	RV College of Engineering® **Department of Computer Science and Engineering** **CIE - II**		
Course & Code	**INTRODUCTION TO CYBER SECURITY (22EM106)**		**Semester: I**
Date : FEB 2023	**Duration:**120 minutes	**Max.Marks**:(10+50)=60 Marks	**Staff :** MH
USN :	**Name :**		**Section : Physics cycle**

Scheme and Solution

Sl.no	**PART - A**	**Marks**
1	Brute-Force Attack	1
2	Firewalls and Antivirus	1
3	2-step verification system	1
4	Eavesdropping	1
5	Steganography	1
6	Social Engineering	1
7	BotNet	1
8	Impersonation	1
9	Adware	1
10	Shoulder Surfing	1

Sl.no.	**PART - B**	**Marks**
1.a	• Bot- computing • A botnet (short for “robot network”) is **a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.”** • Each individual machine under the control of the bot-herder is known as a bot. • Automated program for doing some particular task	6

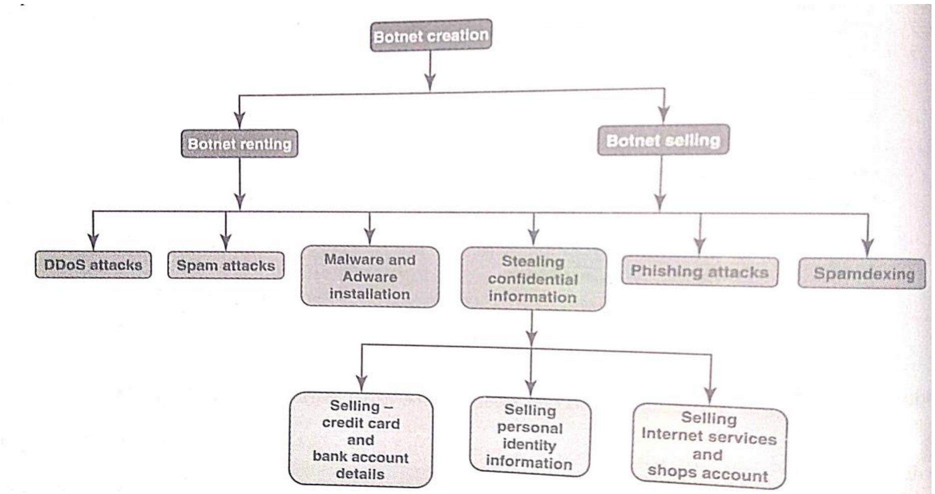
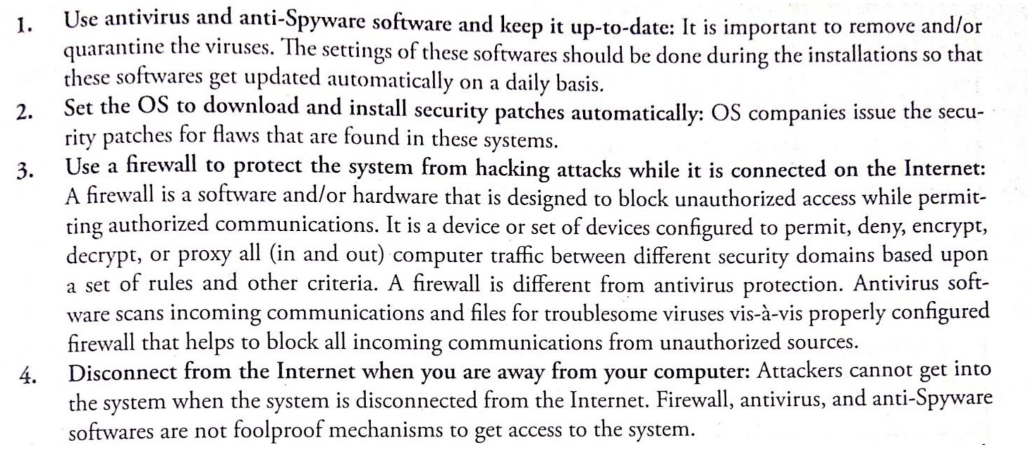
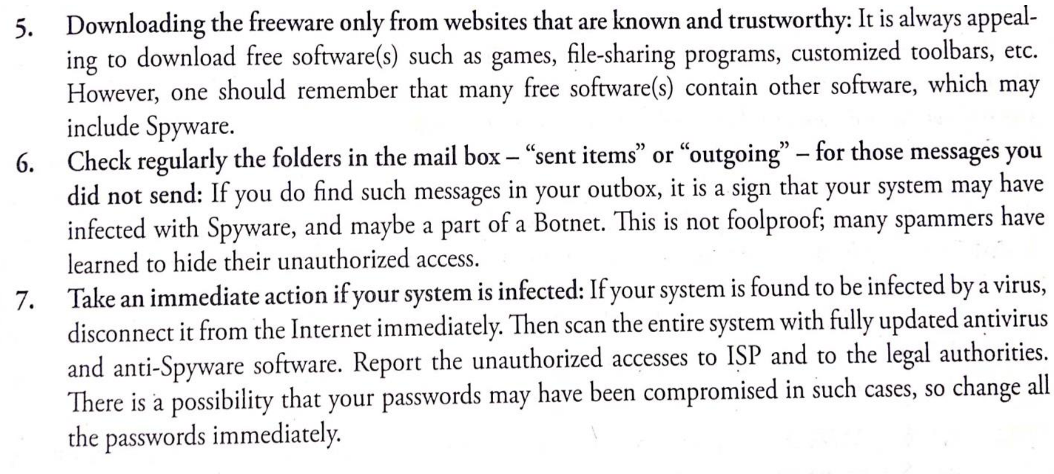

Botnet creation
Botnet renting
Botnet selling
DDoS attacks
Spam attacks
Malware and Adware installation
Stealing confidential information
Phishing attacks
Spamdexing
Selling – credit card and bank account details
Selling personal identity information
Selling Internet services and shops account

Figure 2.8 | Botnets are used for gainful purposes.

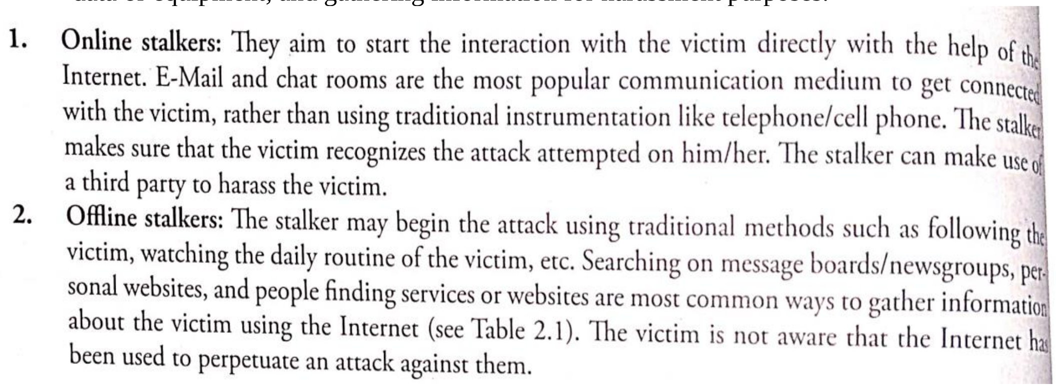
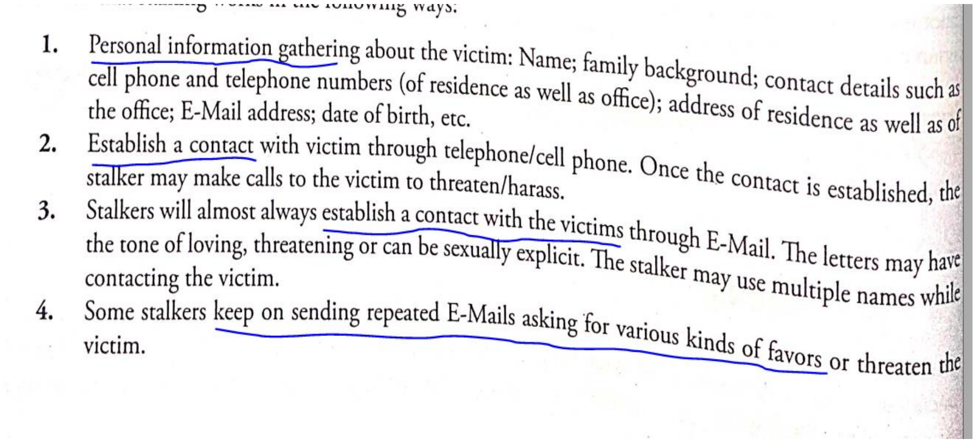
One can ensure the following to secure the system:

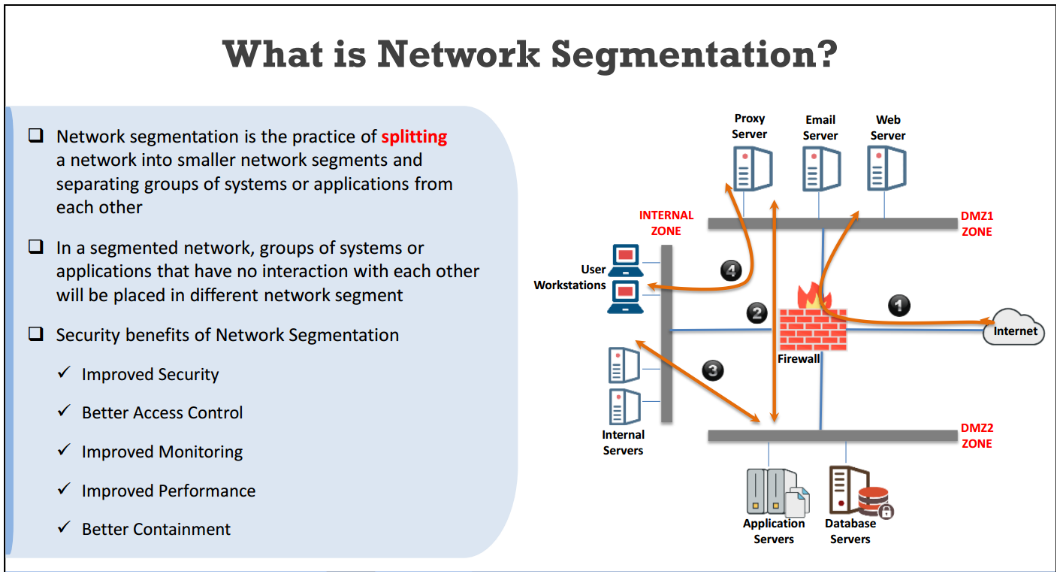
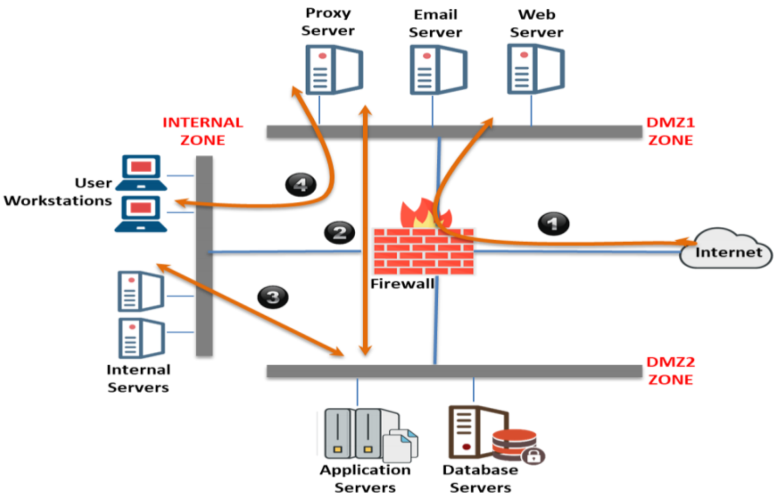


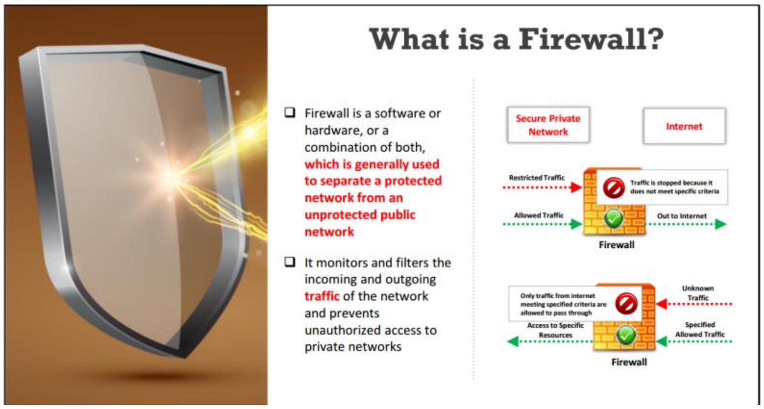
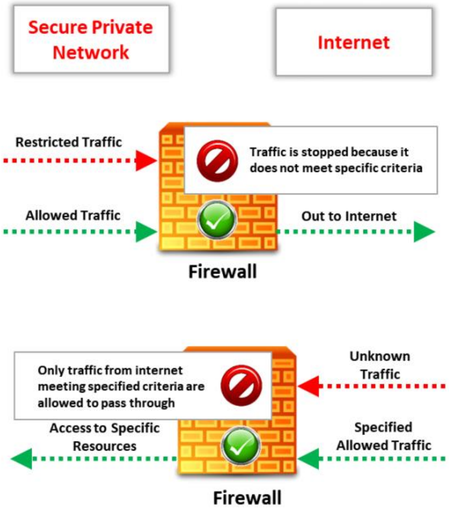
1. **Use antivirus and anti-Spyware software and keep it up-to-date:** It is important to remove and/or quarantine the viruses. The settings of these softwares should be done during the installations so that these softwares get updated automatically on a daily basis.
2. **Set the OS to download and install security patches automatically:** OS companies issue the security patches for flaws that are found in these systems.
3. **Use a firewall to protect the system from hacking attacks while it is connected on the Internet:** A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. A firewall is different from antivirus protection. Antivirus software scans incoming communications and files for troublesome viruses vis-à-vis properly configured firewall that helps to block all incoming communications from unauthorized sources.
4. **Disconnect from the Internet when you are away from your computer:** Attackers cannot get into the system when the system is disconnected from the Internet. Firewall, antivirus, and anti-Spyware softwares are not foolproof mechanisms to get access to the system.

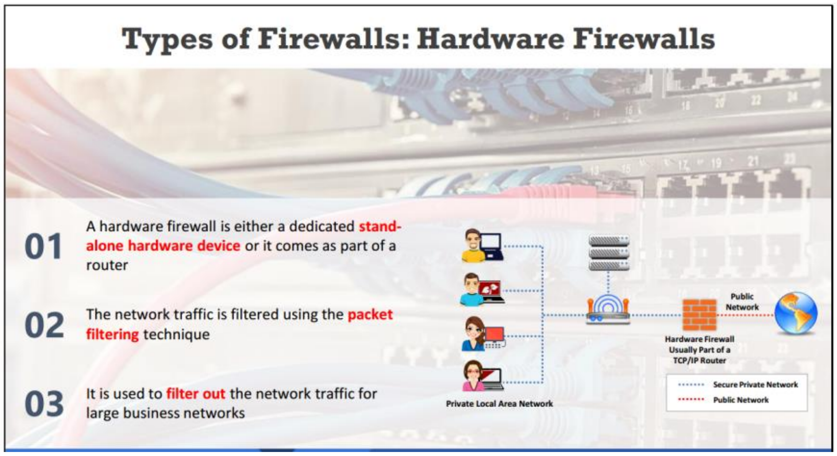


5. **Downloading the freeware only from websites that are known and trustworthy:** It is always appealing to download free software(s) such as games, file-sharing programs, customized toolbars, etc. However, one should remember that many free software(s) contain other software, which may include Spyware.
6. **Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send:** If you do find such messages in your outbox, it is a sign that your system may have infected with Spyware, and maybe a part of a Botnet. This is not foolproof; many spammers have learned to hide their unauthorized access.
7. **Take an immediate action if your system is infected:** If your system is found to be infected by a virus, disconnect it from the Internet immediately. Then scan the entire system with fully updated antivirus and anti-Spyware software. Report the unauthorized accesses to ISP and to the legal authorities. There is a possibility that your passwords may have been compromised in such cases, so change all the passwords immediately.

1.b	• Cyberstalkers **take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected**. The terms cyberstalking and cyberbullying are often used interchangeably. • Trying to approach some-body or something. • Refers to use of internet / ICT/ electronic communications devices to stalk another person • Individual or group of individual to harass another individual, group of individual or organization. • Behaviour includes false accusation, monitoring, transmission of threats, ID theft, damage to data or equipment, and gathering information for harassment purposes.  1. **Online stalkers:** They aim to start the interaction with the victim directly with the help of the Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim. 2. **Offline stalkers:** The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet (see Table 2.1). The victim is not aware that the Internet has been used to perpetuate an attack against them. ***How stalking works***  stalking works in the following ways: 1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc. 2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass. 3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim. 4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.	4
2.a	purpose of social networking: • Sharing. • Learning. • Interacting • Marketing **types of social networking:** • **Social connections** **Ex.** Facebook, Myspace and Instagram • **Professional connections** **Ex. LinkedIn** • **Sharing of multimedia** **Ex. YouTube and Flickr** • **News or informational** **Ex. Reddit, Stack Overflow or Digg.** • **Communication** **Ex. WhatsApp, WeChat and Snapchat** • **Educational** Ex. Google Classroom	6

2.b	**Social media addiction** is becoming common. • People can begin to feel a sense of anxiety if they don't check their social media accounts, or they may compulsively refresh them. • Social networking posts are also highly curated, people only post the good things that happen to them. This can cause a warped view of reality where the viewer thinks that others have better lives than they do. • This leads to a fear of missing out (FOMO) on social events. **Cyberbullying** is when someone makes social media posts with the intention to harm someone else. • This can take the form of publicly posting the private information of someone or sending abusive messages. • Tragically, cyberbullying has led to the suicide of some individuals. It is now a major concern in public schools. • Doxing is when someone publicly posts the personally identifiable information, such as an address or phone number, of someone else.	4
3.a	 **What is Network Segmentation?** ❑ Network segmentation is the practice of splitting a network into smaller network segments and separating groups of systems or applications from each other ❑ In a segmented network, groups of systems or applications that have no interaction with each other will be placed in different network segment ❑ Security benefits of Network Segmentation ✓ Improved Security ✓ Better Access Control ✓ Improved Monitoring ✓ Improved Performance ✓ Better Containment Proxy Server Email Server Web Server INTERNAL ZONE DMZ1 ZONE User Workstations 4 2 1 3 Firewall Internet Internal Servers DMZ2 ZONE Application Servers Database Servers **Working Principle of Network Segmentation**  Proxy Server Email Server Web Server INTERNAL ZONE DMZ1 ZONE User Workstations 4 2 1 3 Firewall Internet Internal Servers DMZ2 ZONE Application Servers Database Servers	6

3.b	Different Types of Digital Security • Antivirus Software • Current, Updated Firewalls • Proxies • Remote Monitoring Software • Vulnerability Scanner Examples of Digital Security Tools Instant Message Encryption Tools • ChatSecure is a messaging app that offers secure encryption for Android and iOS phones, and • Cryph secures your Mac or Windows-based web browsers. Navigation Privacy Tools • Anonymox protects your identity by creating a proxy, letting you change your IP and surf anonymously. It's available as an add-on for Google Chrome and Firefox. • Tor isolates every website you explore, so advertisements and third-party trackers can't lock into you. It also your browsing history, removes cookies, and provides multi-layer encryption. Telephone Encryption Tools • SilentPhone offers smartphone users end-to-end encryption for voice conversations, messaging, file transfer, video, and more. • It's compatible with Android and iOS devices and is free. • Signal is an independent non-profit resource that lets users share text, GIFs, voice messages, photos, videos, and data files.	4
4	 What is a Firewall? ❑ Firewall is a software or hardware, or a combination of both, which is generally used to separate a protected network from an unprotected public network ❑ It monitors and filters the incoming and outgoing traffic of the network and prevents unauthorized access to private networks *Working of a firewall:*  Secure Private Network Internet Restricted Traffic Traffic is stopped because it does not meet specific criteria Allowed Traffic Out to Internet Firewall Only traffic from internet meeting specified criteria are allowed to pass through Unknown Traffic Access to Specific Resources Specified Allowed Traffic Firewall	10



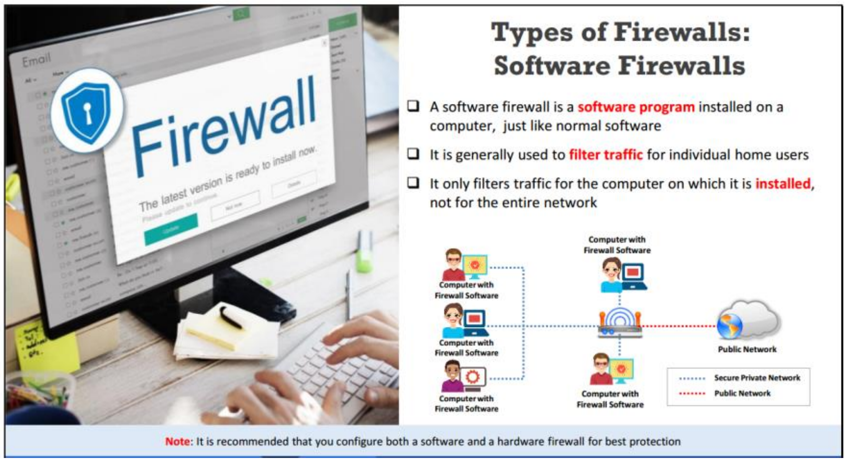
Types of Firewalls: Hardware Firewalls

01 A hardware firewall is either a dedicated **stand-alone hardware device** or it comes as part of a router

02 The network traffic is filtered using the **packet filtering** technique

03 It is used to **filter out** the network traffic for large business networks

Private Local Area Network
Public Network
Hardware Firewall Usually Part of a TCP/IP Router
Secure Private Network
Public Network

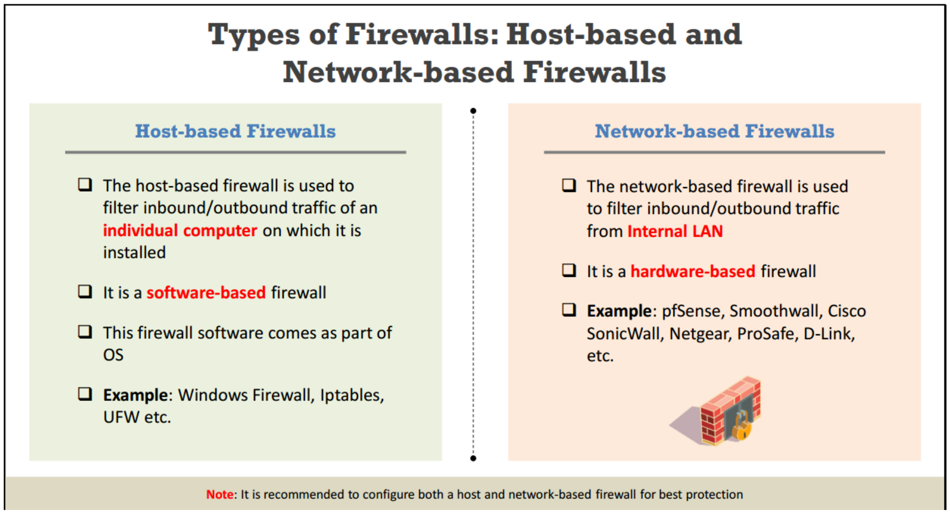


Types of Firewalls: Software Firewalls

- ❑ A software firewall is a **software program** installed on a computer, just like normal software
- ❑ It is generally used to **filter traffic** for individual home users
- ❑ It only filters traffic for the computer on which it is **installed**, not for the entire network

Firewall
The latest version is ready to install now.
Computer with Firewall Software
Computer with Firewall Software
Computer with Firewall Software
Computer with Firewall Software
Computer with Firewall Software
Public Network
Secure Private Network
Public Network

Note: It is recommended that you configure both a software and a hardware firewall for best protection



Types of Firewalls: Host-based and Network-based Firewalls

Host-based Firewalls

- ❑ The host-based firewall is used to filter inbound/outbound traffic of an **individual computer** on which it is installed
- ❑ It is a **software-based** firewall
- ❑ This firewall software comes as part of OS
- ❑ **Example**: Windows Firewall, Iptables, UFW etc.

Network-based Firewalls

- ❑ The network-based firewall is used to filter inbound/outbound traffic from **Internal LAN**
- ❑ It is a **hardware-based** firewall
- ❑ **Example**: pfSense, Smoothwall, Cisco SonicWall, Netgear, ProSafe, D-Link, etc.

Note: It is recommended to configure both a host and network-based firewall for best protection

Software Firewalls:

Advantages:

- Less expensive than hardware firewalls.
- Ideal for personal or home use.
- Easier to configure and reconfigure.

Disadvantages:

- Consumes system resources.
- Difficult to uninstall.
- Not appropriate for environments requiring faster response times.

Host-based Firewalls:

Advantages

- Provides security for devices irrespective of change in location
- Provides internal security and avoids internal attacks by allowing only authorized users
- Setup requires basic hardware/software installation
- Useful for individuals and small businesses with fewer devices as they provide customized protection
- Provide flexibility by allowing applications and virtual machines (VMs) to take their host-based firewalls along with them when they are moved between cloud environments
- Allows configuring a single device for an individual's requirements using custom firewall rules

Disadvantages

- Not suitable for larger networks
- Provide less security because if an attacker can access a host, they can turn off the firewall or install malicious code undetected by the organization
- Must be replaced if bandwidth exceeds firewall throughput or, otherwise, more effort are needed to scale up every device if the number of hosts increase
- Costly, as they require individual installation and maintenance on every server for big organizations
- Dedicated IT staff is needed for maintaining each device

5

A brute force attack:

10

- This is where every possible combination of letters, numbers and symbols in an attempt to guess the password.
- While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated.
- A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.

A dictionary attack:

- A more intelligent method than the brute force attack described above is the dictionary attack.
- This is where the combinations tried are first chosen from words available in a dictionary.
- Software tools are readily available that can try every word in a dictionary or word list or both until your password is found.
- Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

Two step Authentication:

	Two-Step Verification is an additional layer of security that you can add onto your Gmail account. When enabled, you will have to enter your password, and enter a special code that is sent to your device or verify the sign in attempt on your phone. This dramatically increases the security of your account and makes sure that hackers can't get into your account even if the guess or steal your password. *Method 1 Text Message or Voice Call:* 1 Decide if you want to use the text message or voice call option. With this enabled, a code will be sent to your phone via text, or Google will call your phone and tell you the code. You then enter this code into the sign in prompt in order to sign in	