully receiving incoming TCP packets requires the receiver to send outgoing acknowledgment packets back to the sender. The combination of the control information in the incoming and outgoing packets can be used to determine the connection state (e.g. new, established, related) of between the sender and receiver.

network traffic that traverses a firewall is matched against rules to determine if it should be allowed through or not. network traffic is matched against a list of firewall rules in a sequence, or chain, from first to last. More specifically, once a rule is matched, the associated action is applied to the network traffic in question.

It is typical for a chain of firewall rules to not explicitly cover every possible condition. For this reason, firewall chains must always have a default policy specified, which consists only of an action (accept, reject, or drop). Suppose the default policy for the example chain above was set to drop. If any computer outside of your office attempted to establish an SSH connection to the server, the traffic would be dropped because it does not match the conditions of any rules. If the default policy were set to accept, anyone, except your own non-technical employees, would be able to establish a connection to any open service on your server. This would be an example of a very poorly configured firewall because it only keeps a subset of your employees out.

As network traffic, from the perspective of a server, can be either incoming or outgoing, a firewall maintains a distinct set of rules for either case. Traffic that originates elsewhere, incoming traffic, is treated differently than outgoing traffic that the server sends. It is typical for a server to allow most outgoing traffic because the server is usually, to itself, trustworthy. Still, the outgoing rule set can be used to prevent unwanted communication in the case that a server is compromised by an attacker or a malicious executable.

In order to maximize the security benefits of a firewall, you should identify all of the ways you want other systems to interact with your server, create rules that explicitly allow them, then drop all other traffic. Keep in mind that the appropriate outgoing rules must be in place so that a server will allow itself to send outgoing acknowledgements to any appropriate incoming connections. Also, as a server typically needs to initiate its own outgoing traffic for various reasons—for example, downloading updates or connecting to a database—it is important to include those cases in your outgoing rule set as well.