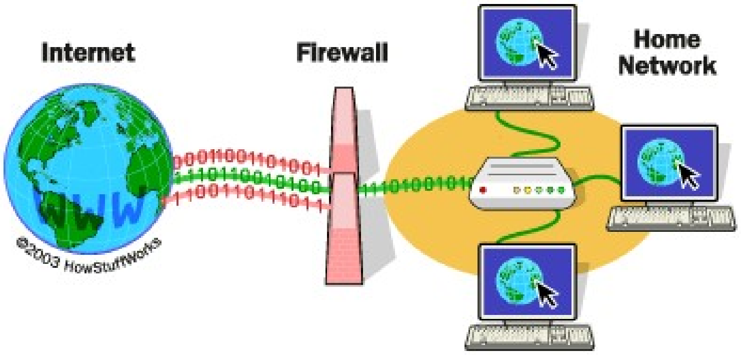
Name: Omprakash Gupta

Roll: 171210041

Network_Programming_Assignment

Q.1: How Firewall helps to secure PC?

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.



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.

Additionally, *firewalls* can prevent outside computers from accessing computers inside the network. 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.

Advantages of Using a Firewall:

A Company network or a home computer will have number of advantages when using a firewall.They are more cost effective than securing each computer in the corporate network since there are often only one or a few firewall systems to concentrate on.There are some firewalls which are able to detect viruses, Trojans, worms and spyware etc.

Disadvantages of Using a Firewall

Even if a firewall helps in keeping the network safe from intruders, but if a firewall is not used properly it would give a false impression to you that the network is safe. The main disadvantage of a firewall is that it cannot protect the network from attacks from the inside.

They often cannot protect against an insider attack.

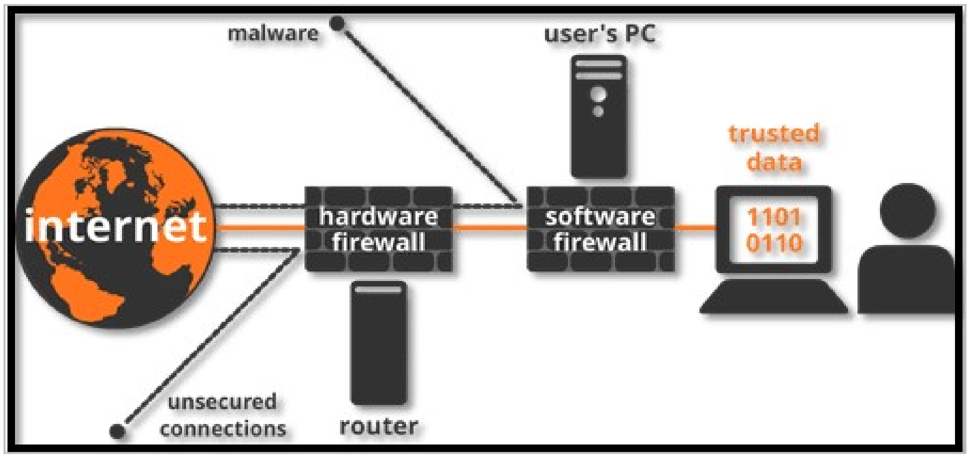
Firewalls cannot protect a network or pc from viruses, Trojans, worms and spyware which spread through flash drives, potable hard disk and floppy etc.

They may restrict authorized users from accessing valuable services.

They do not protect against backdoor attacks.

They cannot protect the network if someone uses a broadband modem to access the internet.

Software Vs Hardware Firewall



Hardware firewall protects the entire network of an organization using it from external threats only. In case, if an employee of the organization is connected to the network via his personal laptop then he can’t avail the protection.

On the other hand, software firewall provision host-based security as the software is installed on each of the device connected to the network, thereby protecting the system from external as well as internal threats. It is most widely used by mobile users to digitally protect their handset from malicious attacks.

Firewall Categories

Based on the filtering of traffic there are many categories of the firewall, some are explained below:

Packet Filtering Firewall:

It is a kind of router which is having the ability to filter the few of the substance of the data packets. When using packet-filtering, the rules are classified on the firewall. These rules find out from the packets which traffic is permitted and which are not

Statefull Firewall:

It is also called as dynamic packet filtering, it inspects the status of active connections and uses that data to find out which of the packets should be permitted through the firewall and which are not.

The firewall inspects the packet down to the application layer. By tracing the session data like IP address and port number of the data packet it can provide a much strong security to the network.

It also inspects both incoming and outgoing traffic thus hackers found it difficult to interfere in the network using this firewall.

Proxy Firewall:

These are also known as application gateway firewalls. The stateful firewall is unable to protect the system from HTTP based attacks. Therefore proxy firewall is introduced in the market.

It includes the features of stateful inspection plus having the capability of closely analyzing application layer protocols.

Thus it can monitor traffic from HTTP and FTP and find out the possibility of attacks. Thus firewall behaves as a proxy means client initiates a connection with the firewall and the firewall in return initiates a solo link with the server on the client's side.

Q.2: If you are a system admin, what precautions/steps you will take to secure it?

The growth and usage of the internet has brought several benefits and ease in the day to day communication for both personal and organizational purposes. But on the other hand, it came out with security issues, hacking problems and other kind of unwanted interference.In order to cope up with these issues, a device which should have the capability of protecting the PC's and the company's assets from these issues is needed.

Precautions/steps:

- In small networks, we can make each of our network device secured by ensuring that all the software patches are installed, unneeded services are disabled, and security software are properly installed within it.

- The centralized security system is a solution to provide a secure network to big networks.

- Most of the attack on the network occurs from inside the system so to deal with it Firewall system should be capable of securing from internal threats also.

- Malicious cyber attacks are the most common type of internal attack. The system administrator or any employee from the IT department who is having access to the network system can plant some virus to steal crucial network information or to damage the networking system.

- Any of the host computers of the internal network of the organization can download malicious internet content with lack of knowledge of downloading the virus also with it. Thus the host systems should have limited access to the internet. All unnecessary browsing should be blocked.

- Information leakage from any of the host PC through pen drives, hard disk or CD-ROM is also a network threat to the system. This can lead to crucial database leakage of the organization to the outer world or competitors. This can be controlled by disabling the USB ports of host device so that they can't take out any data from the system.

- The firewall can be hardware or software which by following a certain set of rules will guard our networking system from the virus and other types of malicious attacks. So, we can use this to secure our PC.

- Revoke the users credentials across all servers network wide. This should include keys as well as passwords.
- If they are aware of root details that do not require being logged in as another user first then these details should be changed as well.
- Other account details such as those relating to server hosting should also be changed as well, as there is always a chance they have a copy of them or can remember them.
- If your network is closed of but you allow traffic from certain IP address such as admin home address in it is important to ensure that those are removed from access as well.
- If possible monitor for attempted logins by the leavers username this would give you an alert as the potential that they are trying to gain access to your systems.

There are many ways to secure or PCs using software and Hardware and by making limited allowance of PCs by putting various restrictions.