6/18/2023

Hasan alhwietat

Network Security

Hasan Alhwietat

Contents

[1- Design a secure networked system to meet the business requirements listed above. You should include in your report a written step-by-step plan on how you are going to design a secure networked system, a clear blueprint of your overall network including all devices in all locations (you can use a packet tracer snapshot). 2](#_Toc137995219)

[2- Investigate the purpose and requirements of the secure network according to the given scenario. 3](#_Toc137995220)

[3- Determine which network hardware and software to use in the network. 3](#_Toc137995221)

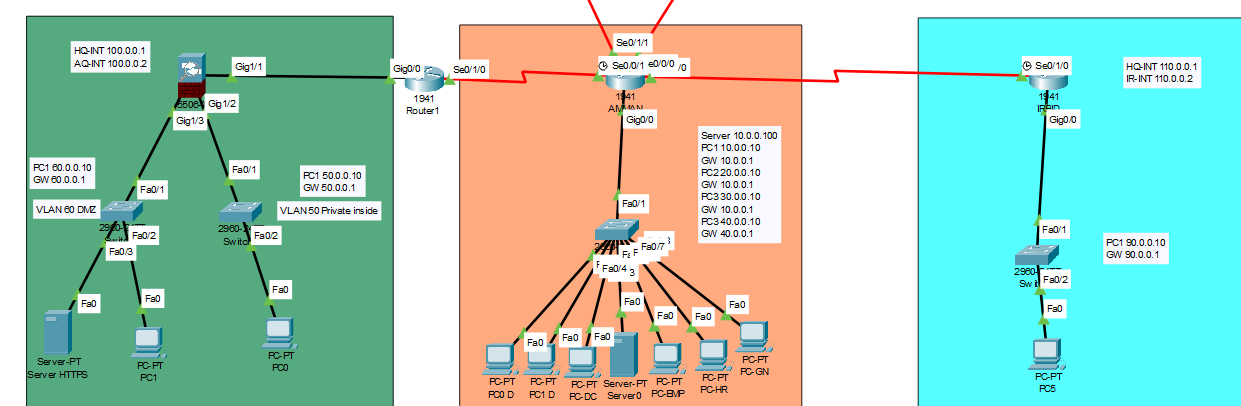
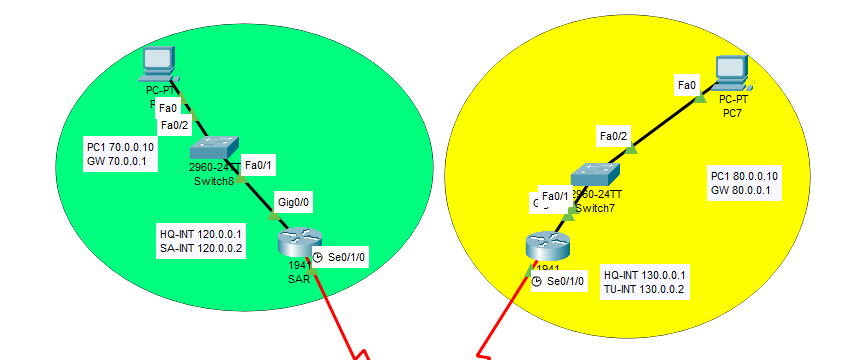
[4- Configure Network Security measures for your network. Those measures include Firewalls, Routers, Switches, Gateways, passwords, SSH, SSL, IPsec, VPN, HTTPs, FTPs, DHCP and DNS. And provide a justification for the choices made in the network security configuration that was implemented. 4](#_Toc137995222)

[5- Create a test plan for your network. Your test plan should consider different testing methods in terms of checks on network security, testing for network vulnerabilities etc. 4](#_Toc137995223)

[6- Comprehensively test your network using the devised test plan. Tests should be carried out on all devices (Firewall, Servers, Routers, Switches, gateways, passwords). Record the test results and analyze these against expected results. You need to provide scripts/files/screenshots of the testing of your network. 5](#_Toc137995224)

[7- Critically evaluate the design, planning, configuration and testing of your network security. Make some improvement recommendations. 20](#_Toc137995225)

# Design a secure networked system to meet the business requirements listed above. You should include in your report a written step-by-step plan on how you are going to design a secure networked system, a clear blueprint of your overall network including all devices in all locations (you can use a packet tracer snapshot).



First, we placed the servers, routers, switches, and PCs and connected them correctly, then we distributed the IP address to all the PCs, servers, and routers, and then we made the Vlans, then we made the AAA and SSH on the Irbid router, then we made the vpn IPsec ESP to connect the network of Oman with Turkey and Saudi Arabia, which provides Authentication, Safety and Availability Then we made the ASA Aqaba and we identified the internal and external network and the DMZ and then we made the ACL and implemented it on the Oman router and then added some security to the network more by making a password for all routers and switches and making Port Security for all interfaces and turning off unused ports and making Port Security on the maximum mac address of two and DHCP security implementation (spoofing and starvation with limit of 5). This detailed report of my network has been implemented in the best way to meet the client's requirements and to design a secure network system.

# Investigate the purpose and requirements of the secure network according to the given scenario.

According to the scenario, the best procedures and accurate plans were applied to provide a secure network, so that the specific requirements were understood, potential threats were identified, and then the devices were distributed to enhance security, the implementation of VPN (Site-to-Site), ASA, ACL, IDS, port security, and a password for all the network to protect from unauthorized access or the occurrence of any penetration and attempt to destroy data so that the network that was established guarantees confidentiality and integrity of communication and works to transfer data with encryption that provides protection for data and network resources while ensuring the continuity of work without any interruption.

# Determine which network hardware and software to use in the network.

Many hardware and software were used for my network, including the following:

Routers: It is a network device responsible for forwarding network data packets between networks that operates in the network layer 3 of the OSI model. It relies on IP addresses in order to direct data to the device to which the packet is to be delivered and depends on the information contained in the routing table.

Switches: It is a network device that operates on the Layer 2 data link layer and is responsible for facilitating communication between devices within the network. It receives packets and distributes them to the appropriate destination for each packet. It relies on the (MAC) of the device to distribute the packet to the intended device.

ASA firewall: It is an adaptive security device manufactured by Cisco. It is an advanced security device that provides protection for networks and data from unauthorized access and prevention of threats. It works on accurate inspection and control of network traffic. It combines firewall, IPS and VPN functions in one device.

PCs: It is a personal computer designed for versatile personal use according to the user's needs

Servers: They are powerful computers that provide services and functions to computers on the network and provide users' requests for services provided by HTTPS, HTTP, DHCP, DNS, FTP, Mail, etc.

VPN IPsec ESP (Site-to-Site): It is an encapsulation of the security payload that configures the VPN tunnel protocol to establish a secure connection between the two separate networks. The IPsec ESP is one of the protocols that provides confidentiality, integrity and credibility for data transferred between networks, which protects it from unauthorized access and works on the network layer (layer 3).

VLAN: It is a Virtual Local Area Network within the network to segment and isolate network traffic based on the requirements that are identified and enhance the network's security and performance. The network is divided in an area into multiple virtual networks.

ACL: It is the access control list, which is a feature to enhance network security. A set of rules are implemented on the network to control and filter network traffic based on the rules. It is implemented on routers, switches, and firewalls through the process of allowing or blocking.

IDS: Intrusion Detection System is a security technology that monitors network traffic, detects malicious activity, attempts unauthorized access, and generates alerts if a threat is detected.

# Configure Network Security measures for your network. Those measures include Firewalls, Routers, Switches, Gateways, passwords, SSH, SSL, IPsec, VPN, HTTPs, FTPs, DHCP and DNS. And provide a justification for the choices made in the network security configuration that was implemented.

Firewalls were used to protect the network from unauthorized access and malicious traffic, to allow only people with authority to access the network, to block others, to implement stateful packet inspection to monitor and control the network, and routers were used and ACLs were configured to filter and control network traffic and port protocols as well Spoofing protection and IP filtering are configured to prevent unauthorized access and authentication and keys are used Port security and allowed MAC addresses are implemented on each port VLANs are configured to separate and isolate network traffic to improve performance and security by default segmentation and implementation of a spanning tree to protect against potential network attacks And network rings, and secure gates such as secure web gates were used to provide advanced protection from threats, intrusion prevention, and web filtering. Passwords were used to ensure that no change occurred to devices and to prevent unauthorized access by imposing strong and complex passwords for more security. SSH was used to manage devices remotely from Through encrypted communication and effective authentication, IPsec ESP was used to ensure the creation of an encrypted and secure tunnel from site to site remotely to ensure confidentiality and authentication of data via VPN. Using DHCP by adding security features to it to prevent intrusion and prevent unauthorized IP address assignment to DHCP, and DNS was applied securely to protect against spoofing and cache corruption

The reason for the choices of procedures that have been implemented is to ensure the security of the network that provides confidentiality, integrity, availability of data and services, and data transfer by encryption through the measures and practices that have been followed, threats will be detected, treated, and prevented from future threats, and it also provides layers of defines to protect against any threat.

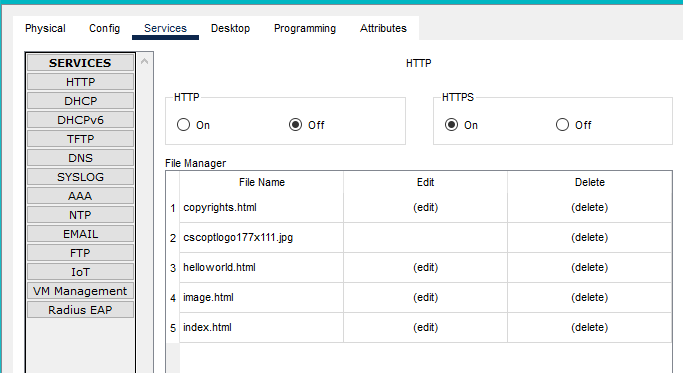
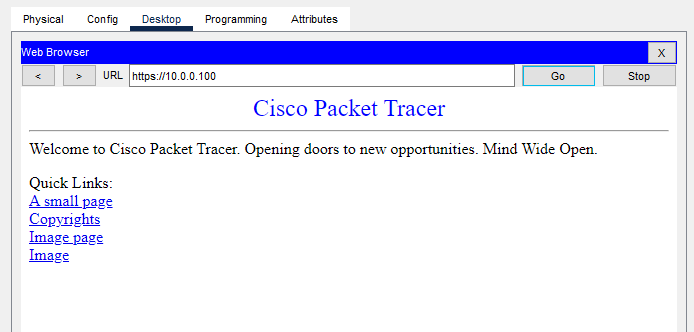
# Create a test plan for your network. Your test plan should consider different testing methods in terms of checks on network security, testing for network vulnerabilities etc.

|  |  |
| --- | --- |
| Test | Expected Result |
| 1. Test if all VLANs and LANs have access to the HTTPs server | Yes |
| 2. Test if all VLANs and LANs have access to the Mail server | Yes |
| 3. Test if all VLANs and LANs have access to the DNS server | Yes |
| 4. Test if only the HQ EMP, and Aqaba office have access to the FTP server | Yes |
| 5. Test if only HQ datacenter VLAN have access to the DHCP server | Yes |
| 6. Test if only HQ EMP LAN have access to the HTTP server | Yes |
| 7. Test if VLAN HQ Datacenter can get IP from the DHCP server | Yes |
| 8. Test if Pc Irbid can get IP from the DHCP server | No |
| 9. A test if a Pc in Irbid can ping a Ping in Saudi Arabia by VPN | No |
| 10. A test if a Pc in Turkey can ping a Pc in Aqaba ASA in VLAN 50 | No |
| 11. Test a VPN between Saudi Arabia and Amman is a work | Yes |
| 12. Test a VPN between Turkey and Amman is a work | Yes |
| 13. Test AAA work | Yes |
| 14. Test SSH work | Yes |
| 15. Test All switches and routers are passwords work | Yes |
| 16. Test All passwords encrypted | Yes |
| 17. Test if the telnet is not working | Yes |
| 18. Test All port unused is a shutdown | Yes |
| 19. Test All port interface fast Ethernet can be is a port security | Yes |

# Comprehensively test your network using the devised test plan. Tests should be carried out on all devices (Firewall, Servers, Routers, Switches, gateways, passwords). Record the test results and analyze these against expected results. You need to provide scripts/files/screenshots of the testing of your network.

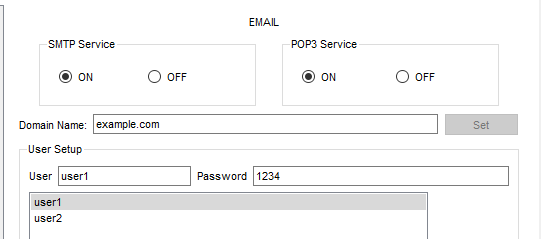
1. Test if all VLANs and LANs have access to the HTTPs server.

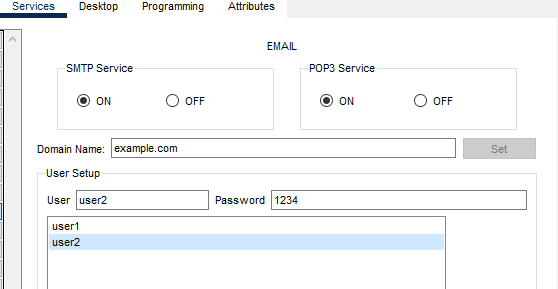
Since all computers are allowed to access the HTTPs, it was expected that the process would be successful

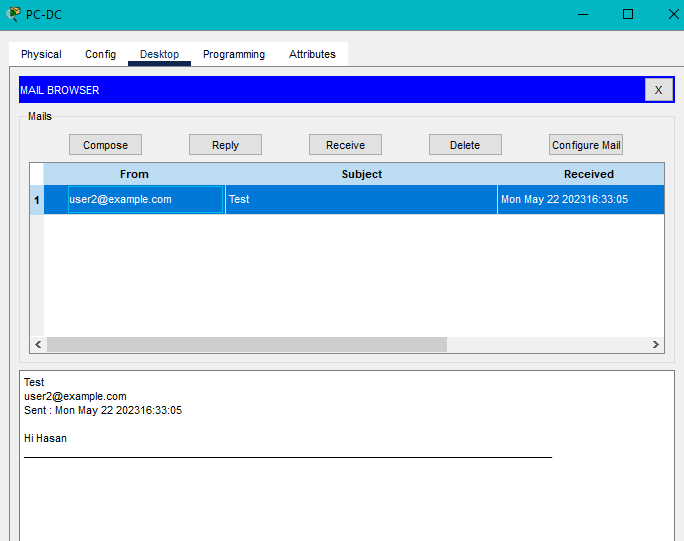


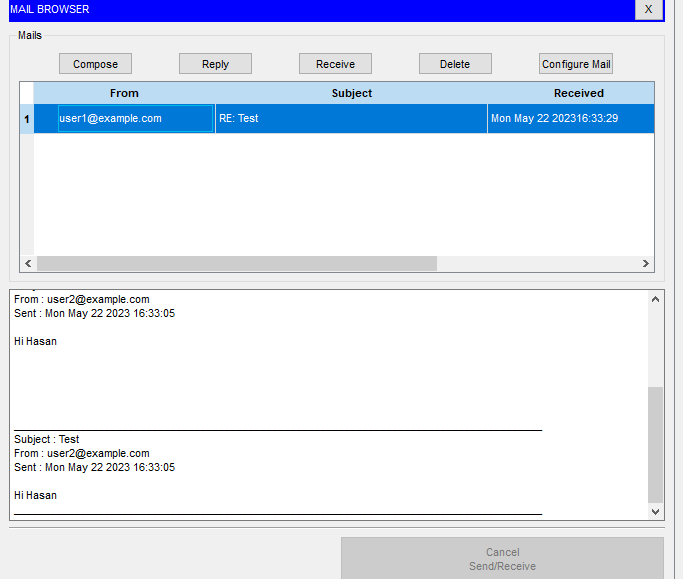
1. Test if all VLANs and LANs have access to the Mail server

Since all computers are allowed to access the Mail, it was expected that the process would be successful



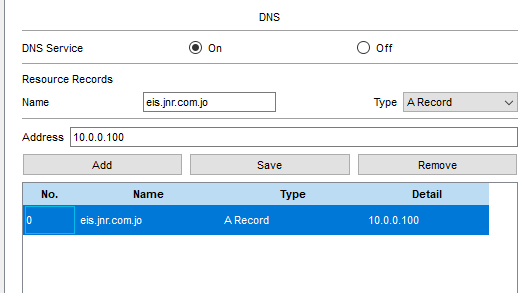


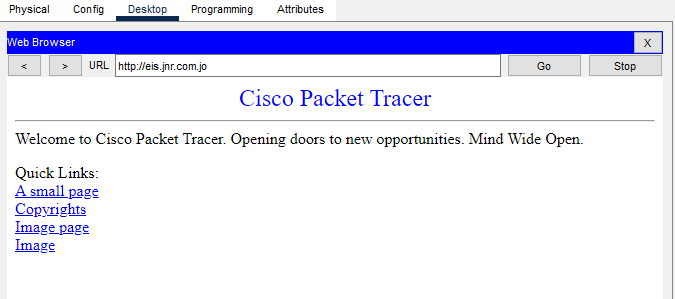




1. Test if all VLANs and LANs have access to the DNS server.

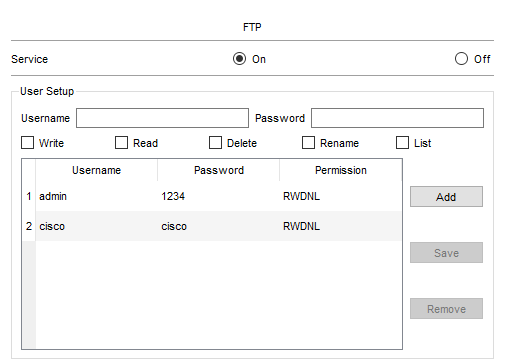
Since all computers are allowed to access the DNS, it was expected that the process would be successful

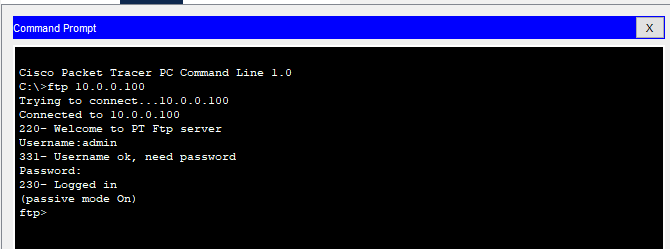




1. Test if only the HQ EMP, and Aqaba office have access to the FTP server

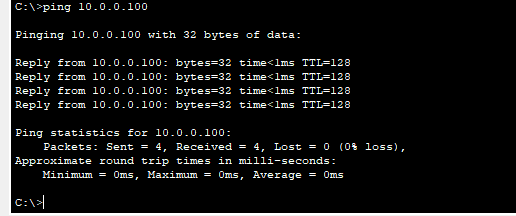
We have created access to the files and specify each of the HQ EMP and the Aqaba office who can access the FTP services, so it was expected that they would be the only ones who can modify the files





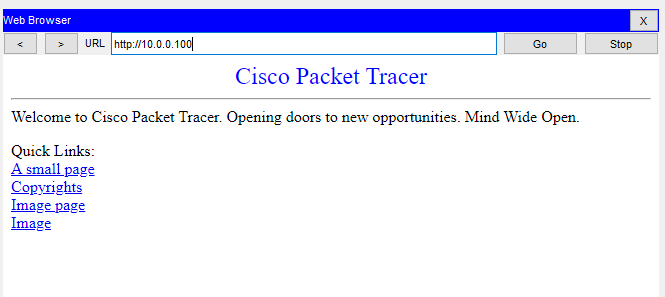
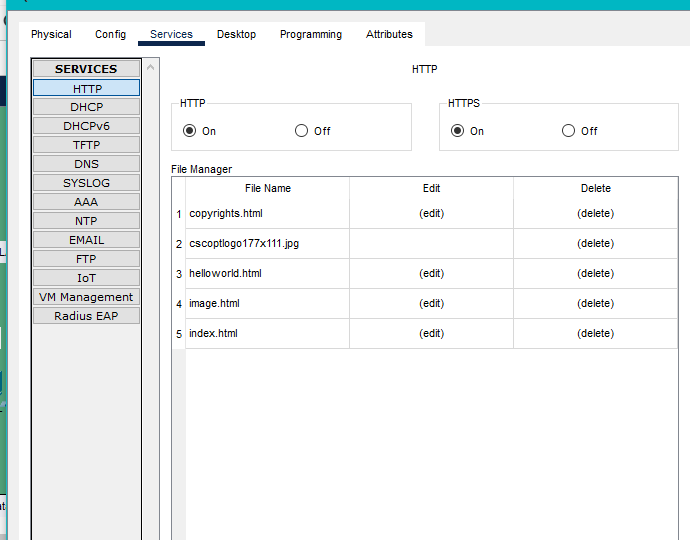
1. Test if only HQ datacenter VLAN have access to the DHCP server

We have created access to DHCP services and the HQ Datacenter has determined who can access it, so it was expected that he would be the only one able to control the service



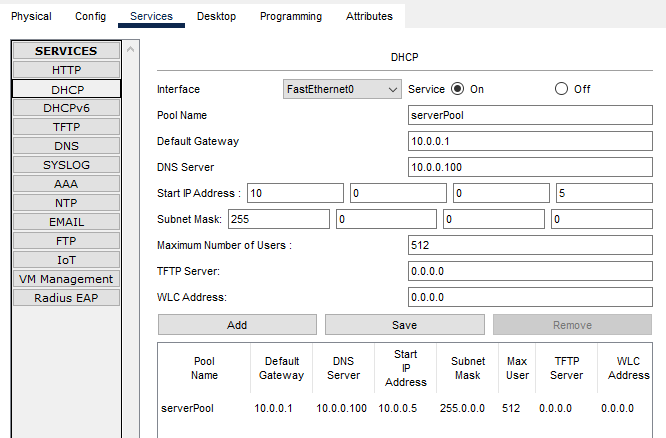
1. Test if only HQ EMP LAN have access to the HTTP server

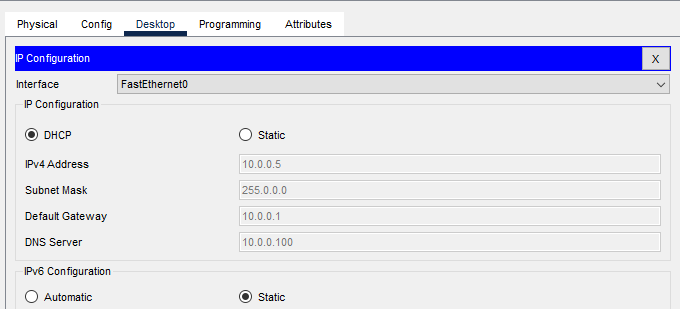
We have created access to HTTP services and the HQ EMP has determined who can get this service, so it was expected that he would be the only one able to access



1. Test if VLAN HQ Datacenter can get IP from the DHCP server

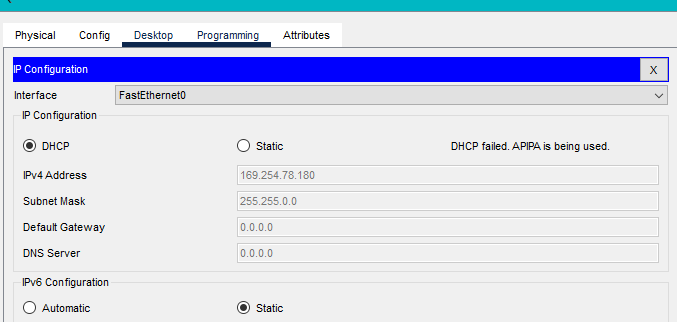
We have created the DHCP service and the VLAN HQ Datacenter has determined who can obtain this service, so it was expected that they would have the ability to obtain an IP from the DHCP server





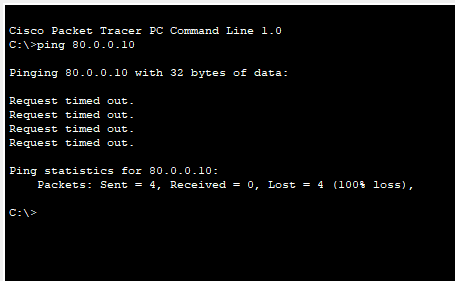
1. Test if Pc Irbid can get IP from the DHCP server

We have created a DHCP service and the VLAN HQ Datacenter has determined who can get this service, so it was expected that those who have the ability to get an IP from the DHCP server are within the VLAN HQ Datacenter so the computer in Irbid cannot get an IP from the server DHCP



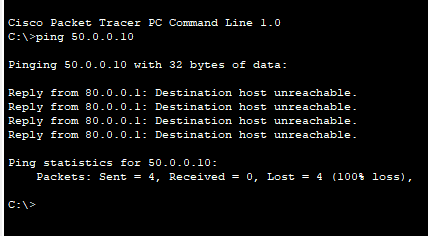
1. A test if a Pc in Irbid can ping a Ping in Saudi Arabia by VPN

We have established a VPN between the routers of Amman, Turkey and Saudi Arabia, so it was expected that only those who are within this connection can access each other, so the Irbid computer cannot enter with them, and it is not within the VPN



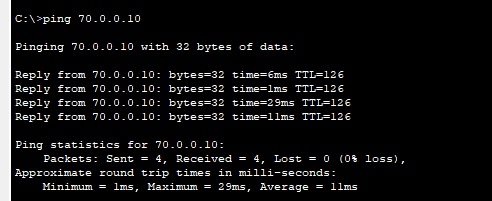
1. A test if a Pc in Turkey can ping a Pc in Aqaba ASA in VLAN 50

We have established a VPN between the routers of Amman, Turkey and Saudi Arabia, so it was expected that only those within this connection would have access to each other, so the Turkey computer cannot make a connection with the Aqaba computer, which is not within the VPN



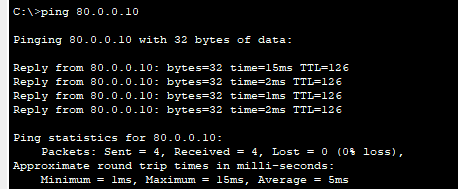
1. Test a VPN between Saudi Arabia and Amman is a work

We have set up a VPN between Amman and Saudi Arabia routers, so it was expected that only those within this connection would have access to each other, so the Saudi computer can make a connection with the Amman computer because they are within the VPN



1. Test a VPN between Turkey and Amman is a work

We have established a VPN between the Amman and Turkey routers, so it was expected that only those within this connection would have access to each other, so the Turkey computer can make a connection with the Amman computer because they are within the VPN



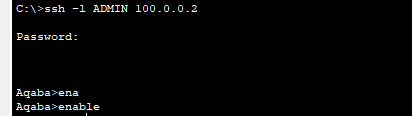
1. Test AAA work

We have made AAA on the Irbid router in order to increase the protection on it, so it is not possible to access the router except by entering the username and password, so it was expected that this matter would be required when entering the Irbid router



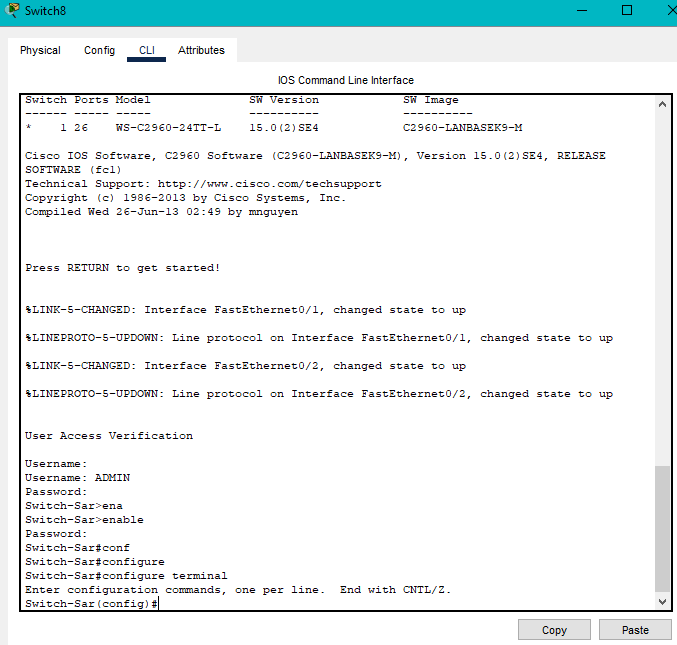
1. Test SSH work

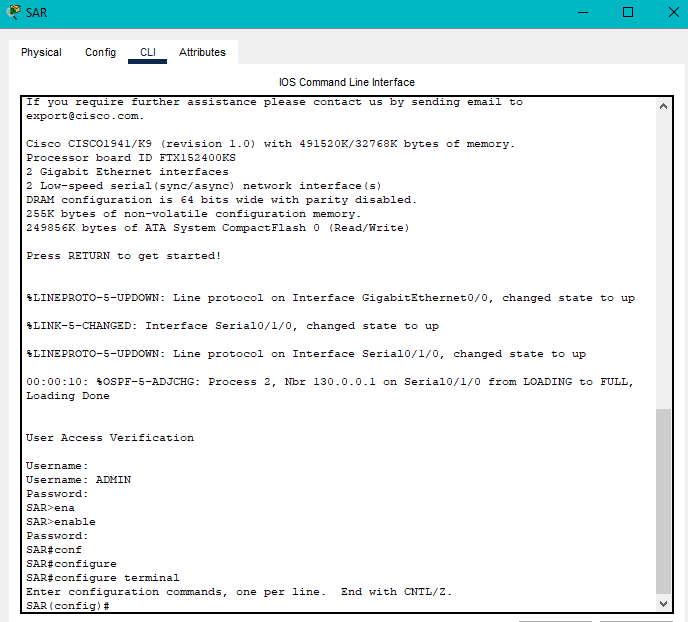
We have done SSH on the Irbid and Aqaba routers in order to establish the authority of who can control the router and modify it through the computer that has access via the password, so it is not possible to access the router except through the password, so it was expected that this matter would be required when entering the router Irbid or obstacle



1. Test All switches and routers are passwords work

We have protected all routers and switches by creating a password so that it is not modified or entered except by entering the password, as it is expected that someone who knows the password will enter





1. Test All passwords encrypted

We have protected all routers and switches by creating a password so that it is not modified or entered except by entering the password, as it is expected that someone who knows the password will enter

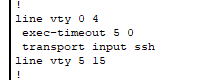






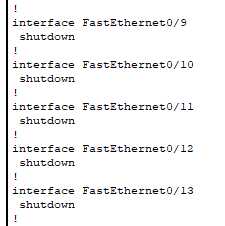
1. Test if the telnet is not working

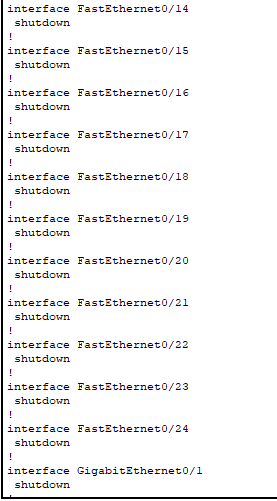
We have made a switch from telnet to SSH, so it will be turned off, and when requesting telnet, it will be told that it is not available



1. Test All port unused is a shutdown

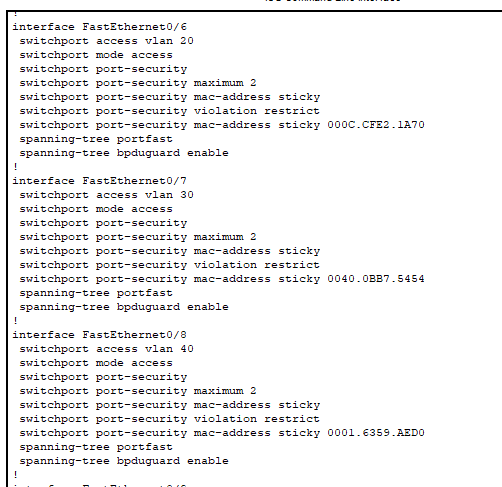
We have turned off the unused ports, so when connecting a wire, it will not work, and this is expected that it will not work



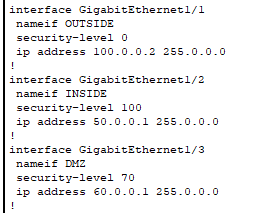
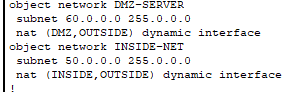


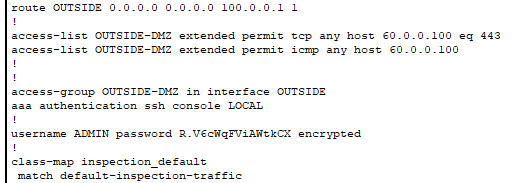
1. Test All port interface fast Ethernet can be is a port security

We have created a protection system for the ports so that they are less vulnerable to danger, and no new device will be accepted unless by reviewing the established permissions



Firewall :





# Critically evaluate the design, planning, configuration and testing of your network security. Make some improvement recommendations.

Based on my own design and planning, best practices such as security measures on switches and routers were followed, a protection strategy was created on the ports, and ACL was implemented with high accuracy. This was done to reduce vulnerabilities and reduce potential threats in order to provide the highest possible protection system, and a plan was developed for By separating the Aqaba router into a switch in order to increase protection, a firewall was put in place to separate the outer zone, which has a protection rate of zero, from the inner zone, which has a protection rate of 100, and from the demilitarized zone, with a protection rate of 70, which limits the potential impact of a security breach. Passing through all routers, switches, and other security policies, multi-factor authentication, and the use of cryptographic protocols to encrypt passwords. As for the tests, we created a table to test the entire network in order to find out the current vulnerabilities that may occur in the future. This test helps to accurately assess the security of networks and find out Threats and security vulnerabilities to ensure that your organization can deal with these disasters As for recommendations and improvements for the network, I suggest at the outset that the important priorities in the network be arranged in order to provide protection gradually and that we use the information management system and security events for networks in order to detect threats and the ability to respond to incidents Denial of service attacks in order to examine the possibility of network penetration and improve vulnerabilities, as well as continuous updating of devices, network and systems to increase security and reduce vulnerabilities. AI can also be used to continuously discover and solve vulnerabilities in order to make the system very complex and difficult to penetrate and use encryption protocols in data transmission such as Secure Sockets Layer ( SSL) and Transport Layer Security (TLS) to secure sensitive data and also use IDS to implement a robust intrusion detection and prevention system to monitor network traffic to search for threats use data backups to recover data in case of loss or problems in network systems that cause In case of data loss, network penetration must occur, no matter how many methods and complexities, because the field is always evolving, so security measures and updates must be carried out regularly in order to provide continuous protection.