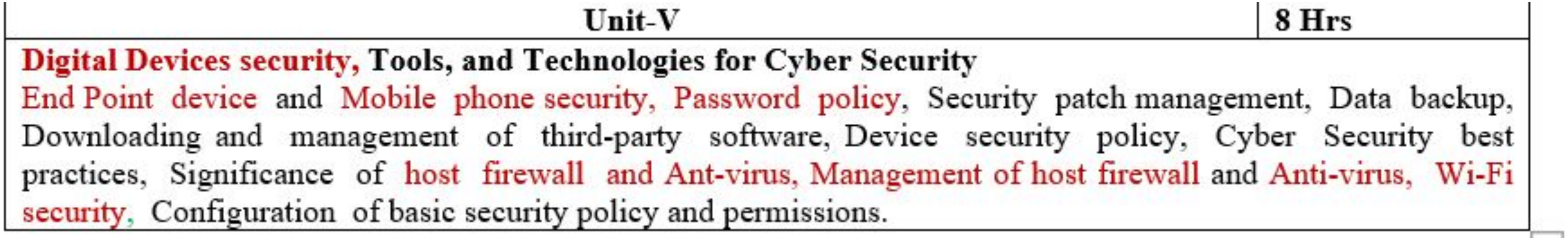
UNIT- V

Chapter-2: Digital Devices security, Tools, and Technologies for Cyber Security

Unit - V Syllabus



Unit-V	8 Hrs
Digital Devices security, Tools, and Technologies for Cyber Security End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	

Digital security: Introduction

- This increased reliance on the internet and digital networks brings risks along with the convenience it provides.
- banking, bill paying, social planning etc. even parts of our job.
- Online criminals, hackers, even just bored mischief-makers lurk in the shadows, waiting to rob you, commit fraud, steal your identity, or simply embarrass.
- digital information security is of paramount concern

What is Digital Security?

- collective term that describes the resources employed to protect your online identity, data, and other assets.
- These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices.
- Digital security is the process used to protect your online identity.

Difference Between Digital Information Security and Cyber Security

- Illegally accessing someone's data, identity, or financial resources is called a "cybercrime."
- Digital security involves protecting online presence (data, identity, assets).
- cyber security covers more ground, protecting entire networks, computer systems, and other digital components, and the data stored within from unauthorized access.
- Digital security a sub-type of cyber security.
- Digital security protects information, and cyber security protects the infrastructure, all systems, networks, and information.

What Kind of Information is Considered a Digital Security Risk?

- Personal Identification Data
- Personal Payment Data
- Personal Health Data

End point Device Security

- Endpoint device security refers to the protection of individual devices, such as computers, smartphones, tablets, and other endpoints, from cybersecurity threats.
- These threats can include malware, phishing attacks, unauthorized access, data breaches, and more.
- Ensuring the security of endpoint devices is crucial because these devices often serve as entry points for attackers trying to gain access to sensitive information or networks.

End point Device Security- Measures

- **Antivirus/Anti-malware Software**: Install reputable antivirus and anti-malware software on all devices to detect and remove malicious software.
- **Firewalls**: Enable firewalls on devices to monitor and control incoming and outgoing network traffic based on predetermined security rules.
- **Regular Updates and Patch Management**: Keep operating systems, applications, and firmware up to date with the latest security patches to address known vulnerabilities.

End point Device Security- Measures

- **Strong Authentication**: Implement strong authentication methods, such as passwords, biometrics, or multi-factor authentication (MFA), to prevent unauthorized access to devices.
- **Encryption**: Encrypt data stored on devices and transmitted over networks to protect it from unauthorized access in case of theft or interception.
- **Mobile Device Management (MDM)**: Use MDM solutions to remotely manage and secure mobile devices, enforce security policies, and enable features like remote wipe in case of loss or theft.
- **Application Whitelisting/Blacklisting**: Allow only approved applications to run on devices (whitelisting) and block known malicious applications (blacklisting).

End point Device Security- Measures

- **User Education and Awareness**: Train users on best practices for device security, such as avoiding suspicious links and attachments, and being cautious when connecting to public Wi-Fi networks.
- **Endpoint Detection and Response (EDR)**: Deploy EDR solutions to continuously monitor endpoint activities for signs of suspicious behavior or security incidents and respond appropriately.
- **Data Backup and Recovery**: Regularly back up data stored on endpoint devices to minimize the impact of data loss in case of a security incident, and ensure that recovery procedures are in place.

End point Device Security- Measures

- **Remote Access Controls**: Limit remote access to devices and use secure connections, such as virtual private networks (VPNs), for remote management and access.
- **Device Inventory and Asset Management**: Maintain an inventory of all endpoint devices connected to the network and implement asset management practices to track their usage and security status.

End point Device Security- Measures

- **Remote Access Controls**: Limit remote access to devices and use secure connections, such as virtual private networks (VPNs), for remote management and access.
- **Device Inventory and Asset Management**: Maintain an inventory of all endpoint devices connected to the network and implement asset management practices to track their usage and security status.

Mobile Device Security

- Mobile device security is essential for protecting smartphones, tablets, and other portable devices from various cybersecurity threats.
- Given the prevalence of mobile devices in both personal and professional settings, ensuring their security is crucial.

Measures:

- **Device Encryption**: Enable full-disk encryption to protect the data stored on the device from unauthorized access in case of loss or theft.
- **Screen Lock**: Set up strong authentication methods, such as PINs, passwords, patterns, fingerprints, or facial recognition, to prevent unauthorized access to the device.

Mobile Device Security

- **Operating System Updates**: Keep the mobile operating system up to date with the latest security patches and firmware updates to address known vulnerabilities.
- **App Permissions**: Review and manage app permissions to limit the data and features that apps can access on the device, and only download apps from trusted sources such as official app stores.

Password Policy

- A password policy is a set of rules and guidelines designed to enhance the security of passwords used to access computer systems, networks, and online accounts.
- A strong password policy helps prevent unauthorized access, data breaches, and other security incidents.

Best Practices

- **Password Complexity**: Require passwords to meet specific complexity criteria, such as a minimum length, a mix of uppercase and lowercase letters, numbers, and special characters. For example, requiring passwords to be at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character.

Password Policy

- **Password Length**: Set a minimum password length to ensure passwords are sufficiently complex and resistant to brute-force attacks. A longer password generally increases security.
- **Password History**: Enforce a password history policy to prevent users from reusing old passwords. This helps mitigate the risk of compromised passwords being reused by attackers.
- **Password Expiration**: Require users to change their passwords periodically to reduce the likelihood of unauthorized access due to compromised passwords. Specify a maximum password age, after which users must create a new password.
- **Account Lockout Policy**: Implement an account lockout policy to temporarily lock user accounts after a certain number of consecutive failed login attempts. This helps prevent brute-force attacks.

Password Policy

- **Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA)**: Encourage or require the use of 2FA or MFA in addition to passwords for authentication, adding an extra layer of security.
- **Password Storage**: Store passwords securely using hashing algorithms and salting to protect them from unauthorized access in case of a data breach.
- **Password Transmission**: Encourage the use of secure protocols (e.g., HTTPS) for transmitting passwords over networks to prevent interception and eavesdropping.
- **User Education**: Provide guidance to users on creating strong passwords, recognizing phishing attempts, and securely managing their passwords. Regularly remind users to update their passwords and be vigilant about security threats.

Password Policy

- **Administrative Passwords**: Enforce stricter password policies for administrative accounts, including stronger complexity requirements, shorter expiration periods, and additional security measures.
- **Monitoring and Enforcement**: Regularly monitor password-related activities, such as failed login attempts and password changes, and enforce policy compliance through audits and enforcement mechanisms.

Security patch management

- Security patch management is the process of identifying, acquiring, testing, and applying patches (software updates) to address vulnerabilities in operating systems, applications, and firmware.
- Effective patch management is crucial for maintaining the security and integrity of computer systems and networks, as it helps protect against known security vulnerabilities that could be exploited by attackers.

Security patch management- Steps

- **Vulnerability Assessment**: Regularly scan systems and networks to identify vulnerabilities and prioritize them based on severity and potential impact on security.
- **Patch Identification**: Stay informed about security advisories and updates released by software vendors, security researchers, and industry sources to identify relevant patches for known vulnerabilities.
- **Patch Prioritization**: Prioritize patches based on the severity of vulnerabilities, the criticality of affected systems, and the potential impact on business operations. Focus on addressing critical vulnerabilities that are actively exploited or have a high likelihood of exploitation.
- **Testing**: Test patches in a controlled environment, such as a test lab or non-production system, to ensure compatibility with existing software and configurations and to verify that the patches do not introduce new issues or conflicts.
- .

Security patch management- Steps

- **Deployment**: Deploy patches to production systems using a phased approach or deployment schedule to minimize disruption to operations. Consider prioritizing critical systems and endpoints that are more vulnerable or critical to business functions.
- **Monitoring and Verification**: Monitor systems after patch deployment to ensure that patches are applied successfully and that there are no adverse effects on system performance or functionality. Verify that vulnerabilities are effectively mitigated by the patches.
- **Patch Management Tools**: Utilize patch management tools and software solutions to automate and streamline the patch management process, including patch deployment, tracking, and reporting.

Security patch management- Steps

- **Change Management**: Integrate patch management processes into overall change management procedures to ensure proper documentation, approval, and coordination of patch deployments, especially in environments with strict change control requirements.
- **Vendor Coordination**: Establish communication channels with software vendors and security researchers to receive timely notifications about new vulnerabilities and patches, and collaborate with vendors to address complex or critical security issues.
- **User Awareness**: Educate users and system administrators about the importance of patch management, including the risks of unpatched vulnerabilities and the need to promptly apply security patches to mitigate these risks.

Security patch management- Steps

- **Regular Review and Update**: Continuously review and update the patch management process to adapt to evolving security threats, technology changes, and organizational requirements. Regularly assess the effectiveness of patch management practices and make adjustments as needed

Downloading and management of third party software

Downloading and managing third-party software involves several steps to ensure the software is obtained from trusted sources, installed securely, and kept up to date.

Guide to effectively downloading and managing third-party software:

- Source Verification.
- Check Software Integrity
- Review Permissions and Privacy Policies
- Install from Trusted Sources
- Keep Software Updated
- Use Official Channels for Updates
- Uninstall Unused Software
- Monitor Software Dependencies

Downloading and management of third party software

Downloading and managing third-party software involves several steps to ensure the software is obtained from trusted sources, installed securely, and kept up to date.

Guide to effectively downloading and managing third-party software:

- Source Verification.
- Check Software Integrity
- Review Permissions and Privacy Policies
- Install from Trusted Sources
- Keep Software Updated
- Use Official Channels for Updates
- Uninstall Unused Software
- Monitor Software Dependencies

Significance of Host Firewall and Antivirus

- Host firewalls and antivirus software play critical roles in protecting individual devices, such as computers and servers, from various cybersecurity threats.
- Host firewalls and antivirus software are essential components of a layered defense strategy, working together to protect devices from a wide range of cybersecurity threats, including network-based attacks, malware infections, and data breaches.
- Their significance lies in their ability to provide proactive and reactive protection, reducing the risk of compromise and maintaining the integrity and security of individual endpoints.

Significance of Host Firewall and Antivirus

Host Firewalls:

- **Network Protection**: Host firewalls monitor incoming and outgoing network traffic on an individual device, allowing or blocking connections based on predefined rules. They act as the first line of defense against unauthorized access and malicious network activity.
- **Defense Against External Threats**: Host firewalls help prevent external threats, such as hacking attempts, port scans, and network-based attacks, by filtering traffic at the device level before it reaches applications and services.

Significance of Host Firewall and Antivirus

Host Firewalls:

- **Network Protection**: Host firewalls monitor incoming and outgoing network traffic on an individual device, allowing or blocking connections based on predefined rules. They act as the first line of defense against unauthorized access and malicious network activity.
- **Defense Against External Threats**: Host firewalls help prevent external threats, such as hacking attempts, port scans, and network-based attacks, by filtering traffic at the device level before it reaches applications and services.

Significance of Host Firewall and Antivirus

- **Protection for Unmanaged Networks**: In situations where devices connect to unsecured or public networks, such as public Wi-Fi hotspots, host firewalls provide an additional layer of protection by filtering incoming connections and blocking potentially malicious traffic.
- **Granular Control**: Host firewalls offer granular control over network traffic, allowing users or administrators to define rules based on specific protocols, ports, IP addresses, or applications. This enables customization to meet the unique security requirements of each device.
- **Complement to Network Firewalls**: Host firewalls complement network firewalls by providing endpoint-level protection, especially for devices outside the organization's network perimeter, such as remote laptops or mobile devices.

Significance of Host Firewall and Antivirus

Antivirus Software:

- **Malware Detection and Prevention**: Antivirus software scans files, programs, and memory for known malware signatures and behaviors, detecting and removing malicious software such as viruses, worms, Trojans, and ransomware.
- **Real-Time Protection**: Antivirus solutions often include real-time scanning capabilities, monitoring system activities and incoming/outgoing data for signs of malware infection. They can quarantine or block suspicious files and processes before they can cause harm.
- **Zero-Day Threat Detection**: Antivirus software employs heuristic analysis and behavioral monitoring to detect and mitigate zero-day threats—previously unknown malware—by identifying suspicious patterns and activities indicative of malicious intent.

Significance of Host Firewall and Antivirus

Antivirus Software:

- **Web Protection**: Many antivirus products include web protection features to block access to malicious websites, phishing sites, and malicious downloads. They provide warnings and alerts to users when visiting potentially harmful web pages.
- **Email Security**: Some antivirus solutions offer email scanning capabilities to detect and block malicious email attachments, links, and phishing attempts, reducing the risk of malware infection through email-borne threats.
- **Scheduled Scans and Updates**: Antivirus software allows users to schedule regular scans of their devices and automatically update virus definitions to ensure protection against the latest threats.

Wifi Security

- Wi-Fi networks are susceptible to various threats, ranging from unauthorized access to eavesdropping and data interception.
- Understanding these threats and implementing appropriate security measures is crucial for protecting Wi-Fi networks and the data transmitted over them.

Unauthorized Access (Wi-Fi Squatting):

Threat: Attackers attempt to gain unauthorized access to Wi-Fi networks by exploiting weak or default passwords or by using brute-force attacks to guess passwords.

Security Measure: Use strong, unique passwords for Wi-Fi networks and change them regularly. Implement Wi-Fi Protected Access (WPA) or WPA2 with strong encryption and authentication methods, such as WPA2-PSK (Pre-Shared Key) or WPA2-Enterprise with 802.1X authentication.

Wifi Security

Man-in-the-Middle (MitM) Attacks:

Threat: Attackers intercept and manipulate data transmitted between devices and the Wi-Fi access point, allowing them to eavesdrop on communications, steal sensitive information, or inject malicious content.

Security Measure: Use encryption protocols such as WPA2-Enterprise with AES (Advanced Encryption Standard) encryption, which provides secure communication between devices and access points. Implement protocols like TLS (Transport Layer Security) for securing data transmitted over Wi-Fi

Wifi Security

Evil Twin Attacks:

Threat: Attackers set up rogue Wi-Fi access points with names similar to legitimate networks to trick users into connecting to them. Once connected, attackers can intercept and manipulate network traffic.

Security Measure: Educate users about the risks of connecting to unfamiliar Wi-Fi networks and encourage them to verify the legitimacy of Wi-Fi access points before connecting. Implement Wi-Fi Protected Setup (WPS) PIN or disable WPS to prevent easy access to Wi-Fi networks.

Wifi Security

Rogue Access Points:

Threat: Unauthorized access points installed within the network infrastructure without the knowledge or approval of the organization's IT department. Rogue access points can provide attackers with an entry point into the network.

Security Measure: Regularly scan the network for unauthorized access points using tools like wireless intrusion detection/prevention systems (WIDS/WIPS). Implement network access control (NAC) solutions to restrict unauthorized devices from connecting to the network.

Wifi Security

Denial of Service (DoS) Attacks:

Threat: Attackers flood Wi-Fi networks with a high volume of traffic or malicious packets, causing network congestion, degradation of service, or complete disruption of connectivity.

Security Measure: Implement Wi-Fi Protected Access (WPA) or WPA2 with features like Wi-Fi Protected Access Protected Management Frames (WPA-PMF) to protect against DoS attacks. Configure access points to limit the number of connection attempts from individual devices.

Wifi Security

Packet Sniffing:

Threat: Attackers use packet sniffing tools to capture and analyze data packets transmitted over Wi-Fi networks, potentially exposing sensitive information such as usernames, passwords, and confidential data.

Security Measure: Use encryption protocols such as WPA2 with AES encryption to encrypt data transmitted over Wi-Fi networks, making it more difficult for attackers to intercept and decipher.

Wifi Security

WLAN Security Misconfigurations:

Threat: Insecure configurations of Wi-Fi access points and routers, such as weak encryption settings, default passwords, or open networks, can leave networks vulnerable to exploitation.

Security Measure: Regularly audit and update Wi-Fi access point configurations to ensure they adhere to security best practices. Disable unnecessary services and features, change default passwords, and implement strong encryption and authentication methods.

Wifi Security

Physical Security:

Threat: Physical access to Wi-Fi access points and network infrastructure can enable attackers to tamper with devices, install malicious firmware, or perform other unauthorized actions.

Security Measure: Physically secure Wi-Fi access points and network equipment in locked cabinets or secure locations to prevent unauthorized access. Implement tamper-evident seals and monitoring to detect and deter physical tampering.

Specific 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

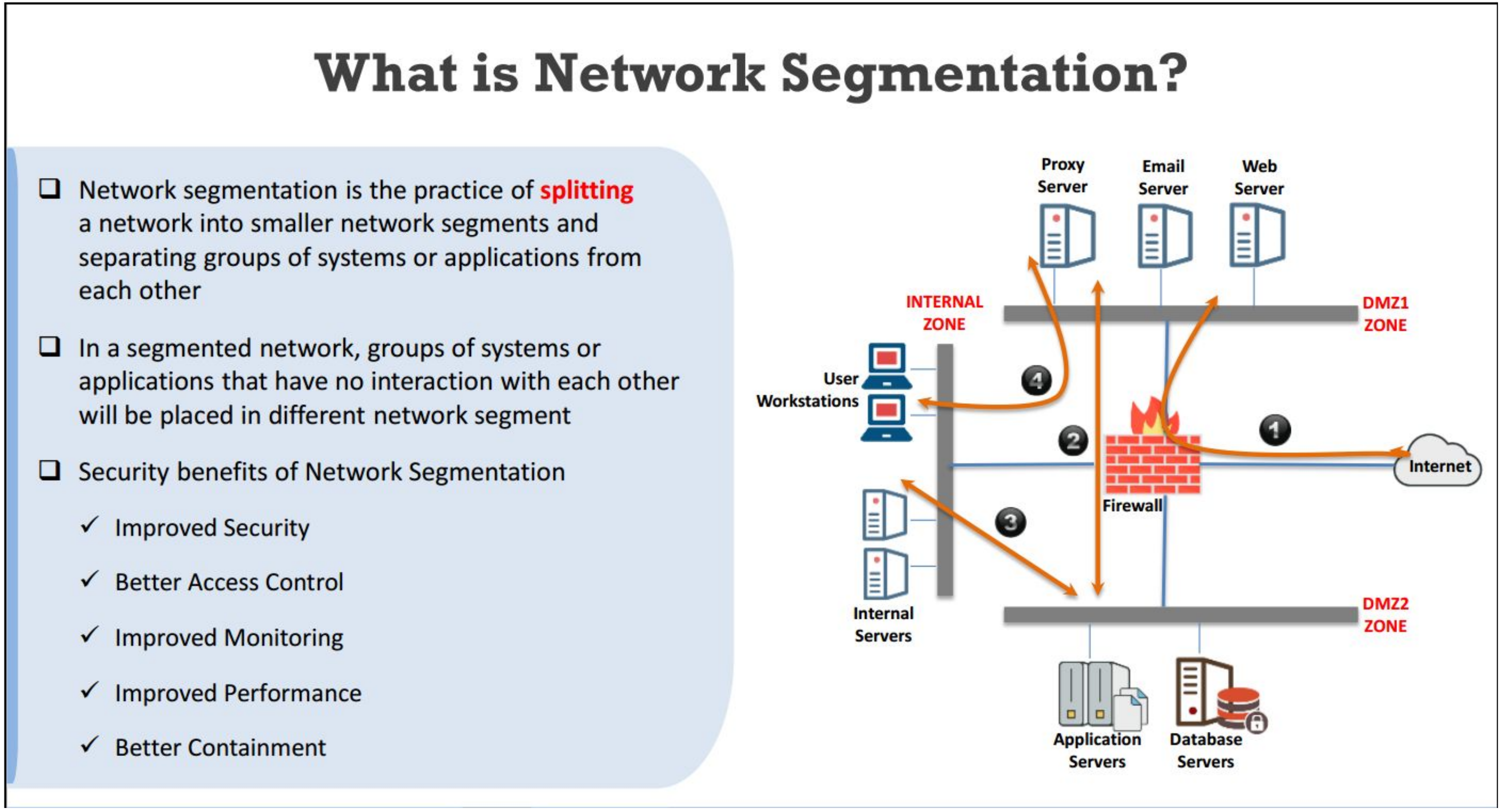
- Anonymox protects your identity by creating a proxy, letting you change your IP and surf anonymously. It's available as an add-on for Google Chrome and Firefox.
- Tor isolates every website you explore, so advertisements and third-party trackers can't lock into you. It also your browsing history, removes 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 nonprofit resource that lets users share text, GIFs, voice messages, photos, videos, and data files.

ADDITIONAL INFORMATION SLIDES

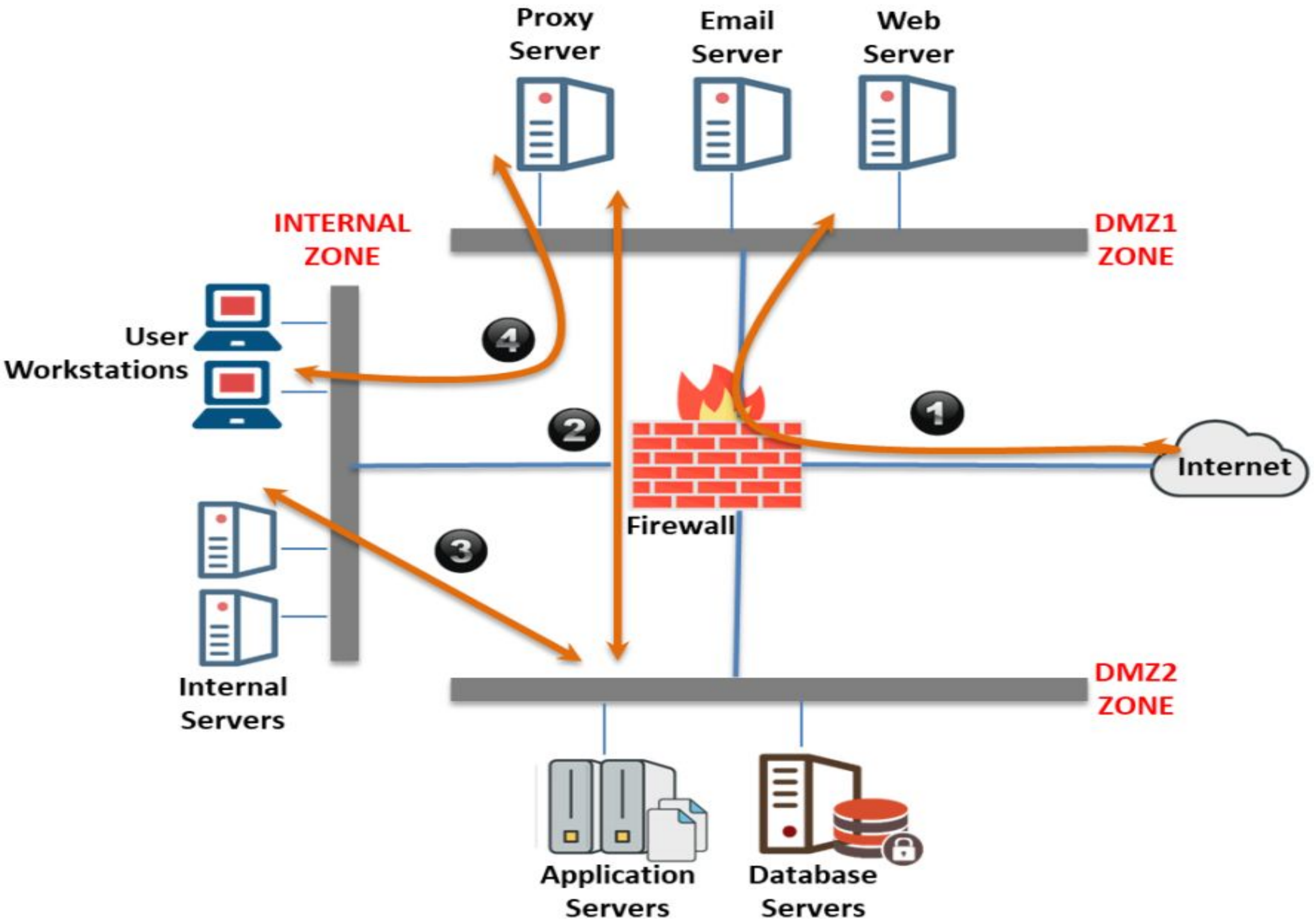
Network Segmentation



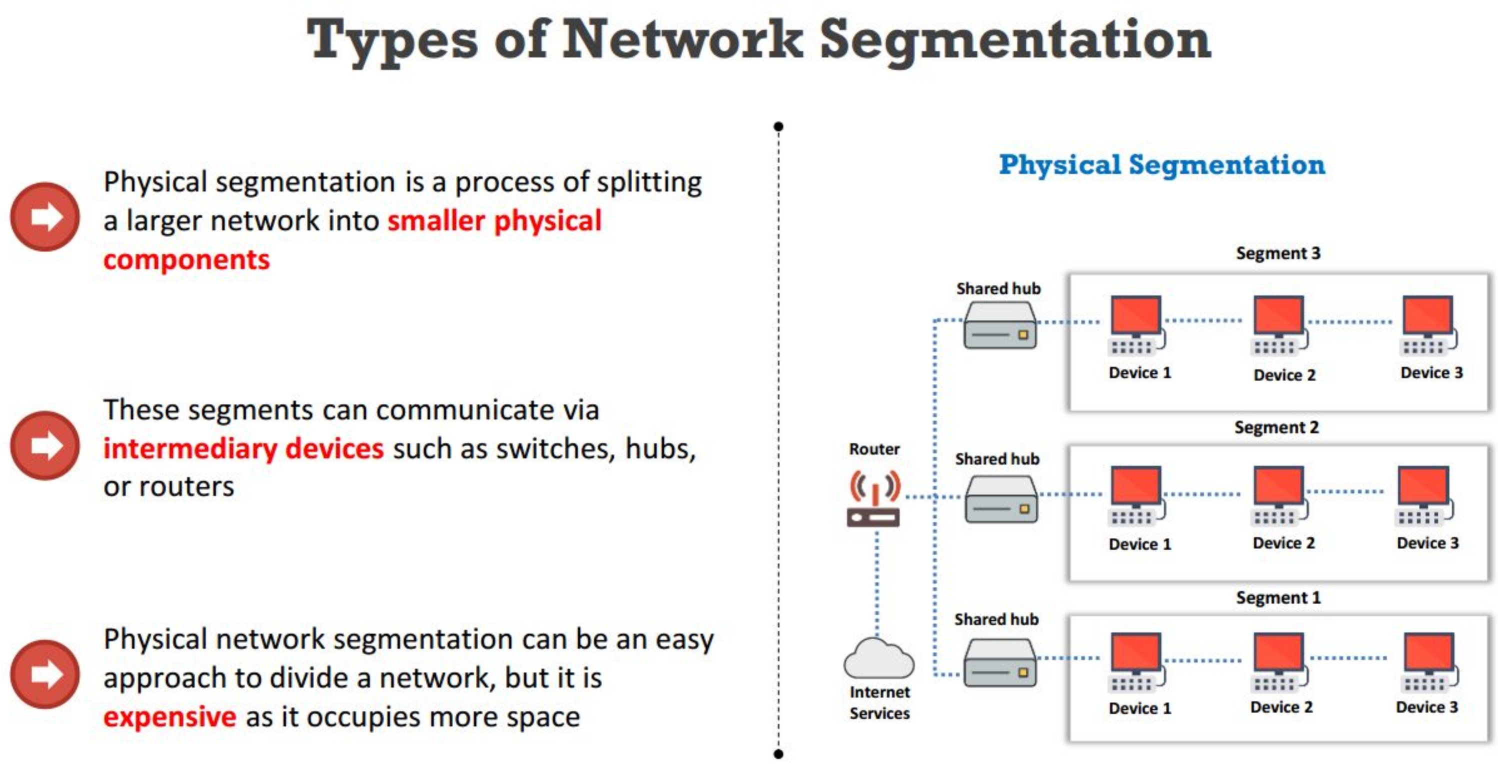
What is Network Segmentation?

- ❑ 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

Working Principle of Network Segmentation



Types of Network Segmentation



Types of Network Segmentation

- Physical segmentation is a process of splitting a larger network into **smaller physical components**
- These segments can communicate via **intermediary devices** such as switches, hubs, or routers
- Physical network segmentation can be an easy approach to divide a network, but it is **expensive** as it occupies more space

Physical Segmentation

Types of Network Segmentation (Cont'd)

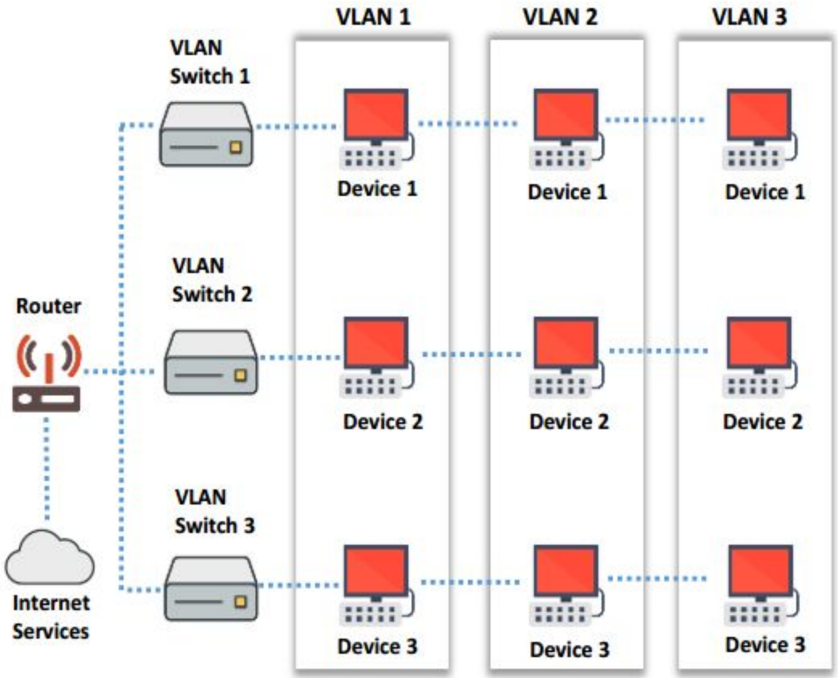
- ❑ Logical segmentation utilizes **VLANs**, which are **isolated logically** without considering the physical locations of devices

- ❑ Each VLAN is considered an **independent logical unit**, and the devices within a VLAN communicate as though they are in their own isolated network

- ❑ In this approach, **firewalls** are shared, and **switches** handle the VLAN infrastructure

- ❑ It is easier to implement and flexible to operate

Logical Segmentation

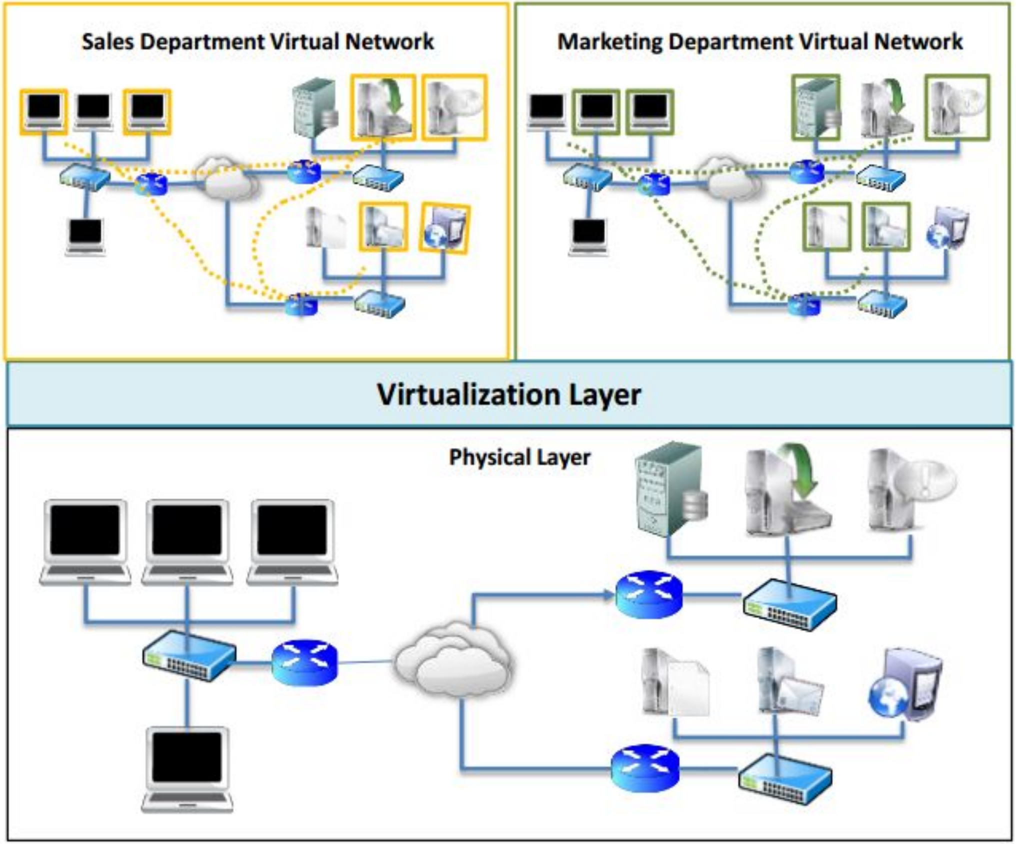


Types of Network Segmentation (Cont'd)

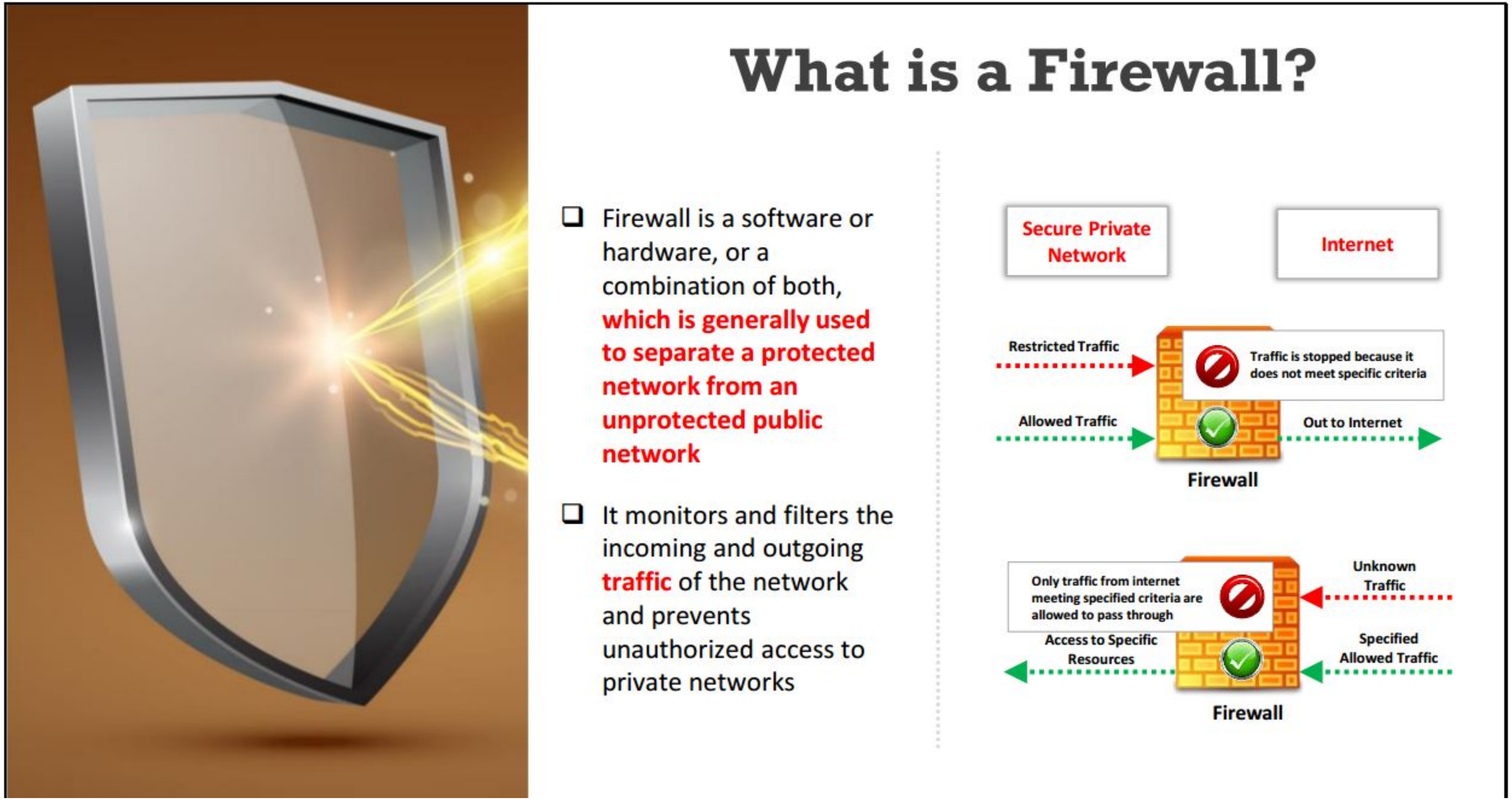
Network Virtualization

- ❑ Network virtualization is a process of combining all the available network resources and enabling security professionals to share these resources amongst the network users using a **single administrative unit**

- ❑ Network virtualization enables each user to access available network resources such as files, folders, computers, printers, hard drives, etc. from their system


Sales Department Virtual Network
Marketing Department Virtual Network
Virtualization Layer
Physical Layer

Firewall

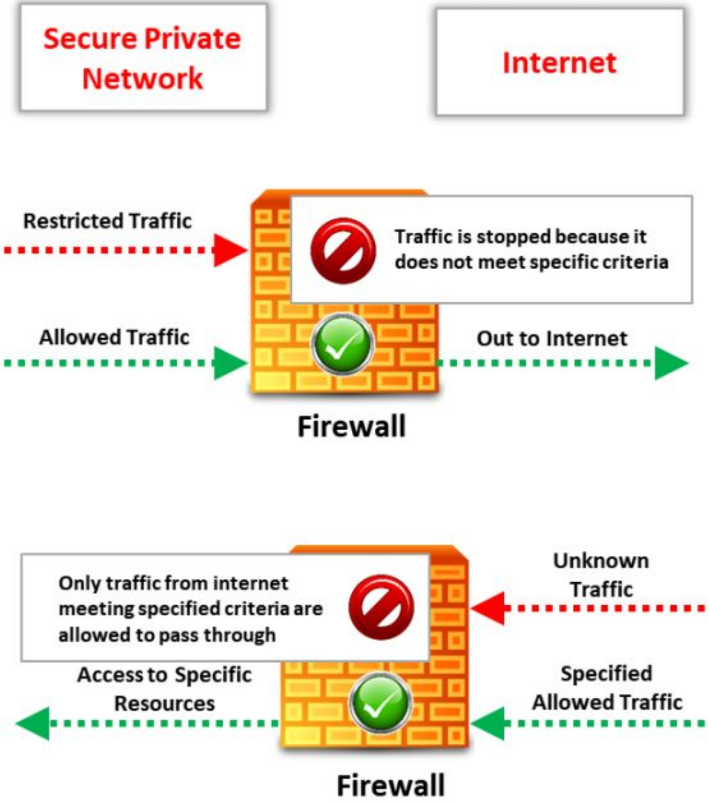


What is a Firewall?

- ❑ 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

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

Working of a firewall:

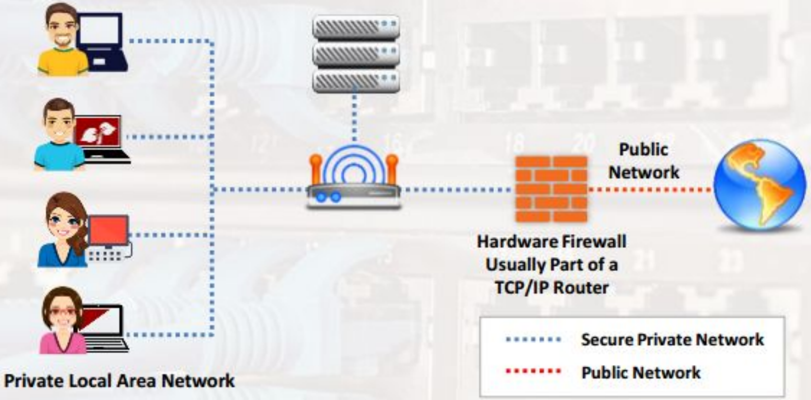

Secure Private Network
Internet
Restricted Traffic
Traffic is stopped because it does not meet specific criteria
Allowed Traffic
Out to Internet
Firewall
Only traffic from internet meeting specified criteria are allowed to pass through
Unknown Traffic
Access to Specific Resources
Specified Allowed Traffic
Firewall

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

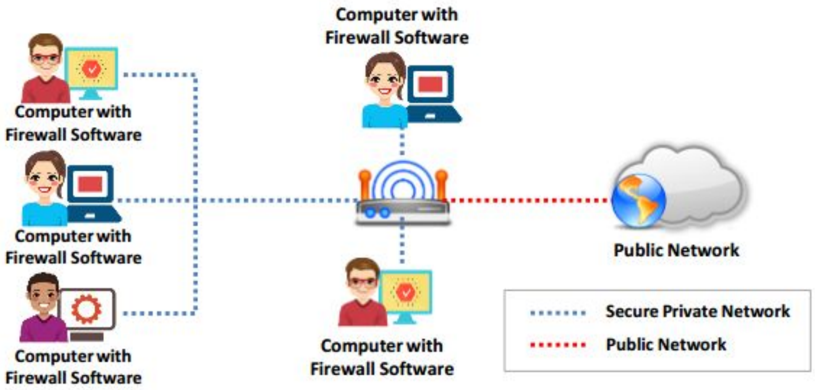
03 It is used to **filter out** the network traffic for large business networks


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

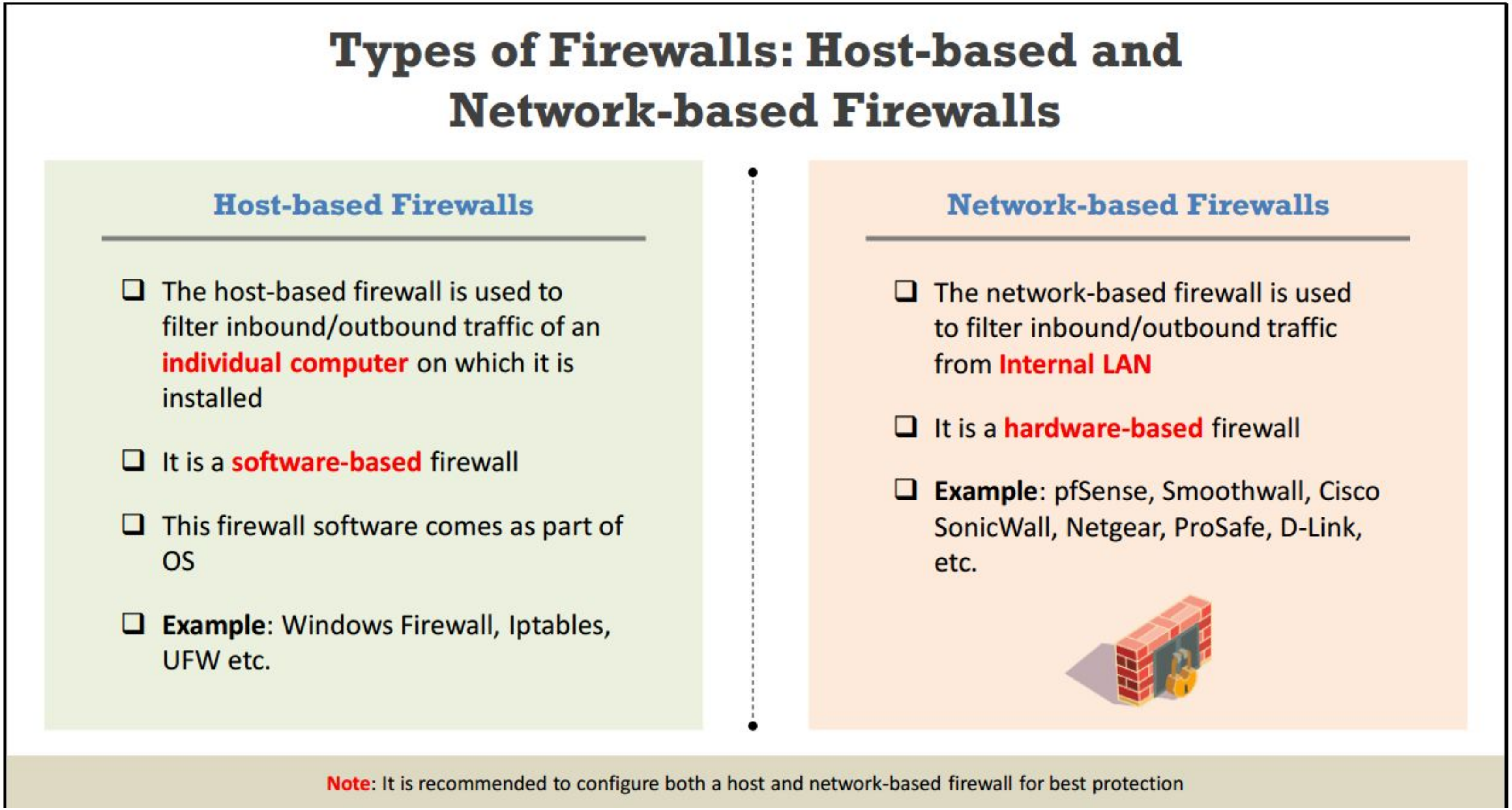
Email
Firewall
The latest version is ready to install now.
Please update to continue
Update
Not now
Details

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


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

INTRODUCTION TO MOBILE PHONES

- Smartphones
- They face most of the security challenges we associate with computers, plus a number of additional threats related to portability, ubiquity, insecure network architecture, location tracking, media capture and other such considerations.

OPERATING SYSTEMS

- Google's Android or Apple's iOS
- iOS works only on Apple devices and makes it much more difficult to run applications that have not been approved by Apple.
- updates is one of the most important considerations
- Some cheaper models do not provide access to updates that are needed to fix important security flaws.
- This could leave you vulnerable to malware or other attacks.

BRANDED AND LOCKED SMARTPHONES:

- Smartphones are often sold locked to a specific carrier or mobile network operator.
- This means that the specific smart phone will only work with that company's SIM card.
- Mobile network operators often customise the operating system and install additional software on locked smartphones.
- They may also disable some functionality. This could leave you with apps on your smartphone that you cannot uninstall or prevent from accessing your information, including your contacts and storage.
- it is usually safer to buy an unlocked smartphone that is not locked to a particular mobile provider.
- Unfortunately, these are often more expensive.

BASIC SECURITY SETUP:

- help to manage the security of the device
- use **Google's Play store for Android or Apple's App Store for iOS devices.**
- Android apps in various places online, Some of these apps contain malware.
- Only install software that comes from a source you trust.
- Applications in the Play Store and in the App Store benefit from a limited review by Google and Apple, respectively
- Even "official" apps sometimes behave poorly.
- it asks for permission to send your contacts over a mobile data connection to a third party, you should be suspicious.

- keep all of your apps up-to-date.
- uninstall apps that you no longer use.
- A new owner could alter an app that you have already installed and push a malicious update.

MOBILITY AND THE VULNERABILITY OF INFORMATION:

- The mobile phones we carry around with us often contain sensitive information.
- Call logs, browser histories, text and voice messages, address books, calendars, photos and other useful functions can become liabilities if the device on which they are stored is lost or stolen.

- sensitive information on your mobile phone as well as the online data to which it grants automatic access.
- These data have the potential to endanger not only the device's owner, but everyone who appears in their address book, inbox or photo album.

DEVICE AND DATA ENCRYPTION

- Recent iOS devices have strong encryption turned on by default, as long as you set a strong passcode.
- Android supports device encryption as well, and you should enable it if you can. Remember to back up the contents of your smartphone before turning on full disc encryption in case there is a problem while the phone is encrypting itself.

SECURITY-RELATED SETTINGS FOR ANDROID

ACCESS TO YOUR PHONE

- Enable Lock SIM card, found under Settings -> Personal -> Security -> Set up SIM card lock.
- Set up a Screen Lock, found under Settings -> Personal -> Security -> Screen Lock, which will ensure that a code, pattern or password needs to be entered in order to unlock the screen once it has been locked.
- Set the security lock timer, which will automatically lock your phone after a specified time.

DEVICE ENCRYPTION

- Settings -> Personal -> Security -> Encryption

NETWORK SETTINGS

- Turn off Wi-Fi and Bluetooth by default. Ensure that Tethering and Portable Hotspots, under Wireless and Network Settings, are switched off when not in use.
- Settings -> Wireless & Networks -> More -> Tethering & Mobile hotspot.

LOCATION SETTINGS

- Switch off Wireless and GPS location (under Location Services) and mobile data (this can be found under Settings -> Personal -> Location).

CALLER IDENTITY

- If you want to hide your caller-ID, go to Phone Dialler -> settings -> Additional Settings -> Caller ID -> hide number.

SOFTWARE UPDATES

- The phone operating system: go to: settings -> About phone -> updates -> check for updates.
- Apps you have installed: Open the Play store app, from the side menu select My Apps.

Password policy

Password- Basics

- Choosing the right password

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.

- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.

- Don't use a word found in a dictionary, English or foreign.

- Never use the same password twice.

Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting e to 3, L or i to 1, o to 0. as in "z3r0-10v3"

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder

Bad Passwords

- Don't use passwords based on personal information such as: **name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address** etc. This includes using just part of your name, or part of your birthdate.

- Don't use passwords based on things located near you. Passwords such as **"computer"**, **"monitor"**, **"keyboard"**, **"telephone"**, **"printer"**, etc. are useless.

- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".

- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.
- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree".

Changing your password

- You should change your password regularly, I suggest once a month is reasonable for most purposes.
- You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- Remember, don't re-use a password

Protecting your password

- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell anyone your password, not even your system administrator
- Never send your password via email or other unsecured channel.
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

- Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. this is a very bad idea.
- Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

Bad Examples

- "fred8" - Based on the users name, also too short.
- "christine" - The name of the users girlfriend, easy to guess
- "kciredref" - The users name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists
- "merde!" - Listed in a foreign language dictionary

Good Examples

- None of these good examples are actually good passwords, always choose your own password don't just use somebody elses.

- "mItWdOtW4Me" - Monday is the worst day of the week for me.

How would a potential hacker get hold of my password anyway?

four main techniques hackers can use to get hold of your password:

Steal it:

- That means looking over your should when you type it, or finding the paper where you wrote it down.
- it's very important that if you do write your password down you keep the paper extremely safe.
- Also remember not to type in your password when somebody could be watching.

Guess it:

- people use a password based on information that can easily be guessed.
- Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.

A brute force attack:

- 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
- 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 process

- 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

- 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.

USING PASSWORD MANAGER

- Password managers are one of the best ways to store, back up and manage your passwords.
- A good password is hard to remember and that's where a password manager comes in handy.
- It encrypts all the different passwords that are saved with a master password, the only one you have to remember.
- USING PASSWORD MANAGER List