****

**Network Security**

**JNR Network Security**

**10203210**

**M/618/7443**

**Section (1)**

**Submitted to**

Eng Sami AL-Mashaqbeh.

**Submitted by**

Hamza AL-Risheq.

**spring 2022 – 2023**

Table of Contents

[Part 1: 3](#_Toc137902562)

[Part 1.1: 3](#_Toc137902563)

[Part 1.2: 6](#_Toc137902564)

[Part 1.3: 6](#_Toc137902565)

[Part 1.5: 7](#_Toc137902566)

[Part 2: 9](#_Toc137902567)

[Part 2.1: 9](#_Toc137902568)

[Part 2.2: 10](#_Toc137902569)

[Part 2.3: 18](#_Toc137902570)

# Part 1:

## Part 1.1:

1. Amman Network (Head Quarter):

Head Quarter (Amman office): HQ datacenter in this part of the network we will have 3 PC’s and server, each end device is connected in separated vlan so we have to create four vlan’s. Vlan10 include`s server, vlan20 includes employees devices, vlan30 includes human resources devices, and vlan40 includes guests devices. So, we will have to buy a switch, and router. The vlans will be configured in the switch. I will use single area ospf routing protocol.

* Switch security:
  + We must enable port security.
  + Shut downing all unused ports.
  + Configure strong passwords for the vty line and console line.
  + Configure ssh to connect virtually to the switch.
  + Because Amman switch has dhcp server we will do the following:
    - Configure the server port as trust port.
    - Giving all the port in vlan 10 maximum number of rates to protect from dhcp starvation (5).
  + All the used ports except the server port will give them violation restrict.
  + The server port will take shutdown violation.
  + Encrypt all the passwords in the switch by using the following command: service password-encryption.
* Our server must contain the following services:
  + HTTPS.
  + HTTP.
  + DNS.
  + FTP.
  + Email.
* Router security:
  + Configure strong passwords for the vty line and console line.
  + Configure ssh to connect virtually to the switch.
  + Configure VPN using IPSec protocol.
  + Encrypt all the passwords in the router by using the following command: service password-encryption.
  + Create access control list that meet the following requirements on the port for vlan 10 in the outgoing packets:
    - Permit HTTPs server is accessible by all VLANs and LANS.
    - Permit Mail server is accessible by all VLANs and LANS.
    - Permit DNS server is accessible by all VLANs and LANS.
    - Permit FTP server is accessible by only the HQ EMP, and Aqaba office.
    - Permit DHCP server is accessible by only HQ datacenter VLAN.
    - Permit HTTP server is accessible only by HQ EMP LAN.
  + Create access control list for the IPSec: this ACL contains the following command:
    - permit ip any 80.0.0.0 0.255.255.255.
    - permit ip any 70.0.0.0 0.255.255.255

1. Turkey and Saudi networks:

We will need a switch, router, and PC for each network. We must configure single area OSPF routing protocol.

* Switch security:
* We must enable port security.
* Shut downing all unused ports.
* Configure strong passwords for the vty line and console line.
* Configure ssh to connect virtually to the switch.
* All the used ports will give them restrict violation.
* Encrypt all the passwords in the switch by using the following command: service password-encryption.
* Router security:
* Configure strong passwords for the vty line and console line.
* Configure ssh to connect virtually to the switch.
* Configure VPN using IPSec protocol.
* Encrypt all the passwords in the router by using the following command: service password-encryption.
* Create access control list for the IPSec: this ACL contains the following command for Saudi branch:
  + permit ip 70.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255.
  + permit ip 70.0.0.0 0.255.255.255 20.0.0.0 0.255.255.255.
  + permit ip 70.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255.
  + permit ip 70.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255.
* Create access control list for the IPSec: this ACL contains the following command for Turkey branch:
  + permit ip 80.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255.
  + permit ip 80.0.0.0 0.255.255.255 20.0.0.0 0.255.255.255.
  + permit ip 80.0.0.0 0.255.255.255 30.0.0.0 0.255.255.255.
  + permit ip 80.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255.

1. Aqaba branch

We will need a switch, ASA firewall, server, and PC. We have to configure a single area OSPF. For the switch we must create two vlans. Vlan 50 contains PC, and vlan 60 contains server (redundant HTTPS server.):

* + Switch security:
    - We must enable port security.
    - Shut downing all unused ports.
    - Configure strong passwords for the vty line and console line.
    - Configure ssh to connect virtually to the switch.
    - All the used ports except the server port will give them violation restrict.
    - The server port will take shutdown violation.
    - Encrypt all the passwords in the switch by using the following command: service password-encryption.
  + ASA firewall:
* Configure strong passwords for the vty line and console line.
* Configure ssh to connect virtually to the switch.
* Encrypt all the passwords in the router by using the following command: service password-encryption.
* We must configure the DMZ for VLANS (VLAN 50 Private inside, VLAN 60 DMZ, Aqaba WAN as Public Outside.
* We must permit only PC 10.0.0.10 to connect SSH to the ASA firewall in Aqaba.

1. Connectivity between branches:

* All the branches must be connected directly to the Amman network.
* The networks out of Jorden must connect to Amman branch by using VPN site to site (IPSec).
* Amman and Aqaba branches have Vlan’s.
* A picture containing text, screenshot, diagram, line

  Description automatically generatedEach branch must have adopted the security measures that I mentioned to them.

## Part 1.2:

The following are necessary for a secure network:

1. ACL: there are many benefits and usages of ACL. We use it to control and restrict unauthorized access, to control the flow of the packets, controlling the requests and sessions that can be opened and it helps to reduce network traffic.
2. VLAN Segmentation: creating and using VLANs will help to reduce the number of hardware devices which will reduce the number of the devices that we have to protect.
3. Firewall: Firewalls serve as a barrier between internal networks and public networks. They filter and block potentially malicious or illegal data packets in incoming and outgoing network traffic. It is useful in the prevention of unwanted access, network invasions, and malware attacks. The ability to keep an eye on network activity. Threats can potentially jeopardize your operations by accessing and leaving your systems with data. Also, it has IPS to protect the network.
4. VPN: VPN can help to hide private information when someone connects to our network remotely by encrypting the data. Also, it can help to add one more layer of security by changing the real IP address of the source.
5. Triple AAA server: A security system called authentication, authorization, and accounting (AAA) regulates access to computer resources, upholds policies, and audits usage. By screening users and monitoring their online behavior, AAA and its combined operations play a significant part in network management and cybersecurity.

## Part 1.3:

Network devices to use:

* Hardware devices:
  + Routers.
  + Switches.
  + End devices.
  + ASA firewall.
  + Media (cables).
* Software:
  + Services, such as Https, Http, DNS, DHCP, FTP, Email.
  + VPN, using site to site (IPsec).
  + ACL.
  + Single area OSPF routing protocol.
  + SSL.
  + Port security.
  + Triple AAA on routers.
  + SSH.

## Part 1.5:

Justification for the choices made in the network security configuration that was implemented:

* + Firewalls:
    - We used ASA firewall which is cisco firewall. We chose this type of firewall because ASA firewall delivers many things such as, IPS, IDS, ACL stateful, anti-virus, SSL device, VPN device, and antispam.
  + Router:
    - Are used to choosing the best path for the packet then forward it. Also, we can use it as a security measure by adding an ACL in port ingoing or outgoing which will increase the security.
    - Also, are used in NAT which will help to hide the private IP and use the public IP. As result it will increase security.
  + Switches:
    - Used to create many Vlans (virtual lans in one physical switch). So, it will split the network traffic so it will improve security. Because using Vlan reduced the device that needs to be secured and in new versions of switches we can create ACL to control the network traffic.
  + Gateways:
    - Gateways serve as a point of connection for networks with various protocols or architectural styles.
  + Passwords:
    - Using strong unique passwords will increase the security in the network because it will be hard to guess by using brute force technique. Also, passwords must be updated every 3 months to increase security. Furthermore, demanding additional verification for access, enabling multi-factor authentication offers a further layer of security.
  + SSH:
    - Between two devices linked via an open network, such as the internet, a Secure Shell connection can be protected using both public key authentication and a strong password. In addition to offering secure encryption, SSH is frequently used to remotely administer systems and programs, allowing network administrators to connect to another computer across a network and run commands and move files.
    - We must use SSH to connect to switches, routers, and ASA firewall remotely because SSH encrypts the connection and protects against unauthorized access.
  + SSL:
    - Ensures the security of data transit between a web browser and a server. All data exchanged between a web server and a browser is kept private and secure thanks to SSL, which encrypts the connection between them.
  + IPSec (Internet Protocol Security):
    - A collection of protocols known as IPsec is used to secure connections between devices. Data transported over open networks is kept secure with the help of IPsec. It functions by encrypting IP packets and authenticating the source from which the packets originate, and it is frequently used to build up VPNs.
    - It offers data confidentiality, integrity, and authentication. Additionally, it describes the authenticated, encrypted, and decrypted packets. It defines the protocols required for safe key management and key exchange.
  + VPN (virtual private network):
    - VPN offers an encrypted between a device and a network via the Internet is known as a virtual private network, or VPN. The two ends of the connection produce a common encryption key before configuring the VPN connection. Secure transmission of sensitive data is aided by the encrypted connection. It makes it impossible for unauthorized parties to eavesdrop on the traffic and enables remote work for the user.
  + HTTPs:
    - The main purpose of HTTPS is to offer a higher level of security than the open HTTP protocol for sensitive data and transactions including user logins, credit card transactions, and billing information. regardless of whether the connection is compromised, HTTPS uses SSL or TLS encryption to encrypt each data packet while it is in transit, preventing intermediary hackers and attackers from obtaining the communication's content.
  + FTPs:
    - We should use FTPs not FTP because it is a file protocol with Secure Sockets Layer (SSL) that encrypts data to protect information during transmission.
    - Also support Secure Transmission, Screen sessions, SSH3 protocol implementation, and command execution over SSH channel.
  + DHCP:
    - A network's IP addresses can be managed automatically with the help of DHCP. Device IP addresses are assigned dynamically, doing away with the requirement for manual setting. So, by automating IP address assignment, centralizing IP address management, implementing access control via MAC address filtering enabling network segmentation and enabling monitoring and analysis of IP address assignments.

# Part 2:

## Part 2.1:

Testing plan:

Firstly, we must determine the objectives that we have to test:

* Network devices:
  + Firewall.
  + Routers.
  + End device.
  + Servers.
  + ACLs.
* Network security.

Secondly, create the test plan for each object:

* Network devices test plan:

|  |  |
| --- | --- |
| Devices: | Testing method: |
| Routers | Traceroute from end device to another device in different network. |
| Switches: | Pinging two devices in same network. |
| Servers: | Trying to open a website from any devices.  Trying to upload a file to FTP.  For DHCP check the end device within the same network if they got an IP address or not. |
| Firewall: | By checking the configuration of the firewall specially the configuration for choosing the public, private and the DMZ zones.  Test the firewall's ability to inspect and filter application-layer protocols, such as HTTPs.  Finally review the logs. |
| ACL: | Trying to do something the opposite of the thing inside the ACL if it works that means the ACL is not working normally. |

* Network Security test plan:
  + Firstly, we have to do network scanning for all the network by using the following tools:
    - Nmap, Zenmap: is a useful method for finding operating services, open ports, and active hosts on the network.
    - SuperScan: is a useful method for teating everything in the network, such as TCP SYN scanning, Simple HTML report generation, Source port scanning, and Extensive banner grabbing capabilities etc.
  + Secondly, we have to check the vulnerabilities in network by using the following methods:
    - Nessus.
    - GFI LANguard
  + Thirdly, penetration testing:
    - By simulating real-world attacks and attempt to bypass the firewall's security controls.
    - Metasploit.
    - Trying to attack our network by real attacks.
  + Fourthly, Password cracking by using the following methods:
    - L0phtCrack.
    - John the Ripper.
  + Fifthly, log review,
    - By checking and detecting the logs that the firewall and triple aaa server have.
    - SIEM: SIEM provides many functions, such as Forensic analysis, Correlation, Aggregation, and Retention.
  + Sixthly, Integrity checkers:
    - By checking the hash value of the packets.
  + Seventhly, Viruses detection:
    - By using antiviruses application, such as Macfee.

## Part 2.2:

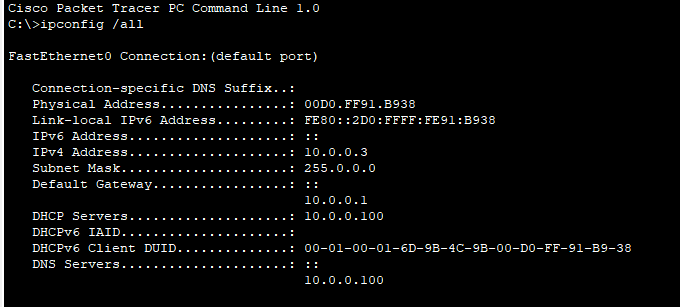
* Servers: we have to test all the services that the servers provide it. We have 5 main servers which are DHCP, FTP, HTTP, HTTPS, and DNS.

|  |  |  |
| --- | --- | --- |
| What we are testing: | The expected results: | Results: |
| DHCP | When we go to the device within same network with DHCP server then choose the dynamic IP they must take Ips. | All the devices that must take Ips from the DHCP server took Ips. |
| FTP | When we try to open the FTP server from an end device it must open. | When I tried to open FTP server from an end device it works correctly. |
| HTTP | If we tried to open a website from the end device and that website already existed in the server, it must open. The only end device is accessible to use HTTP is HQ EMP | It works correctly because when we tried to open the website by using HTTP protocol it worked. And the only device that can use HTTP is HE EMP device. |
| HTTPS | If we tried to open a website from the end device and that website already existed in the server, it must open. All the devices can use HTTPs to open the website. | It works correctly because when we tried to open the website by using HTTPs protocol it worked. And we can test that from any end device. |
| DNS | If we tried to open our website by using the website name, it must work if the DNS protocol is working correctly. | When I try to open the website by writing the website name it worked normally. |

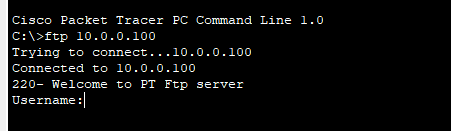
DHCP testing results:

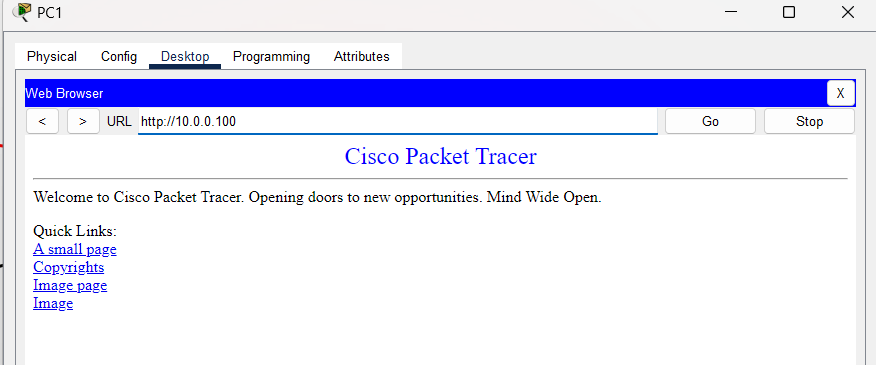
A screenshot of a computer

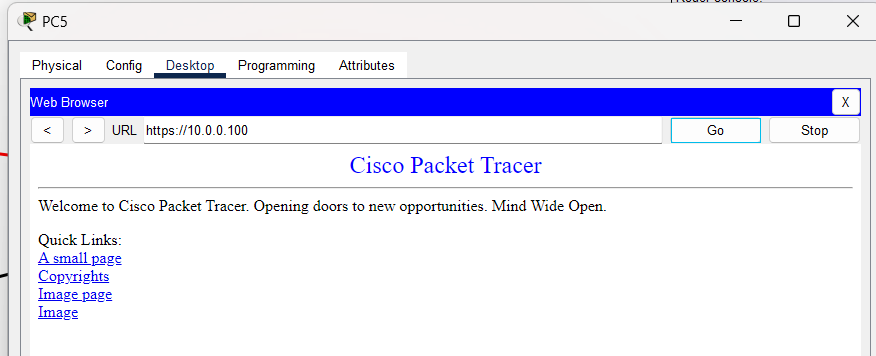
Description automatically generated with medium confidence

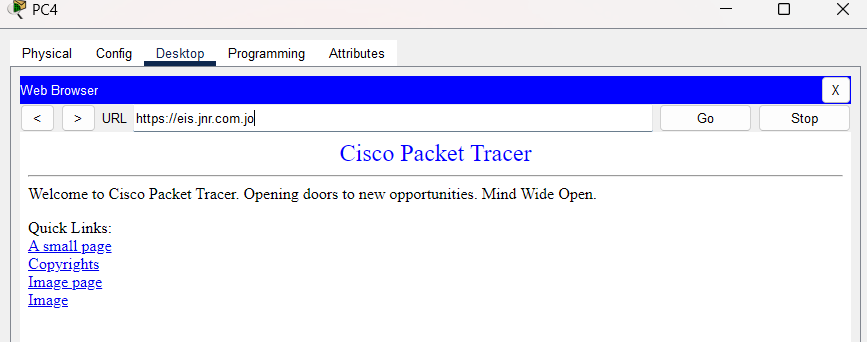


FTP testing result:



HTTP testing result:

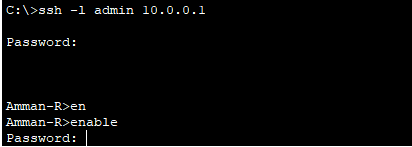
HTTPs testing result:

DNS testing result:

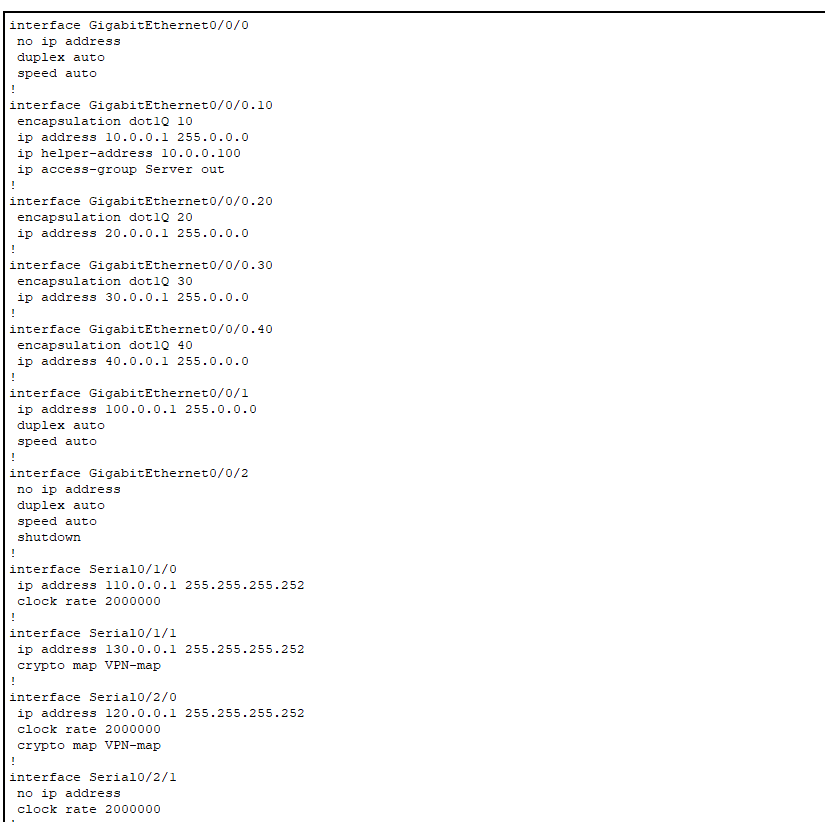
* Routers:

|  |  |  |
| --- | --- | --- |
| What to be tested: | The expected results: | Results: |
| That the routing protocol that we are using is working normally. (OSPF) | When we try to open the website by HTTPs protocol from a device out of the network it must open the website. | When I tried to open the website from the PC in Irbid network, it worked normally. |
| Amman ACL. | That the ACL commands are working correctly. To test that if we tried to open the website by using HTTP it must not work because the only network that accessible to open the website by using HTTP is HQ EMP. | When I tried to open the website from Irbid device by using HTTP it did not work, which means that the ACL is working correctly. |
| SSH | If we tried to connect to the router remotely it must work by using SSH protocol. | When I tried to connect to Amman router from Saudi PC by using SSH protocol it worked. |
| Checking that all the ports in the router has the correct IP and configuration. | That based on the scenario each port has specific IP.  We can check that by the writing this command in the router “show running-config” | That each port has the correct IP. |

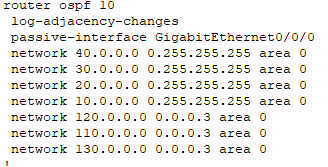
SSH testing result:



Router ports testing result:



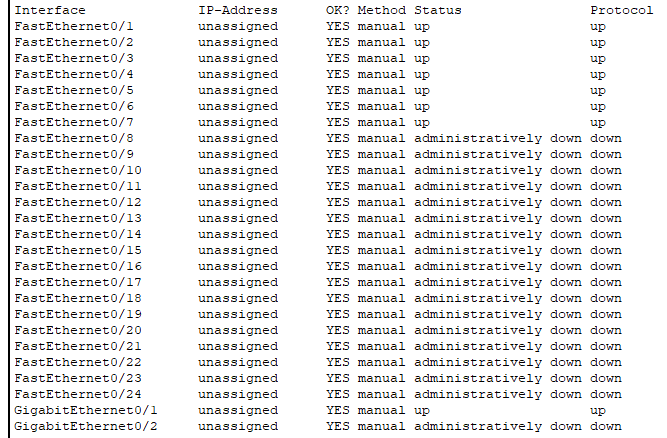
OSPF testing results:



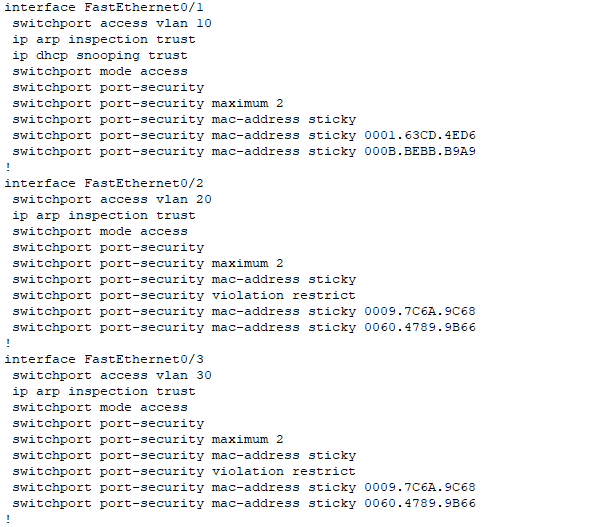
* Switches:

|  |  |  |
| --- | --- | --- |
| What to be tested: | The expected results: | Results: |
| That all the unused port shutdown. | By the “show ip interface brief” command when we write in the switch it will show us the shutdown and un shutdown ports. | Only the used ports are working all the other ports are shutdown which is what we are looking for. |
| Port security. | By the “show running-config” command when we write in the switch it will show us the shutdown and un shutdown ports.  Also, we can from using this command “show port-security”. | When we check our configuration for each port. We find all the configuration are done correctly that’s mean we configured the port security correctly. |
| SSH | If we tried to connect to the switch remotely it must work by using SSH protocol. | When I tried to connect to Amman switch from Saudi PC by using SSH protocol it worked. |

unused port shutdown testing result:



Port security testing result:



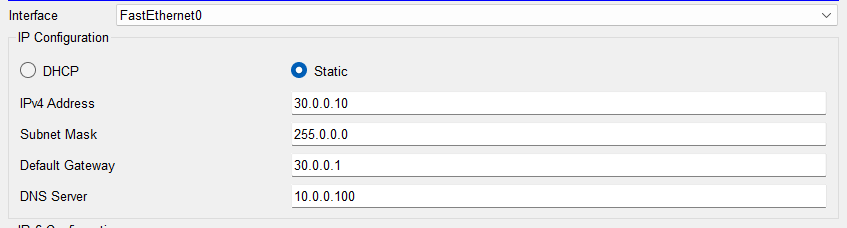
A picture containing text, screenshot, font, number

Description automatically generated

* Gateways:

|  |  |  |
| --- | --- | --- |
| What to be tested: | The expected results: | Results: |
| That all the gateways took the correct IP | Each network has corrected gateway. Also, all the device in each network has the correct gate IP. | All the networks have correct gateway and all the devices have correct IP gatewat. |

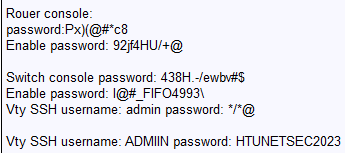
Sample of device in Amman network has the correct gateway:



* Passwords:

|  |  |  |
| --- | --- | --- |
| What to be tested: | The expected results: | Results: |
| The strength for the passwords that we are using. | Strong passwords are created from numbers, letters, and symbols. Minimum password 8 characters. (Unique passwords). | All our passwords are strong passwords. |

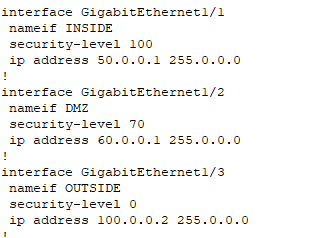
Sample of the passwords that I used (Password testing results):



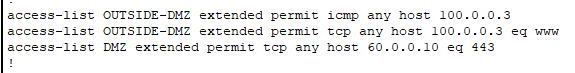
* Firewall:

|  |  |  |
| --- | --- | --- |
| What to be tested: | The expected results: | Results: |
| Configuration of the zones are correct with correct security number. | That the inside zone has the biggest security number then the outside has the least, and the DMZ has number between inside and outside number. | Inside zone has 100.  Outside has 0.  DMZ has 70. |
| ACL. | That the ACL configured well that no one can get access to the inside zone (private). Also, the ACL must deny everything except the HTTPS request. | Permit only HTTPS and deny everything else. Also, permit SSH only from PC 1 in vlan 10. Which is the correct ACL. |
| Firewall Rules: | Experiment with different services and ports from different source IPs to see how successful the firewall rules are. | Trying to access the private network from outside the firewall dropped the packet and prevent it which is the correct results. |
| Network Address Translation (NAT) | Translating private to public. | When we try to go outside the network the device will go with public IP which means that the NAT is working correctly. |
| SSH Access: | Try to connect to firewall remotely with SSH. | I tried to connect to the firewall from Amman network by using SSH and it work correctly. |

Results of configuration the zones:

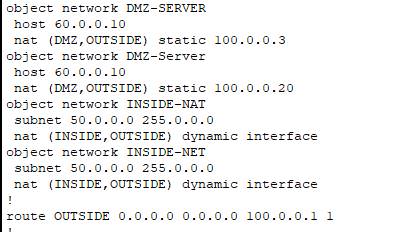


Results of ACL:d





Results of firewall rules:



## Part 2.3:

To evaluate the design that I create we must evaluate many things:

* Network architecture: the network that I designed met all the requirements, all the branches connected with Amman office, each branch has specific devices based on the scenario, and based on the requirements we have main 2 servers (2 assets).
* Security policy: I have designed security polices to protect the assets and the network from attack and malware. Also, the security policies that I employed. They ensure comprehensive, up to date, and aligned with industry best practices and compliance requirements.
* Configuration: all the configurations that I used are the best configuration for our scenario to meet JNR company requirements, and to protect the assets.
* Based on the testing planes and testing results we will find out that the design, configurations, devices, and the security policies are the best practices to meet the requirements of the JNR company.

Improvement recommendations:

* Implement redundant cables between the devices (trying to create partially mesh topology.)
* Implement centralized log management and correlation, use security information and event management (SIEM).
* Implement firewalls for all the networks.
* Implement IPS system to the firewalls.
* Implement redundant servers for all the services.
* Use 3-way authentication to access the data center room.
* Use WSA to the ASA firewalls.
* Use triple AAA server. (Implement the server to all the servers).
* Employees should get regular security awareness training to inform them of potential hazards as well as how to recognize and report security events.
* Update and patch network hardware, software, and operating systems often to fix known vulnerabilities.

# References:

Cloud Infrastructure Services. (2022). *SFTP vs FTPS - What’s the Difference for Secure FTP (Pros and Cons)*. [online] Available at: <https://cloudinfrastructureservices.co.uk/sftp-vs-ftps-whats-the-difference-for-secure-ftp/>.

Poston, H. (2020). *10 Most Popular Password Cracking Tools [Updated 2020]*. [online] Infosec Resources. Available at: <https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/>.

MyBib Contributors (2019). *Harvard Referencing Generator – FREE – (updated for 2019)*. [online] MyBib. Available at: <https://www.mybib.com/tools/harvard-referencing-generator>.

Cisco (2019). *Cisco Adaptive Security Appliance (ASA) Software*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html>.

Hamza Khan (2014). *What is SSL?* [online] SSL.com. Available at: <https://www.ssl.com/faqs/faq-what-is-ssl/>.

Loshin, P. (2021). *What is SSH (Secure Shell)? Definition from SearchSecurity*. [online] SearchSecurity. Available at: <https://www.techtarget.com/searchsecurity/definition/Secure-Shell>.

‌Imperva (n.d.). *What is Access Control List | ACL Types & Linux vs Windows | Imperva*. [online] Learning Center. Available at: <https://www.imperva.com/learn/data-security/access-control-list-acl/>.

www.microsoft.com. (n.d.). *What is SIEM? | Microsoft Security*. [online] Available at: <https://www.microsoft.com/en-us/security/business/security-101/what-is-siem#:~:text=SIEM%20defined->.

Techopedia.com. (n.d.). *What is Security Policy? - Definition from Techopedia*. [online] Available at: <https://www.techopedia.com/definition/4099/security-policy#:~:text=A%20security%20policy%20is%20a>.