**How does fire wall helps to protect computer?**

A firewall is a system designed to prevent unauthorised access to or from a private computer network. A firewall indirectly improves the performance of your computer by not allowing Trojans, viruses and other forms of malware onto the computer. Firewalls use one or a combination of the following three methods to control traffic flowing in and out of the network:

* **Packet filtering**
* **Proxy service**
* **Stateful inspection**

There are two types of firewall. They are:

1. Hardware firewall
2. Software firewall

Hardware firewalls are built into network devices such as routers and can protect every single machine on a network and require little configuration to work effectively. They use packet filtering techniques to examine the header of a packet, determining his source and destination and then, comparing the data to a set of predefined rules, they decide whether to drop the packet or forward it to the next step or to its destination.

Software firewalls are the most popular network protection method for home users. They usually come as stand-alone applications or as part of a complete antivirus protection software, such as the one BullGuard provides. Besides providing protection for inbound and outbound traffic, a software firewall can also protect against Trojan or Worm applications and allows various options of control over its functions and features.

Selecting a precise firewall is critical in building up a secure networking system. Firewall provisions the security apparatus for allowing and restricting traffic, authentication, address translation and content security. It ensures 365 \*24\*7 protection of network from hackers. It is a onetime investment for any organization and only needs timely updates to function properly. By deploying firewall there is no need of any panic in case of network attacks.

A firewall system can work on five layers of OSI-ISO reference model. But most of them run at only four layers i.e. data-link layer, network layer, transport layer and application layers.The number of layers envelops by a firewall is dependent upon the type of firewall used. Greater will be a count of layers it covers more efficient will be the firewall solution to deal with all kind of security concerns.

**Types of threats and the solution of it:**

**#1)** 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.

The solution to deal with it is to monitor the activities of every employee and guard the internal network by using multiple layers of the password to each of the servers. The system can also be protected by giving access of system to least of the employees as possible.

**#2)** 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.

**#3)** 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.

**If you were a system admin, what steps you will take to secure it?**

As a system administrator, I will perform flowing tasks to secure:

Monitoring,

Deployment and

Troubleshooting

Monitoring means that I should have my list of all systems under my responsibility to check their availability, performance, backup...etc. Many available tools are available for this purpose both commercial and free tools.

Deployment is when I respond to a business need or to a request from other department within my organization to deploy a new system.

Finally, troubleshooting, this is my respond to emergencies once they happen. As a system administrator my core responsibility is to keep my organization's business up and running by making sure that my systems are available upon my organizations rules.The first line of security defense is to control access to your system. You can control and monitor system access by doing the following:

* Maintaining physical site security
* Maintaining login control
* Restricting access to data in files
* Maintaining network control
* Monitoring system usage
* Setting the path variable correctly
* Securing files
* Installing a firewall
* Reporting security problems

I will set up a firewall system to protect the resources in my network from outside access. A firewallsystem is a secure host that acts as a barrier between your internal network and outside networks.

The firewall has two functions. The firewall acts as a gateway that passes data between the networks and it acts as a barrier that blocks the free passage of data to and from the network. The firewall requires a user on the internal network to log in to the firewall system to access hosts on remote networks. Similarly, a user on an outside network must log in to the firewall system before being granted access to a host on the internal network.

In addition, all electronic mail that is sent from the internal network is sent to the firewall system for transfer to a host on an external network. The firewall system receives all incoming electronic mail, and distributes it to the hosts on the internal network.