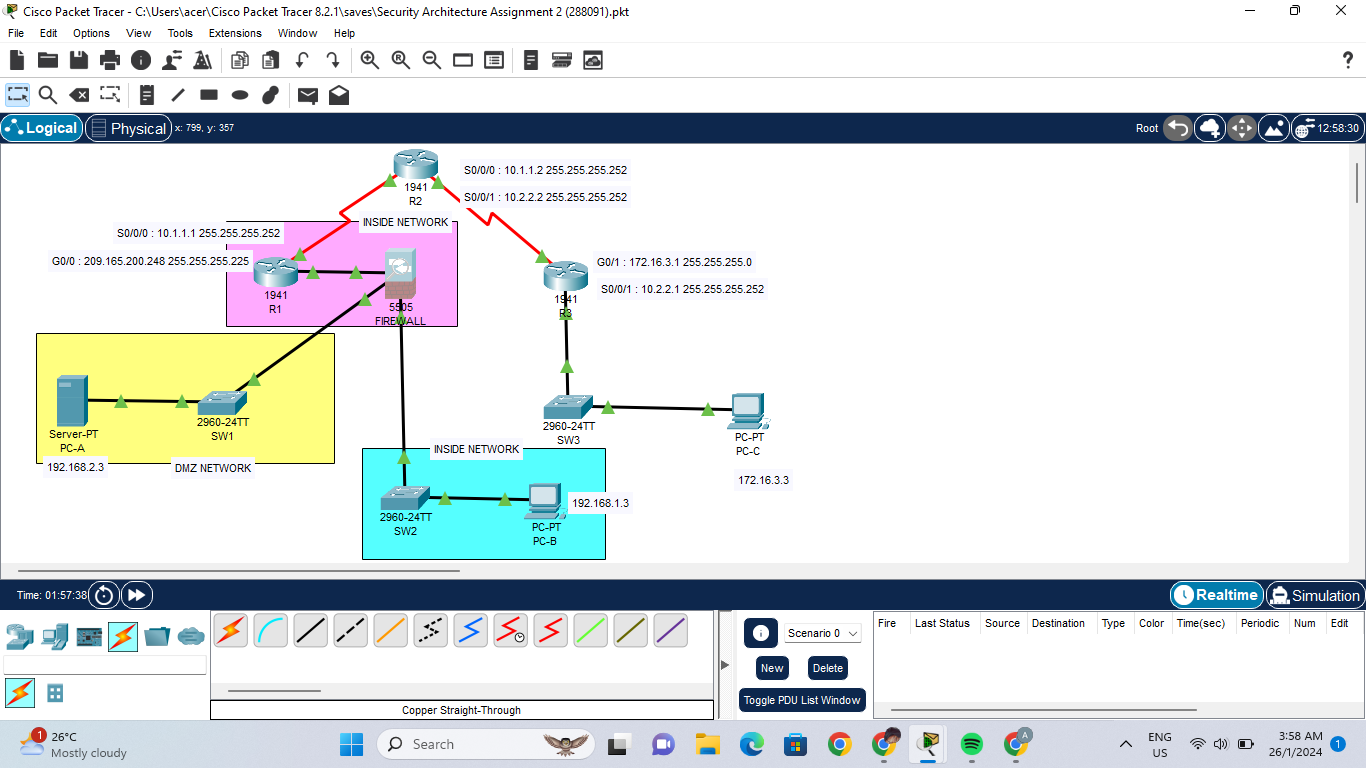


| Student’s Name | AINUR HANIM BINTI ABDUL HALIM |
| --- | --- |
| Matric Number | 288091 |
| Lecturer’s Name | DR. MOHAMMED GAMAL AHMED AL-SAMMAN |
| Subject | SECURITY ARCHITECTURE (SKIC3013) |

Individual Assignment 2

1. **NETWORK TOPOLOGY**



**Addressing Table**

| **Components** | **Interface** | **IP ADDRESS** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- |
| **R1** | **G0/0** | **209.165.200.225** | **255.255.255.248** | **N/A** |
| **S0/0/0** | **10.1.1.1** | **255.255.255.252** | **N/A** |
| **R2** | **S0/0/0** | **10.1.1.2** | **255.255.255.252** | **N/A** |
| **S0/0/1** | **10.2.2.2** | **255.255.255.252** | **N/A** |
| **R3** | **G0/1** | **172.16.3.1** | **255.255.255.0** | **N/A** |
| **S0/0/1** | **10.2.2.1** | **255.255.255.252** | **N/A** |
| **FIREWALL** | **VLAN 1** | **192.168.1.1** | **255.255.255.0** | **N/A** |
| **FIREWALL** | **VLAN 2** | **209.165.200.226** | **255.255.255.248** | **N/A** |
| **FIREWALL** | **VLAN 3** | **192.168.2.1** | **255.255.255.0** | **N/A** |
| **PCA-A** | **NIC** | **192.168.2.3** | **255.255.255.0** | **192.168.2.1** |
| **PC-B** | **NIC** | **192.168.1.3** | **255.255.255.0** | **192.168.1.1** |
| **PC-C** | **NIC** | **172.16.3.3** | **255.255.255.0** | **172.16.3.1** |

1. **ROUTER CONFIGURATION**

* **Configure router interface IP addresses**

R1(config)#int g0/0

R1(config-if)#ip add 209.165.200.225 255.255.255.248

R1(config)#exit

R1(config)#int s0/0/0

r1(config-if)#ip add 10.1.1.1 255.255.255.252

R1(config-if)#exit

R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0

R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1

R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0

R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1

* **Crypto Keys for SSH**

R1(config)# line console 0

R1(config-line)# login local

R1(config-line)# exec-timeout 5 0

R1(config-line)# logging synchronous

Configure line vty 0 4 to use the local user database for logins and restrict access to only SSH connections

R1(config)# line vty 0 4

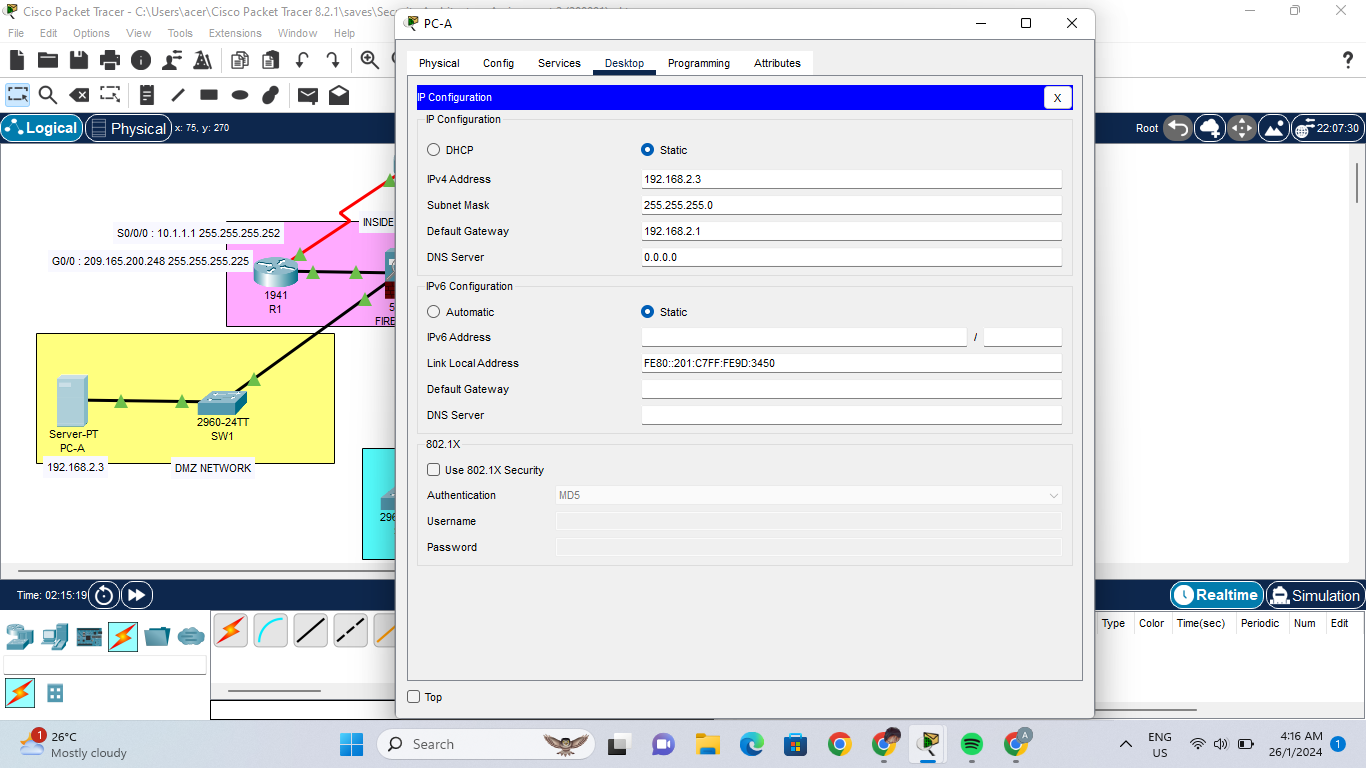
R1(config-line)# login local

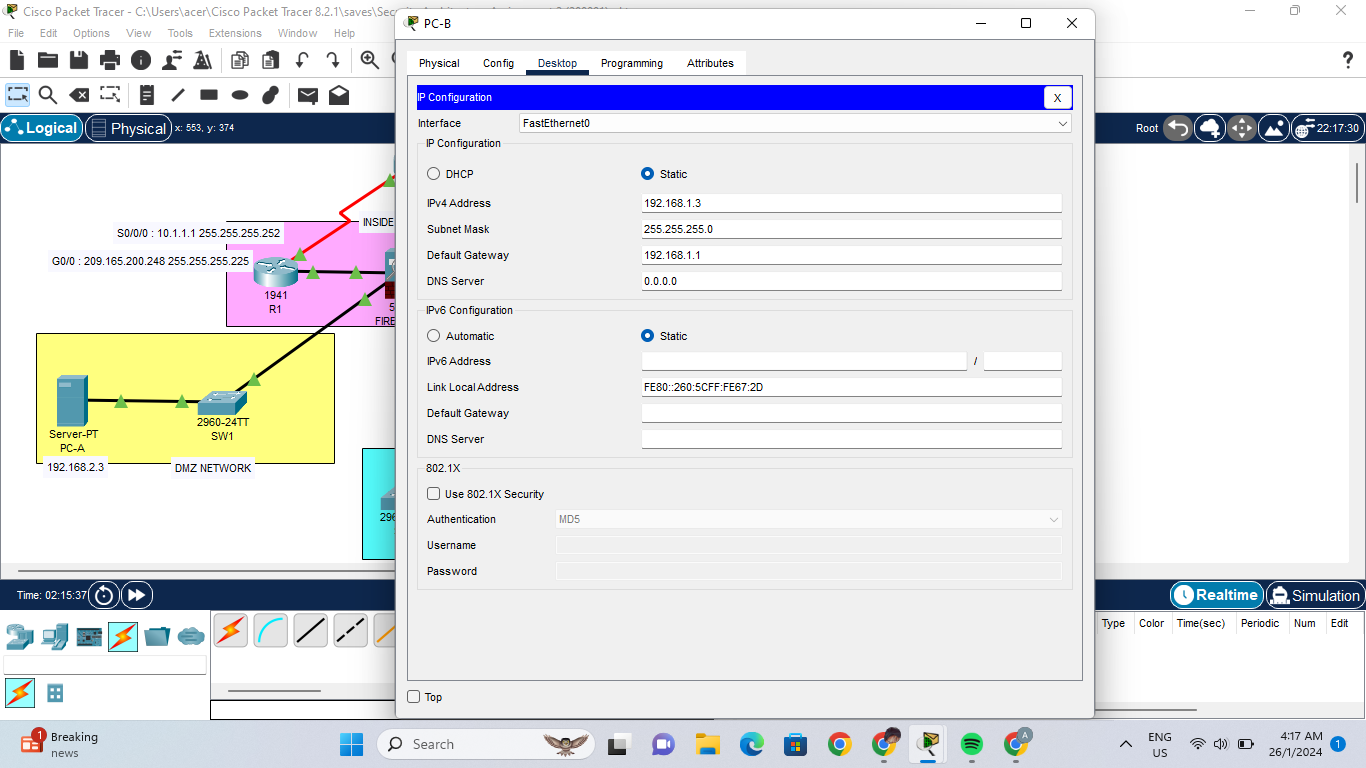
R1(config-line)# transport input ssh

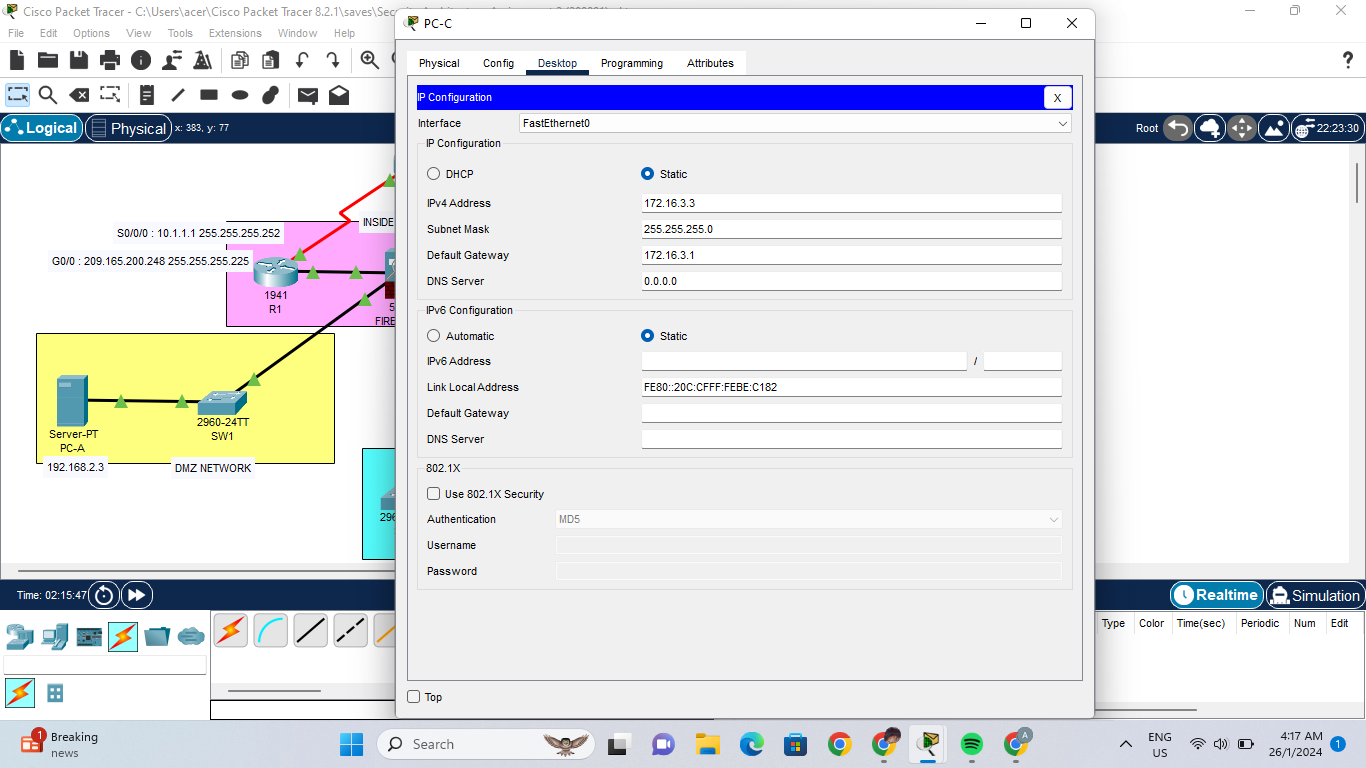
R1(config-line)# exec-timeout 5 0

* **Configure PC host IP settings**

-#show version



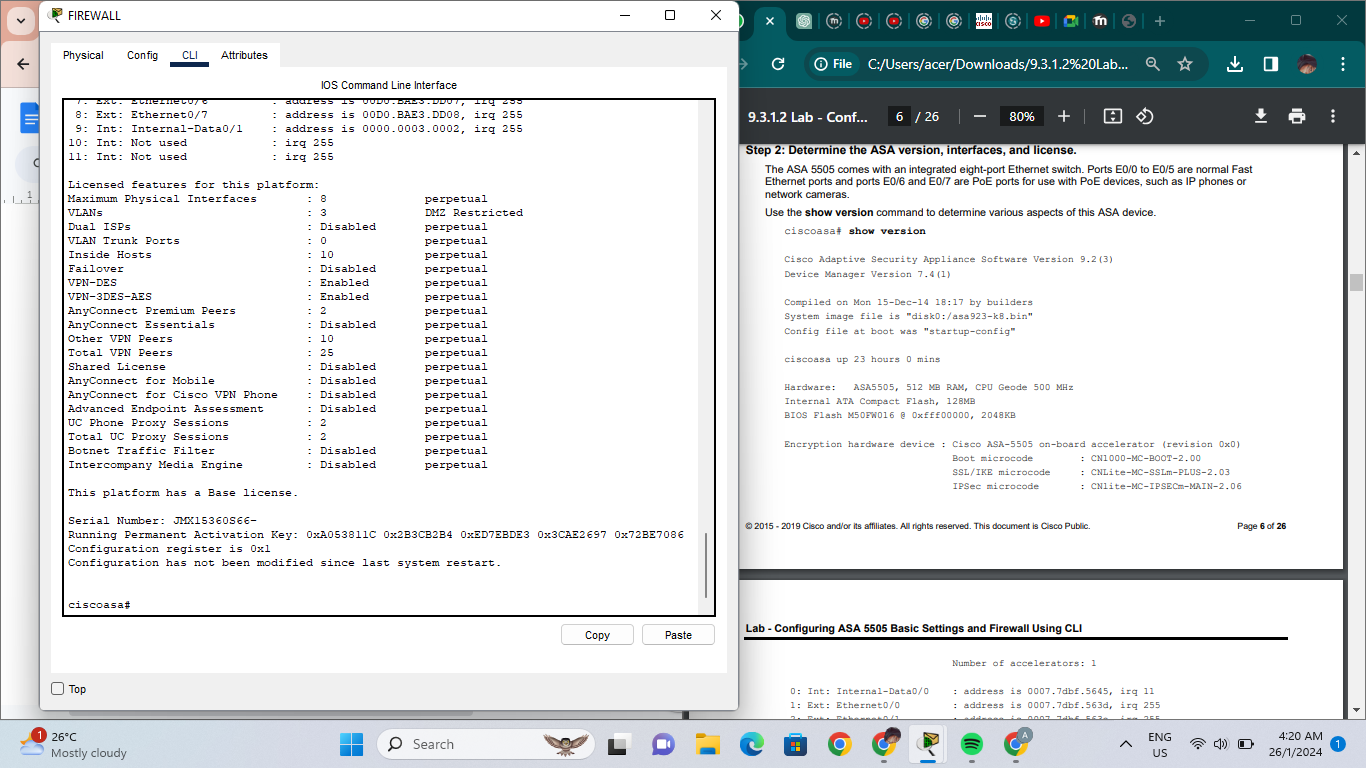




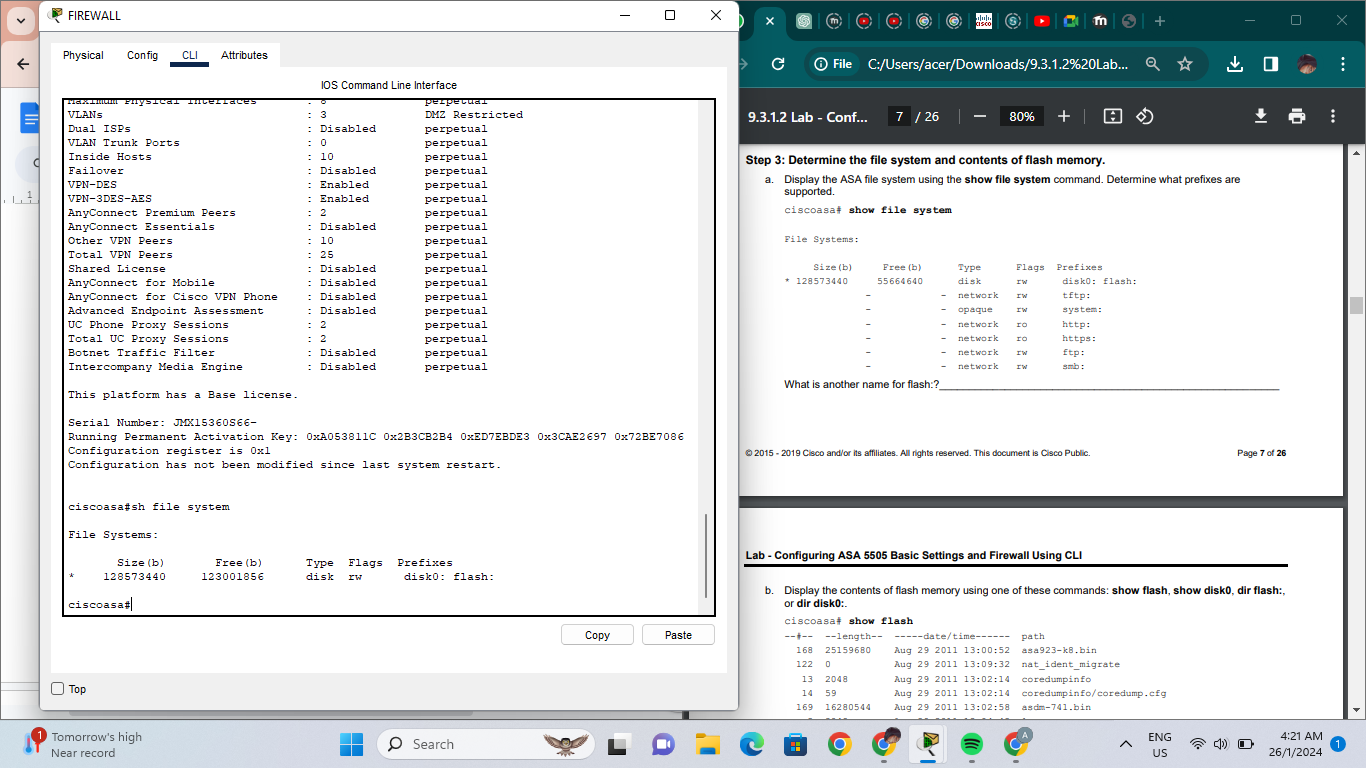
**2. Configure Basic Settings**

* **Determine the Firewall version, interface and license**

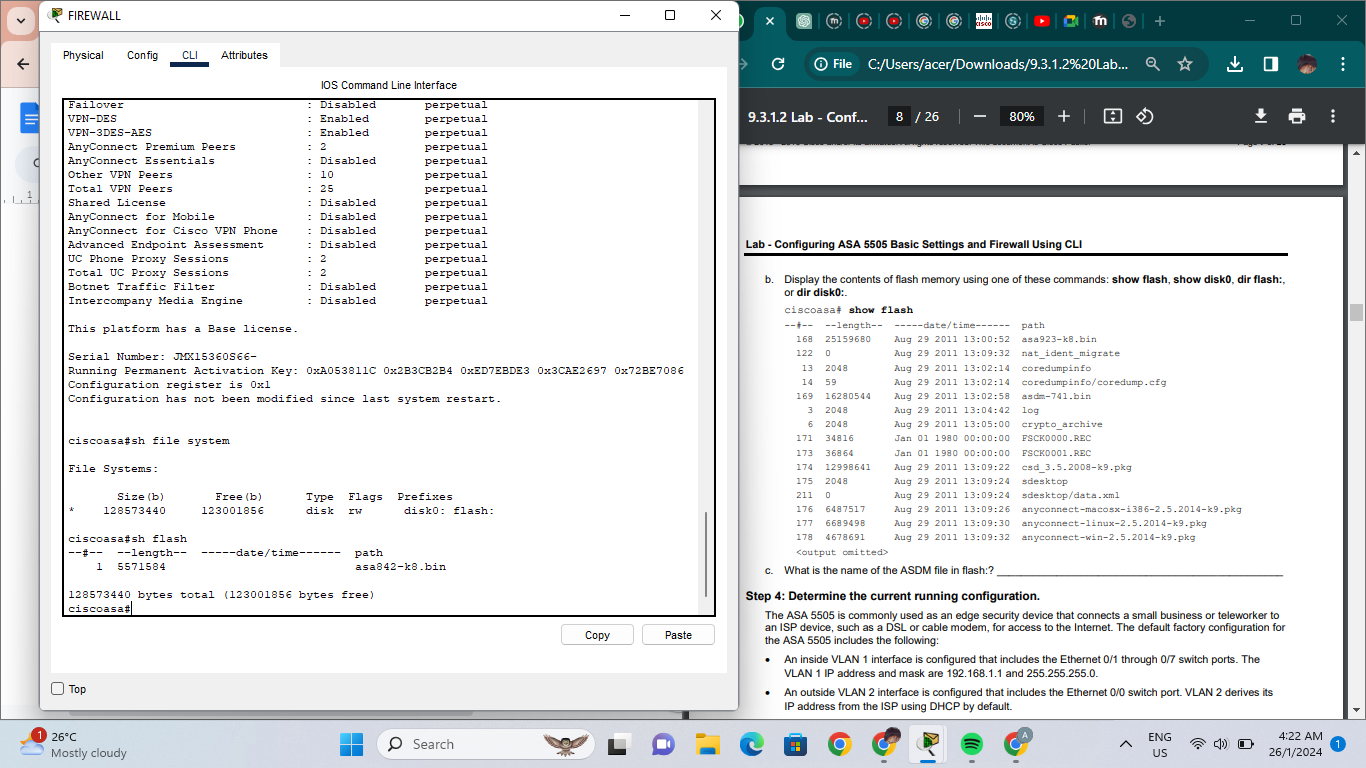


****

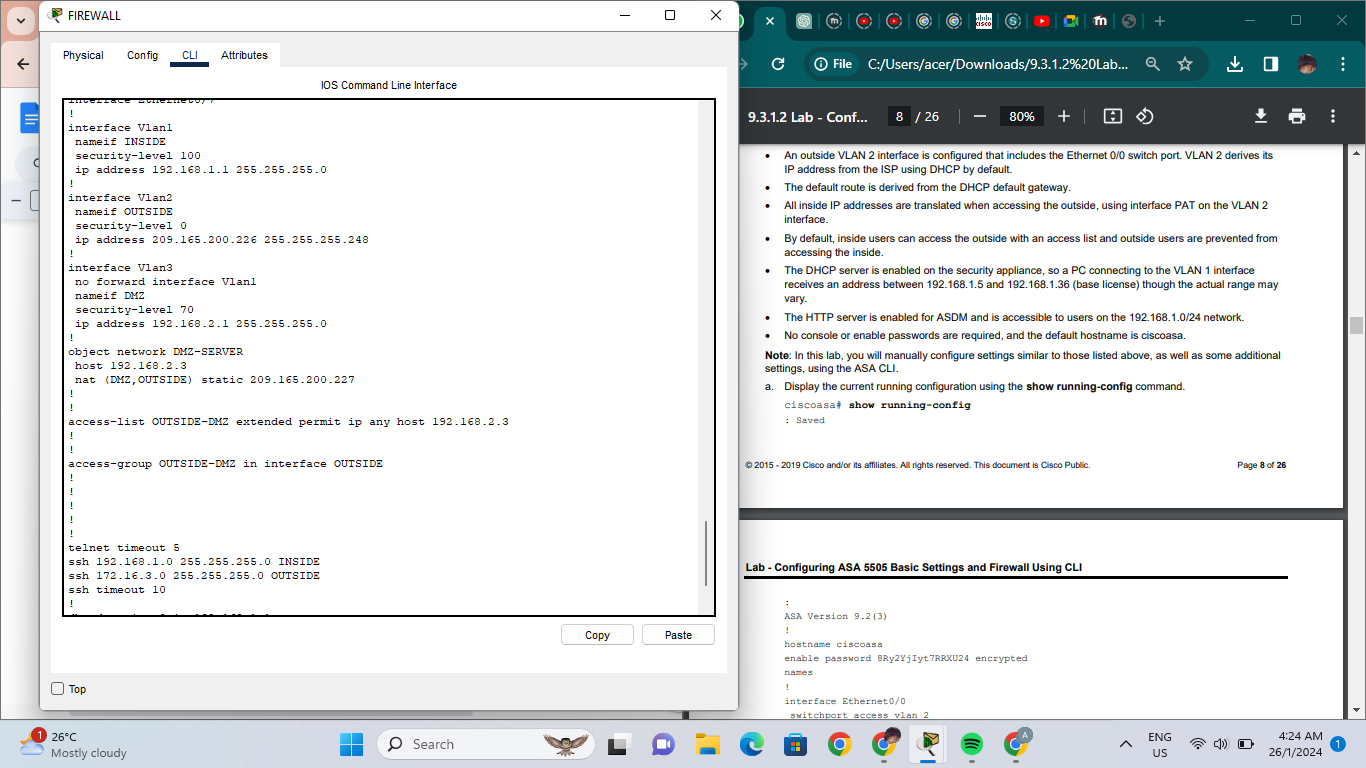
**-#show file system**

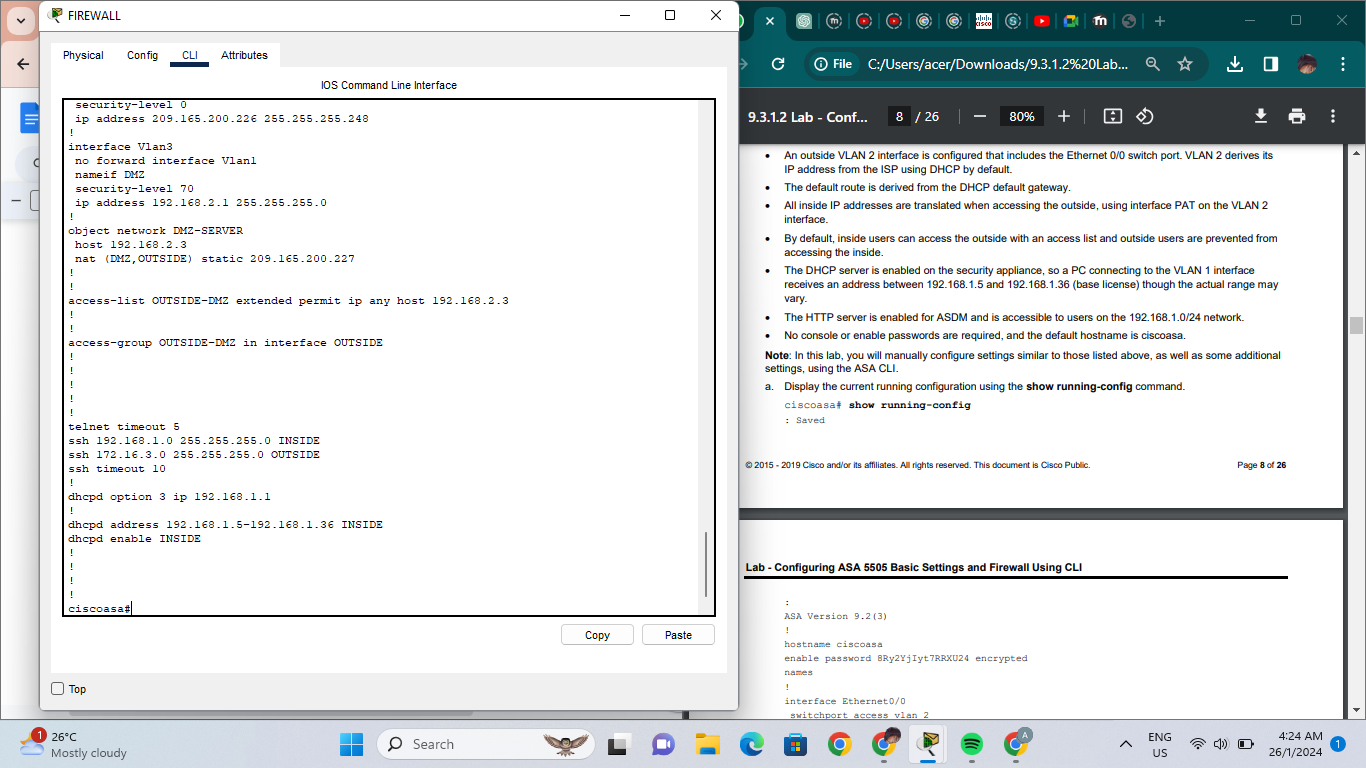
****

**-#show flash**

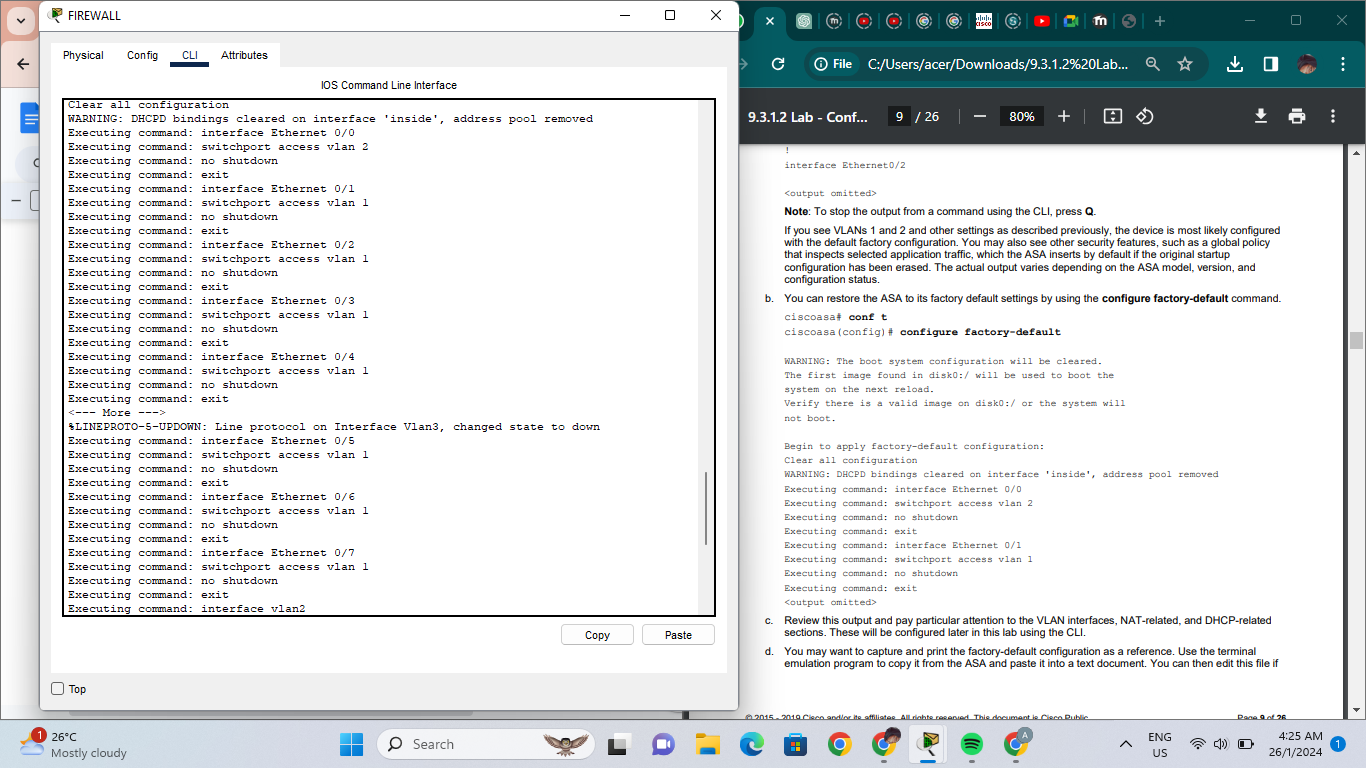
****

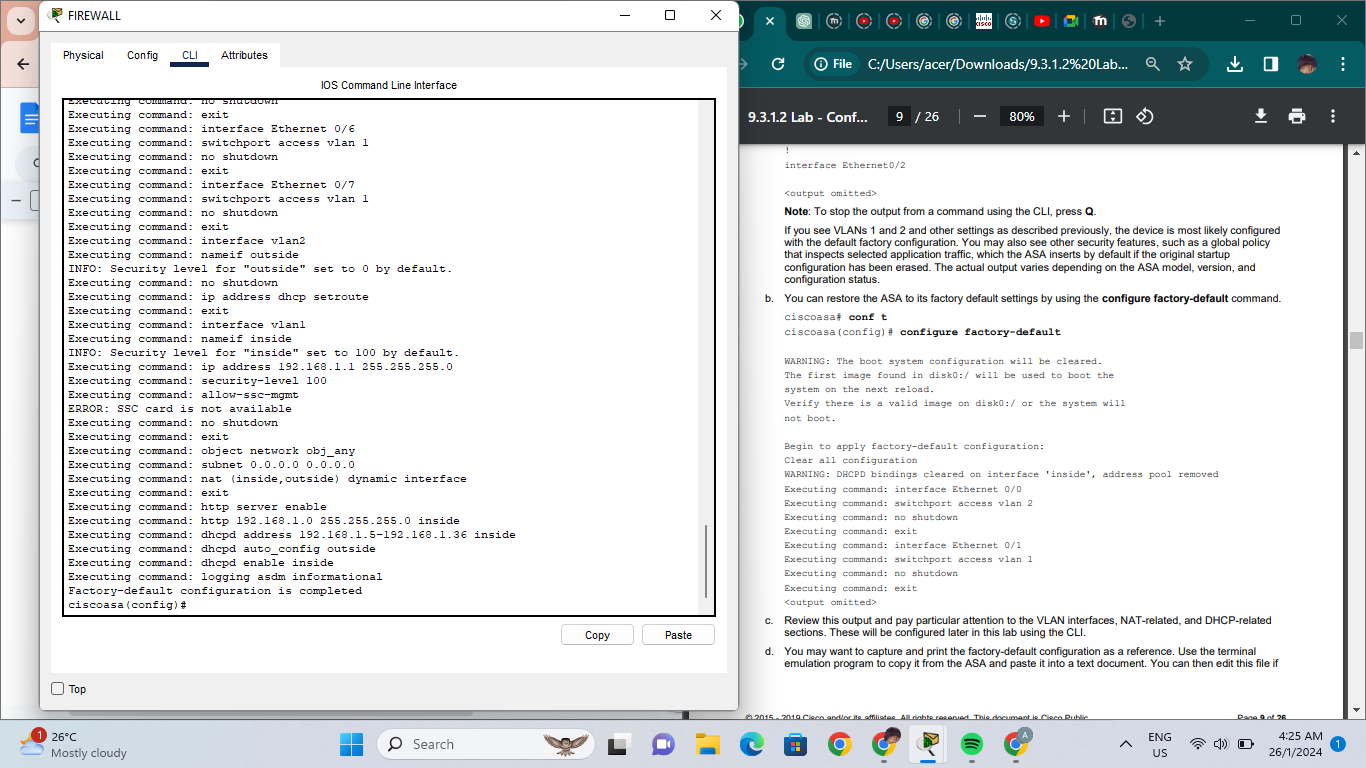
* **Determine the current running configuration**
* **#show running-config**

****

****

* **#conf t**
* **#configure factory-default**

****

****

1. **Configure the inside and outside interfaces**

FIREWALL(config)# interface vlan 1

FIREWALL(config-if)# nameif inside

FIREWALL(config-if)# ip address 192.168.1.1 255.255.255.0

FIREWALL(config-if)# security-level 100

FIREWALL(config-if)# interface vlan 2

FIREWALL(config-if)# nameif outside

INFO: Security level for "outside" set to 0 by default.

FIREWALL(config-if)# ip address 209.165.200.226 255.255.255.248

FIREWALL(config-if)# no shutdown

* **Assign FIREWALL Layer 2 port E0/1 to VLAN 1 and port E0/0 to VLAN 2**.

FIREWALL(config)# interface e0/1

FIREWALL(config-if)# switchport access vlan 1

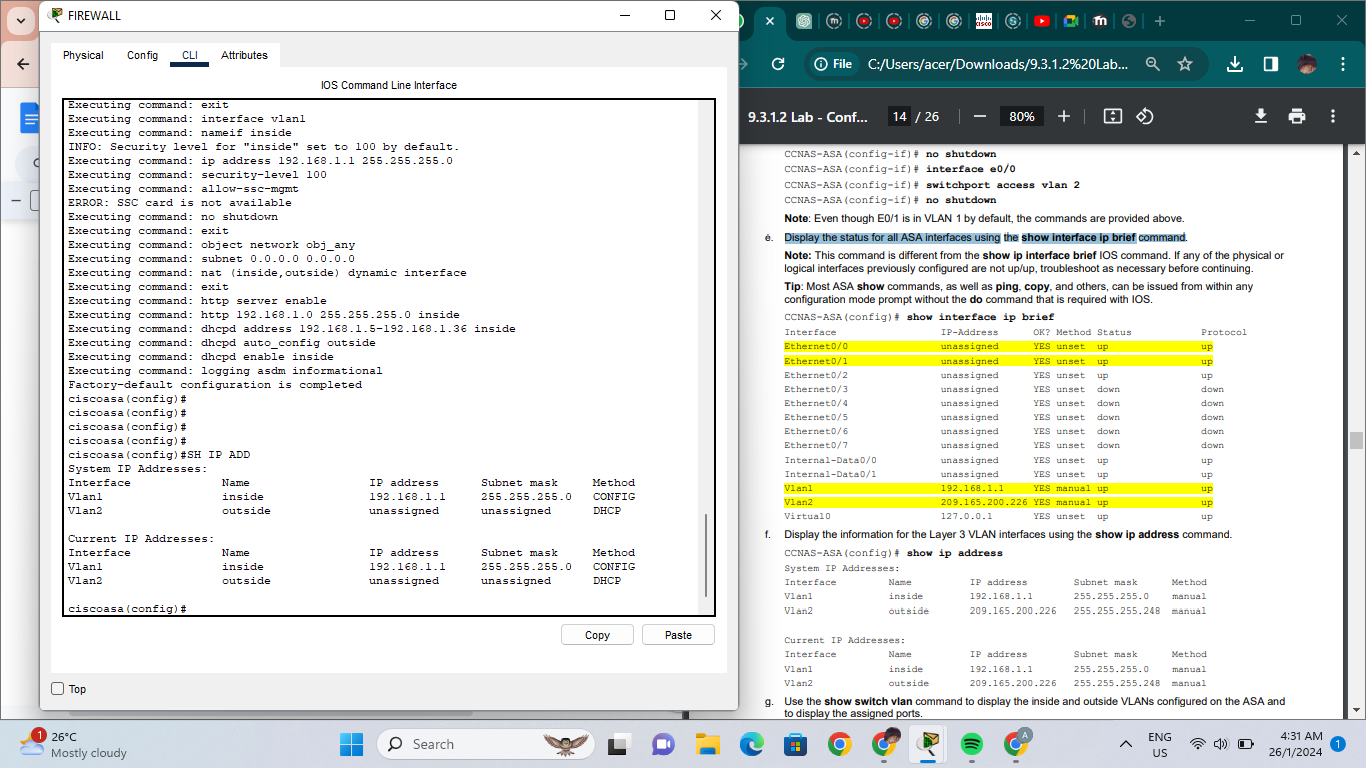
FIREWALL(config-if)# no shutdown

FIREWALL(config-if)# interface e0/0

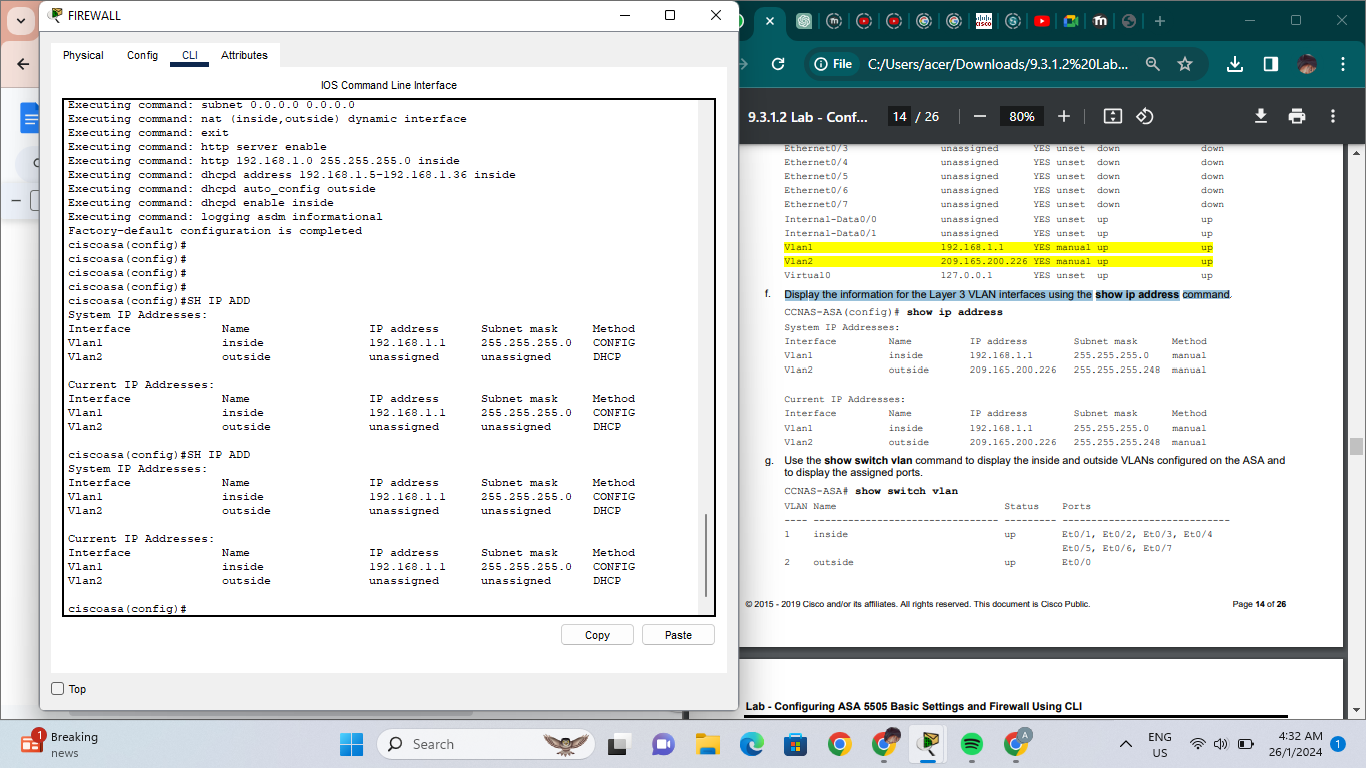
FIREWALL(config-if)# switchport access vlan 2

FIREWALL(config-if)# no shutdown

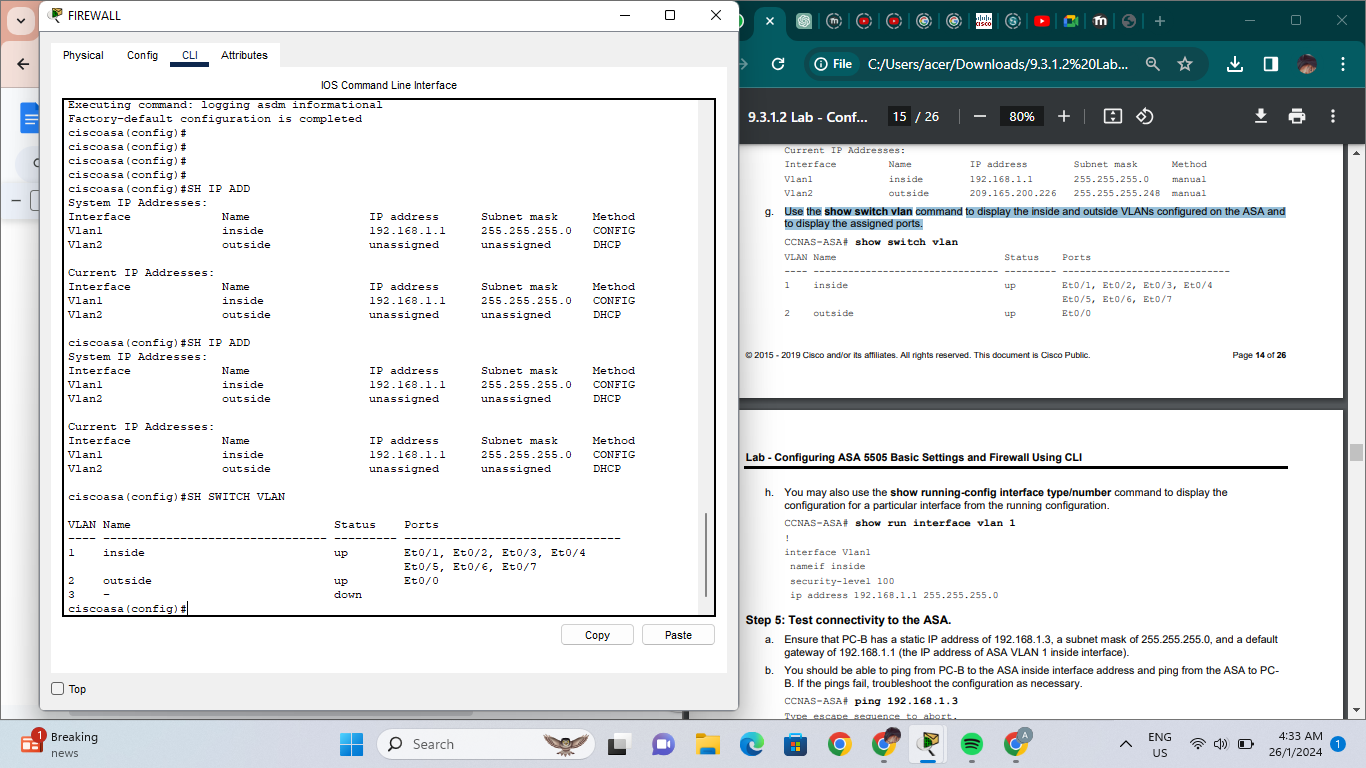
* **Display the status for all FIREWALL interfaces using the show interface ip brief command**

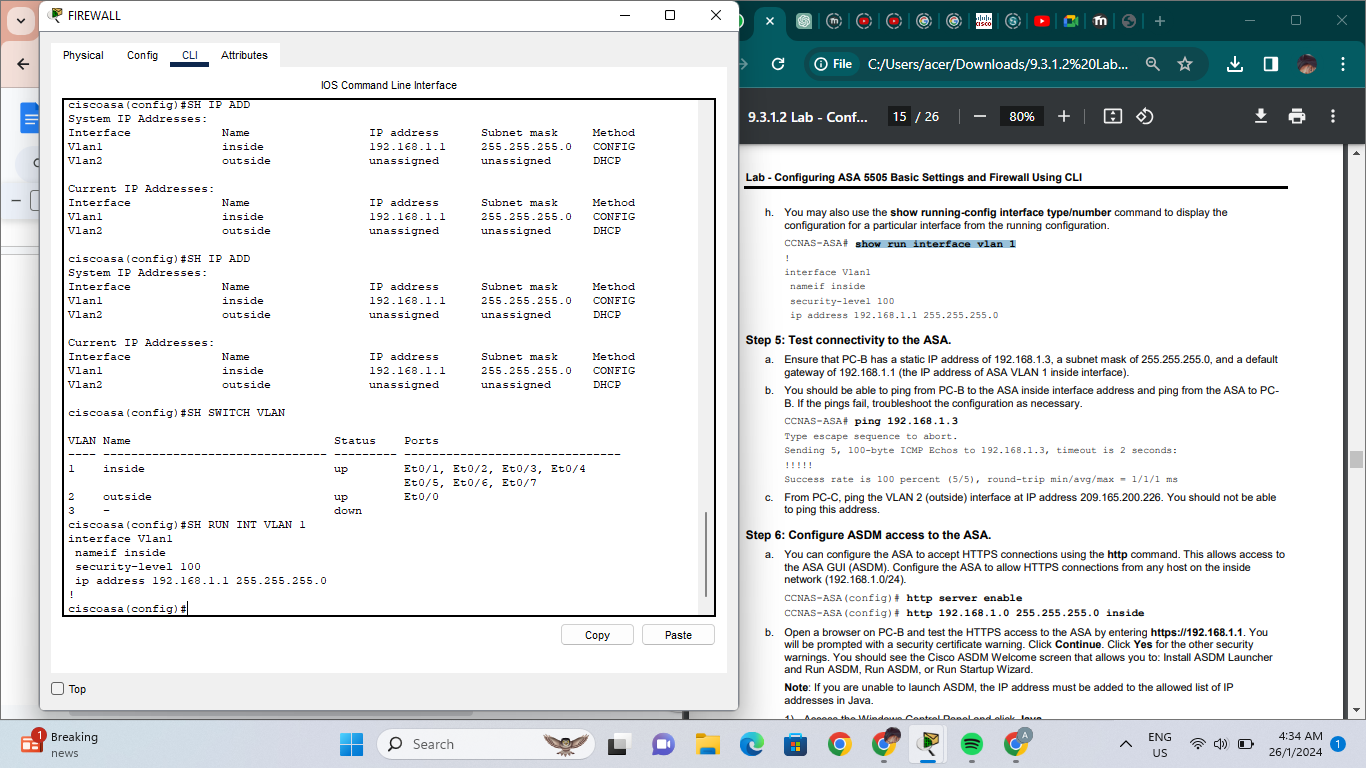


* **Display the information for the Layer 3 VLAN interfaces using the show ip address command**



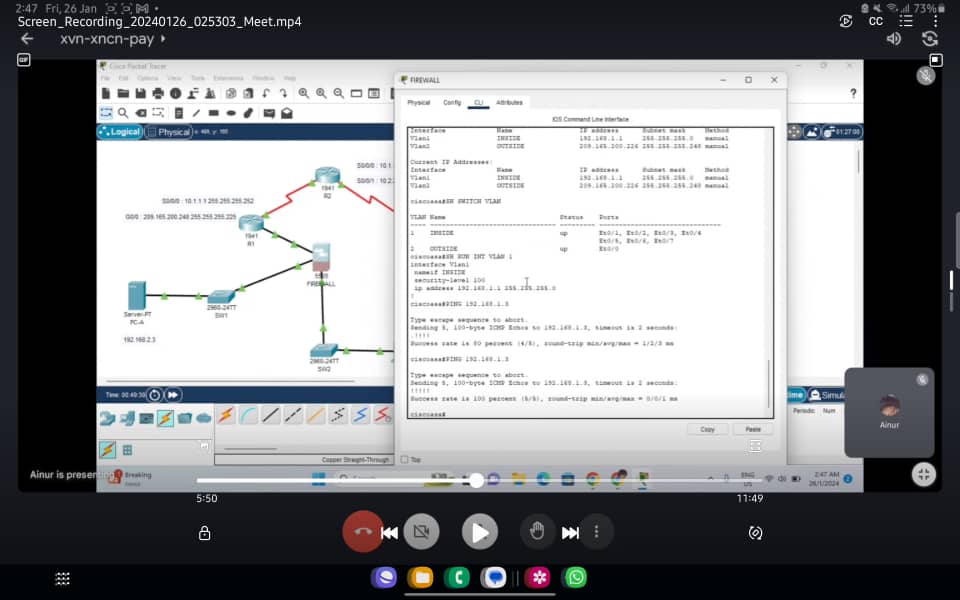
* **Use the show switch vlan command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.**





* **Test connectivity to the FIREWALL**

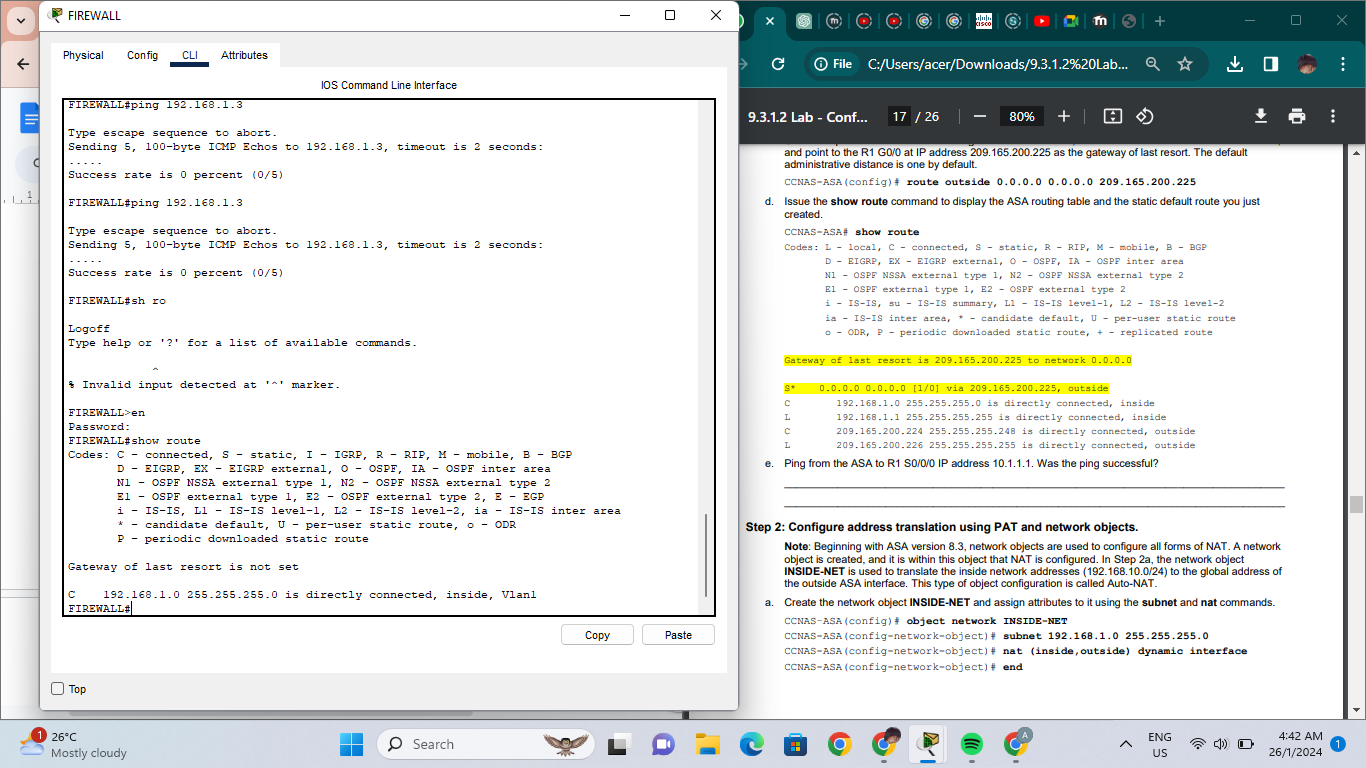
PC-B should be able to ping FIREWALL



PC-C cannot ping 209.165.200.226



1. **Configure Routing, Address Translation and Inspection Policy using CLI**



1. **Configure DHCP and SSH**

FIREWALL(config)# dhcpd address 192.168.1.5-192.168.1.100 inside

Warning, DHCP pool range is limited to 32 addresses, set address range as:

192.168.1.5-192.168.1.36

FIREWALL(config)# dhcpd address 192.168.1.5-192.168.1.36 inside

FIREWALL(config)# dhcpd enable inside  
FIREWALL(config)# show run dhcpd

dhcpd dns 209.165.201.2

!

dhcpd address 192.168.1.5-192.168.1.36 inside

dhcpd enable inside

* **Configure SSH to FIREWALL**

FIREWALL(config)# crypto key generate rsa modulus 1024

FIREWALL(config)# ssh 192.168.1.0 255.255.255.0 inside

FIREWALL(config)# ssh 172.16.3.3 255.255.255.255 outside

FIREWALL(config)# ssh timeout 10

1. **Configure DMZ, Static NAT and ACLs**

FIREWALL(config)# interface vlan 3

FIREWALL(config-if)# ip address 192.168.2.1 255.255.255.0

FIREWALL(config-if)# nameif dmz

FIREWALL(config-if)# no forward interface vlan 1

FIREWALL(config-if)# nameif dmz

INFO: Security level for "dmz" set to 0 by default.

FIREWALL(config-if)# security-level 70

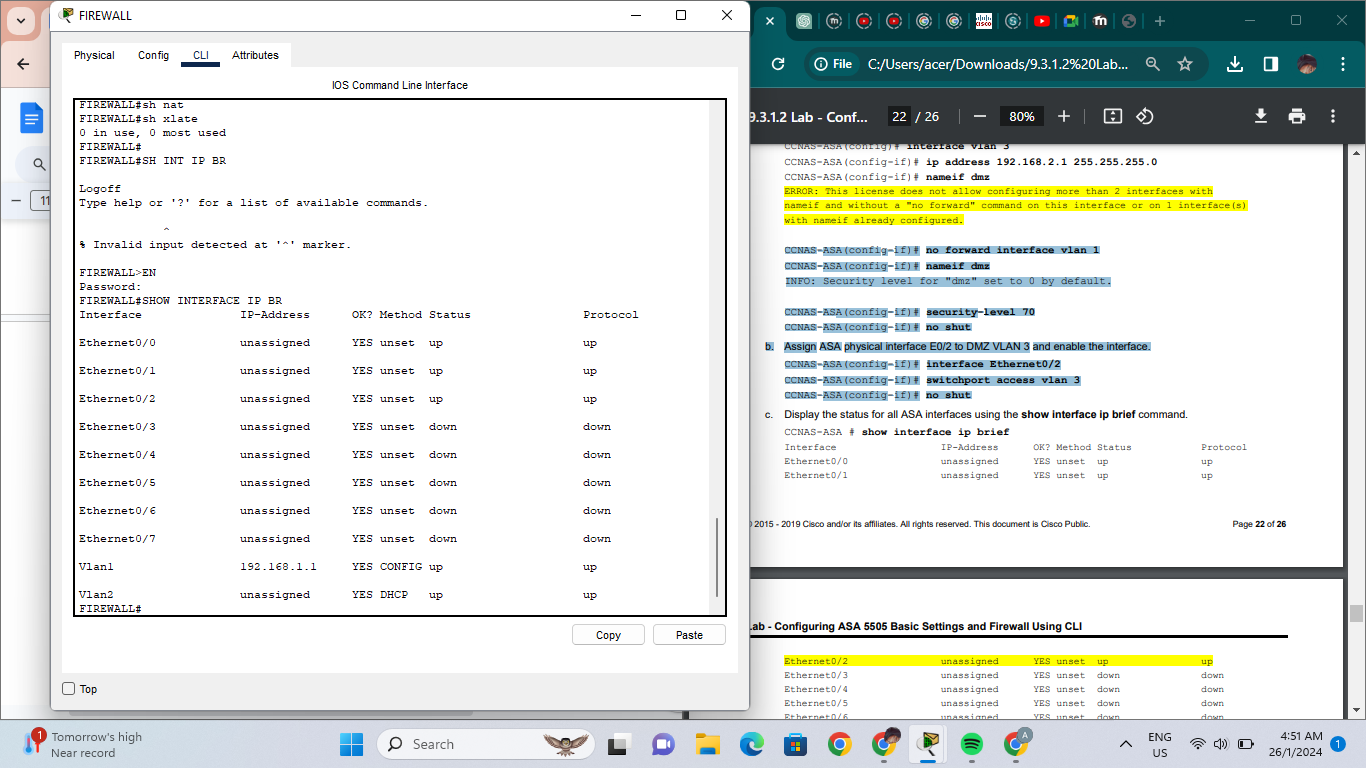
FIREWALL(config-if)# no shut

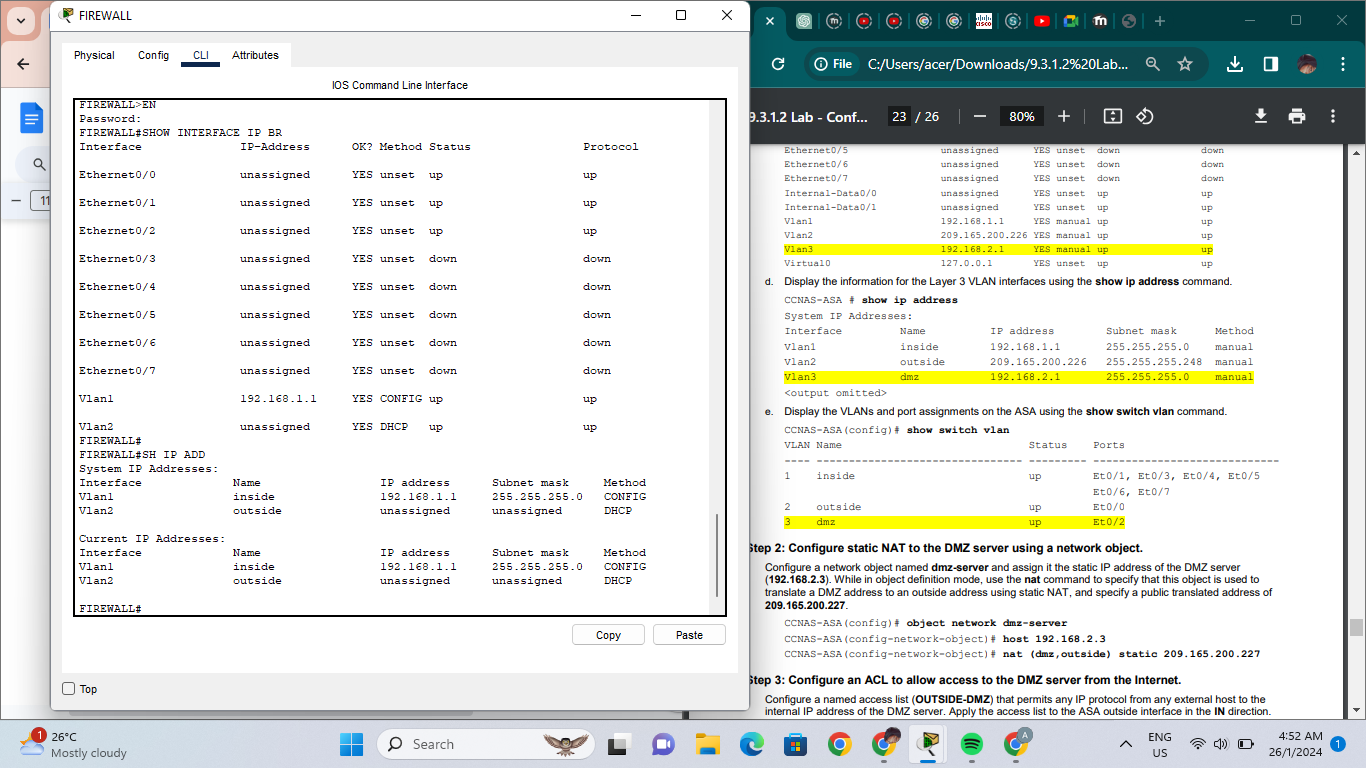
Assign FIREWALL physical interface E0/2 to DMZ VLAN 3 and enable the interface.

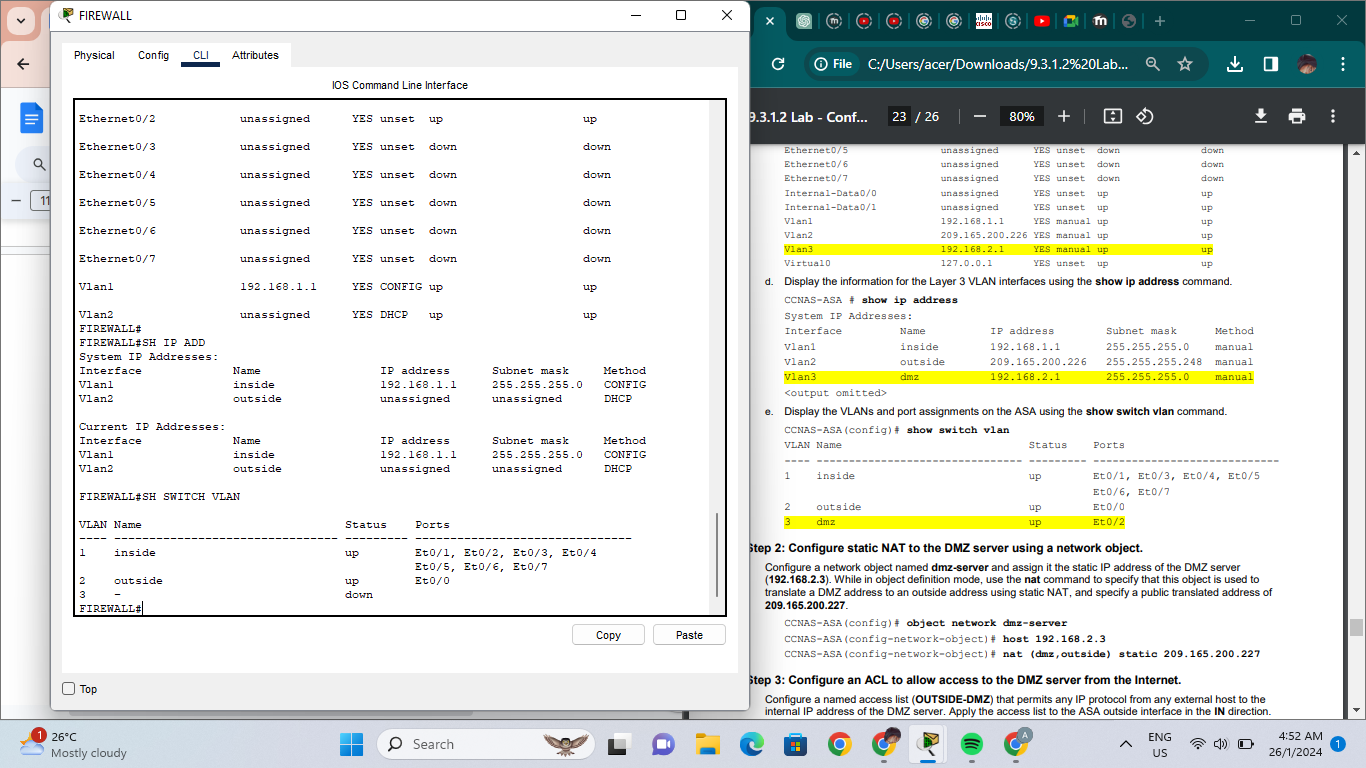
FIREWALL(config-if)# interface Ethernet0/2

FIREWALL(config-if)# switchport access vlan 3

FIREWALL(config-if)# no sh







* **Configure static NAT to DMZ**

CCNAS-ASA(config)# object network dmz-server

CCNAS-ASA(config-network-object)# host 192.168.2.3

CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227

* **Configure ACL to allow access to DMZ server from internet**

CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3

CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside

* **Test access to DMZ network**

R2(config-if)# interface lo0

R2(config-if)# ip address 172.30.1.1 255.255.255.0

R2(config-if)# end

R2# ping 209.165.200.227 source lo0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:

Packet sent with a source address of 172.30.1.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

FIREWALL# show nat

Auto NAT Policies (Section 2)

1 (dmz) to (outside) source static dmz-server 209.165.200.227

translate\_hits = 0, untranslate\_hits = 4

2 (inside) to (outside) source dynamic INSIDE-NET interface

translate\_hits = 4, untranslate\_hits = 0

FIREWALL# show run interface vlan 3

!

interface Vlan3

no forward interface Vlan1

nameif dmz

security-level 70

ip address 192.168.2.1 255.255.255.0

**An explanation of how the network design aligns with security principles, including Domains of Trust, access controls, and encryption.**

1. Domain of Trust

* Domains of Trust are parts of a network where specific security controls are implemented according to the degree of trust that is connected to the devices and users in that particular segment.
* In my topology has 3 segmentation which is Internal Network, External Network and DMZ Network
* According to the unique trust level and security requirements, each domain will have its own set of security policies, access restrictions, and monitoring systems.

1. Access Controls

* The resources that users can access on the network and the actions they can do are controlled by access controls.
* In my topology, i implement the access control mostly at the firewall
* I configure the ACL and NAT at the DMZ interface vlan 3 on firewall
* I also configure static NAT to the DMZ server
* Configure the ACL to allow the DMZ server from internet
* Then test the access to the DMZ server

1. Encryption

* The encryption is not shown in the topology
* This network design can use encryption to secure data while it's in transit.
* Often used methods for encrypting data in transit over a network, Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) offer secrecy and integrity.
* By establishing encrypted tunnels over open networks, virtual private networks, or VPNs, enable distant users to safely access internal resources.
* Data at rest is safeguarded by encryption technologies like database and disk encryption, which guarantee that even in the event that physical equipment are hacked, the data will remain unreadable in the absence of the necessary decryption keys.

**Youtube Link**

<https://youtu.be/RoG4cin7Tmg?si=iGDsvDIYAgIqWqO->