Module 6. Network security, Maintenance and Troubleshooting procedures

Topic: A SOHO Networks

1. **What is the SOHO network?**
    - SOHO stands for small Office / Home Office. It refers to a type of computer network commonly used in small offices or home offices. SOHO networks are designed to be easy to set up and manage, while providing basic networking functions such as file sharing, printing, and internet access.

2. **What does SOHO mean networking?**
    - SOHO network is generally designed to be simple and easy to setup and manage. They usually have multiple computers, a router or switch, and a broadband modem, and are mostly used for basic communications such as file sharing, printing, and internet use.

3. **How does a SOHO network work?**
    - Here's how a SOHO network Works:
    - **Connected devices:** Devices are connected wirelessly using an Ethernet cable or a Wi-Fi network.
    - **Internet Access:** The modem provides internet access over the service provider's network.
    - **Router Configuration:** The router is configured with internet connection details and network settings such as ip address and subnet mask.
    - **Device Configured:** Each device is configured to use a network configuration, such as assigning a unique IP address and subnet mask.
    - **Communication:** Devices can communicate with each other through a router that allows data sharing, printing, and other networking functions.
    - **Security:** A router may include security features such as a firewall to protect the network from unauthorized access.
    - **Maintenance:** Updates and troubleshooting are available via the router's web interface or network maintenance software.

4. **Issues with SoHo Networking?**
    - It can have many issues such as limitations, poor security, limited network performance, limited performance, reliability issues, and limited support options. Therefore, it is important to consider these factor when designing and Implementing a SOHO network

5. **How small is the "S" in SOHO?**
    - The "s" in SOHO also means "small" in this context, emphasizing that the hardware and software are designed to meet the needs of small operations. SOHO network equipment typically includes router, switches, and firewalls, as well as network attached storage devices are generally smaller and simpler in size and complexity than business communication devices, making them easier to use and install for businesses, small and home offices.

6. **SOHO Routers vs. Home Routers?**
    - SOHO routers are generally more powerful and efficient than home routers. It is designed to support multiple users and provide a high level of network connectivity. They often include advanced security features such as VPN support and firewalls to help protect sensitive data and prevent unauthorized network access.
    - Home routers, on the other hand, are generally simpler and less expensive. It is designed for small homes or home offices with fewer users and network connections. They usually don't include as many features as SOHO routers, but they are easy to set up and use.

Topic: NAT & PAT

Module 6. Network security, Maintenance and Troubleshooting procedures

1. **What is NAT?**
   - NAT stands for Network Address Translation, Which is a technique used to allow multiple devices on a private network to share a single IP address.
2. **What is PAT?**
   - PAT stands for Port Address Translation and is a modification to NAT that allows multiple devices on a private network to share individual IP addresses using different ports.

3. **However, Will Nat work?**
   - NAT works by changing the IP address of packets leaving the private network and replacing it with the public IP address of the NAT device. The NAT device then maintains a table that maps private IP addresses of network devices to public IP addresses and uses this message to route traffic to the correct devices on a private network.

4. **Explain NAT?**
   - NAT devices sit between the private network and the internet and update the location and/IP address of files as they pass through them. When a private device sends data to the internet, the NAT will replace the IP address of the data packet with its own IP address in the community. NAT also manages to map private IP addresses to public IP addresses so that packets can be routed to the correct devices on the private network.
   - NAT is two type
   - 1. Static NAT 2. Dynamic NAT

5. **What is the difference between Static & Dynamic NAT?**

Feature	**Static NAT**	**Dynamic NAT**
Mapping	One-to-One	Many-to-Many
IP Assignment	Fixed	Dynamic
Configuration	Manual	Automatic
Address Pool	Not Required	Required

Scalability	Limited	High
Security	Hosting Server	General Internet Access

6. **NAT stands for?**
    - Network Address Translation.

7. **PAT stands for?**
    - Port Address Translation.

Topic: Authentication and Access Control

1. **What Is ACl?**
    - ACL stands for Access Control List. A set of rules defined on a network, such as a router or firewall, to filter and control network traffic. ACLs are used to allow or deny traffic based on deny traffic based on criteria such as source IP address, destination IP address, protocol type, and port number.

2. **What Are Different Types of Acl?**
    - There are Three types of ACL
    - 1. Standard ACL
    - 2. Extended ACL
    - 3. Named ACL

3. **Explain Standard Access List?**
    - A Standard Access list is set of rules that filter traffic based on the IP address of the packet. It means using a number from 1 to 99 and is used to allow or deny access to the network based on the IP address of the IP address of the packet. They are often used to prevent certain hosts or network from accessing certain resources.

4. **Explain Extended Access List?**
    - An extension list is a set of rules that control access to network resources based on various factors such as location and IP address, port number, and protocol type. It means using numbers from 100 to 199 for further filtering. Extended ACLs provide more flexibility than standard ACLs as they can filter traffic based on various factors such as source IP address, port number, and protocol type. They are often used in mesh networks to control access to certain applications and services and to block unwanted traffic from unknown sources. However, extended ACLs can be difficult to configure and manage and can affect network performance if not set properly.

5. **What Is a Wildcard Mask?**
    - A wildcard mask is a 32-bit value used with an IP address to specify multiple IP addresses for connectivity and filtering. Specifies which part of the IP address should be ignored when comparing the IP address with other addresses. Wildcard masks are often used in access control lists to define a set of IP addresses to allow or deny access to network resources. However, they are not the same as subnet masks and should not be used interchangeably.

6. **In Which Directions We Can Apply an Access List?**
    - Access list can be used inbound or outbound to the interface to filter traffic before or after it is sent to the external interface. Using the inbound ACLs helps prevent attacks from outside the network, while using it externally helps prevent attacks from outside the network. The implementation aspect of the ACL depends on the specific requirements of the network. Access lists should be used as close to the traffic center as possible to minimize the impact of unwanted traffic on the network.

Topic: WAN Technologies

1. **Fiber-optic communication**
   - Fiber optic communication is a method of sending light through optical fibers to transfer data from one place to another. Fiber optics are made of glass or plastic and are designed to carry light over long distances without losing too much signal strength.

2. **What is a Leased Line?**
   - A leased line, also known as a leased line or leased line, is a telecommunications net work that provides a shared, fixedbandwidth connection between two locations. A communication line received by an organization from a service provider (usually a telecommunications company).

3. **Explain Circuit switching**
   - Circuit switching is a communication method in which physical communication is established by two devices or nodes talking to each other. This means that resources such as bandwidth, capacity, and transmission are private to both nodes throughout t he entire session, regardless of whether data is sent or not.

4. **Explain Packet Switching**
   - Packet switching is a communication method in modern computer networks and the Internet where data is transmitted in small discrete units called packets. These packages are not only the information to be sent, but also the address, address and other information required for delivery.
   - Packet swapping involves breaking data into smaller packets and sending them independently over the network. Each packet is sent separately and will follow a different path to its destination. The packet is then reprocessed at the receiving end to reconstruct the original data.

5. **What is the difference between leased line and broadband?**
   -

	Leased Line	Broadband
Bandwidth	**Dedicated, guaranteed, symmetrical bandwidth**	**Shared, asymmetrical bandwidth**
Cost	**Expensive**	**Relatively inexpensive**
Reliability	**Highly reliable, consistent performance**	**Prone to fluctuations and external factors**
Use Case	**Best for large organizations that require high-speed, reliable connectivity between locations**	**More suitable for smaller businesses or individuals who require moderate bandwidth and lower costs**
Service level Agreement (SLA)	**Typically includes an SLA with guaranteed uptime, latency, and packet loss**	**May or may not include an SLA and may have less stringent uptime and performance guarantees**
Installation charge	**Longer installation time due to the need for physical cabling and setup**	**Faster installation time as it often involves using existing infrastructure and plug-and-play setup**

6. **How much is a 100mb Leased Line?**
   - 100mb line rental fee may vary depending on many factors such as location, service provider and connection type. As a rough estimate, the monthly cost of 100mbps leased lines in India annually charges can range from INR 20,000 to INR 50,000 or more depending on the conditions mentioned above.

Module 6. Network security, Maintenance and Troubleshooting procedures

7. **Difference between a POTS line and a leased line?**
    -

Feature	**POTS Line**	**Leased line**
Connection Type	Analog	Digital
bandwidth	56kbps	2mbps or higher
reliability	Unreliable and subject to interference	Highly reliable and consistent
Usage	Basic voice communication and low-speed data transfer	High-speed data transfer and mission-critical applications
Cost	Inexpensive	Expensive
Installation	Easy to install, available almost everywhere	Complex installation process, limited availability in certain areas
Maintenance	Minimal maintenance required	Regular maintenance required
Security	Less secure due to vulnerability to wiretapping and eavesdropping	More secure due to encryption and dedicated connection
Speed	Slow speed, limited capacity for data transfer	High speed, dedicated bandwidth for data transfer
Availability	Available to the general public	Usually leased to businesses and organizations

8. **What is the process of packet switching?**
    - Packet switching is a method of sending data over a network by dividing it into smaller packets and sending them to their individual destinations. The packet exchange process is detailed as follows:

    - **Packing**: Data is divided into small packets, usually 1000-1500 bytes, to be transmitted over the network.

- **Routing:** Each packet is assigned an address, which can be an address or an IP address that determines the route it will follow on the network.

- **Relay:** Each packet is sent to its destination via multiple transfers, which are the devices responsible for delivering the packet to the appropriate destination.

- **Forwarding:** When the package reaches its final destination, it is repackaged in its original form and forwarded to the recipient.

- **Confirmation:** The receiver sends a confirmation to the sender that the package has been received successfully.

- **Error handling:** If a problem occurs during transmission, such as packet loss or damage, the sender is notified and the packet is returned.

- packet switching is designed to be fast, efficient and reliable. Packet switching is fast and reliable, by splitting data into smaller packets and sending them separately over the network, making more efficient use of network resources and speeding up data transmission.

9. Difference between circuit switching and packet switching?

-

Feature	**Circuit Switching**	**Packet Switching**
Connection Setup	Dedicated connection established before data transmission	No dedicated connection required
Resource allocation	Dedicated resources allocated for the entire duration of the connection	Resources dynamically allocated as needed

Data Transmission	Data transmitted as a continuous stream	Data broken down into smaller packets and transmitted individually
Delay	Delay introduced at the beginning of connection setup	Delay introduced due to packetization and reassembly of data
Efficiency	Less efficient, cannot transmit multiple connections at once	More efficient, can transmit multiple packets simultaneously
Network Topology	Commonly used in point-to-point networks	Used in both point-to-point and multipoint networks
Cost	Typically more expensive due to the need for dedicated resources	Typically less expensive due to dynamic resource allocation
Error Handling	Built-in error checking and correction mechanisms	Relies on higher-level protocols to handle errors
Traffic management	Limited traffic management capabilities	Sophisticated traffic management and QoS mechanisms

10. Practice on printer sharing

- Select the Start button, then select Settings > Devices > Printers & scanners.
- Choose the printer you want to share, then select Manage.
- Select Printer Properties, then choose the Sharing tab.
- On the Sharing tab, select Share this printer.
- If you want, edit the share name of the printer. You'll use this name to connect to the printer from a secondary PC.

11. **Use of IIS [Via "add and remove" feature from control panel. "appwiz.cpl" command**
    - Using "appwiz.cpl" command:
    - Press the "Windows" key + "R" key to open the Run dialog box.
    - Type "appwiz.cpl" and press "Enter".
    - Click on "Turn Windows features on or off" link.
    - Scroll down and find "Internet Information Services" in the list of features.
    - Expand the "Internet Information Services" option and select the features you want to install (such as Web Server, FTP Server, etc.).
    - Click "OK" to install the selected features.

Topic: Communication technologies Cloud and Virtualization

1. **What is virtualization?**
    - Virtualization is the process of using software to create virtual physical devices such as servers, operating systems, networks or storage devices. Virtual versions, also known as virtual machines (VMs), are created on top of physical infrastructure and are designed to operate and behave like physical capabilities.
2. **What are two types of virtualization in cloud?**
    - Two types of virtualization in cloud
    - 1. Server virtualization
    - 2. Network virtualization
3. **What are the two types of virtualization?**
    - **Full virtualization:** In this type of virtualization, a hypervisor or virtual machine monitor (VMM) is used to create an environment that can host multiple operating systems and applications. Each virtual machine (VM) overwrites the hypervisor, which acts as the underlying hardware and controls access to the host's resources. Full virtualization provides maximum isolation and security, but can also incur some performance overhead due to the need to process the hardware.

    - **Paravirtualization:** In this type of virtualization, guest operating systems know they are running in a virtual machine and interact directly with the host to access the host's resources. This approach can provide better performance than the full implementation because the administrator does not need to keep track of the

hardware, but needs to update the guest's work to be aware of the virtualization process.Paravirtualization is very useful in computing where performance matters.

4. **What is VMware virtualization technology?**
    - VMware is a company that provides virtualization technology, including software products and services that enable organizations to create and manage virtual machines (VMs) and virtualized infrastructure. VMware's virtualization technology uses a type 1 hypervisor (also known as a bare metal hypervisor) to create multiple virtual machines on a single host.

5. **What is the difference between cloud and virtualization?**
    - Virtualization is a technology that enables more efficient sharing and use of resources by allowing multiple virtual machines to run on a single physical machine. It provides the ability to create a virtualized environment that can run multiple operating systems and applications on a physical server, helping to reduce and simplify hardware costs.

    - Cloud computing is a service that provides on-demand services for computing resources such as storage, processing, and Internet access. Cloud computing relies on virtualization to resource users, but also includes additional services such as self-service, auto-scaling, and pay-as-you-go.

6. **What are the benefits of implementing virtualization in cloud computing?**
    - Virtualization is an important technology that allows cloud computing to provide many benefits to users, including:

    - Performance Improvements: Virtualization allows multiple virtual machines (VMs) to run on a physical server, which means more efficient use of resources. This helps reduce hardware costs and increases capacity as additional VMs can be added as needed.

- Cost Savings: Virtualization allows multiple VMs to run on a single physical server, reducing the number of physical servers needed to support operations. This means businesses can save on equipment and building costs and reduce electricity and air conditioning costs.

- Flexibility: Virtualization makes it easy for businesses to move offices between servers and data centers and even between cloud providers.
- This makes it easy to increase or decrease resources as needed without worrying about physical limitations.

- Enhanced Security: Virtualization provides a layer of security by isolating VMs from each other and from the core of the physical infrastructure. This means that if one virtual machine is affected, it will not affect other virtual machines on the same physical server.

- Disaster Recovery: Virtualization facilitates the implementation of disaster recovery strategies because virtual machines can be quickly migrated to other physical servers or data centers in the event of a disaster or destruction.

Topic: Monitoring Tools

1. **Why are network monitoring tools used?**
    - Network monitoring tools are used to identify and analyze network problems, increase network security, analyze and improve network connectivity, prepare for possible future needs, and ensure compliance with regulatory requirements. They help network administrators maintain network health and security and ensure that network services are used efficiently and effectively.

Module 6. Network security, Maintenance and Troubleshooting procedures

2. **Explain firewalls**
    - A firewall is a security device that creates a barrier between the internal network and the outside world, monitoring and controlling the traffic in and out of the network to protect from unauthorized access, hacking and other security threats. They use a variety of techniques to filter and control network traffic, such as packet filtering, state inspection, and application-level gateways. Firewalls can be implemented as software, hardware, or a combination of the two, and can be implemented around the network, between segments, or on the host. A firewall is an essential tool for the security and integrity of the computer network.

3. **Explain core switches**
    - The core switch, the central hub of the network, connects multiple switches and access points. It is responsible for sending a lot of traffic between different segments and usually runs at a very high speed.

    - core switches are typically used in large enterprises, data centers or service providers. It is designed to provide a high level of reliability, repeatability and availability by providing fast and efficient network connectivity.

    - core switch also provides excellent features such as quality of service (QoS) and priority operation, allowing network administrators to prioritize certain traffic.

    - This ensures that applications and critical services receive the required bandwidth and priority even at high connection times.

    - In addition, key switches are designed to support communication protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) used for traffic between different locations.

4. **Explain client systems**
   - A client is a computer or device that accesses and uses resources or services provided by a server or network. In the client-server model, the client is the device or application that requests data or services from the server. Examples of
   - user devices include PCs, laptops, smartphones, tablets and other connected devices. These systems usually run client software or applications that allow them to communicate with the server and access the resources or services it provides.
   - Clients can store and manage local information such as files, documents, and user preferences, as well as requesting information and services from servers.

5. **What is network management?**
   - Network administration is the process of managing and controlling computer networks. It includes monitoring, maintenance, configuration and optimization of network resources and services to ensure their availability, reliability and security.
   - Network administration includes tasks ranging from simple tasks such as monitoring network activity and responding to alerts, to complex tasks such as configuring network devices and implementing designed security measures.
   - Network management includes network monitoring, performance management, error management, configuration management, security management, and cost management.
   - Network management can be done manually, but this usually requires specialized software tools and systems.
   - These tools automate many of the tasks involved in network administration, making it easier for network operators to manage and manage complex communications.

6. **Explain Event Viewer**
    - Event Viewer is a Microsoft Windows tool that allows users to view and manage event logs and logs. It provides a central place to view information about various system events, including errors, warnings, and instructions.

    - You can access the Event Viewer by typing "Event Viewer" in the Windows Search bar or by opening the Control Panel and selecting System and Security and then Administrative Tools.

    - Event Viewer displays various event categories such as Application, Security, Settings, and System. Each group has an event log with detailed information about the event.

    - Users can filter events by date, event level, location, and other criteria to narrow their search to specific events. Event Viewer also provides advanced features to create custom views and filter by specific keywords or event IDs.

    - Administrators and technicians use Event Viewer to troubleshoot and identify system problems. For example, if a system error or warning message appears, you can view it in Event Viewer to help diagnose and fix the problem. By analyzing conditions in the body, experts can identify the cause of the problem and take steps to correct it.

7. **Practice "parental control" or "family safety" option in control panel**
    - Certainly, here are the steps to set up parental controls or family safety in Windows 10:
    - 1. Open the Start menu and click on the Settings gear icon.
    - 2. In the Settings window, click on "Accounts."
    - 3. Click on "Family & other users" in the left-hand pane.
    - 4. If you haven't already, you will need to set up a Microsoft account for your child. Click on "Add a family member" and follow the prompts to create a child account.
    - 5. Once the child account is set up, click on "Manage family settings online" to access the Microsoft Family Safety website.
    - 6. In the Family Safety website, select the child's account and customize the settings according to your preferences.
    - 7. Under the "Activity" tab, you can view the child's activity reports, including websites they visited, apps and games they used, and screen time.
    - 8. Under the "Content restrictions" tab, you can set up filters for apps, games, and websites based on age appropriateness and content type.
    - 9. Under the "Screen time" tab, you can set limits for the amount of time your child can spend on the computer each day.
    - 10. Once you have customized the settings, click on "Save" to apply the changes
    - That's it! The parental controls or family safety settings you set up will now be applied to the child's account on the computer.

Topic: Network Security, Network vulnerabilities

1. **What are network vulnerabilities?**
    - A network vulnerability is a vulnerability or weakness in a computer network that an attacker can exploit to gain unauthorized access or compromise the integrity or availability of the network. Vulnerabilities can be caused by outdated software, missing passwords, faulty hardware, phishing attacks, malware, and social engineering. Vulnerabilities can be identified through vulnerability assessment or penetration testing and should be addressed through security patches, modifications or other exploit risk mitigation strategies.

2. **What are the types of network security attacks?**
    - There are many types of network security attacks such as malware attacks, phishing attacks, denial of service (DoS) attacks, man-in-the-middle (MitM) attacks, SQL injection attacks, password attacks, malware attacks, and DNS spoofing attacks. . These attacks can be used to prevent, disrupt or gain unauthorized access to a network or system. It is important to be aware of these threats and take appropriate measures to prevent them. This includes security measures such as firewalls, antivirus software, and intrusion detection systems, as well as regular security audits and employee security training.

3. **What is virus in network security?**
    - A network security virus is a type of malware designed to infect a computer or network and spread from one to another. Viruses often send themselves to legitimate services or files and can infect via email links, compromised websites, or removable media such as USB drives. When a virus infects a system, it can cause a lot of damage, including deleting files, stealing personal information, or infecting other systems.

4. **What is the difference between virus and antivirus?**
    - A virus is malware designed to infect a computer or network and spread from one to another. Viruses often send themselves to legitimate services or files and can infect via email links, compromised websites, or removable media such as USB drives. When a virus infects a system, it can cause a lot of damage, including deleting files, stealing personal information, or infecting other systems.
    - Antivirus software, on the other hand, is a software program designed to detect, prevent, and remove viruses and other malware from a computer or network. Antivirus software works by analyzing files and programs to identify malware patterns and monitor operating systems for signs of infection.
    - When a virus is detected, antivirus software can isolate or delete infected files, preventing the virus from spreading to other systems.

5. **Who is vulnerable in network security?**
    - In network security, a single computer or network can pose a security threat. This includes individuals, businesses, organizations and governments. However, some groups may be more vulnerable than others, depending on factors such as the size and complexity of their networks, the type of data they hold, and the security measures in place.

    - Here are some examples of groups that may be particularly vulnerable to network security threats:

    - Small businesses: Small businesses may not have the same resources to invest in security measures as large companies, making them a prime target for hackers.

    - Home Users: People using personal computers or home networks may not be aware of online security and may be more vulnerable to fraud, malware scares and other threats.

    - Government: Government agencies are often targeted by cybercriminals and national actors who want to steal sensitive information or disrupt operations.

    - Healthcare Organizations: Doctors and organizations that process sensitive patient information are often targeted by hackers looking to steal personal information or disrupt essential healthcare services.

    - Financial Institutions: Banks and other financial institutions are often the target of hackers looking to steal money or personal financial information.

6. **How do you assess vulnerability?**
    - Vulnerability assessment is an important part of network security as it helps identify potential vulnerabilities and risk areas that need to be addressed. Here are some common steps you can take to assess vulnerabilities:

    - Identify Assets: Identify assets that need protection, such as computers, servers, applications, and information.

    - Identify Threats: Identify potential threats to these assets, such as malware, hacking, social engineering, and natural disasters.

    - Vulnerability Assessment: Perform vulnerability assessments to identify potential weaknesses in the system, such as outdated software, weak passwords, and open ports.

    - Risk Assessment: Evaluate the risk associated with each vulnerability to determine the probability and impact of an attack.
    - Prioritize treatment: Prioritize treatment based on risk and available resources.

    - Security Measures: Use security measures such as updating software, strengthening passwords, and using firewall and antivirus software to resolve identified problems.

    - Monitoring and Evaluation: Monitor systems for potential vulnerabilities and continually evaluate and update security measures as needed.

7. **What are the principles of network security?**
    - Defense in depth: Use multiple layers of security controls to build a strong and robust security system. This includes firewalls, intrusion detection/prevention systems, antivirus software, and access controls.

    - Minimum: Reduce the risk of loss of access or data by giving users only the access and privileges they need to do their job.

- Risk Management: Conduct regular risk assessments to identify threats and vulnerabilities and implement measures to reduce or control risks.

- Security by Design: Integrating security into all aspects of networking and design, including software development, hardware configuration, and network architecture.

- Continuous monitoring: Use real-time notifications to continuously monitor for security threats and quickly respond to systems and situation.

- Regular Updates and Patching: Keep software and systems up-to-date with the latest security updates and updates to ensure there are no security vulnerabilities.

- User Awareness: Educate users about security threats such as phishing scams and malware, and promote best practices such as strong password management and web security scanning.

8. What is a firewall to use for?

- A firewall is a network security device designed to monitor and control network access based on predefined security policies. The main purpose of the firewall is to act as a barrier between the internal network and the external network (such as the Internet) to prevent unauthorized access and prevent secure threats.

- Some specific uses of firewalls are:

- Network security: Firewalls can be used to monitor and filter network traffic to prevent unauthorized access, block malware and other malicious activity, and identify and respond to security threats.

- Access Control: A firewall can be used to control access to the network, for example by blocking certain types of traffic or restricting access to certain applications or services.

- Traffic Shaping: Firewalls can be used to prioritize or restrict certain types of network traffic, such as limiting bandwidth usage for business-critical operations or non-essential activities.
- Logging and Reporting: Firewalls can be used to log network activity and generate reports on network usage and security issues, helping administrators identify and respond to security events.

9. configure advanced firewall setting?

- General steps for configuring advanced firewall settings are:

- Determine the purpose of the firewall: specify the type of traffic to allow or block. Decide which ports and protocols you need to allow on the network.

- Set Traffic Rules: Create rules that define what traffic is allowed or blocked. Firewall rules can be based on IP address, port, protocol, application, or other criteria.

- Configure logging and notifications: configure the firewall to log traffic and generate notifications when problems are detected.
- This will help you identify and respond to potential security threats.

- Testing and Refinement of Firewall Policies: Test your firewall policies to ensure they are working as intended. Upgrade your policies as needed to improve network security and performance.

- Keep Your Firewall Updated: Keep your firewall software up-to-date with the latest security and firmware updates.

10. configure "date and time" options

- Click on the clock in the bottom-right corner of the screen.
- Click on "Date and time settings."
- In the "Date and time" tab, ensure that the "Set time automatically" option is toggled on. This will automatically synchronize your computer's clock with an internet time server.
- If you want to manually adjust the time, you can toggle off the "Set time automatically" option and then click on the "Change" button. This will allow you to set the date and time manually.
- In the "Time zone" tab, select your current time zone from the drop-down menu.
- If you want to adjust additional time settings, click on the "Additional date, time & regional settings" link at the bottom of the page. This will take you to the "Region" settings, where you can adjust settings such as the date and time format, the first day of the week, and more.
- Once you've made your changes, click "OK" or "Apply" to save them.