**Ahmad Marwan Maghaireh**

**23110205**

**1. Introduction**

AI Security Inc. is a technology company specializing in artificial intelligence solutions with its headquarters in Amman, Jordan. As part of its expansion, it is setting up offices in Oman, Kuwait, Saudi Arabia, and Qatar. Ensuring a secure and reliable network architecture is critical for interconnecting these offices while maintaining data confidentiality, integrity, and availability (CIA). This report outlines the design, configuration, and testing of a secure network for AI Security Inc., focusing on network security best practices and threat mitigation strategies.

**2. Network Security Principles, Protocols, and Standards**

**Overview of Network Security**

Network security involves protecting network infrastructure and data from unauthorized access, cyberattacks, and data breaches. It includes implementing security devices, cryptographic techniques, and access control mechanisms to safeguard organizational assets.

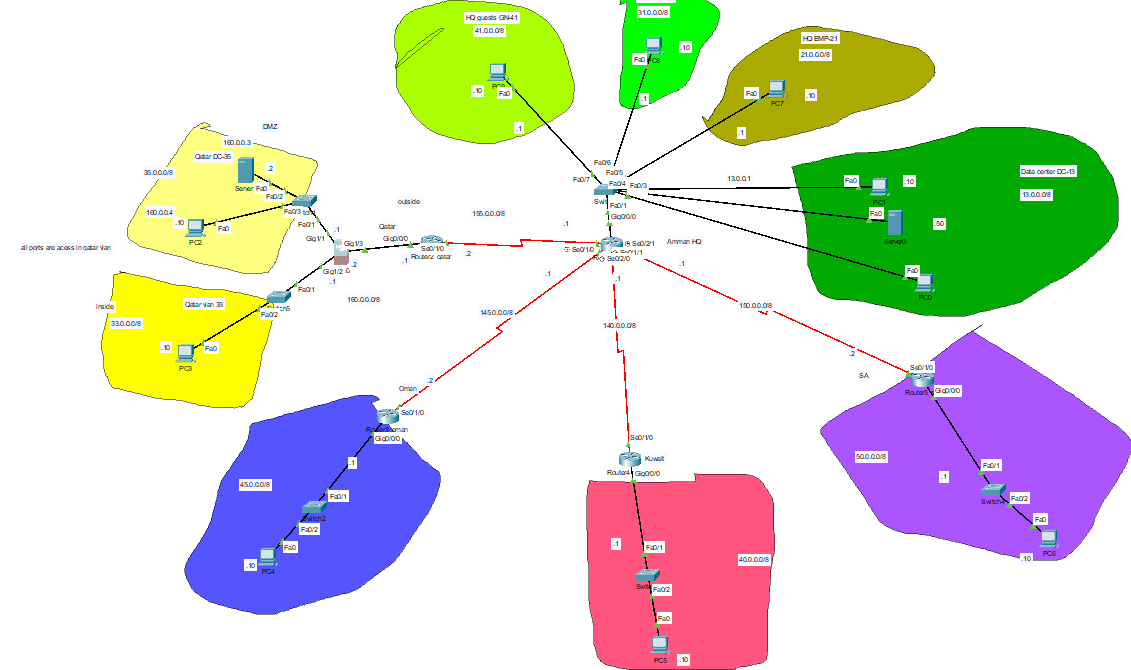
**Network Security Devices**

* **Firewalls:** Used to filter and monitor incoming/outgoing traffic.
* **Routers and Switches:** Configured with security policies to prevent unauthorized access.
* **VPN Gateways:** Securely connect remote offices to the headquarters.

**Network Security Protocols**

* **IPSec VPN:** Ensures encrypted communication between sites.
* **HTTPS (SSL/TLS):** Encrypts web-based communications.
* **SSH:** Provides secure remote access to network devices.

**3. Secure Network Design**

****

**A computer network diagram with different colored squares

AI-generated content may be incorrect.**

**A map of a network

AI-generated content may be incorrect.**

**Business Requirements and Constraints**

AI Security Inc. requires a network that enables secure data transfer between remote offices and the Amman data center while ensuring high availability and protection against cyber threats.

**Network Topology and Design**

* **HQ Datacenter:** Hosts critical services such as HTTPS, FTP, DHCP, and DNS.
* **Remote Offices:** Each location has a dedicated subnet with secure VPN access.
* **Qatar Office:** Functions as a disaster recovery site with VLAN 33 (internal) and VLAN 35 (DMZ).

**Hardware and Software Selection**

* **Cisco ASA Firewall:** Deployed in Qatar for securing network traffic.
* **Cisco Routers and Switches:** Used for efficient traffic management and security enforcement.
* **Packet Tracer:** Used for network simulation and security testing.

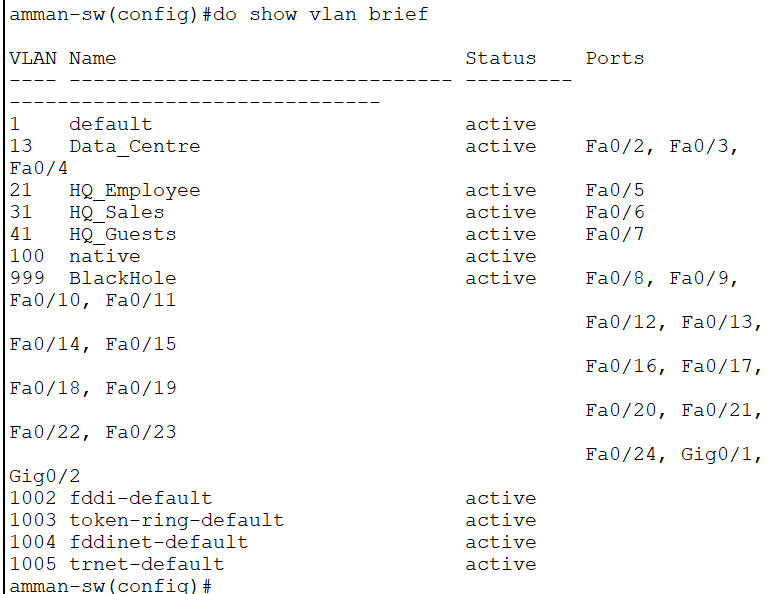
**Step-by-Step Plan for Secure Network Development in Packet Tracer**

**Phase 1: Planning and Network Design**

1. **Identify Business and Security Requirements**
   * Ensure connectivity between HQ, remote offices, and the Qatar disaster recovery site.
   * Maintain CIA (Confidentiality, Integrity, Availability).
   * Implement VLANs and VPNs for secure access.
   * Use an ASA firewall to protect Qatar’s network.
2. **Define Network Topology**
   * Create a detailed topology for HQ, Qatar, and remote sites.
   * Assign subnets for each VLAN and interconnecting WANs.
   * Document IP addressing for devices.

**Phase 2: Network Setup in Packet Tracer**

1. **Deploy Network Devices**
   * Add Cisco routers, switches, and an ASA firewall.
   * Place end-user devices like PCs and servers.
   * Label interfaces based on topology.
2. **Configure IP Addressing**
   * Assign static IPs to critical devices (servers, firewalls, and gateway routers).
   * Configure dynamic IPs for employees via DHCP in hq datacenter
   * Set up subnets for each VLAN.
3. **Implement VLANs and Inter-VLAN Routing**
   * Create VLAN 33 (Inside) and VLAN 35 (DMZ) for Qatar.
   * Configure VLAN 13 for the data center.
   * Set up trunk ports for inter-VLAN routing.



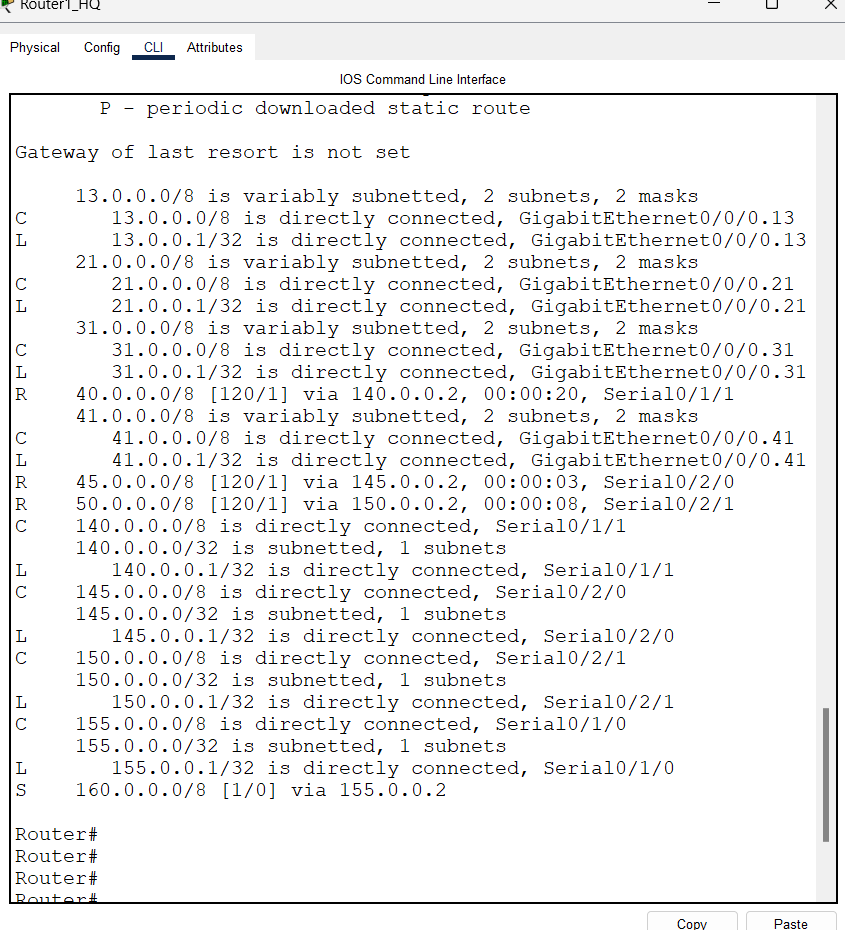
Qatar switch :

A screenshot of a computer

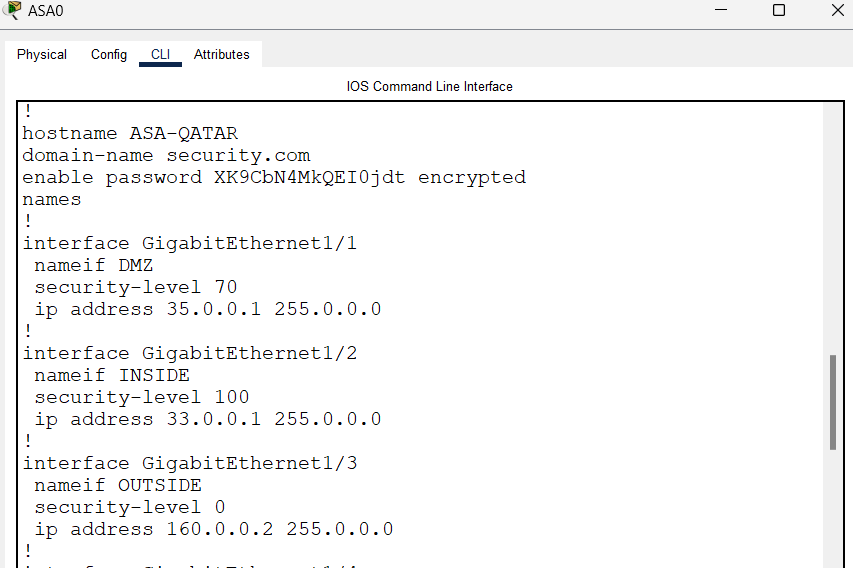
AI-generated content may be incorrect.

**Phase 3: Security Implementation**

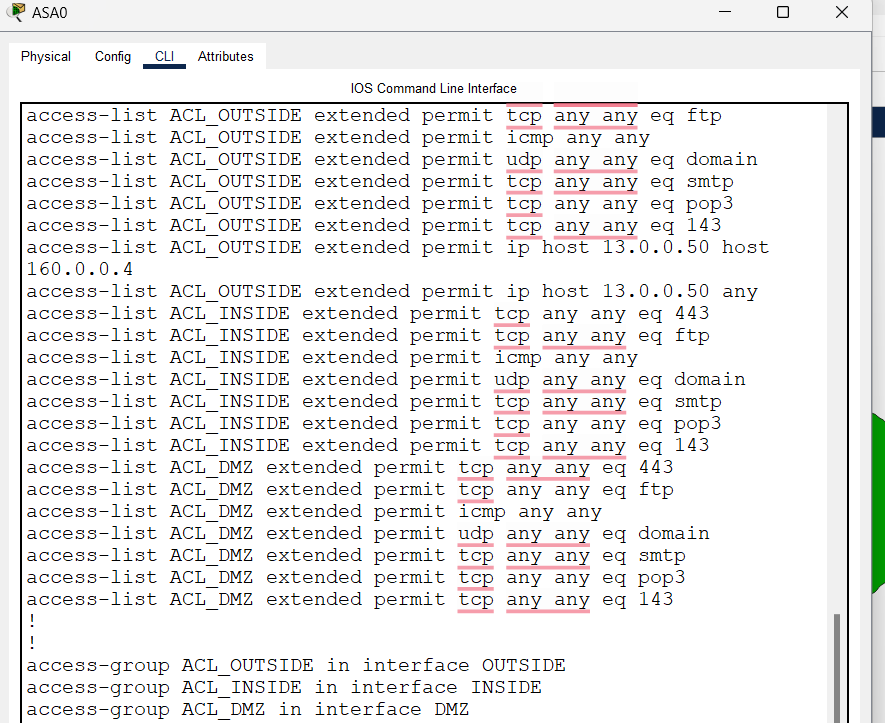
1. **Configure Routing**
   * Implement **RIP** for inter-office connectivity.
   * Apply static routing on routers for secure, controlled traffic flow.



1. **Deploy ASA Firewall in Qatar**
   * Configure **inside (VLAN 33), DMZ (VLAN 35), and outside (WAN) interfaces**.



* + Define **access control lists (ACLs)** to restrict unauthorized traffic.

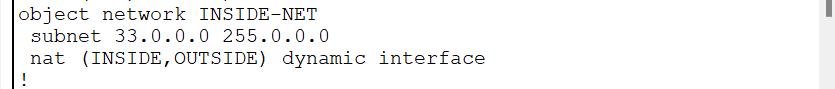


1. **Configure Network Address Translation (NAT)**
   * Apply **static NAT for DMZ servers** to be publicly accessible.

A white background with black text

AI-generated content may be incorrect.

* + Configure **dynamic NAT for inside users** to access external resources.



Default route :



Ssh and inspection :



1. **Set Up VPN (IPSec) for Remote Offices**
   * Create a **site-to-site VPN** to encrypt communication between offices.
   * Use IPSec tunnels to secure data exchange with the data center.

Evidence and screenshot below

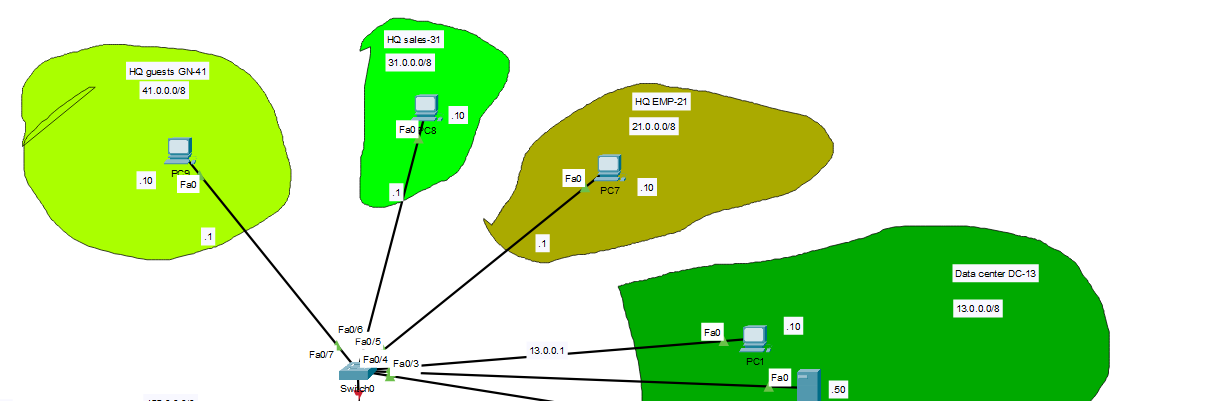
1. **Enable Secure Communication Protocols**

* **SSH** for router and firewall access.
* **HTTPS** for internal web applications.

1. Cisco ASA Firewall Configuration  
Implementation:  
  
Set up ASA firewall as perimeter security for Qatar office.  
Set up three interfaces:  
INSIDE (VLAN 33 - Private)  
DMZ (VLAN 35 - Redundant HTTP Server)  
OUTSIDE (Public WAN)  
Access Control Lists (ACLs) implemented:  
Permitted HTTPS, FTP, ICMP, DNS, and email services.  
Denied unauthorized access from outside networks.  
Allowed internal devices to access VLAN 13 services.  
  
Justification:  
  
The ASA firewall protects the Qatar office by controlling incoming and outgoing traffic.  
ACLs implement least privilege access to essential services.  
NAT (Network Address Translation) safeguards internal devices from being exposed to outside threats.  
  
2. Router Security  
Implementation:  
  
Configured static routes for direct control of data flows.  
Disabled unnecessary services.  
Implemented access control lists (ACLs) to allow only essential traffic.  
Enforced SSH via Telnet for remote management.  
  
Rationale:  
  
Avoids unauthorized access to routers.  
Minimizes exposure to routing-based attacks (e.g., route poisoning).  
Reduces the attack surface by restricting services.  
  
3. Switch Security  
Implementation:  
  
Port Security set to permit a maximum of two MAC addresses per port.  
Unused switch ports disabled to prevent unauthorized device connections.  
DHCP Snooping enabled to protect against spoofing attacks.  
  
Justification:  
  
Protects against MAC flooding attacks.  
Only authorized devices can connect to switch ports.  
Rogue DHCP servers cannot provide malicious IP addresses.  
  
4. Secure Authentication (Passwords, SSH, AAA)  
Implementation:  
  
SSH (Secure Shell) enabled for remotely connecting to equipment securely.  
AAA (Authentication, Authorization, Accounting) configured on the Saudi Arabia router through RADIUS.  
Strong password policies enforced:  
Encryption used on stored passwords.  
  
Reasoning:  
  
Blocks unauthorized access to devices.  
AAA ensures centralized authentication of users.  
SSH provides encrypted remote management over insecure networks.  
  
5. SSL & HTTPS Configuration  
Implementation:  
  
Configured HTTPS for secure web traffic.  
Ensured encryption of employees' access to the website  
SSL certificates are configured to secure HTTPS connections.  
  
Justification:  
  
Encrypts sensitive information (login details, files).  
Prevents man-in-the-middle (MITM) attacks.  
Maintains data integrity and confidentiality.  
  
6. IPSec VPN (For Secure Remote Access)  
Implementation:  
  
IPSec VPN tunnels established to connect remote offices (Oman, Kuwait, Saudi Arabia) securely with HQ.  
Pre-shared keys and encryption algorithms (AES-256) utilized.  
  
Justification:  
  
Allows secure communication across untrusted networks.  
Safeguards data in transit against interception and alteration.  
Allows employees to access company resources securely from remote locations.  
  
7. FTP & Secure File Transfers  
Implementation:  
  
Configured VLAN 13 (HQ Data Center) FTP service for file sharing.  
Limited FTP access to HQ Employees and Qatar Office only.  
Configured FTPS (FTP over SSL) for encryption.  
  
Justification:  
  
Allows secure file transfers in internal communication.  
Bars unauthorized access to company files.  
Guarantees data integrity in file transfers.  
  
8. DHCP Configuration  
Implementation:  
  
DHCP configuration in VLAN 13 (HQ Data Center) for dynamic IP assignment.  
DHCP Snooping enabled on switches to prevent rogue DHCP servers.  
  
Justification:  
  
Makes IP address management simpler.  
Prevents rogue DHCP attacks that divert traffic to malicious websites.  
  
9. DNS Security  
Implementation:  
  
DNS server set up in VLAN 13 (HQ Data Center).  
ACL has been applied to permit DNS queries only from trusted internal networks.  
  
Justification:  
  
Guarantees stable domain resolution.  
Prevents DNS spoofing and cache poisoning attacks.

**Evaluation of the Importance of Network Security**  
1. Protection of Sensitive Data  
  
AI Security Inc. handles confidential project details and client information.  
Without security, data breaches would lead to financial losses and loss of reputation.  
  
2. Business Continuity and Availability  
  
A secure network ensures uptime and reduces downtime due to cyberattacks.  
Redundant systems (Qatar DR site, VPNs) allow business continuity during downtime.  
  
3. Compliance with Industry Standards  
  
Encryption, VPNs, and firewalls meet GDPR, ISO 27001, and other security standards.  
Complies with laws and regulations.  
  
4. Protection from Cyber Threats  
  
Ransomware, phishing, and DDoS attacks are hazardous cyber threats.  
Implemented firewalls, ACLs, VPNs, and intrusion detection systems to thwart threats.  
  
5. Secure Remote Work and Branch Offices  
  
IPSec VPN offers Omani, Kuwaiti, and Saudi Arabian workers secure remote access.  
Blocks unauthorized access to business resources.  
  
6. Maintenance of Customer Trust  
  
Customers expect secure handling of their data.  
Network security measures enhance customer trust and safeguard business reputation

Switch 0 configrations :

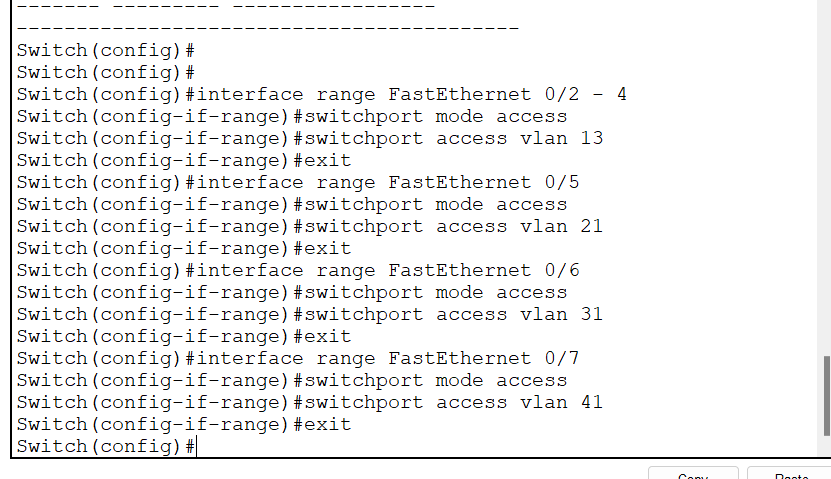


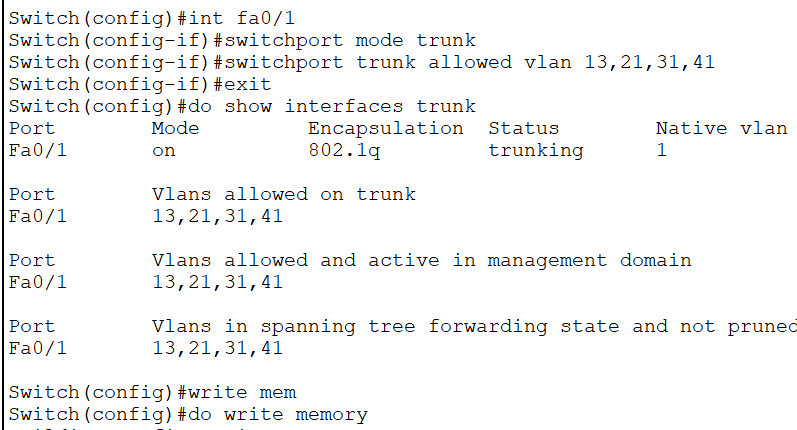
A screenshot of a computer program

Description automatically generated

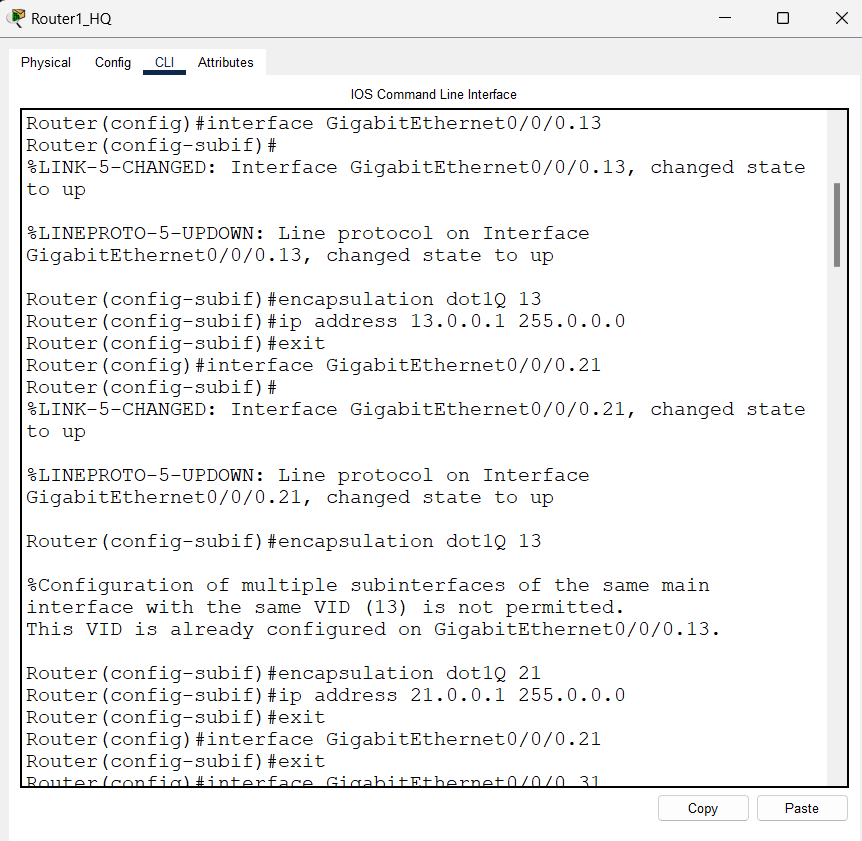
A close-up of a text

Description automatically generated





Router 1\_HQ

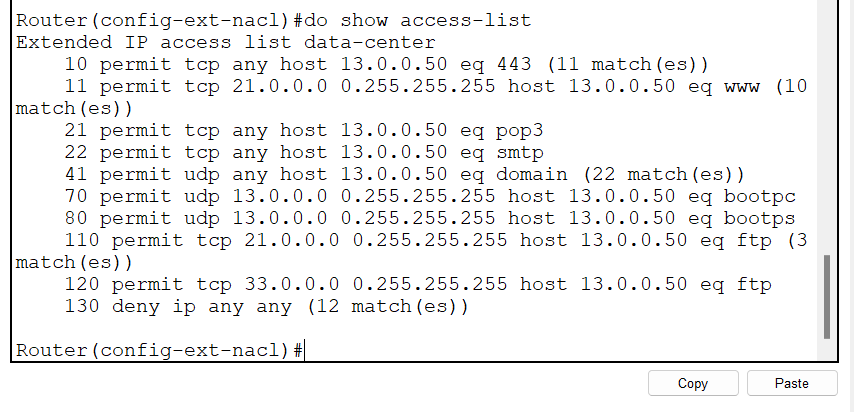


A screenshot of a computer

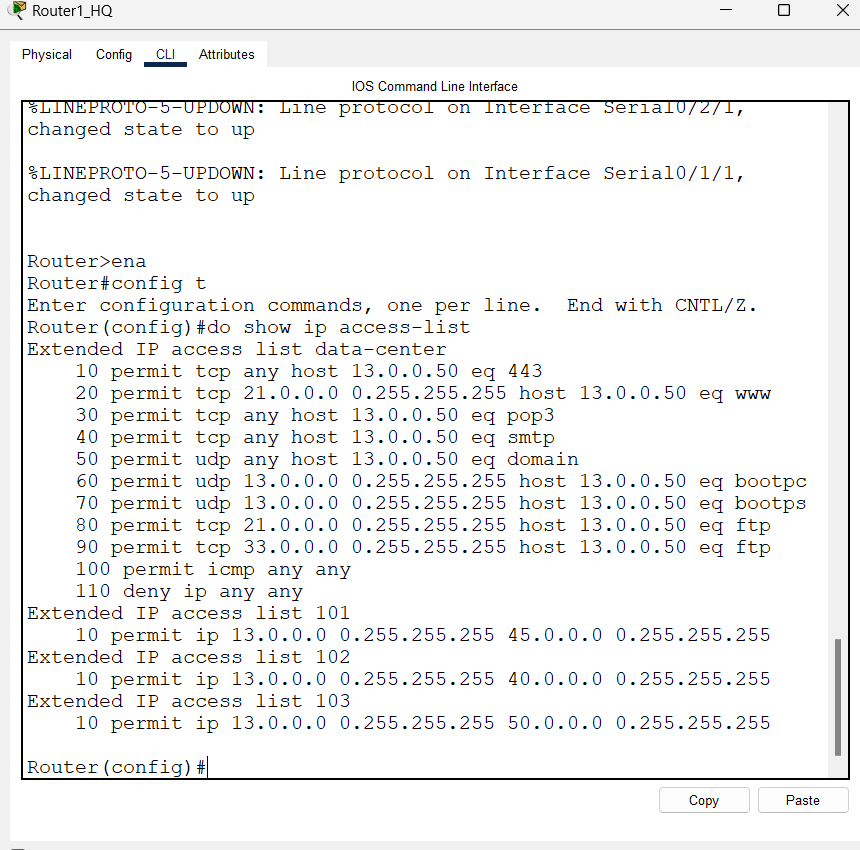
Description automatically generated

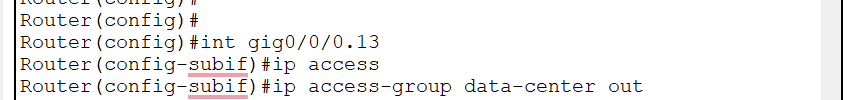
ACL





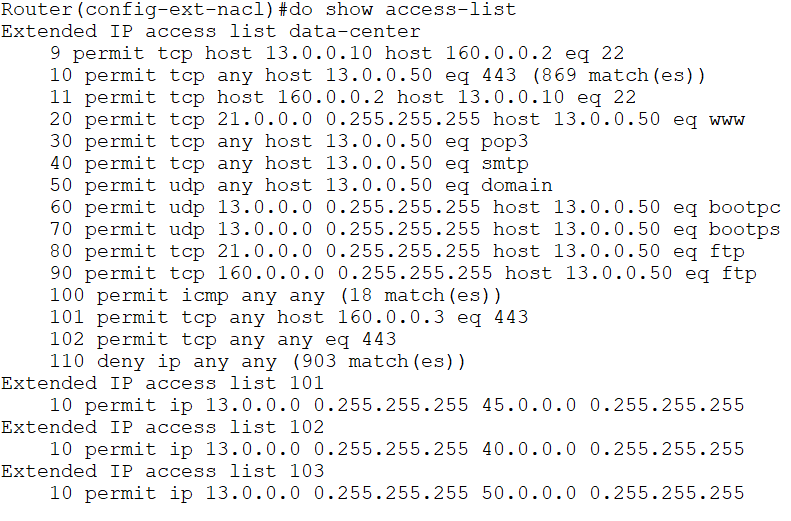
I add a rule to allow ping between devices





I added rules to allow trafic for the qatar network (ssh,ftp,https)

And I updated the address for the qatar office after implementing nat :

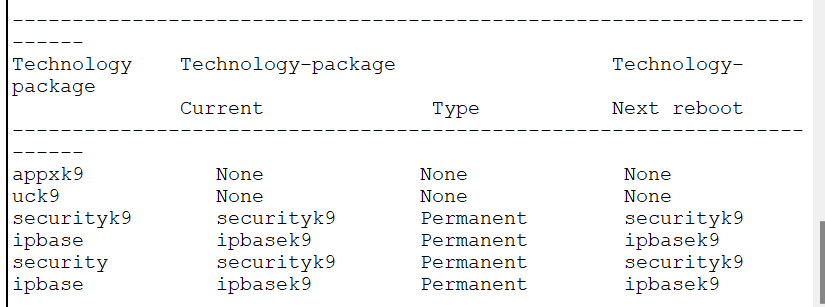


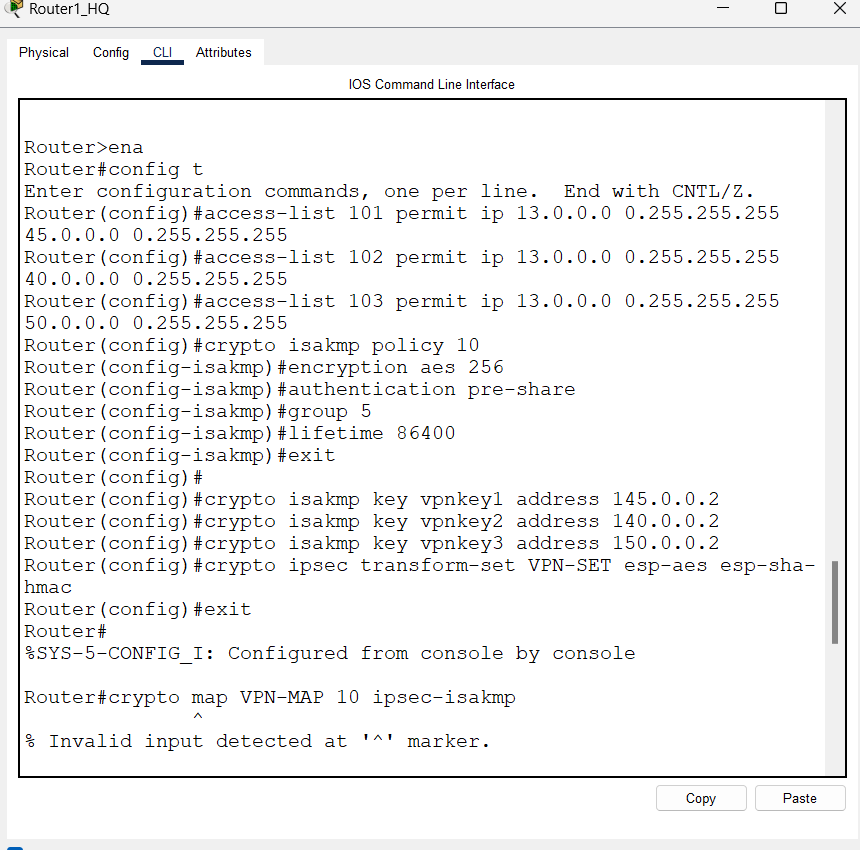
Vpn

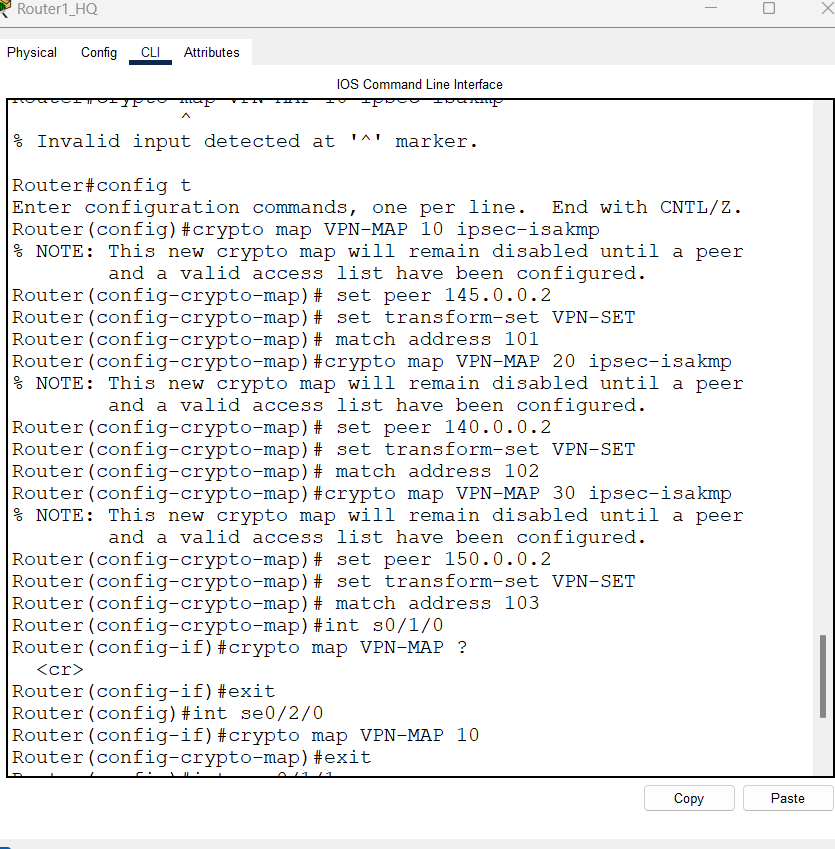
I run :

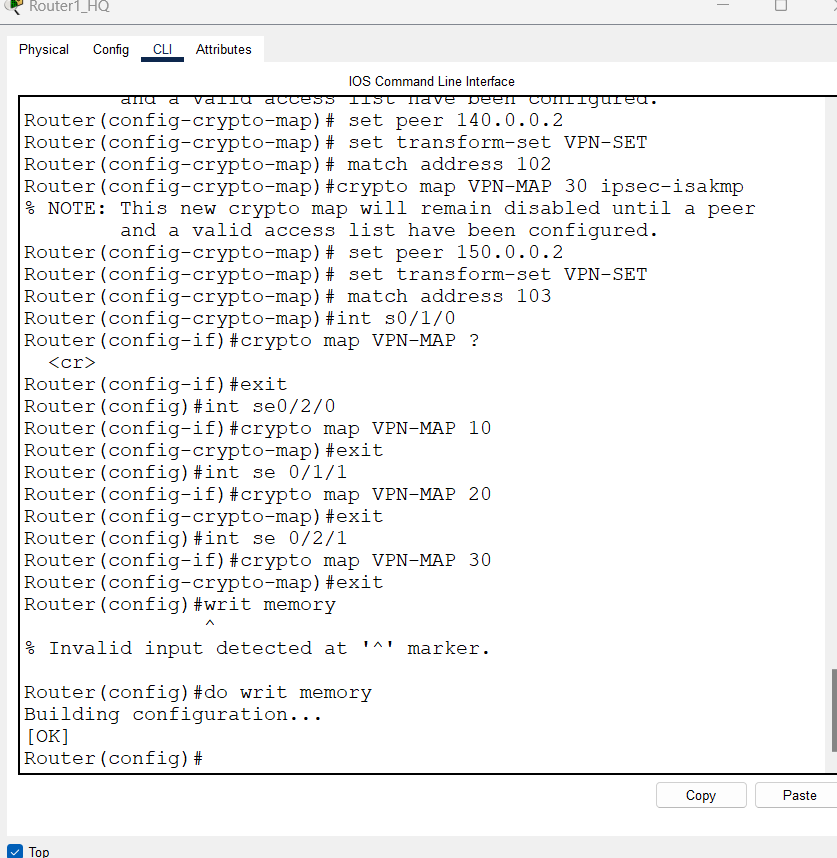
do show version

I already have the package so no need to install it and reboot the router

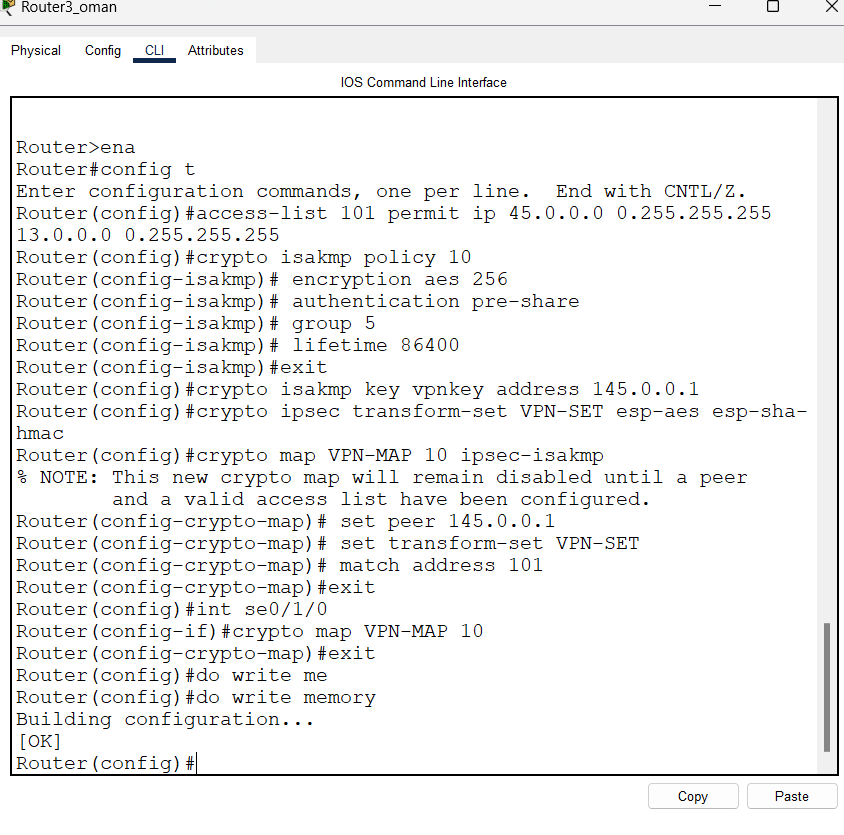


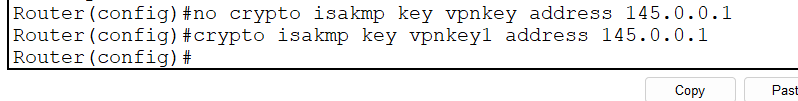




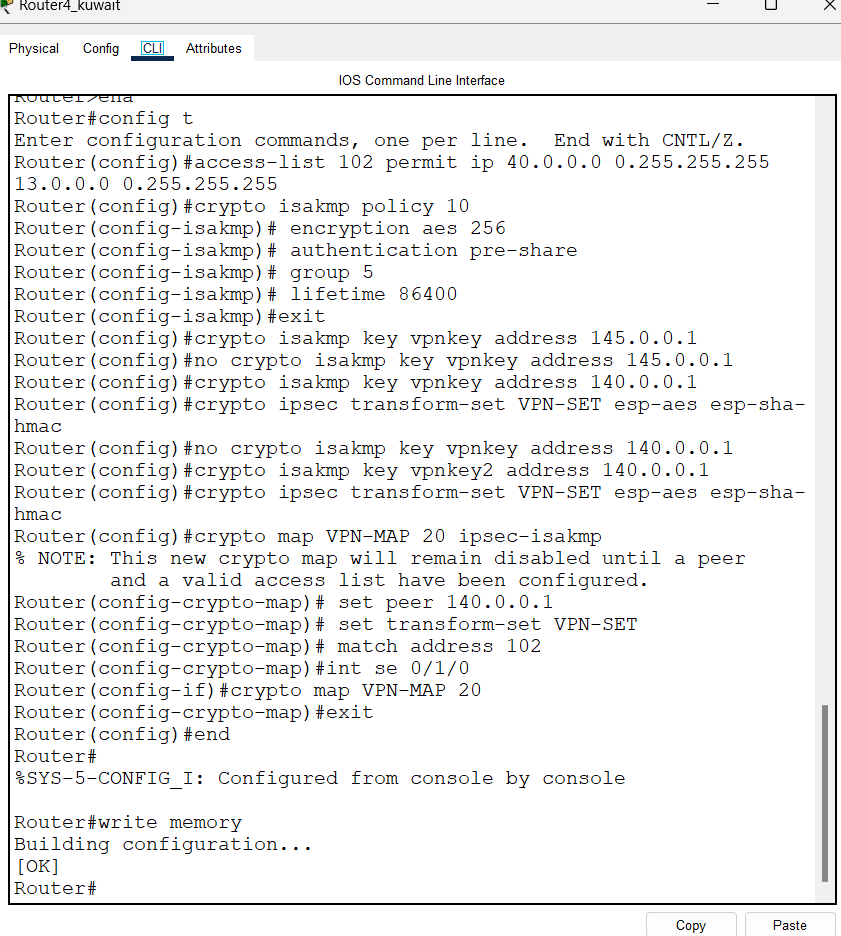


Oman

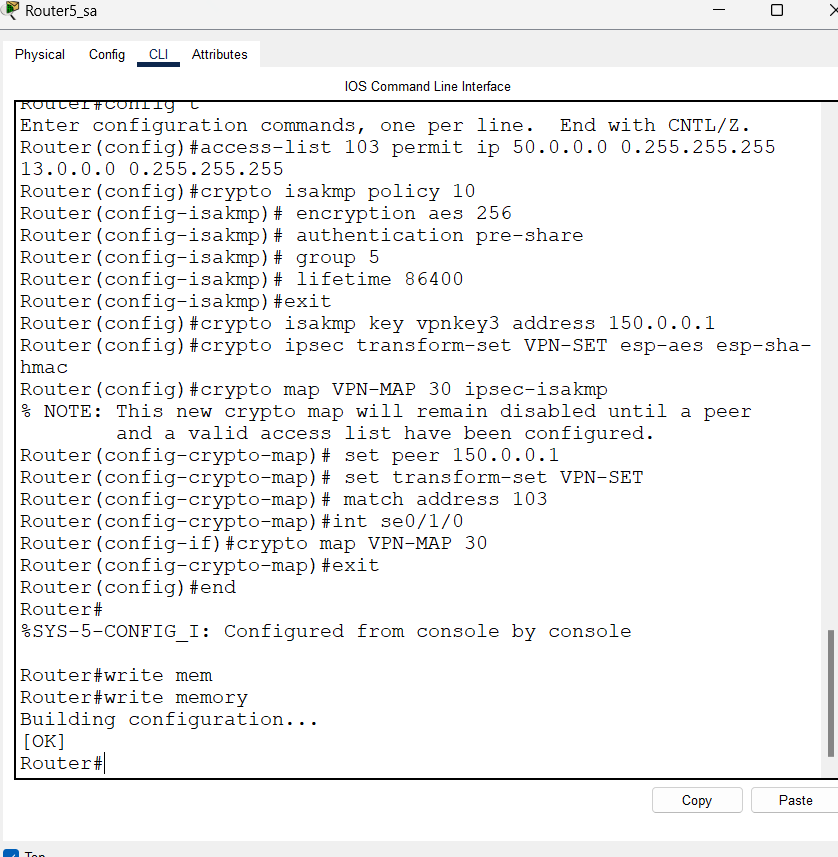




Kuwait

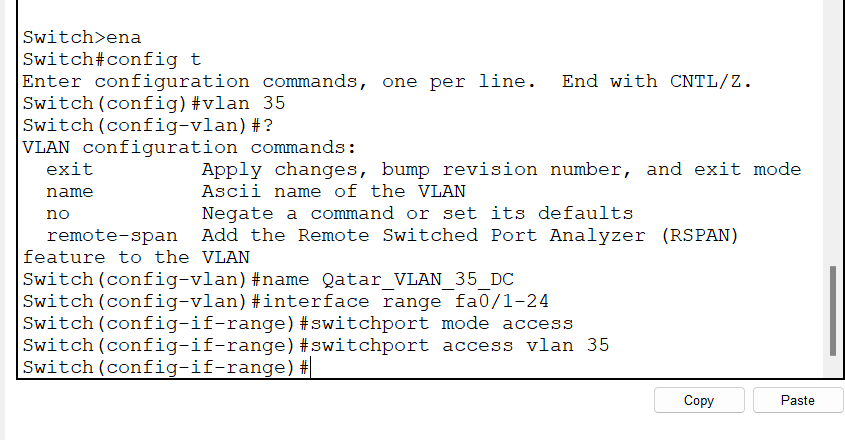


Sa

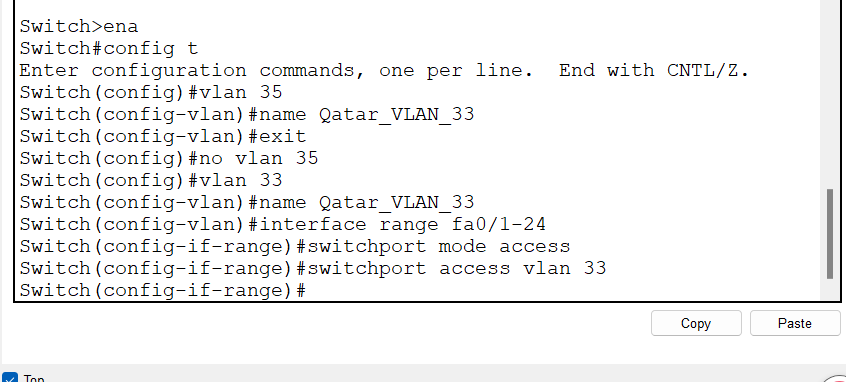


Instead of crypto map VPN-MAP (num) I modified it to be without the num in the interfaces “crypto map VPN-MAP”

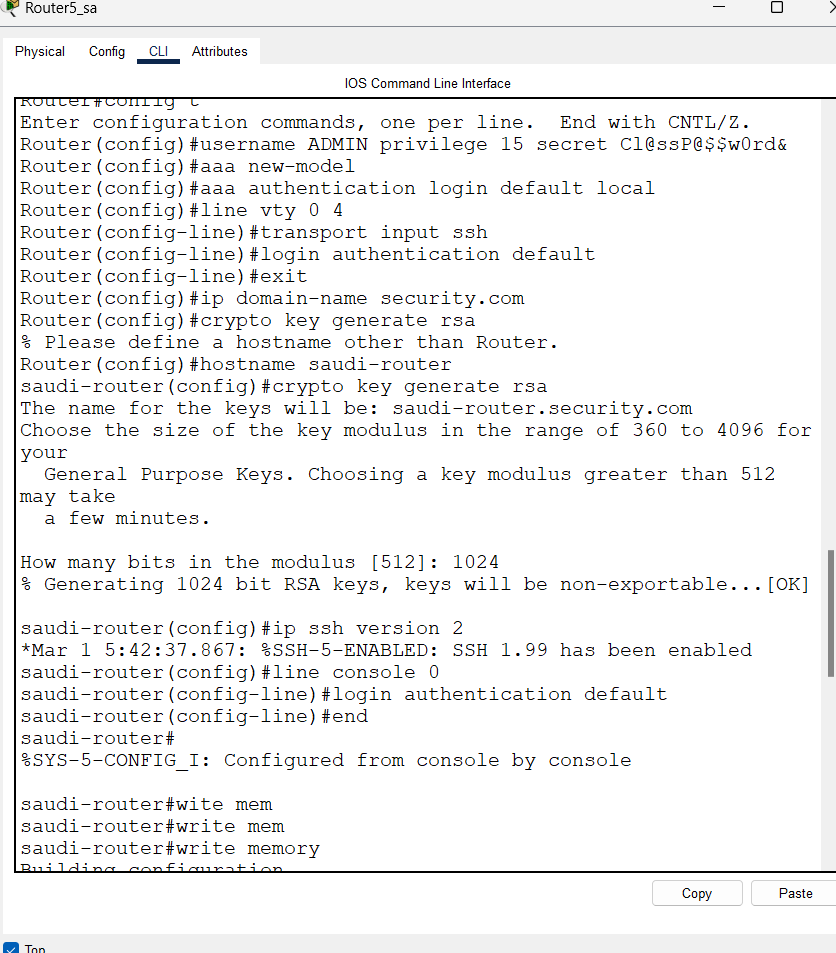
Switch1



Switch 5



SA router aaa



Switch security

Amman switch :

1. Set Strong Passwords

line console 0

password console123

login

exit

line vty 0 4

password vty123

login

transport input ssh

exit

enable secret ena123

ip domain-name security.com

hostname (depends on the switch)

crypto key generate rsa

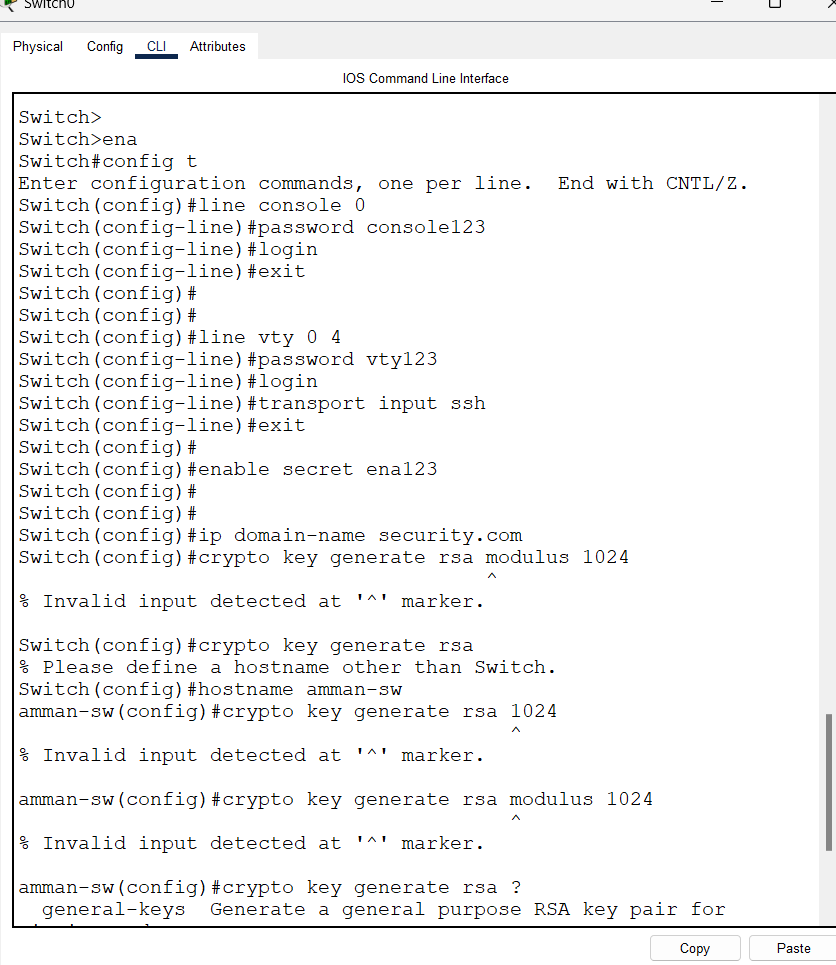
1024

ip ssh version 2

line vty 0 4

transport input ssh

exit

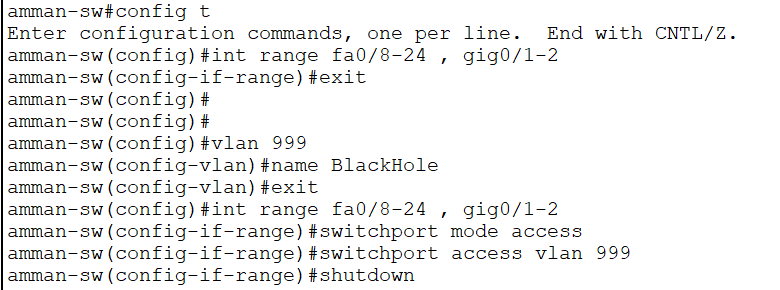


A screenshot of a computer code

Description automatically generated

Same thing for other switches but with different hostnames

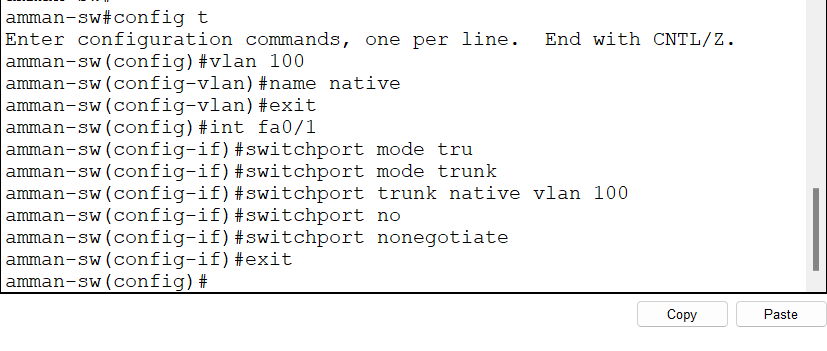
Shutdown Unused Ports :



Same thing for other switches but different interfaces

Port security :

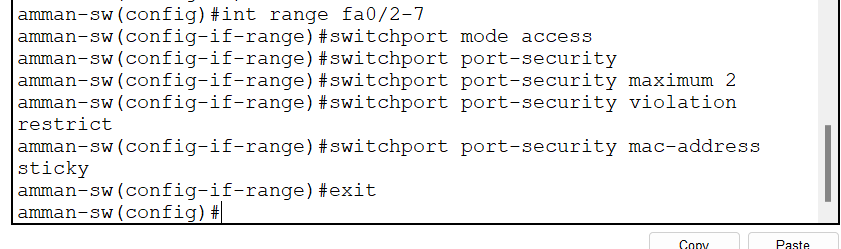
Secure Trunk ports :



Only applied on amman switch because other switches don’t have a trunk port because it have a stick desghn with one vlan so no need for trunking

And the Qatar vlan are al access ports because threre is a firewall

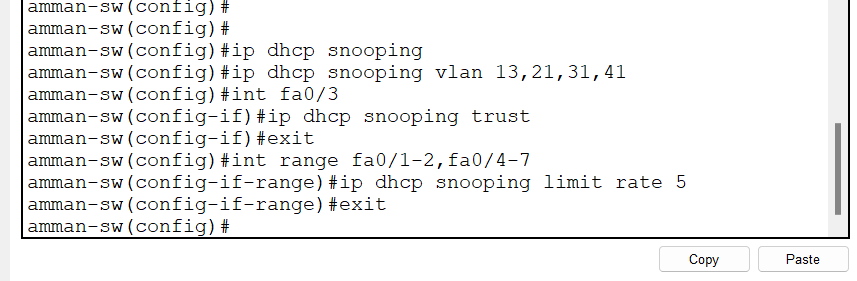
Port security :



Same thing for other switches but different interfaces

(we only apply port security to interfaces that have access mode , the int that connects to end devices )

Dhcp snooping



The fa0/3 is the interface the connect to the dhcp server , I didn’t include the fa0/1 that connects to the router because the only dhcp server I have is on fa0/3

There is no need to apply dhcp snooping on other switches because they don’t have dahcp pool , I only configured dhcp for data center vlan

Apply PortFast and BPDU Guard

A black text on a white background

Description automatically generated

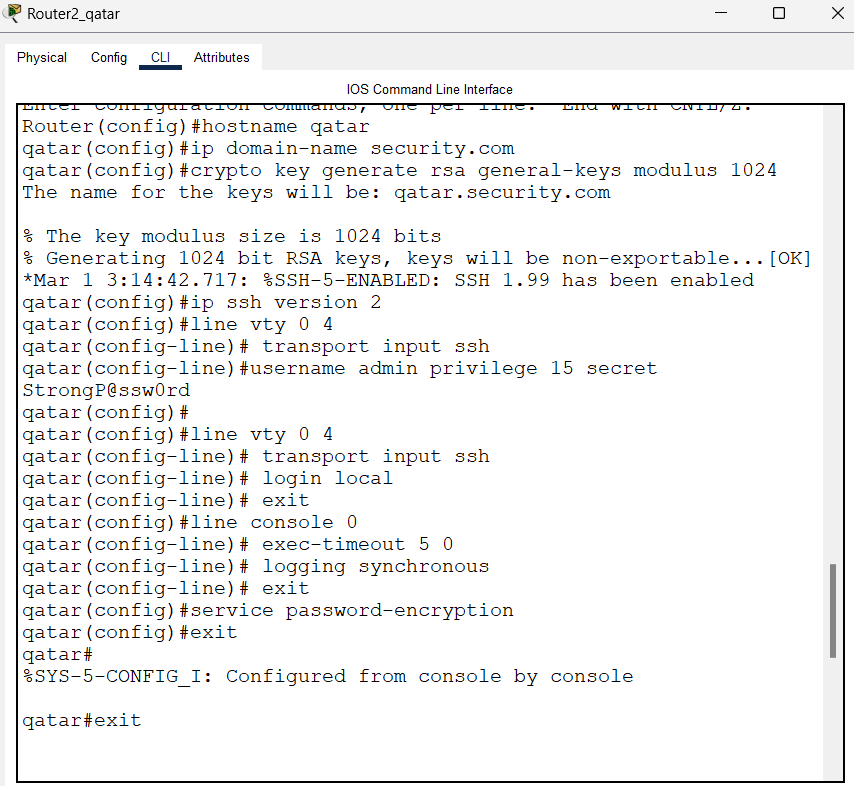
A close-up of a computer screen

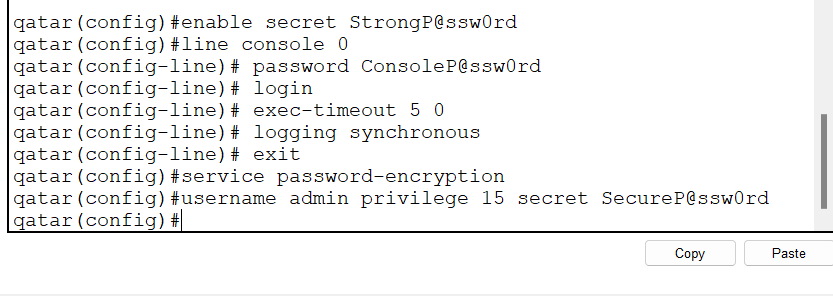
Description automatically generated

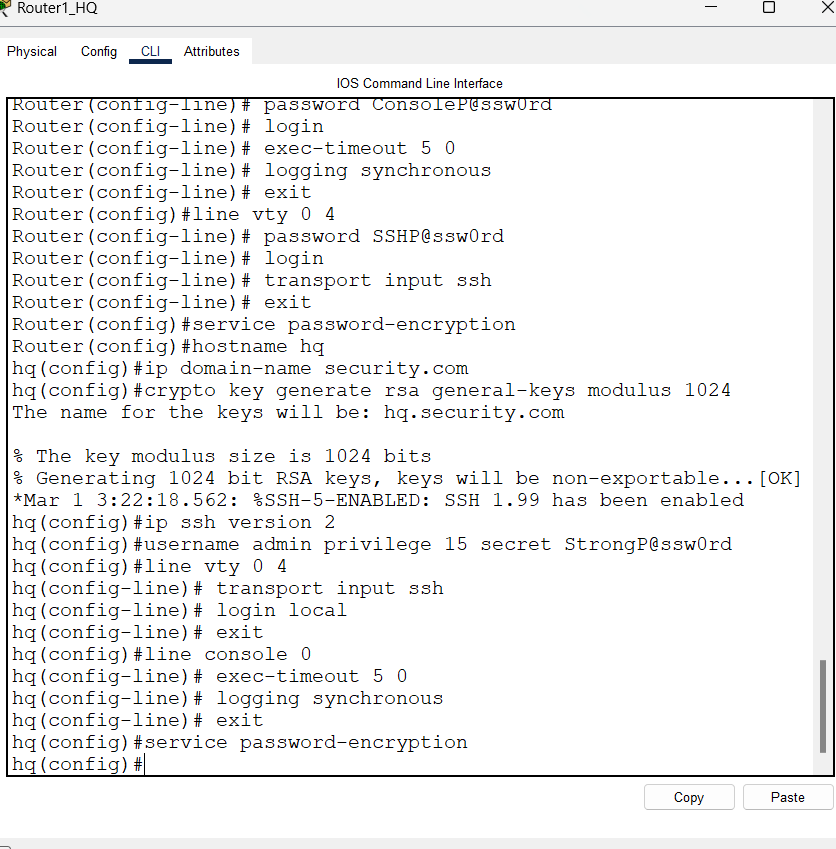
Same thing to all switches , applied on access ports only

1. **Harden Routers**

**Enable ssh on router**

****

****

****

**Rip passive interface no rip updates to this interface :**

**A close-up of a black line

AI-generated content may be incorrect.**

**Network Security Test Plan and Testing Commands**

This **test plan** outlines a structured approach to verify the security and functionality of the network implemented in **Cisco Packet Tracer**. It covers **firewalls, routers, switches, passwords, and various security protocols**.

**1. Test Plan Overview**

This test plan is designed to assess:

* **Network connectivity** (ping, traceroute)
* **Access control and firewall rules** (ACLs, NAT)
* **Router and switch security measures** (SSH, strong passwords)
* **VPN/IPSec functionality**
* **Server accessibility** (HTTPS, FTP, DNS)
* **Device authentication (passwords and access control)**

**2. Testing Methods & Commands**

**A. Network Connectivity Testing**

**Check basic connectivity using Ping**

✅ Expected Result: Successful response for all **allowed connections**  
❌ Failure indicates a misconfigured firewall, ACL, or routing issue.

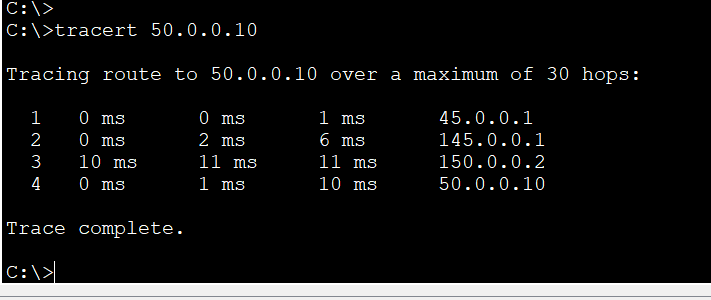
A screenshot of a computer

AI-generated content may be incorrect.

Check the path of packets using Traceroute

✅ Expected Result: Shows all routers in the path

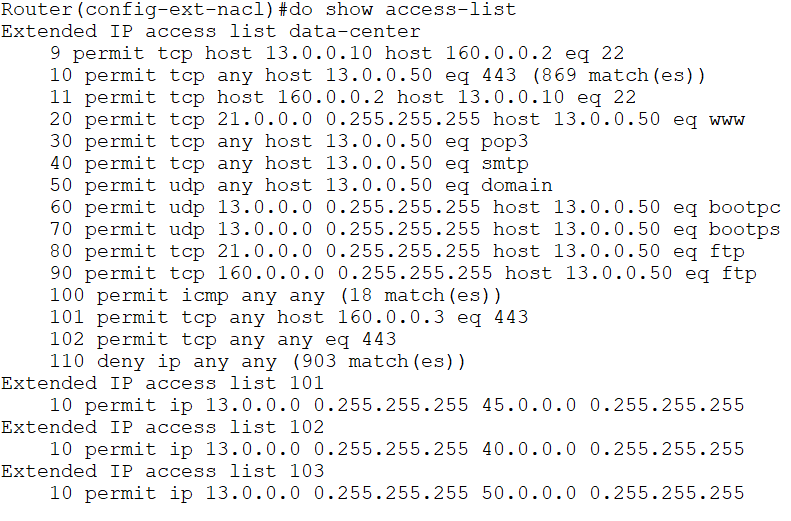
❌ If packets are blocked, check firewall rules and routing.



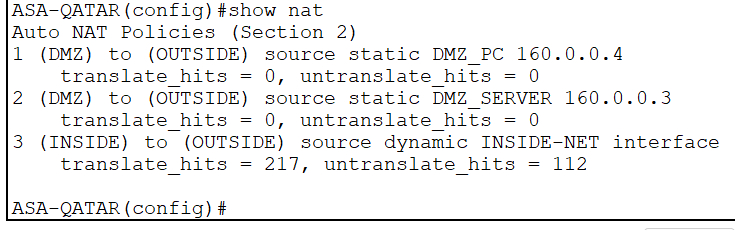
B. Firewall & ACL Testing

Verify applied ACL rules on ASA Firewall

✅ Expected Result: **ACLs should allow authorized services** while blocking others.



**Verify NAT configuration**



See if the ip changes :

A screenshot of a computer

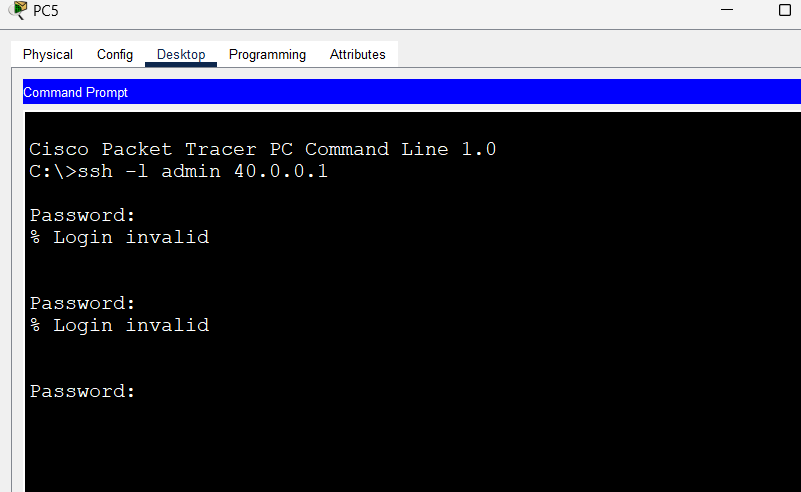
AI-generated content may be incorrect.

✅ Expected Result: Static and dynamic NAT translations should be correctly applied.

C. Router Security Testing

Attempt tpo enter worng password :

In ssh



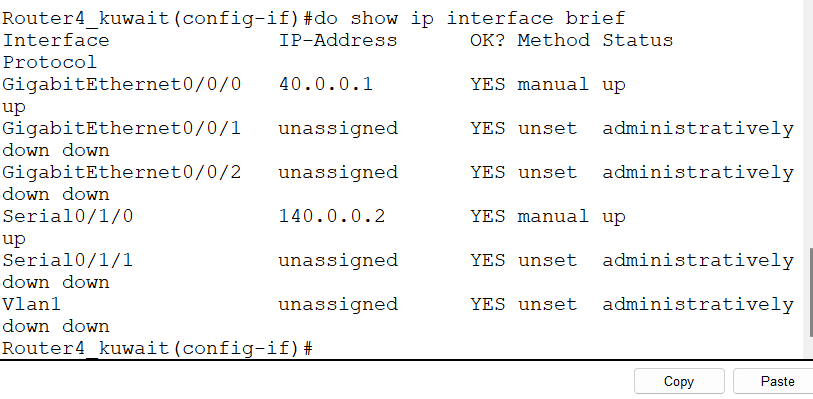
A black line with black text

AI-generated content may be incorrect.

Check interface security

✅ Expected Result: Only active, necessary interfaces should be UP.

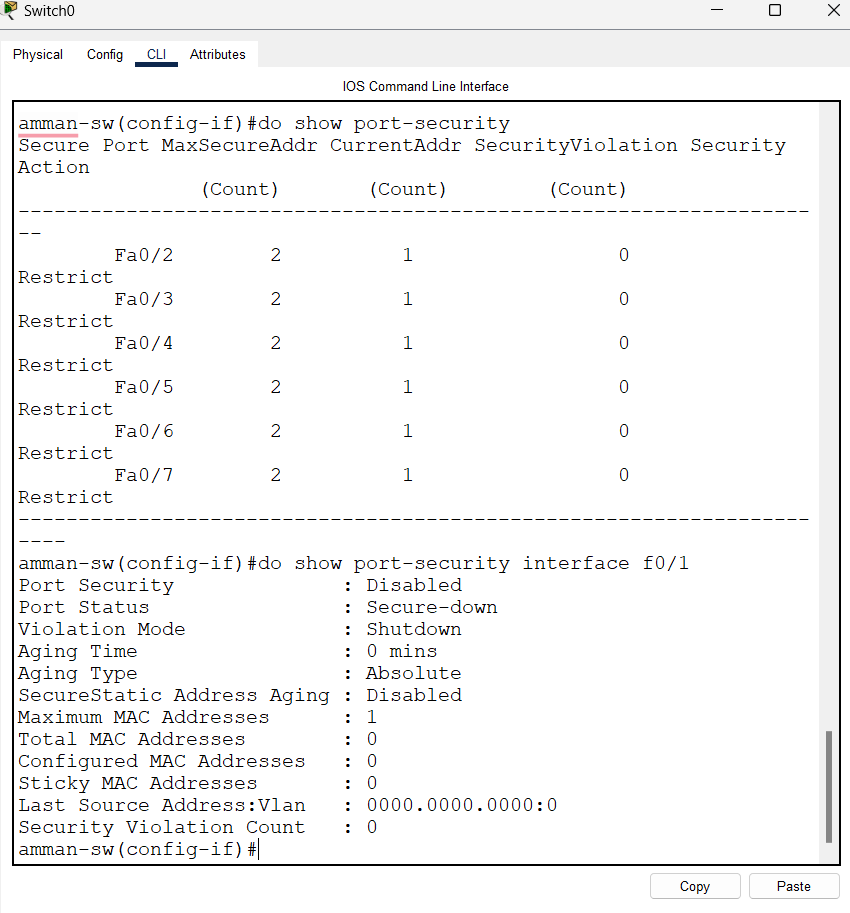
❌ If extra ports are active, shut them down:



D. Switch Security Testing

A close up of a screen

AI-generated content may be incorrect.



Verify unused ports are disabled

A screenshot of a computer

AI-generated content may be incorrect.

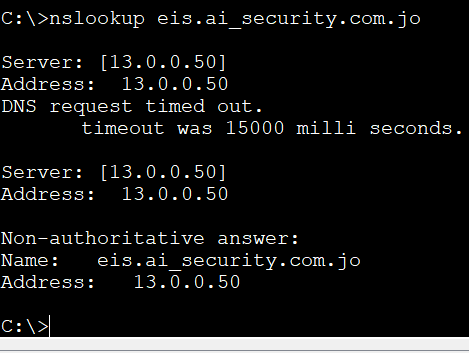
Check DHCP Snooping

A screenshot of a computer program

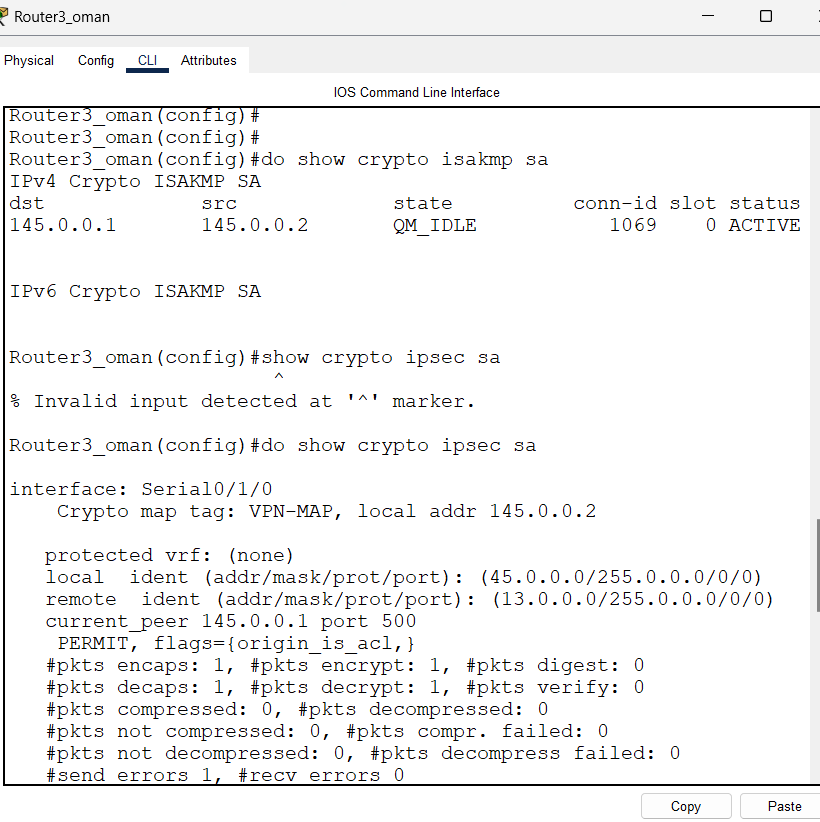
AI-generated content may be incorrect.

E. Server & VPN Testing

Verify DNS Resolution

  
Expected Result: **Correct DNS resolution**.

Check VPN Tunnel Status



Expected Result: **VPN tunnels should be active**.

Test https server :

A screenshot of a computer

AI-generated content may be incorrect.

Test redundent https server :

A screenshot of a computer

AI-generated content may be incorrect.

Test mail service :

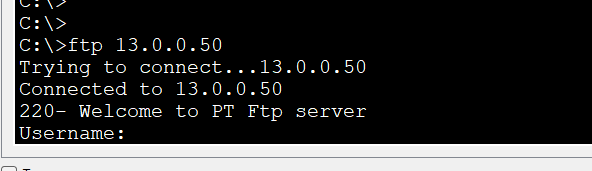
A screenshot of a computer

AI-generated content may be incorrect.

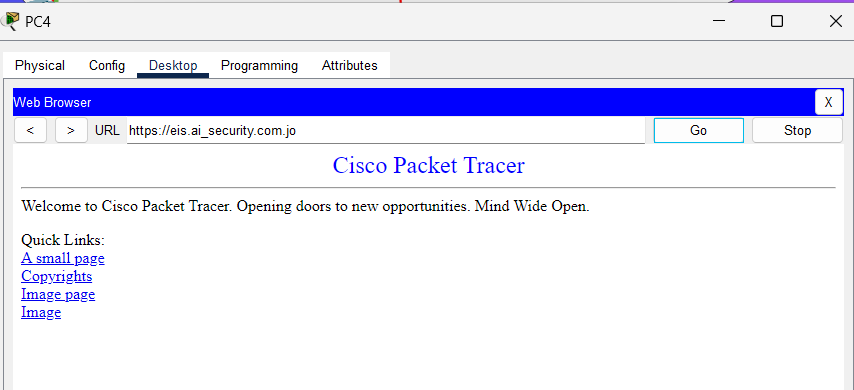
A screenshot of a computer

AI-generated content may be incorrect.

Test ftp server access from the qatar office :



Dns is working :



I tested some acl rules:

only https allowed :A screenshot of a computer

AI-generated content may be incorrect.

**critical Evaluation & Recommended Improvements**

Findings & Resolutions:

Routing Issues in Certain Areas

Issue: Some networks were not reachable due to improper routing.

Solution: Implemented static routes to ensure proper network reachability.

SSH Misconfiguration

Issue: SSH was not functioning due to missing RSA key generation.

Solution: Successfully generated RSA keys and enforced SSH access instead of Telnet for secure remote management.

ACL Misconfigurations

Issue: Certain traffic was unintentionally blocked, causing connectivity failures.

Solution: Reviewed and adjusted ACL rules to permit necessary traffic (HTTPS, FTP, DNS, ICMP) while maintaining strict security.

Recommendations for Further Improvements:

1. Enable AAA Authentication

Why? Enhances access control by requiring authentication for network access.

Benefit: Prevents unauthorized logins and improves user accountability.

2. Implement IDS/IPS for Better Threat Detection

Why? Intrusion Detection/Prevention Systems help identify and block suspicious traffic and potential attacks.

Benefit: Improves real-time attack mitigation and strengthens network defense.

3. Upgrade from RIP to OSPF

Why? RIP is less scalable and inefficient for large networks.

Solution: Implement OSPF (Open Shortest Path First) for dynamic and efficient routing updates.

Benefit: Reduces network congestion, improves convergence time, and supports larger networks effectively.

4. Strengthen Firewall Rules with Stateful Inspection

Why? Enhances packet filtering by tracking active connections rather than relying on simple ACL rules.

Benefit: Blocks malicious traffic more effectively without interfering with legitimate connections.

5. Enhance Network Monitoring & Logging

Why? Helps track security events and identify anomalies.

Solution: Implement Syslog and SNMP monitoring to maintain detailed security logs.

Benefit: Improves incident response and forensic analysis.

6. Regular Security Audits & Penetration Testing

Why? Helps uncover new vulnerabilities and ensures security policies are enforced.

Benefit: Strengthens network resilience by proactively identifying and addressing security gaps.

Final Assessment:

While the current security implementation effectively protects the network, further enhancements such as AAA authentication, OSPF routing, IDS/IPS, and advanced monitoring will significantly improve security, scalability, and resilience against cyber threats.