Topic: Physical security

• Assignment Level Basic

1. Why physical security needed?

Physical security has an important role to play in protecting critical information and data. With work and collaboration paradigm shifts, new cases of security threat arise.

The physical security structure consists of three main components: access control, permanent active surveillance and testing. The success of an organisation’s physical security program can often be attributed to how each of these components are implemented, improved, and maintained.

Physical Security definition

Physical security aims to protect people, property, and physical assets from any action or event that could lead to loss or damage. Physical security is crucial, and security teams must work together to ensure the security of digital assets.

Physical Security important

Physical security keeps your employees, facilities, and assets safe from real-world threats. These threats can arise from internal or external intruders that question data security.

**Physical attacks** can cause a safe area to break into or the invasion of a restricted area part. An attacker can easily damage or steal critical IT assets, install malware on systems, or leave a remote access port on the network.

It is important to have strict physical security to protect against **external threats**, as well as equally effective measures to avoid the risks of any internal intruder.

The key is to understand that **physical security refers to the entire space**, and it should not be restricted only to the front door, but to the entire building. Any area that is left unprotected – such as the smoking area (with doors for example facing the outside of the building, without the main entrance controls) or the entrance to the car park, can pose a risk.

Security experts refer to this form of protection as a deep or layered protection, since there are several control points in the physical infrastructures.

Physical damage is as harmful as digital loss, and therefore strict physical security measures must be taken.

1. what is physical security?

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events.

The physical security framework is made up of three main components: [access control](https://www.techtarget.com/searchsecurity/definition/access-control), surveillance and testing. The success of an organization's physical security program can often be attributed to how well each of these components is implemented, improved and maintained.

• Assignment Level Intermediate

1. list out the ways of physical security.

Physical security for the safety of personal computers is necessary to maintain computers in proper condition, prevent damages and improve efficiency.

Some of the basic measures like regular cleaning, organizing power cables, setting BIOS password, switching off computers when not in use go a long way in improving efficiency and longevity of the digital devices.

* Regularly clean your system and its components.
* (Note: Turn off your PC before cleaning it)
* Properly organize the power cables, wires to protect from water, insects etc.,
* While working with a personal computer,  be careful not to spill water or food items on it.
* Always follow the “Safely Remove” option while disconnecting the USB devices.
* By setting a BIOS password, you can prevent unauthorized access to your personal computer.
* (Note: To setup BIOS password refer “Setting password to BIOS” section)
* Switch off the computer when not in use.
* **Enable Auto-updates**of your Operating System  to update it regularly.
* **Download Antivirus Software**from a trusted website and install. Make sure it automatically gets updated with the latest virus signatures.
* **Download Anti-Spyware Software**from a trusted website and install. Make sure it automatically updates with the latest definitions.
* **Use “Encryption”**to secure your valuable Information.
* **Strong password**should be used for “**Admin**” Account on computer and for other important applications like email client, financial applications (accounting etc.,).
* **Periodically backup**your computer data on a CD/ DVD or a USB drive in case it may get corrupted due to hard disk failures or when reinstalling/formatting the system.
* Always **keep the recovery disk supplied by the Manufacturer/ Vendor**of the computer system to recover the Operating System in the event of boot failures.
* Startup programs should be monitored/ controlled for optimal system performance

2-How to protect system from malfunctioning due to electrical fluctuation?

Variations in an electrical power supply’s voltage or current levels are called power fluctuations. Numerous variables, including shifts in demand, issues with the machinery, or outside impacts like lightning strikes, might cause these fluctuations. Energy supply can become inconsistent or unstable due to power fluctuations, which could cause disruptions, equipment damage, or data loss. Using voltage regulators and surge protectors frequently reduces the consequences of power fluctuations.

You can take the following precautions to protect your electronics against power surges:

##### **Surge protectors :**

Use power strips or surge-protected protectors. During a power surge, these devices help in reducing and rerouting excess electricity, protecting linked electronics. Check that the surge protector has the proper joule rating and indication lights to check its functioning.

##### **Uninterruptible power supplies :**

Consider utilising a UPS to filter out voltage spikes or sags, and a UPS offers battery backup during power outages. It avoids data loss or hardware harm while enabling you to shut down devices safely.

##### **Surge protective devices:**

Install surge safety devices at the main electrical panel or distribution points in your house or place of business. With the help of these gadgets, your entire home is protected from power surges brought on by lightning strikes or changes in the utility system.

##### **Grounding :**

Make sure the grounding of your electrical system is proper. A conduit for extra electrical energy to dissipate is provided through grounding, which lowers the likelihood of power surges. Speak with an authorised electrician to check the integrity of your electrical system’s grounding.

##### **Disconnect during storms :**

Unplug delicate electronic equipment during thunderstorms or when severe weather is anticipated. Utility wires can experience power spikes due to lightning strikes, endangering the associated equipment.

##### **Insurance :**

If power surges cause damage, consider getting equipment breakdown insurance or surge protection coverage.

It is essential to ensure the security of your gadgets during power fluctuations. You can reduce the risks brought on by power fluctuations by taking proactive measures like using surge protectors, using uninterruptible power supplies (UPS), installing surge protective devices (SPDs), ensuring proper grounding, disconnecting during storms, taking insurance coverage into account, and performing routine maintenance. By accepting these precautions, you can protect your electronics from voltage spikes and dips and ensure they function correctly, even under unstable power conditions.

Topic: Firewall settings .

• Assignment level basic:

1. What is firewall ?

A firewall is a computer network security system that restricts internet traffic in to, out of, or within a private network.

This software or dedicated hardware-software unit functions by selectively blocking or allowing data packets. It is typically intended to help prevent malicious activity and to prevent anyone—inside or outside a private network—from engaging in unauthorized web activities.

Firewalls can be viewed as gated borders or gateways that manage the travel of permitted and prohibited web activity in a private network. The term comes from the concept of physical walls being barriers to slow the spread of fire until emergency services can extinguish it. By comparison, network security firewalls are for web traffic management — typically intended to slow the spread of [web threats](https://www.kaspersky.com/resource-center/threats/web).

Firewalls create 'choke points' to funnel web traffic, at which they are then reviewed on a set of programmed parameters and acted upon accordingly. Some firewalls also track the traffic and connections in audit logs to reference what has been allowed or blocked.

Firewalls are typically used to gate the borders of a private network or its host devices. As such, firewalls are one security tool in the broader category of user access control. These barriers are typically set up in two locations — on dedicated computers on the network or the user computers and other endpoints themselves (hosts).

2. Why is firewall needed?

A firewall is a crucial component of network security that acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. Its primary purpose is to monitor and control incoming and outgoing network traffic based on predetermined security rules. Here are several reasons why a firewall is needed:

1. **Network Security:**
   * **Unauthorized Access Prevention:** Firewalls help prevent unauthorized access to a network by monitoring and controlling incoming and outgoing traffic. They act as a barrier that filters out potentially harmful data packets.
   * **Intrusion Detection and Prevention:** Firewalls can detect and block suspicious activities, such as hacking attempts or malicious software trying to infiltrate the network.
2. **Data Protection:**
   * **Confidentiality:** Firewalls protect sensitive data from being accessed or stolen by unauthorized users or malicious software.
   * **Integrity:** By controlling the flow of data, firewalls ensure that information is not altered or tampered with during transmission.
3. **Malware Defense:**
   * **Virus and Malware Prevention:** Firewalls can block or filter out known malware, viruses, and other malicious software, preventing them from entering the network and infecting systems.
4. **Content Filtering:**
   * **Controlled Access to Websites and Content:** Firewalls can be configured to block access to certain websites or types of content, helping organizations enforce acceptable use policies and protect against potentially harmful or inappropriate material.
5. **Network Performance Optimization:**
   * **Bandwidth Management:** Firewalls can optimize network performance by regulating the flow of traffic, preventing bandwidth-intensive activities that could negatively impact overall network speed and performance.
6. **Logging and Monitoring:**
   * **Activity Monitoring:** Firewalls provide logs and reports on network activities, helping administrators identify potential security threats, track user behavior, and investigate security incidents.
7. **Compliance Requirements:**
   * **Regulatory Compliance:** Many industries and organizations are subject to regulatory requirements that mandate the implementation of firewalls and other security measures to protect sensitive information and maintain compliance with data protection standards.
8. **Remote Access Security:**
   * **Virtual Private Network (VPN) Support:** Firewalls often include VPN functionality to secure remote connections, allowing employees to access the network securely from remote locations.

In summary, firewalls are essential for safeguarding networks, protecting sensitive data, and maintaining the overall security and integrity of computer systems in the face of evolving cyber threats.

• Assignment level Intermediate:

1-What are the features of firewall?

## Top Firewall Features

Traditional [firewalls](https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/) were designed to protect traditional networks against traditional cyber threats. As organizations’ networks and the cyber threat landscape grow and evolve, [network firewalls](https://www.checkpoint.com/cyber-hub/network-security/what-is-network-firewall/) require additional functionality and features to ensure the security of the company’s network and the sensitive data that it contains.

Below, we list the top 5 features:

### 1. Unified Security Management

Organizations must cope with rapidly increasing [network security](https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/) complexity. Most companies’ networks are growing larger and more complex as mobile devices, cloud deployments, and Internet of Things (IoT) devices join traditional user workstations and on-premises servers on the corporate network. At the same time, cyber threats are becoming more sophisticated and numerous. As a result, companies must deploy, monitor, and maintain a growing array of security solutions to manage their cyber risk.

An organization’s [next-generation firewall](https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/) should help to alleviate security complexity, not contribute to it. A firewall with integrated Unified Security Management (USM) functionality enables an organization’s security team to easily and efficiently manage and enforce security policies across their entire network environment. This allows the security team to keep up with the company’s expanding digital attack surface and minimize the organization’s cyber risk.

### 2. Threat Prevention

The longer that a cyber threat has access to an organization’s network, the more expensive it will be to remediate it. Cyberattacks can cause damage and additional expense in a number of different ways. Exfiltration of sensitive data can result in legal and regulatory penalties, ransomware can decrease productivity and cause a loss of profits, and even simple malware often has persistence mechanisms designed to make it difficult and time-consuming to remove from a system.

Minimizing the damage that a cyberattack can cause to a network requires threat prevention. By identifying and blocking an attack before it crosses the network boundary, an organization nullifies the threat it poses to the network. This is why a network firewall with integrated threat prevention functionality – including anti-phishing, anti-malware, anti-bot, and integration with high-quality threat intelligence feeds – is an essential component of an organization’s cybersecurity strategy.

### 3 - Application and Identity-Based Inspection

Digital transformation efforts mean that an organization’s network landscape is constantly evolving. New applications are deployed on the corporate network to accomplish certain goals, and others are phased out when they become obsolete. Different applications require different policies. Some applications may be high-priority traffic, while others should be blocked, throttled, or otherwise managed on the network. An organization’s next-generation firewall should be capable of identifying the application that generates a particular stream of traffic and applying application-specific policies to that traffic.

Organizations are also composed of a number of individuals with different job roles and responsibilities. An organization’s security policies should also be configurable based upon the identity of the user. Employees within an organization should have access to different systems and be able to use varying sets of applications. A firewall should support policy creation and enforcement based upon user identity.

### 4 - Hybrid Cloud Support

Almost all organizations are using cloud computing, and the vast majority are using a hybrid cloud deployment. Private and public cloud deployments have different security requirements, and it is necessary for an organization to be able to enforce consistent security policies across cloud-based environments hosted by multiple vendors.

For this reason, an organization’s next-generation firewall should incorporate hybrid cloud support. The firewall should be easily deployable and scalable in any major cloud environment and enable an organization’s security team to manage all of their security settings from a single console. According to Gartner, [99% of cloud security failures through 2025 will be the customer’s fault](https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/), a problem that the company’s firewall should help the organization to avoid.

### 5- Scalable Performance

Many organizations have transitioned to cloud-based infrastructure due to its increased scalability and flexibility. Ultimately, we want the benefits of the cloud, in the cloud and on-premises. In the cloud this simply means choosing a NGFW template. In regards to on-premises, this means looking beyond legacy HA clustering solutions.

Hyperscale is the ability of an architecture to scale appropriately as increased demand is added to the system. This involves the ability to seamlessly provision and add more resources to the system that make up a larger distributed computing environment. Hyperscale is necessary to build a robust and scalable distributed system. In other words, it is the tight integration of storage, compute, and virtualization layers of an infrastructure into a single solution architecture.

2-Describe types of firewall

Firewalls are essential network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules. There are several types of firewalls, each with its own characteristics and functionalities. The main types of firewalls include:

1. **Packet Filtering Firewalls:**
   * **Description:** Packet filtering is the most basic form of firewall protection. It examines packets of data and makes decisions to allow or block them based on predefined rules.
   * **How it works:** Filters packets based on criteria such as source and destination IP addresses, port numbers, and protocols. It operates at the network layer (Layer 3) of the OSI model.
   * **Limitations:** Limited in its ability to inspect the contents of data packets.
2. **Stateful Inspection Firewalls:**
   * **Description:** Also known as dynamic packet filtering, these firewalls keep track of the state of active connections and make decisions based on the context of the traffic.
   * **How it works:** Monitors the state of active connections and allows or denies traffic based on the state table. This adds a layer of intelligence compared to packet filtering firewalls.
   * **Advantages:** Offers better security by considering the state of connections.
3. **Proxy Firewalls (Application Layer Firewalls):**
   * **Description:** Operate at the application layer (Layer 7) of the OSI model. They act as intermediaries between client and server, forwarding requests on behalf of the client.
   * **How it works:** Receives requests from clients, forwards them to servers, receives responses, and then sends them to clients. It hides the internal network structure and can perform content filtering.
   * **Advantages:** Provides a high level of control over specific applications and content.
4. **Circuit-Level Gateways:**
   * **Description:** Works at the session layer (Layer 5) of the OSI model. It monitors the sessions or connections between computers, but it does not inspect the content of the packets.
   * **How it works:** Verifies the legitimacy of the connections and makes decisions based on session information.
   * **Advantages:** Efficient for allowing or blocking entire sessions.
5. **Next-Generation Firewalls (NGFW):**
   * **Description:** Integrates features of traditional firewalls with additional security functions such as intrusion prevention, deep packet inspection, and application-layer filtering.
   * **How it works:** Combines traditional firewall capabilities with advanced security technologies to provide a more comprehensive defense against modern threats.
   * **Advantages:** Enhanced security through advanced features and better visibility into network traffic.
6. **Hardware Firewalls:**
   * **Description:** Dedicated physical devices that provide firewall protection. Often used as the primary defense at the perimeter of a network.
   * **How it works:** Implemented in hardware and can offer high-performance filtering.
   * **Advantages:** Typically more robust and efficient for large-scale deployments.
7. **Software Firewalls:**
   * **Description:** Software-based firewalls that run on general-purpose operating systems. Can be installed on individual devices or as part of network operating systems.
   * **How it works:** Utilizes software to control and monitor network traffic based on predefined rules.
   * **Advantages:** Flexible and can be implemented on various platforms.

Organizations often use a combination of these firewall types to create a layered security approach, known as defense-in-depth, to protect their networks from a wide range of cyber threats.

• Assignment level advance:

1-Do a practical to allow anydesk through firewall.

Yes , we are complete done a practical to allow anydesk through firewall .

Allowing AnyDesk through your firewall can be practical if you need to use the AnyDesk remote desktop software for legitimate purposes. AnyDesk uses specific ports and protocols for communication, and allowing it through your firewall ensures that the software can establish connections between computers.

Here are the general steps to allow AnyDesk through a firewall:

1. **Open AnyDesk Ports:**
   * AnyDesk primarily uses ports 7070 and 6568. Make sure these ports are open on your firewall.
   * You may need to configure your firewall settings to allow incoming and outgoing connections on these ports.
2. **Configure Firewall Rules:**
   * Access your firewall settings and create rules to allow traffic on the specified ports.
   * This process varies depending on the firewall software or hardware you're using.
3. **Whitelist AnyDesk Executable:**
   * In addition to opening ports, you might need to whitelist the AnyDesk executable file. The specific file may vary based on your operating system.
4. **Consider Security:**
   * While allowing AnyDesk, always consider security implications. Only allow the necessary ports and protocols, and be cautious about allowing remote access to your computer.
5. **Network Policy:**
   * If you are part of a larger network, such as a corporate environment, consult with your IT department or network administrator before making changes to firewall settings.

Always ensure that you are following security best practices and only allow traffic that is necessary for your use case. Unauthorized or unrestricted access through firewalls can pose security risks. If you're unsure about the steps or the security implications, it's a good idea to seek assistance from your IT department or a knowledgeable professional.

2-do a practical to turn off the services of firewall.

Yes , we are complete a practical to turn off the services of firewall .

Turning off the firewall services on your computer or network can have serious security implications and is generally not recommended unless you have a specific and well-understood reason for doing so. Firewalls play a crucial role in protecting your system from unauthorized access, malware, and other security threats.

Here are some reasons why it's not practical to turn off the firewall services:

1. **Security Risk:** The primary purpose of a firewall is to act as a barrier between your computer and the outside world, filtering incoming and outgoing traffic based on a set of predetermined rules. Disabling the firewall removes this layer of protection, exposing your system to potential security threats.
2. **Malicious Attacks:** Without a firewall, your computer becomes more vulnerable to various types of cyber attacks, such as hacking attempts, viruses, worms, and other malware. A firewall helps block unauthorized access and prevents the spread of malicious software.
3. **Data Protection:** Firewalls help safeguard sensitive data on your computer by controlling the flow of information in and out of your network. Disabling the firewall increases the risk of unauthorized access to personal or confidential information.
4. **Network Vulnerabilities:** If your computer is part of a larger network, disabling the firewall can potentially expose other devices on the network to security risks. This is especially important in business or organizational settings where network security is critical.
5. **Built-In Protections:** Modern operating systems come with built-in firewalls that are designed to work seamlessly with the system. Disabling these services may undermine the security features that are integrated into the operating system.

If you are experiencing issues with certain applications or services due to the firewall, it's generally better to configure the firewall settings to allow the necessary traffic rather than turning off the entire firewall. Most firewalls allow you to create exceptions or rules to permit specific types of traffic while still maintaining overall security.

In summary, it's strongly advised to keep your firewall enabled to ensure the security and integrity of your computer or network. If you have concerns about specific issues, it's recommended to seek guidance on properly configuring the firewall settings rather than completely disabling this important security feature.

3-Do a practical to block ip messenger to access the network

Yes , we are complete a practical to block ip messenger to access the network .

Blocking IP Messenger or any application from accessing a network can be practical in certain situations, depending on your organization's policies, security requirements, and the reasons behind the decision. IP Messenger is a peer-to-peer messaging application commonly used in local networks, and there may be legitimate reasons to restrict its usage. Here are some considerations:

1. **Security Concerns:**
   * **Malicious Use:** If there are concerns about the potential misuse of IP Messenger for spreading malware, transferring sensitive information, or other malicious activities, blocking it may be justified.
   * **Vulnerabilities:** If the application has known vulnerabilities that could be exploited, blocking it can help mitigate potential security risks.
2. **Productivity and Bandwidth Management:**
   * **Distraction:** In some cases, organizations may choose to block IP Messenger to prevent employees from using it for non-work-related conversations and distractions.
   * **Bandwidth Usage:** If the application consumes a significant amount of network bandwidth, blocking it can help in managing overall network performance.
3. **Corporate Policies:**
   * **Policy Compliance:** If the use of specific applications is against your organization's policies, blocking them can help enforce compliance.
   * **Confidentiality:** If your organization deals with sensitive information, restricting the use of certain messaging applications can help maintain confidentiality.
4. **Alternative Communication Channels:**
   * **Encouraging Official Channels:** If there are official communication tools in place, blocking unauthorized applications may encourage employees to use approved channels for work-related communication.
5. **Legal and Ethical Considerations:**
   * **Legal Compliance:** Ensure that blocking IP Messenger or any other application complies with local laws and regulations.
   * **Ethical Considerations:** Consider the ethical implications and employee privacy concerns associated with blocking communication tools.
6. **User Awareness and Communication:**
   * **Informing Users:** If you decide to block IP Messenger, communicate the reasons to users to avoid confusion and frustration.
   * **Providing Alternatives:** If possible, provide alternative communication tools that are approved for use within the organization.
7. **Network Configuration:**
   * **Firewall Rules:** Implement firewall rules or use network-level solutions to block the specific ports or IP addresses associated with IP Messenger.

It's important to note that blocking applications should be done judiciously and with a clear understanding of the potential impact on users and business operations. Additionally, regular security audits and updates to policies should be conducted to adapt to changing security landscapes and technology environments.