

National Institute of Technology, Delhi



ASSIGNMENT

CSB-351

(Network Programming)

Submitted To:

Dr. Ravi Kumar Arya
**Dept. Of Electronics &
Communication Engineering**
NIT, Delhi

Submitted By:

Vimlesh Kumar
171210059
Computer Science & Engineering
Date : 10/03/2020

Q1- How firewall help to secure PC?**Answer :-****Firewall Introduction**

Firewall is a software for network security system which behaves like a filter between computer and external network (Internet). It monitors and controls incoming and outgoing traffic based on the some determined rules and protocols. Firewall does not allow each and every information to pass through it. Firewall makes computer system secure by filtering out threats and malwares to the information security. Basically a firewall provides protection to our computer systems. It also prevents the confidential information such as Passwords, Bank Details and many more private information to sent out without your permission.

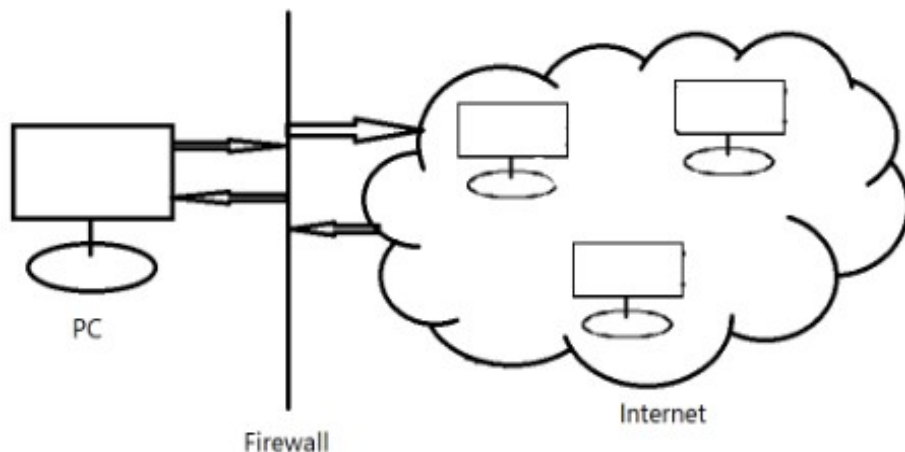


Diagram - showing PC exchange information with internet through firewall
(sketch drawn by me in Paint software)



How a firewall works

There are several different methods which are used by firewall to filter out information which can cause security issue to the system. Basically, a firewall examines all data trying to pass through it to determine whether to forward it to its destination or not. This is done according to the some set of rules and protocols which are set by users by means of programming. Protocols and rules are implemented to establishing which sorts of traffic to be allowed and which traffic not.

One of the most important elements of a firewall is its access control features, which distinguish between good and bad traffic. Modern firewall can filter traffic based on the many packet attributes like source IP Address, destination IP Address, source Port, destination Port, services like WWW (World Wide Web) or FTP. They can filter based on the protocols, TTL (Time-To-Live) values, netblock of originator, domain name of the source and some other attributes like this.

Methods to control traffic flowing in and out of the network :-

Packet Filtering

In this method packets are analyzed against a set of traffic. Packets which satisfy all rules and protocols are sent to the requesting address and rest packets are discarded.

Proxy Service

In this method firewall retrieve information from internet and then send information to the requesting system.

Stateful Inspection

This method does not examine the each packets instead it compares a key part of packet to a trusted database information. Information which is going outside



of firewall is monitored for specific characteristics which are compared with incoming information. If it match information is allow otherwise discarded.

Firewall Configuration

Firewalls are customizable. i.e we can add or remove some filters based on several different conditions. We can configure the firewall according to our needs and requirements. For example we can block a IP Address if it is trying to access many file at a time, we can block the exchange of information if it contain some specific string or characters. Any type of configuration errors should be avoided. Admin must examine whole process after every time when firewall configuration updates done. Some common and most used protocols which we can set for firewall filters are IP (Internet Protocol), TCP (Transmission Control Protocol), HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), UDP (User Datagram Protocol), SMTP (Simple Mail Transport Protocol).



Q2- If you are a system admin, what precautions or steps you will take to secure it?

Answer :-

Computer security is one of the most important aspect to take in consideration when working with outside internet network in today's digital world. It is computer system admin's responsibility to protect computer from all outside threats, malwares and attacks. There are many softwares and applications are availbale on market which are made to make our PC more secure. As a system admin we can take many actions and precautions in practice to make our PC secure.

Some common and important security practices :

Use Standard Account

Operating System provides a certain level of rights and privileges depending upon the type of account you have. We should use a Standard Administrator user account to prevent all other users from making changes to our computer important settings, or installing new software and apps.

Password-Protection

We can make our system more secure by using a strong password for accessing business networks, programs and specific applications. We should use strong password for user and admin accounts. We should use password at every where we can not compromise with our security.

Using Firewalls

We can use some best firewalls or similar internal network controls which monitor and control incoming and outgoing traffic between our computer and outside internet.

Using Security-softwares

There are many Security softwares are available in the market which protect our PC system from outside world. Security softwares include Anti-virus, Anti-



spyware, and Anti-malware software. These software block intentionally damaging viruses from taking hold of our Computer devices.

Vulnerability Testing

Everyone know that the prevention is better than cure. As s system administrator we should regularly scan our PC for different vulnerabilities and take action against them if found. There are many tools available which scan PC system and report security problems if found.

Keeping Our PC Updated

We should keep our PC system up to date to its latest version. All operating system are keep on updating regularly. Some of these updates can be important security patches which should not be compromised to install. Check your computer system regularly for new updates and install them.

Safe Browsing

There are many dodgy or affected sites on internet which are intentionally created to harm your system or infect your computer with virus. As a system admin it is our responsibility to be careful while browsing on internet ans don't click on suspicious links. We may block these sites in firewall.

Backup and Recovery

There are times when our system or PC get crash or fail due to some reasons like system hacking, threats, virus or malware attacks. A good computer system Administrator always have a reliable backup and recovery procedure. We can use built-in tools for backup and recovery or use some dedicated software only build for these purpose.

As today's information infrastructure and internet become more complex and larger it is more challenging for system administrators to keep system secure. System admins should keep on updating their knowledge about systems and networks which they are managing. As a system administrator we should be more cautious towards security and always follow some good habits and practices while doing different tasks.

END