A picture containing logo

Description automatically generated

**Network Security**

**10203280**

**(D/618/7406)**

**Section (2)**

**Submitted To:**

Dr. Sami almashqba

**Submitted By:**

Farouq Hassan

Spring 2023

**Table Of Contents**

* 1. Part A ……………………………………………. (3)

2.1. Part B …………………….………………………… (8)

3.1. Part C …………………………….…………………….……… (14)

4.0. Part D …………………….…………………………………… (16)

4.1. A …………………….…………………….………………………… (16)

4.2. B…………………….………………………………………………… (16)

4.3. C…………………………………………….………………………… (17)

5.1. Part E…………………….………………………… (19)

6.1. Part F…………………………………………………. (21)

7.1. Part G………………………………….…………….……... (24)

8.1. Part H, I,J ………………………….……………….…... (25)

9.1. Part K………………………………………………….…... (32)

10.1. Resources………………………….……………….…... (34)

**------------------------------------------------------------------------------**

Part 1:

I have set up a network topology with routers in Amman, Aqaba, Turkey, Irbid, and Saudi Arabia, as well as data centers in Amman and Aqaba. Here's a breakdown of the network setup:

Amman:

Router: HQ-Amman

Data Center: HQ-DataCenter

IP addressing: VLAN 10: 10.0.0.0/8, VLAN 450: shutdown

HQ-DataCenter:

It is the data center located in Amman.

VLAN 10 (10.0.0.0/8) with the IP address 10.0.0.1/8 assigned to the interface GigabitEthernet0/0/0.10.

Amman HQ:

VLAN 10 (10.0.0.0/8) with the IP address 10.0.0.1/8 assigned to the interface GigabitEthernet0/0/0/0.10.

VLAN 20 (20.0.0.0/8) with the IP address 20.0.0.1/8 assigned to the interface GigabitEthernet0/0/0.20.

VLAN 30 (30.0.0.0/8) with the IP address 30.0.0.1/8 assigned to the interface GigabitEthernet0/0/0.30.

VLAN 40 (40.0.0.0/8) with the IP address 40.0.0.1/8 assigned to the interface GigabitEthernet0/0/0.40.

The ACL "DC-Server" is applied to the interface GigabitEthernet0/0/0.10, allowing specific traffic to reach the host with IP address 10.0.0.2.

Aqaba:

Router: HQ-Aqaba

IP addressing: VLAN 50: 50.0.0.0/8

Aqaba Data Center (DC):

VLAN 60 is configured for the Aqaba Data Center.

The IP address range for VLAN 60 is 60.0.0.0/8.

The Aqaba DC has the IP address 60.0.0.1 assigned to it.

There is a Server connected to VLAN 60 with the IP address 60.0.0.10.

Turkey:

Router: HQ-Turkey, IP addressing: VLAN 70: 70.0.0.0/8

Irbid:

Router: HQ-Irbid, IP addressing: VLAN 80: 80.0.0.0/8

Saudi Arabia:

Router: HQ-Saudi, IP addressing: VLAN 90: 90.0.0.0/8

Data Centers:

HQ-DataCenter in Amman and HQ-AqabaDataCenter in Aqaba

The network configuration includes the following connections and security measures:

VPN Connections:

Two VPN connections are established using IPsec (Internet Protocol Security) between HQ-Amman and other locations:

VPN connection between HQ-Amman and HQ-Saudi: VPN-MAP-Saudi:

VPN connection between HQ-Amman and HQ-Turkey: VPN-MAP-Turkey:

It connects to using the transform-set "VPN-SET" and matches ACL 120 for Saudi, 130 for Turkey.

Crypto isakmp policy with AES encryption and pre-shared key authentication

Crypto isakmp key for the VPN connection

Crypto ipsec transform-set for encryption and hashing algorithms.

Crypto map VPN-MAP-Saudi to establish the VPN connection.

Access Control:

Access control lists (ACLs) to control traffic:

ACL "sl\_def\_acl" denies Telnet, HTTP, and SSH traffic and permits SSH traffic from any source

ACL "DC-Server" permits specific traffic from various sources to a host with IP address 10.0.0.2, including HTTPS, SMTP, DNS, FTP, and HTTP

Routing:

OSPF (Open Shortest Path First) routing protocol is configured with process ID 300.

Network statements in the OSPF configuration define the networks to be advertised:

The network statements cover the VLANs in Amman, Aqaba, Turkey, Irbid, Saudi Arabia, and the data centers, The area ID for all the networks is set to 0

configuration of the Aqaba-Firewall, here is a breakdown of the settings:

Hostname: Aqaba-Firewall

Interfaces: GigabitEthernet1/1 (OUTSIDE):

Nameif: OUTSIDE

With Security-level: 0

IP address: 140.0.0.1/8

GigabitEthernet1/2 (INSIDE): Nameif: INSIDE

With Security-level: 100

IP address: 50.0.0.1/8

GigabitEthernet1/3 (DMZ):

Nameif: DMZ

With Security-level: 70

IP address: 60.0.0.1/8

GigabitEthernet1/4-8: These interfaces are shut down and have no configuration.

NAT Configuration:

DMZ-NAT: Object network for the host with IP address 60.0.0.10 in the DMZ.

NAT configuration: It is statically translated to the public IP address 140.0.0.7.

INSIDE-NAT: Object network for the inside subnet 50.0.0.0/8.

NAT configuration: It uses dynamic NAT with the interface IP address as the global address.

Routing:

Default route configured for outbound traffic: route OUTSIDE 0.0.0.0 0.0.0.0 140.0.0.2 1

Access Control:

Access-list DMZ permits TCP traffic from any source to the host with IP address 60.0.0.10 on port 443.

The access-group DMZ is applied to the OUTSIDE interface.

Policy Maps:

Class-map inspection\_default matches default-inspection-traffic.

Policy-map type inspect dns preset\_dns\_map is defined with parameters.

Global policy-map named global\_policy:

Class inspection\_default is inspected with preset\_dns\_map, as well as FTP, ICMP, and TFTP traffic.

Service Policy:

The service-policy global\_policy is applied globally.

SSH and Telnet:

SSH is allowed from the INSIDE network (50.0.0.0/8) to the firewall.

SSH is allowed from the specific host 10.0.0.10 on the OUTSIDE interface.

Telnet timeout is set to 5 seconds.

SSH timeout is set to 5 seconds.

configuration of the WAN-HQ-Aqaba router, here is a breakdown of the settings:

Hostname: WAN-HQ-Aqaba

Security:

Service password encryption is enabled.

Minimum password length is set to 9 characters.

The "Aqaba" username is configured with an encrypted password.

Login Block:

It blocks login attempts for 150 seconds after 5 failed attempts within 200 seconds.

Enable Secret:

An encrypted enable secret password is configured.

IP Configuration:

Domain lookup is disabled.

Domain name is set to "Aqaba.com".

Interfaces:

GigabitEthernet0/0/0: IP address: 140.0.0.2/8

GigabitEthernet0/0/0.50: VLAN 50, IP address: 50.0.0.1/8

GigabitEthernet0/0/0.60: VLAN 60, IP address: 60.0.0.1/8

GigabitEthernet0/0/1-2: No IP address configured

Clock rate: 2000000

Serial0/1/1: IP address: 100.0.0.2/8

Vlan1: No IP address configured

OSPF Configuration:

OSPF process ID: 300

Passive interface: GigabitEthernet0/0/0

Networks advertised:

50.0.0.0/8 in area 0

60.0.0.0/8 in area 0

100.0.0.0/8 in area 0

140.0.0.0/8 in area 0

IP Classless:

IP classless routing is enabled.

IP Access List:

Access-list sl\_def\_acl is configured to deny Telnet, HTTP, and SSH traffic and permit SSH traffic from any source.

Line Configuration:

VTY lines 0 to 4 and line VTY 5 are configured for SSH login with local authentication.

configuration of the HQ-DataCenter router, here is a breakdown of the settings:

Hostname: HQ-DataCenter

Security:

Service password encryption is enabled.

Minimum password length is set to 9 characters.

The "Amman" username is configured with an encrypted password.

Login Block:

It blocks login attempts for 150 seconds after 5 failed attempts within 200 seconds.

Enable Secret:

An encrypted enable secret password is configured.

IP Configuration:

Domain lookup is disabled.

Domain name is set to "Amman.com".

Crypto Configuration:

Crypto ISAKMP policies are configured for VPN connections.

Two pre-shared keys are defined for peers with addresses 120.0.0.2 and 130.0.0.2.

Crypto IPsec Configuration:

A transform set named VPN-SET is defined for ESP (Encapsulating Security Payload) with AES encryption and SHA HMAC authentication.

Crypto Maps:

VPN-MAP-Saudi:

Description: VPN connection to WAN HQ-Saudi

Peer: 120.0.0.2

Transform set: VPN-SET

Match address: 120

VPN-MAP-Turkey:

Description: VPN connection to WAN HQ-Turkey

Transform set: VPN-SET

Match address: 130

Interfaces:

GigabitEthernet0/0/0: No IP address configured

GigabitEthernet0/0/0.10: VLAN 10 IP address: 10.0.0.1/8

Inbound and outbound access-lists named "DC-Server" are applied.

GigabitEthernet0/0/0.20: VLAN 20 IP address: 20.0.0.1/8

GigabitEthernet0/0/0.30: VLAN 30 IP address: 30.0.0.1/8

GigabitEthernet0/0/0.40: VLAN 40 IP address: 40.0.0.1/8

GigabitEthernet0/0/1-2: No IP address configured, Shutdown

Serial0/1/0: IP address: 130.0.0.1/16, Crypto map: VPN-MAP-Turkey

Serial0/1/1: IP address: 100.0.0.1/8

Serial0/2/0: IP address: 110.0.0.1/8

Serial0/2/1: IP address: 120.0.0.2/8, Crypto map: VPN-MAP-Saudi

OSPF Configuration:

OSPF process ID: 300

Networks advertised:

10.0.0.0/8 in area 0

20.0.0.0/8 in area 0

30.0.0.0/8 in area 0

40.0.0.0/8 in area 0

100.0.0.0/8 in area 0

120.0.0.0/8 in area 0

130.0.0.0/8 in area 0

110.0.0.0/8 in area 0

140.0.0.0/8 in area 0

IP Access List:

Access-list sl\_def\_acl is configured to deny Telnet, HTTP, and SSH traffic and permit SSH traffic from any source.

Access-list 110 permits IP traffic from 10.0.0.0/8 to 70.0.0.0/8.

Access-list 120 permits IP traffic from 10.0.0.0/8 to 80.0.0.0/8.

Line Configuration:

VTY lines 0 to 4 and line VTY 5 are configured for SSH login with local authentication.

running configuration of the HQ-Amman switch. Here's a breakdown of the configuration:

The enable secret password is encrypted.

The hostname is set to HQ-Amman.

The no ip domain-lookup command disables DNS lookup.

The ip domain-name is set to HQ.com.

There is a username "HQ" with an encrypted password.

Spanning Tree Protocol (STP) is enabled with the PVST (Per-VLAN Spanning Tree) mode.

The switchport interfaces are configured with various settings:

FastEthernet0/1 is configured as an access port in VLAN 20 with port security.

FastEthernet0/2 is configured as an access port in VLAN 30 with port security.

FastEthernet0/3 is configured as an access port in VLAN 40 with port security.

FastEthernet0/4 to FastEthernet0/24 are shutdown.

GigabitEthernet0/1-2 are configured as trunk ports with a native VLAN of 200 and no negotiation.

VLAN 1 is shutdown.

SSH is enabled for remote management on line vty 0 to 4.

configuration of the WAN-HQ-Saudi router. Here's a breakdown of the configuration:

The enable secret password is encrypted.

The hostname is set to WAN-HQ-Saudi.

The login block-for command is configured to block login attempts after 15 failed attempts within 5 minutes.

There is a username "Saudi" with an encrypted password.

IPsec VPN configuration is present:

The crypto isakmp policy specifies encryption, authentication, and group parameters.

The crypto isakmp key defines the pre-shared key for the VPN connection.

The crypto ipsec transform-set specifies the encryption and authentication algorithms for the VPN.

The crypto map VPN-MAP defines the VPN connection parameters, including the peer IP address, transform-set, and ACL.

The no ip domain-lookup command disables DNS lookup.

The ip domain-name is set to Saudi.com.

Spanning Tree Protocol (STP) is enabled with the PVST mode.

The router has the following interfaces configured:

GigabitEthernet0/0/0 is assigned the IP address 70.0.0.1 with a subnet mask of 255.0.0.0.

GigabitEthernet0/0/1 and GigabitEthernet0/0/2 have no IP address configured.

Serial0/2/1 is assigned the IP address 120.0.0.2 with a subnet mask of 255.0.0.0 and is associated with the crypto map VPN-MAP.

Vlan1 has no IP address configured.

OSPF (Open Shortest Path First) is configured with the process ID 1500 and the following network statements:

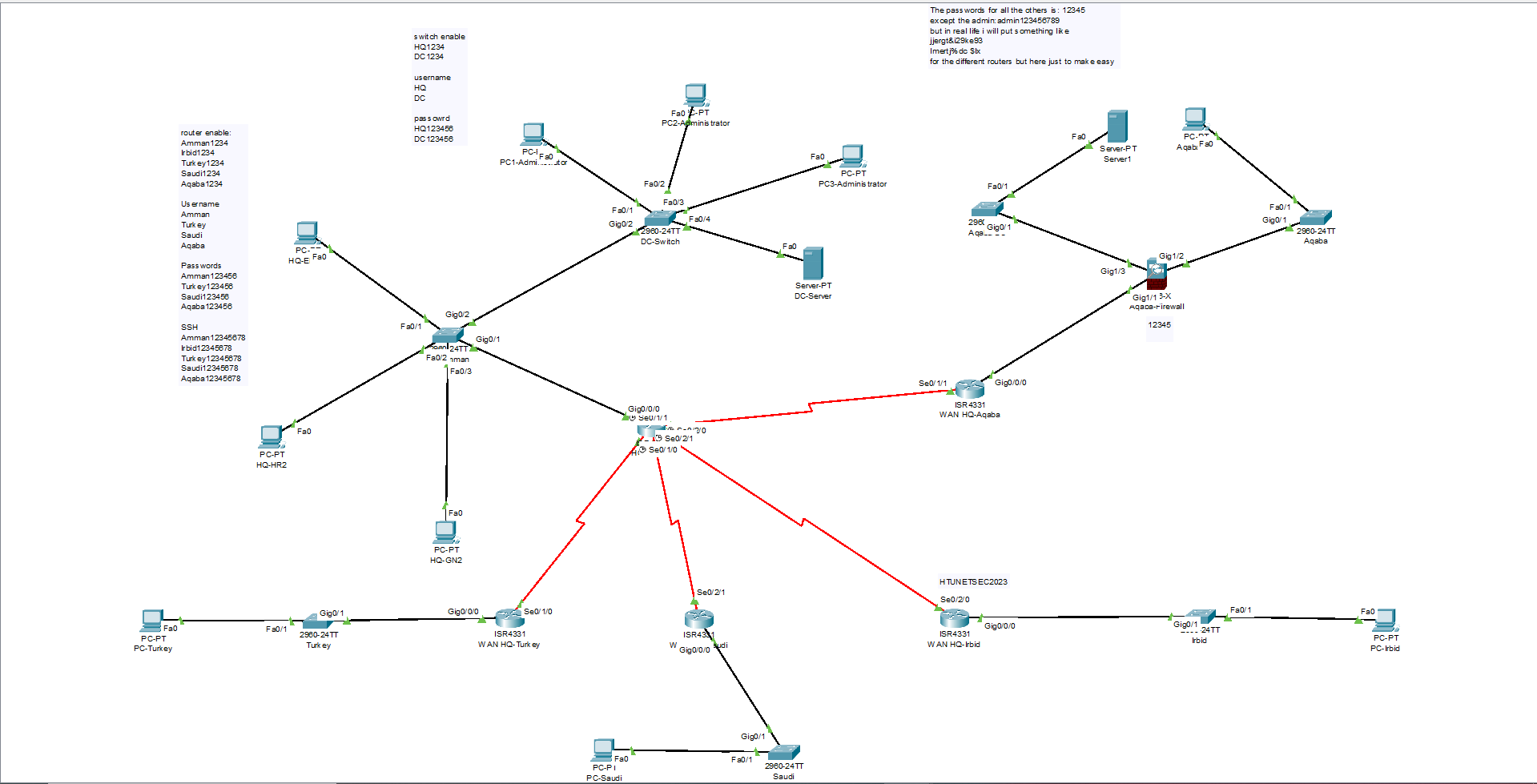
network 70.0.0.0 0.255.255.255 area 0

network 120.0.0.0 0.255.255.255 area 0

network 140.0.0.0 0.255.255.255 area 0

The ip access-list extended sl\_def\_acl is defined to control traffic, allowing SSH (port 22) and denying telnet (port 23) and web (port 80) traffic.

There are line configurations for console, auxiliary, and virtual terminal (SSH) access.



**2-**

The secure network connects JNR's Amman headquarters with its new locations in Saudi Arabia and Turkey by way of a dependable and secure infrastructure. Employees should be able to access the Employee Information System (EIS) through a secure website, as well as mail and FTP servers, thanks to the network's guarantee of the security, integrity, and availability of data and services. In order to guard against unauthorized access and harmful activity, the network should also provide correct routing, VPN connectivity, and network security best practices.

Requirements of the Secure Network:

Secure Connectivity: Establish site-to-site VPN/IPsec connections between the offices outside Jordan and the Amman data center to ensure secure and encrypted communication.

Hardened Switches and Routers: Configure switches and routers with strong passwords, enable SSH for remote management, shut down unused ports, apply port security with a maximum MAC address limit of two, and implement DHCP security to protect against spoofing and starvation.

Proper Routing: Implement dynamic routing protocols to support efficient and scalable routing within the network, avoiding static routing configurations.

Access to Servers: Configure access control rules to allow access to specific servers based on the requirements:

HTTPs server: Accessible by all VLANs and LANs.

Mail server: Accessible by all VLANs and LANs.

DNS server: Accessible by all VLANs and LANs.

FTP server: Accessible by HQ EMP and Aqaba office only.

DHCP server: Accessible by HQ data center VLAN only.

HTTP server: Accessible only by HQ EMP LAN.

Local AAA Authentication: Configure local AAA authentication for VTY lines on the IRBID router using the username "ADMIN" and password "HTUNETSEC2023" for SSH protocol.

Disaster Recovery Site: Configure Aqaba office as a disaster recovery site with two VLANs:

VLAN 50: Aqaba office.

VLAN 60: Redundant HTTPS server.

ASA Firewall for Aqaba Office: Replace the router in Aqaba office with an ASA firewall and configure it with the following rules:

SSH service on Aqaba ASA router accessible only by HQ Datacenter PC1 (10.0.0.10).

Configure DMZ for VLANs (VLAN 50 private and VLAN 60 public).

DHCP Security: Implement DHCP security measures to protect against spoofing and starvation attacks, setting a rate limit of 5.

By addressing these requirements, the secure network design will ensure secure connectivity, protect against unauthorized access, support proper routing, and facilitate the access and availability of services for JNR's employees across different offices.

**3-**

I must choose suitable network hardware and software components that fulfill the criteria and offer the required security features in order to construct the secure network. Here are the network hardware and software components that are advised based on the provided scenario:

Network Hardware:

Choose business-grade routers that can enable VPN/IPsec connection, dynamic routing protocols, and security capabilities like SSH. Cisco ISR series routers are a few examples of routers.

Select managed switches with VLAN, port, and other security features. Verify that they have enough ports and performance abilities. Cisco Catalyst switches are an example of a switch.

ASA (Adaptive Security Appliance) firewalls should be installed for improved security, VPN functionality, and DMZ setup. Advanced threat prevention is offered by ASA firewalls, which may also be configured with access control rules. Firewalls like the Cisco ASA are an example.

Servers: we are able For hosting services like HTTPs, FTP, DHCP, and DNS, use dedicated servers. Make sure the servers are equipped with enough resources to handle the anticipated workload.

Network Software:

Operating Systems: Choose the correct operating systems for servers, firewalls, switches, and routers. Use of Cisco IOS or Cisco IOS XE is possible for routers and switches. Cisco ASA software is suggested for firewalls. Operating systems like Windows Server or Linux distributions can be the foundation of a server.

Configure routers and firewalls with VPN/IPsec software to create secure site-to-site connection. The required VPN/IPsec capabilities can be provided by Cisco IOS or Cisco ASA software.

Routing Protocols: To allow effective routing throughout the network, implement dynamic routing protocols like OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol).

Security Software: To defend the network from dangers, use security software for intrusion detection and prevention, antivirus, and other security measures.

**4- in file**

**5-**

Here's how we can implement security measures for each component:

Firewalls:

For improved security and access management, install ASA (Adaptive Security Appliance) firewalls. Set up the firewalls' access control rules to permit or prohibit traffic depending on parameters including source and destination IP addresses, ports, and protocols.

Access control rules should be used to limit SSH access to the Aqaba ASA router to just the HQ Datacenter PC1 (10.0.0.10) utilizing ASA firewall's capabilities.

Routers:

To safeguard the credentials saved on the router, enable password encryption using the "service password-encryption" command.

On the routers, set up strong administrator passwords, as well as the "enable secret" command, which employs a more secure method of password encryption.

Use local authentication on the IRBID router with the login "ADMIN" and a secure password (HTUNETSEC2023) to govern remote SSH access by implementing AAA (Authentication, Authorization, and Accounting).

Switches:

Switches with port security can only allow a certain amount of MAC addresses per port. To stop unwanted devices from connecting to the network, restrict the number of MAC addresses that may be used to two.

Unused switch ports should be disabled to prevent unwanted access.

Set up SSH access to handle switches remotely instead of using insecure protocols like telnet.

Gateways:

To guarantee dependable network connectivity and prevent unwanted changes to the gateway IP addresses, assign static IP addresses to the gateway devices.

Passwords:

Enforce strong password policies for all devices and user accounts. Use a combination of uppercase and lowercase letters, numbers, and special characters. Set a minimum password length and enforce regular password changes.

Use password encryption to protect stored passwords from unauthorized access.

SSL and SHH:

Set up SSH (Secure Shell) as the firewall, switch, and router remote administration protocol. SSH offers encrypted secure communication, making it safer than telnet.

For secure communication between clients and the HTTPS server, use SSL (Secure Sockets Layer). For sensitive data exchanged over the network, SSL provides encryption and data integrity.

VPN and IPSec

Establish safe, encrypted connections between the remote offices and the headquarters data center by configuring IPSec (Internet Protocol Security). Network traffic's secrecy, integrity, and authentication are provided via IPSec.

Use IPSec to implement a site-to-site VPN (Virtual Private Network) to safely link the outlying offices to the headquarters data center. This makes sure that data is encrypted and secured against unwanted access while being sent between destinations.

FTPS and HTTPS

To communicate securely with the Employee Information System (https://eis.jnr.com.jo), use HTTPS (HTTP over SSL/TLS). Data integrity and confidentiality are protected during transmission between clients and the web server thanks to HTTPS encryption.

To protect file transfers between authorized clients and the FTP server, use FTPS (FTP over SSL/TLS). Data in transit is encrypted using FTPS to prevent unwanted access.

DNS and DHCP:

To stop spoofing and starvation attacks, configure DHCP (Dynamic Host Configuration Protocol) security measures. For the purpose of reducing excessive DHCP traffic, enable rate restriction on DHCP queries.

To defend against DNS-based attacks like DNS cache poisoning and DNS spoofing, use DNS security measures. To assure the accuracy and legitimacy of DNS answers, use DNSSEC (DNS Security Extensions).

**Justification for the chosen network security configuration:**

Firewalls: Because ASA firewalls offer comprehensive security features, access control, and VPN capabilities, they are recommended for safeguarding the network perimeter.

Routers: To prevent unwanted access and provide secure remote administration, enable password encryption, apply strong passwords, and use AAA for authentication.

Switches: SSH access enables safe remote management, and port security prevents unwanted devices from connecting to the network.

Gateways: Using static IP addresses for gateways guarantees dependable network connectivity and shields them from illegal modifications.

Strong password policies and encryption help protect network assets and user accounts against illegal access.

SSH and SSL: Setting up SSH for remote management and SSL for encrypted communication guarantees safe access to network devices and guards against the transmission of sensitive data.

IPSec and VPN: Implementing IPSec and site-to-site VPNs provides secure encrypted connections between remote offices and the HQ data center, ensuring the confidentiality and integrity of data transmitted over the network.

Using HTTPS and FTPS allows secure data transfer and communication between clients and servers, safeguarding sensitive data.

DHCP and DNS: Setting up DHCP and DNS security measures helps to improve overall network security by thwarting assaults including spoofing, starvation, and DNS-based attacks.

**Part 2**

A Network Security Test Plan

This test plan's goal is to evaluate the network security mechanisms put in place in the network design and find any gaps or vulnerabilities. Network monitoring, vulnerability scanning, penetration testing, and checks on network security setups are some of the testing techniques.

Testing Network Security Configuration:

To verify that firewalls, routers, switches, and gateways are appropriately deployed and operating as intended, test their configuration.

Check that firewall access control rules are set up properly to permit or prohibit traffic depending on specified criteria.

Verify that the HQ Datacenter PC1 (10.0.0.10) only has SSH access to the Aqaba ASA router in accordance with the access control rules.

Check that the maximum MAC address limit is set to two and that port security is enabled on switches.

To guarantee safe remote management, test the SSH access to routers and switches.

Apply the appropriate patches, upgrades, or configuration modifications to fix any vulnerabilities that have been found.

Analyze the efficiency of security measures and pinpoint any weaknesses or potential improvement areas.

Check the network security policies and procedures to make sure they are current and follow best practices in the industry.

Verify that topics like access control, password management, incident response, and data protection are covered by the security policies.

Check to see if the security measures in place adhere to industry standards and legal obligations.

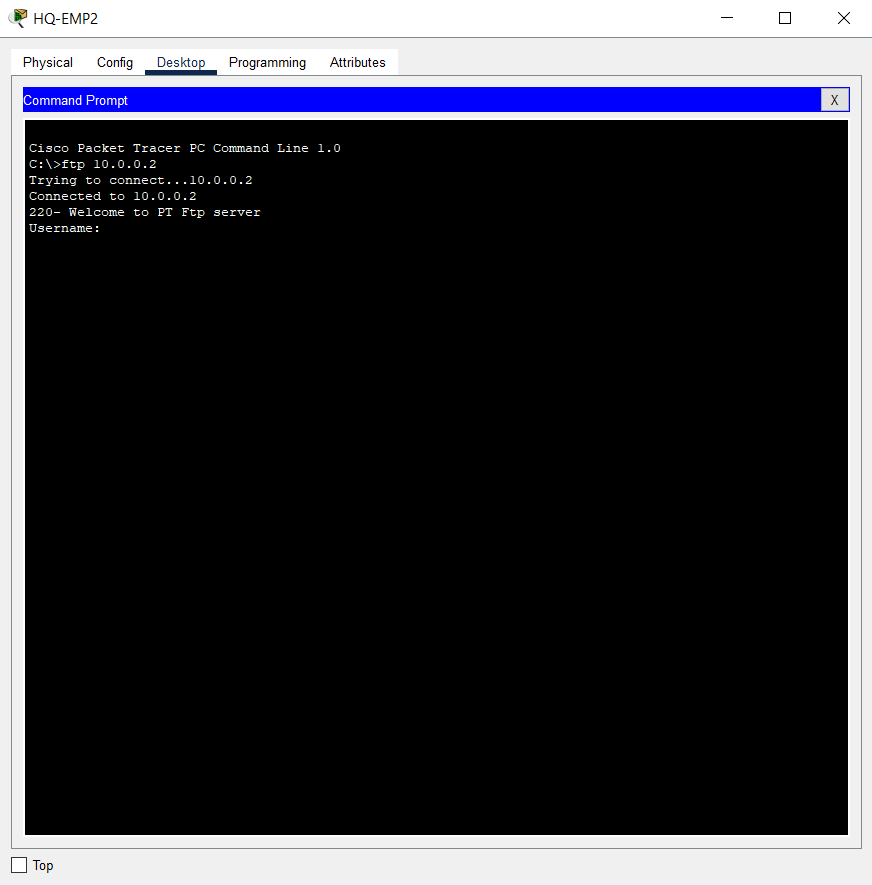
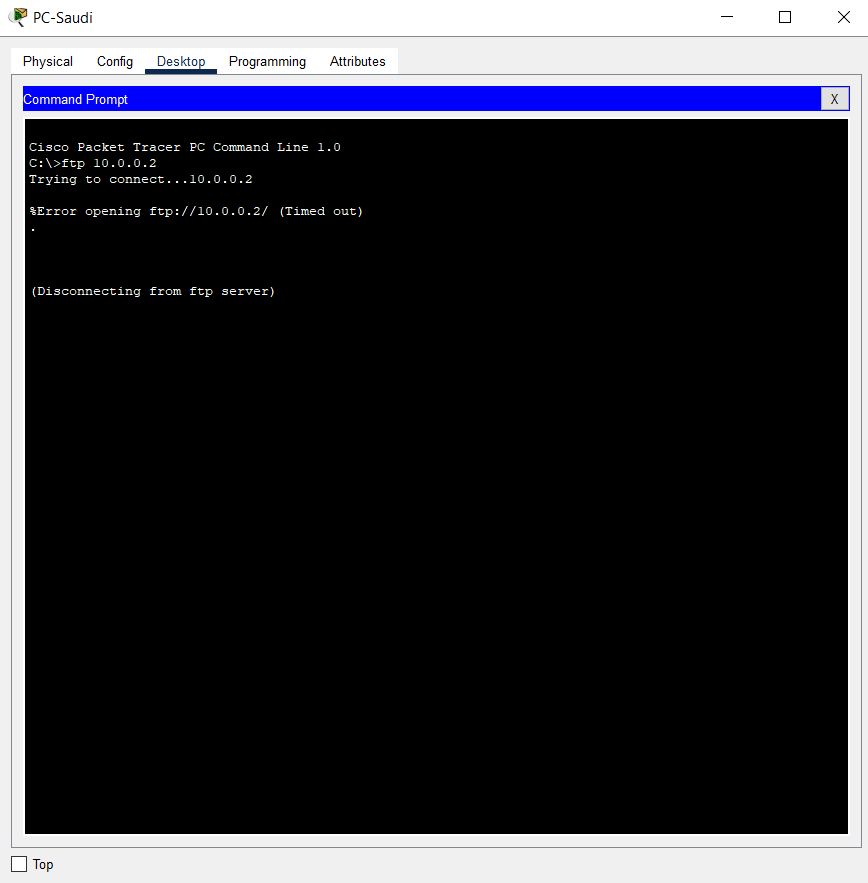
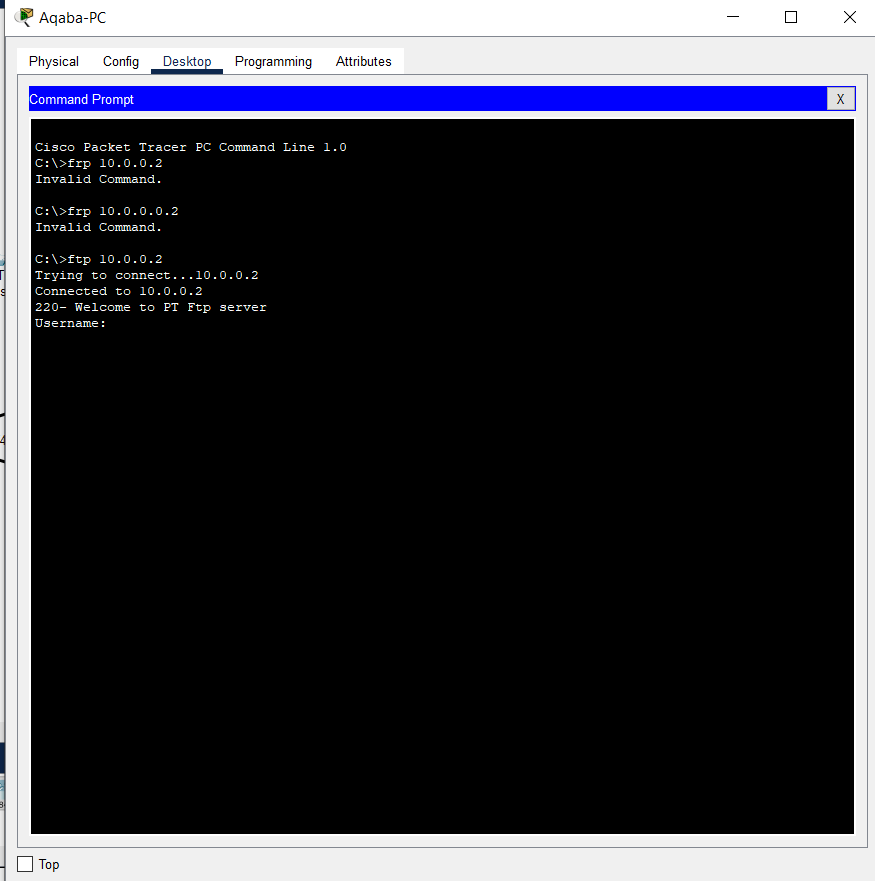
Check the correctness and completeness of the network documentation, which includes network diagrams, device settings, and security guidelines.

Make sure the documentation matches the security configurations and procedures that have been deployed.

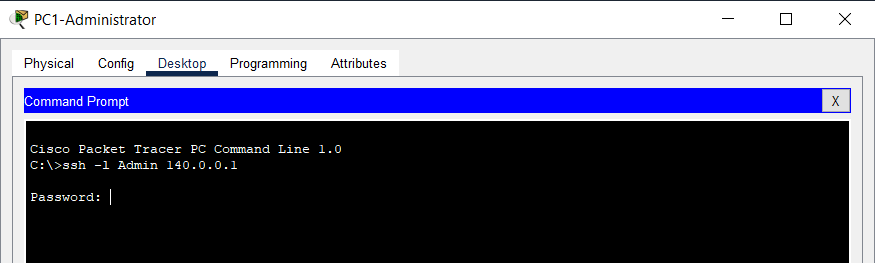
Record all test results, including conclusions, security holes, and correctional advice.

Describe the test methodology, findings, and suggested actions for enhancing network security in a thorough report.

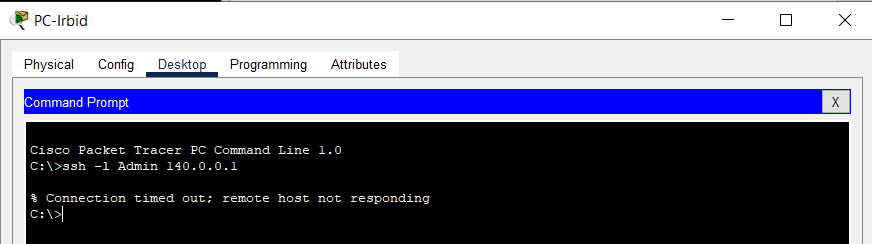
For the ACL I tested the FTP server I tried from the two allowed network and one from the don’t have

access to it, so the first to connect and the third isn’t so its works.

For the ssh to the Aqaba office from PC1 administrator

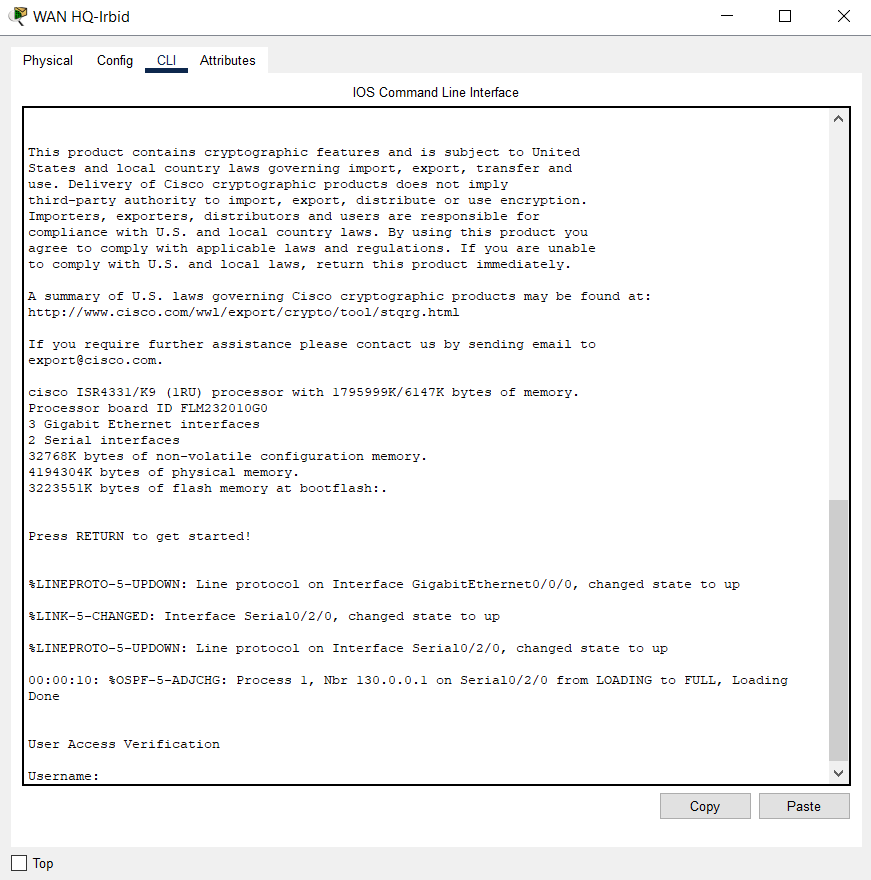


And when I try from another PC

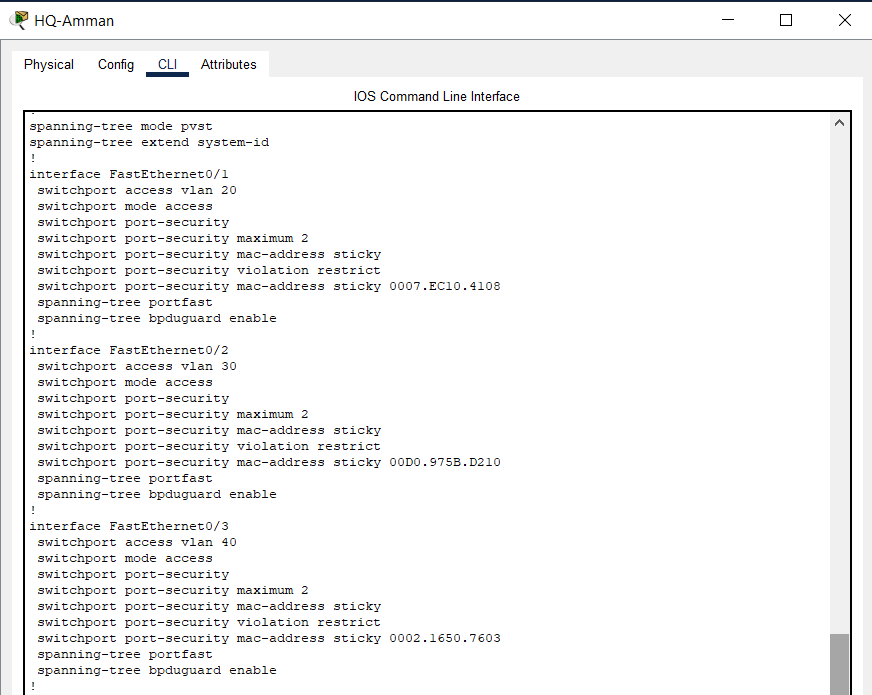


Here in Irbid, I have the AAA and I test it

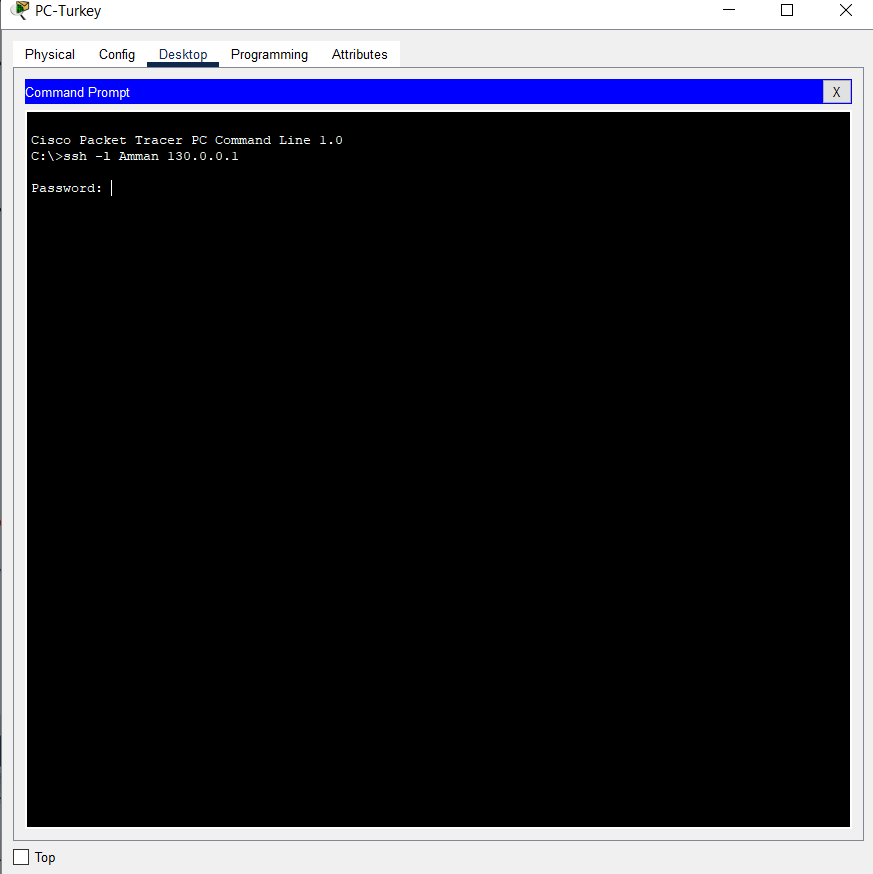
And for every router and switch have a password for the enable mode, ssh, and users (I turned this off to make it easier to get in the router, switch in the packet tracer)

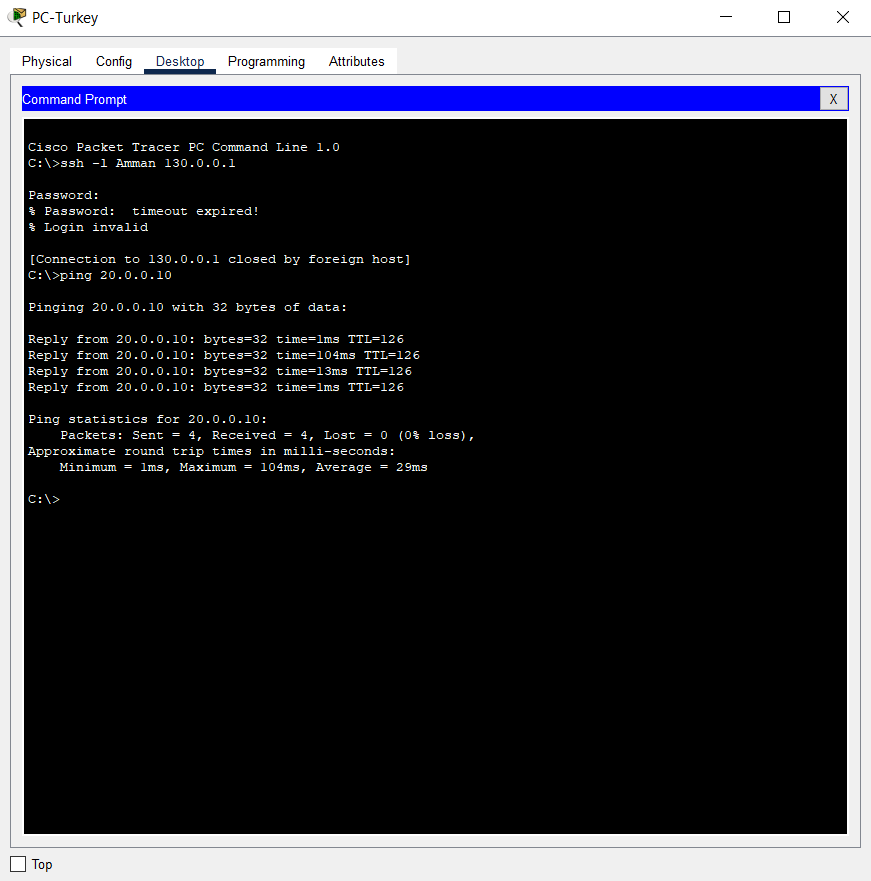


Here we can see it set the port security to all ports and the mac address set to two



Here I test the VPN from turkey to amman by ssh command, and it connect



Here we can see that I can communicate so the routing is successful, and by that I test the gateways

**3-**

Design Assessment:

The network security implementation's general architecture is well-organized and takes into account the need to securely connect satellite offices to the main office.

Network traffic is properly segmented through the use of VLANs and subnetting, improving security and effectiveness.

A appropriate method for securing communication is to construct a VPN/IPsec site-to-site connection for distant offices outside of Jordan.

The setup of DMZs and the usage of the ASA firewall for disaster recovery at the Aqaba office show the need of taking preventative security measures.

Planning Assessment:

The detailed strategy offered a clear road map for developing and putting into place the secure network.

A wide range of network devices and their security settings were taken into account.

It is laudable that best practices for network security have been implemented, including the use of secure passwords, SSH, SSL, IPSec, VPNs, and appropriate access controls.

The network is rigorously tested for security flaws with the use of test plans and test scenarios.

Configuration Assessment:

Best practices for security are followed in the setup of firewalls, routers, switches, gateways, and other network equipment.

Network security is enhanced by the use of routing protocols, VLAN segregation, and access control lists.

Data transmission over networks is more secure and reliable when encryption techniques like AES and SHA are used.

An additional degree of protection is added by configuring AAA authentication for SSH access on the IRBID router.

Testing Assessment:

The developed test strategy includes testing for firewall setups, server vulnerabilities, router operation, and password strength, among other areas of network security.

Potential security flaws can be found through the use of traffic analysis, penetration testing, and vulnerability scanning.

The documenting of test findings and their interpretation offer important insights into the security posture of the network.

Enhancement suggestions:

Use intrusion detection and prevention systems (IDPS) to quickly identify and stop network threats.

Update and patch servers and network equipment often to fix any vulnerabilities that are found.

To find possible security weaknesses and assure continuous adherence to industry standards, conduct recurring security audits and assessments.

Boost network monitoring skills to quickly identify and address security events.

To ensure that all staff members are aware of their roles and responsibilities in ensuring network security, provide security awareness training.