1. What is a Firewall and how does it protect your PC?

Sol: Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. A widely accepted alternative or at least complement to host-based security services is the firewall. The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed. The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function. The firewall, then, provides an additional layer of defence, insulating the internal systems from external networks.

The International Computer Security Association (ICSA)classifies firewalls into three categories: Packet filter firewalls, Application-level proxy servers, and stateful packet inspection firewalls.

Packet Filter Firewall

Every computer on a network has an address commonly referred to as an IP address. A packet filter firewall checks the address of incoming traffic and turns away anything that doesn't match the list of trusted addresses. The packet filter firewall uses rules to deny access according to information located in each packet such as: the TCP/IP port number, source/destination IP address, or data type. Restrictions can be as tight or as loose as you want. An ordinary router on a network may be able to screen traffic by address, but hackers have a little trick called *source IP spoofing* that makes data appear to come from a trusted source, even from your own network. Unfortunately, packet filter firewalls are prone to IP spoofing and are also arduous and confusing to configure. And any mistake in configuration could potentially leave you wide open to attack.

Application-Level Proxy Server

An application-level proxy server examines the application used for each individual IP packet to verify its authenticity. Traffic from each application such as HTTP for Web, FTP for file transfers, and SMTP/POP3 for e-mail—typically requires the installation and configuration of a different application proxy. Proxy servers often require administrators to reconfigure their network settings and applications (i.e., Web browsers) to support the proxy, and this can be a labour -intensive process.

Stateful Packet Inspection Firewall

This is the latest generation in firewall technology. Stateful packet inspection is considered by Internet experts to be the most advanced and secure firewall technology because it examines all parts of the IP packet to determine whether to accept or reject the requested communication. The firewall keeps track of all requests for information that originate from your network. Then it scans each incoming communication to see if it was requested, and rejects anything that wasn't. Requested data proceeds to the next level of screening. The screening software determines the state of each packet of data, hence the term *stateful packet inspection.*

2. If you are a system admin how do you protect your PC?

Sol: Following the below steps helps in securing our PC (mostly):

1. Protection against Viruses

Ensure the computer has the most recent Anti-virus software installed. Make sure the computer’s operating system updates are installed. Exercise Caution when opening your e-mail attachments.

2. Protect against spyware

Spyware is software that collects personal information without your knowledge or permission. You might be the target of spyware if you download music or videos from file-sharing programs, free games from untrusted sites or other software from an unknown source. Many free tools are available online to eliminate spyware.

3. Secure your wireless network

If you use a wireless network in your home, take precautions to secure it against hackers. Encrypting wireless communications is the first step.

4. Manage your system and browser to protect your privacy

Hackers are constantly trying to find flaws or holes in operating systems and browsers. To protect your computer and the information on it, ensure your security settings in your system and browser are set at medium or higher.

5. Remember that public hot spots may not be secure

Avoid accessing or sending sensitive personal information over a public wireless network.

6. Choose Unique Passwords

Choose passwords that are a minimum of eight characters long and include a combination of letters, numbers, and special characters. Use a unique password for each login ID. Disable the web browser "auto complete" function of your login IDs or passwords to prevent others using your computer from having instant access. Keep your passwords confidential. Change your password.

7. Online User Tips

Do not open unsolicited or unfamiliar email – spam often contains damaging software.

Do not click on links within unsolicited email – the link may take you to a counterfeit website that will solicit your personal and financial information, this scam is known as ‘*Phishing*’.

References:

1.https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work

2.https://computer.howstuffworks.com/firewall1.htm

3.https://www.comodo.com/resources/home/how-firewalls-work.php

4.https://www.lifewire.com/what-is-a-firewall-2487290

5.https://www.theguardian.com/technology/askjack/2015/jan/15/how-can-i-make-my-pc-completely-secure

6.https://www.windowscentral.com/best-ways-keep-your-pc-secure