ASSIGNMENT TWO WRITE UP:

CONFIGURE ASA BASIC SETTINGS AND FIREWALL USING THE CLI

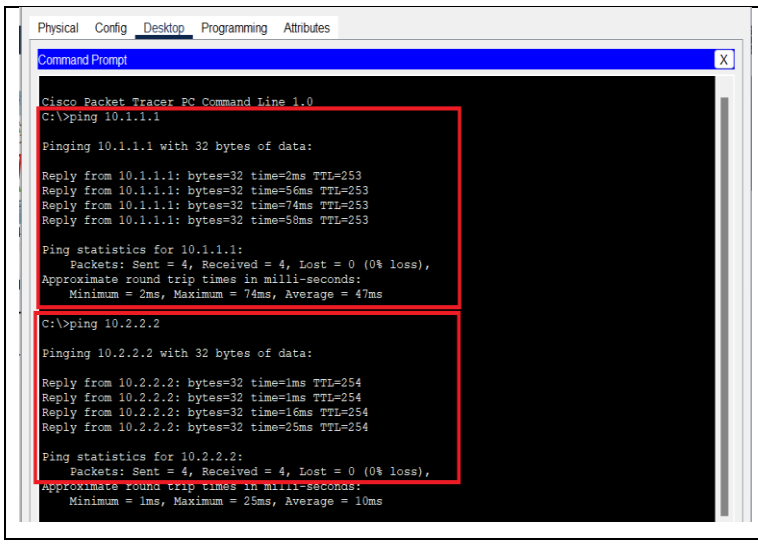
Introduction

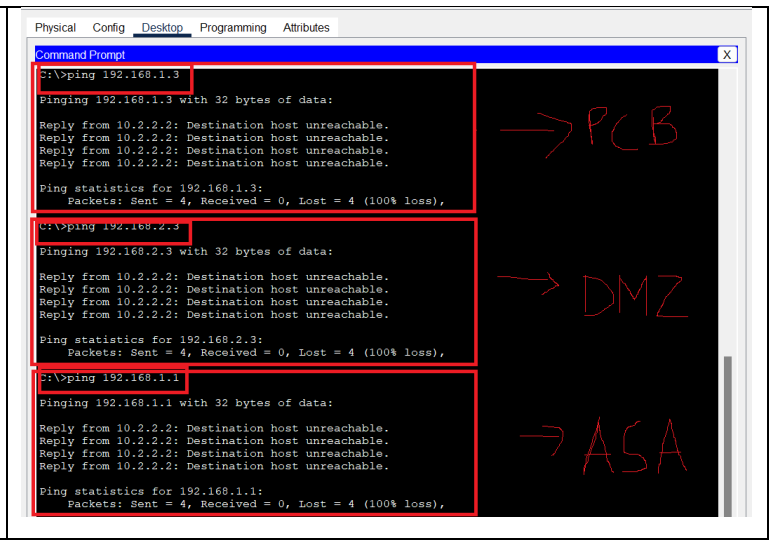
In the world of networking, the Cisco Adaptive Security Appliance (ASA) plays a critical role in ensuring the security and smooth operation of networks. As a fundamental skill for aspiring network professionals, configuring ASA basic settings and implementing firewall rules using the Command Line Interface (CLI) is an essential task to master. This write up details the key components of ASA configuration, including network interfaces, IP addressing and access control lists (ACLs) to establish a solid foundation in network security.

Part 1: Verify Connectivity and Explore the ASA

Step 1: Verify connectivity.

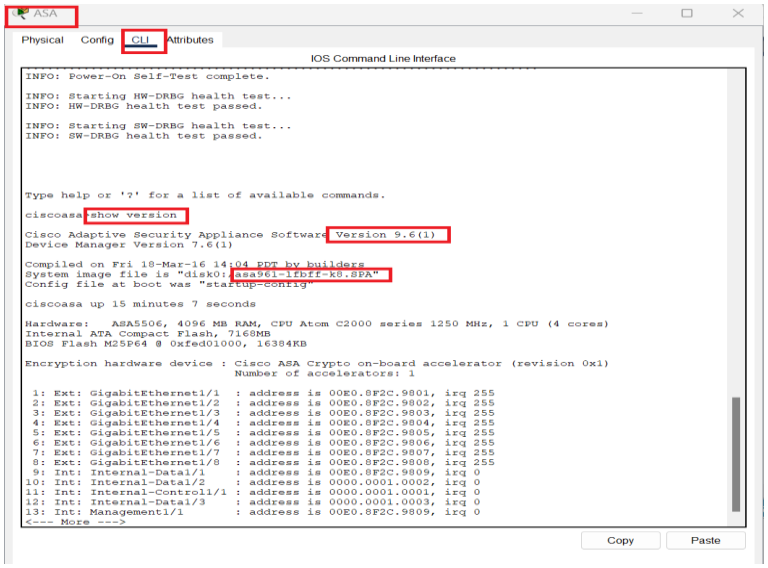
The ASA is not currently configured. However, all routers, PCs, and the DMZ server are configured. Verification of connectivity of PC-C to any router interface and inability to connect to the ASA, PC-B, or the DMZ server can be shown below.





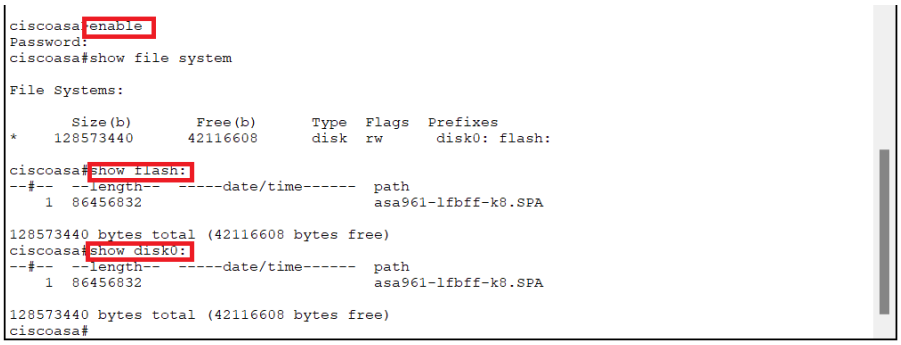
Step 2: Determine the ASA version, interfaces, and license.

Using the show version command on the CLI of the ASA was determined.



Step 3: Determine the file system and contents of flash memory.

This was done through the EXEC mode and using the show system and show flash/ show disk0 commands as shown below.



```
ciscoasa>enable
Password:
ciscoasa#show file system

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
*    128573440      42116608      disk  rw      disk0: flash:

ciscoasa#show flash:
--#--  --length--  -----date/time------  path
    1  86456832                          asa961-lfbff-k8.SPA

128573440 bytes total (42116608 bytes free)
ciscoasa#show disk0:
--#--  --length--  -----date/time------  path
    1  86456832                          asa961-lfbff-k8.SPA

128573440 bytes total (42116608 bytes free)
ciscoasa#
```

Part 2: Configure ASA Settings and Interface Security Using the CLI

The following is a step-by-step process of configuring ASA settings and Interface security was done using CLI.

Step 1: Configure the hostname and domain name.

Configure the ASA hostname as NETSEC-ASA and domain name netsec.com

```
128573440 bytes total (42116608 bytes free)
ciscoasa#configure terminal
ciscoasa(config)#hostname NETSEC-ASA
```

Step 2: Configure the enable mode password.

The enable password command is used to change the privileged EXEC mode password to ciscoenpa55.

```
NETSEC-ASA(config)#domain-name netsec.com
NETSEC-ASA(config)#enable password ciscoenpa55
NETSEC-ASA(config)#exit
```

Step 3: Set the date and time.

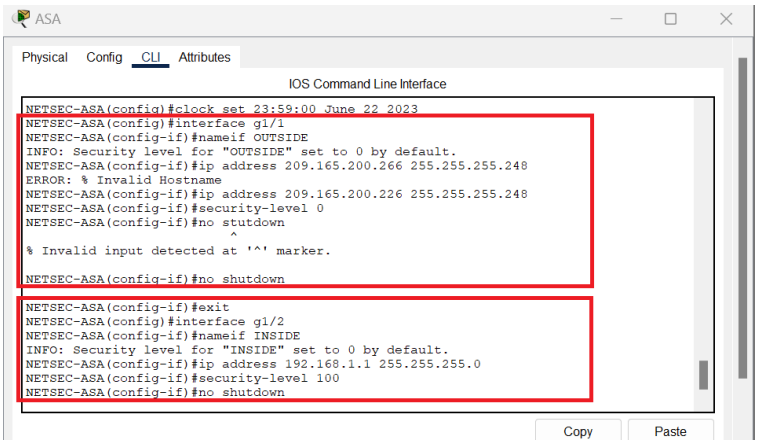
The clock set command is used to manually set the date and time (this step is not scored).

```
NETSEC-ASA(config)#clock set 23:59:00 June 22 2023
NETSEC-ASA(config)#
```

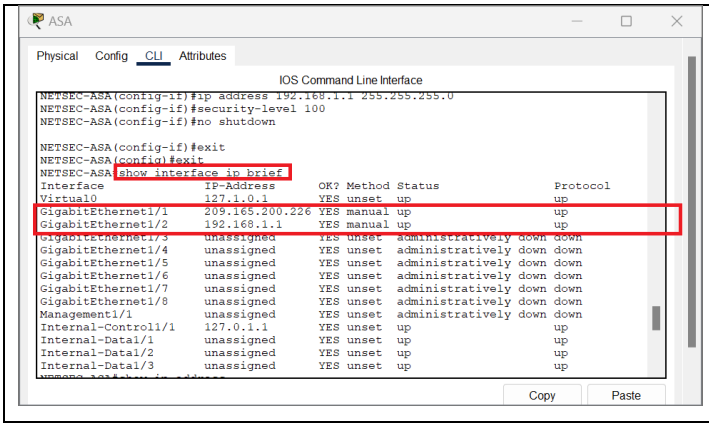
Step 4: Configure the INSIDE and OUTSIDE interfaces.

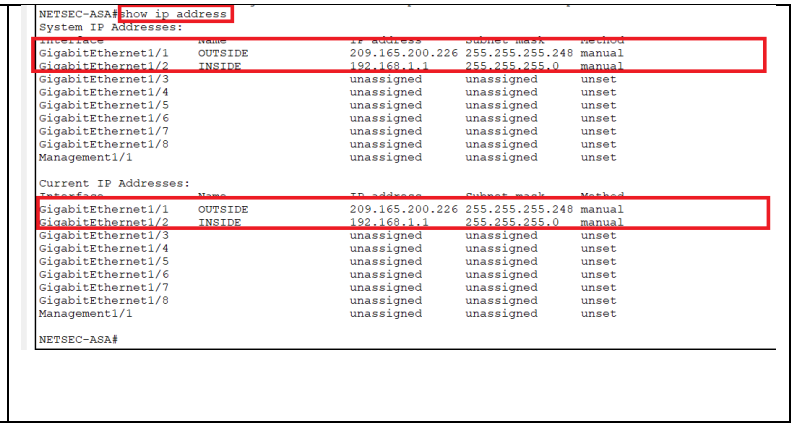
To configure the inside interface, create a G1/1 interface for the outside network (209.165.200.224/29) and setting the security level to the lowest setting of 0 and enable the interface.

Configuring the G1/2 interface for the inside network (192.168.1.0/24) and setting the security level to the highest setting of 100 and enable the interface.



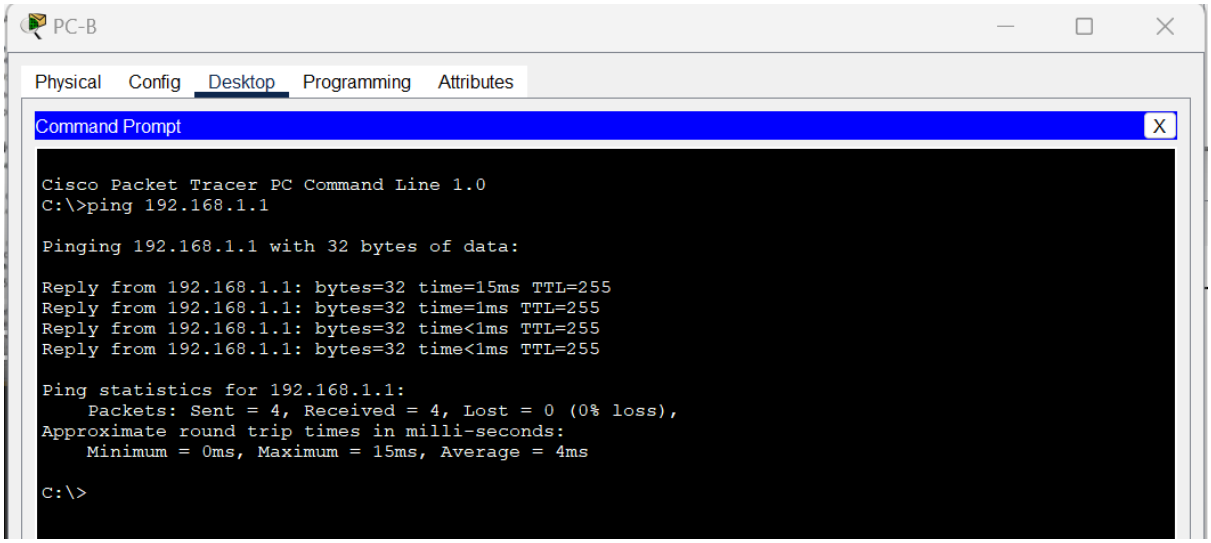
Using show interface ip brief and show ip address to verify the configurations.



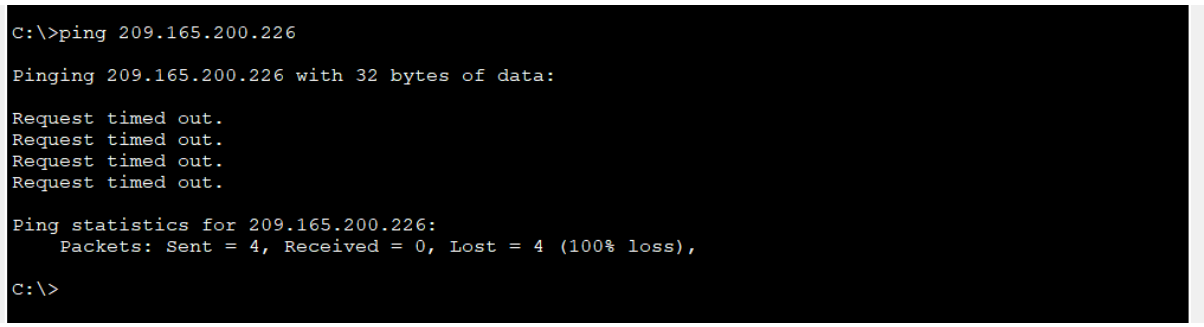


Step 5: Test connectivity to the ASA.

To test the connectivity, ping PC-B to ASA and it should be successful as shown below:



From PC-B, ping the G1/1 (OUTSIDE) interface at IP address 209.165.200.226. This should fail and not be able to ping this address.



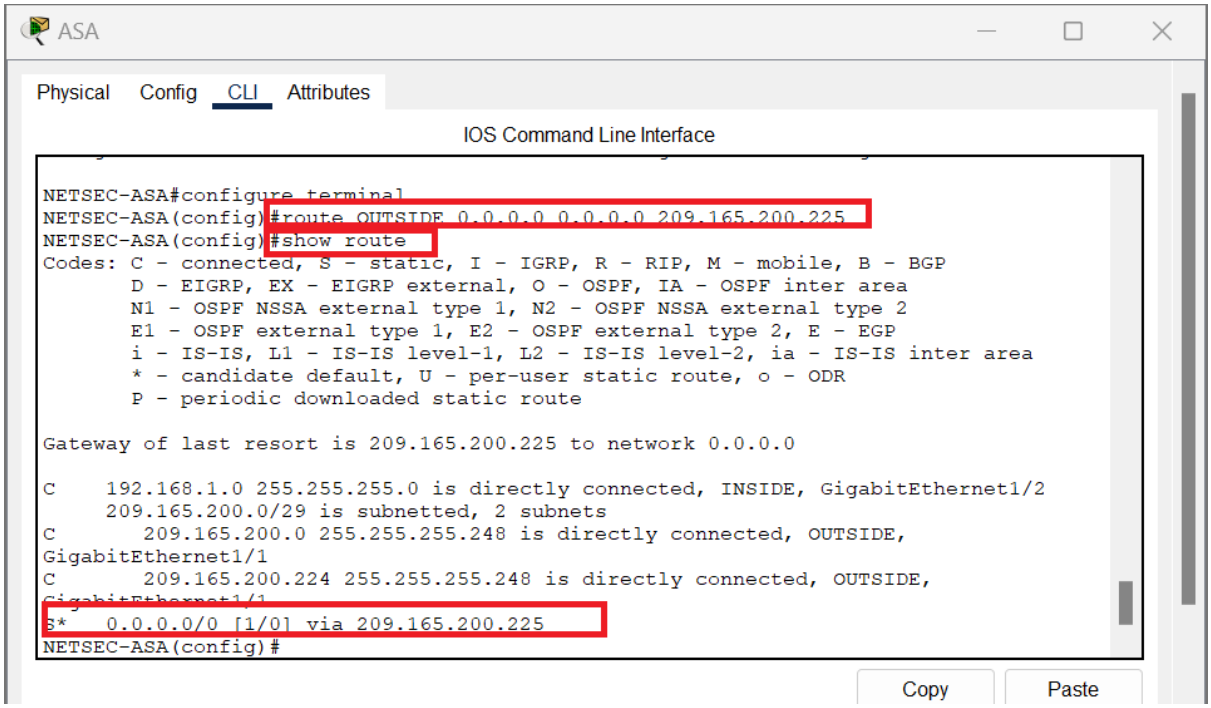
Part 3: Configure Routing, Address Translation, and Inspection Policy Using the CLI

This section is a step-by-step process of configuring the route, Address Translation, and Inspection Policy Using the CLI

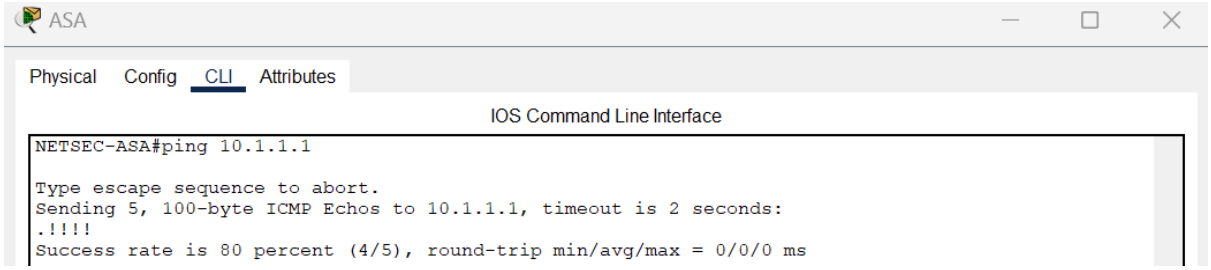
Step 1: Configure a static default route for the ASA.

Configuring a default static route on the ASA OUTSIDE interface to enable the ASA to reach external networks. To achieve that Create a “quad zero” default route using the route command, associate it with the ASA OUTSIDE interface, and point to the R1 G0/0 IP address (209.165.200.225) as the gateway of last resort.

To verify the static default route is in the ASA routing table using show route command.

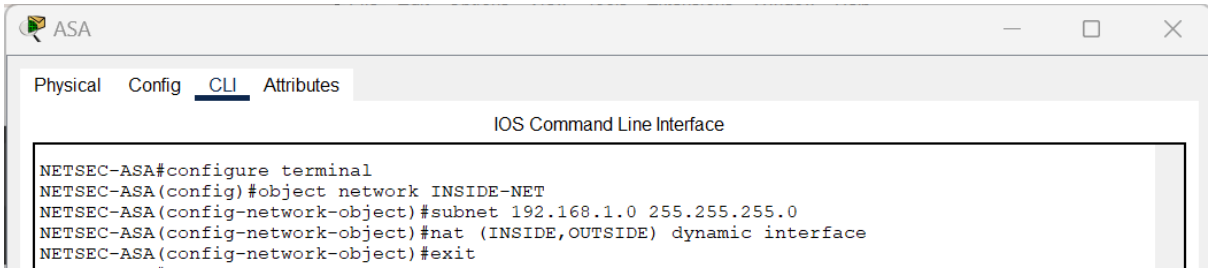


To verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1.

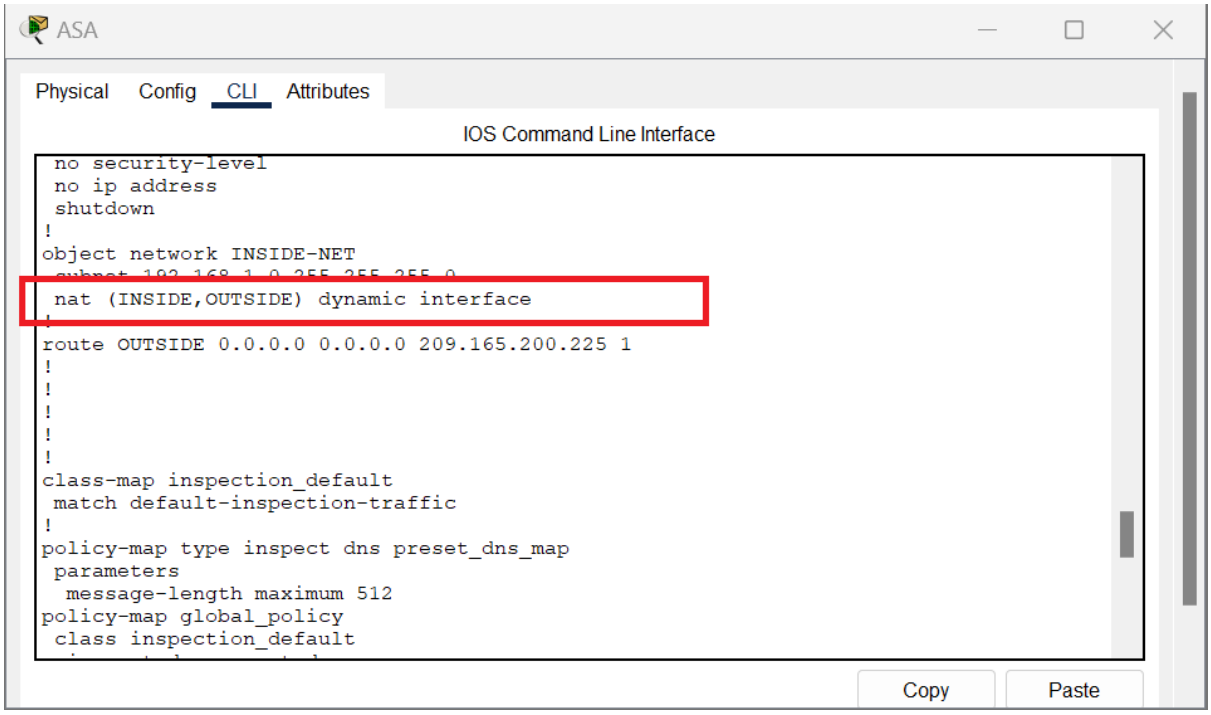


Step 2: Configure address translation using PAT and network objects.

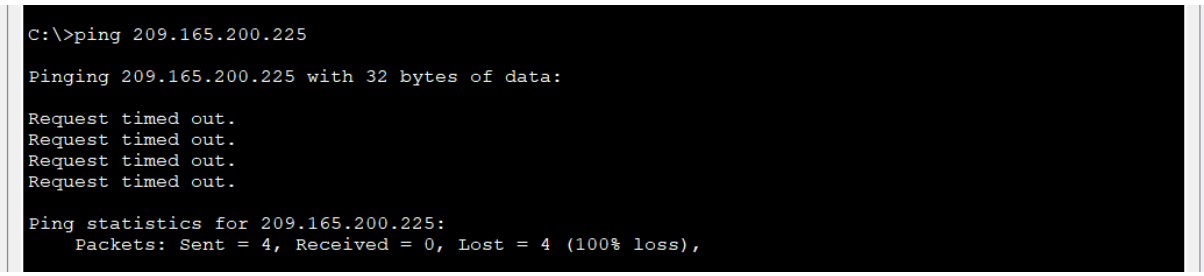
To configure address translation using pat and network objects, create network object INSIDE-NET and assign attributes to it using the subnet and nat commands.



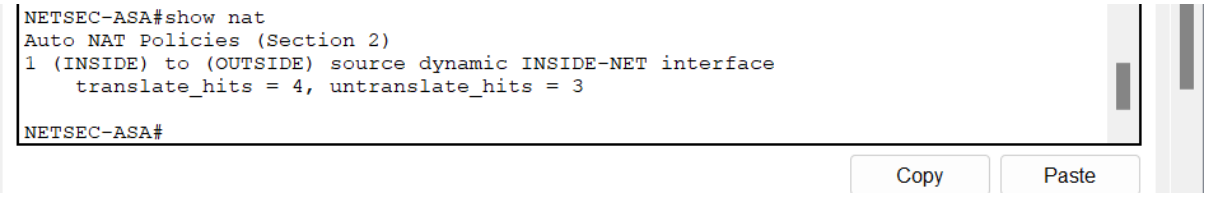
To verify use the show run command.



To further test this, from PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should fail.



Use the show nat command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, four were translated and four were not. The outgoing pings (echos) were translated and sent to the destination. The returning echo replies were blocked by the firewall policy.

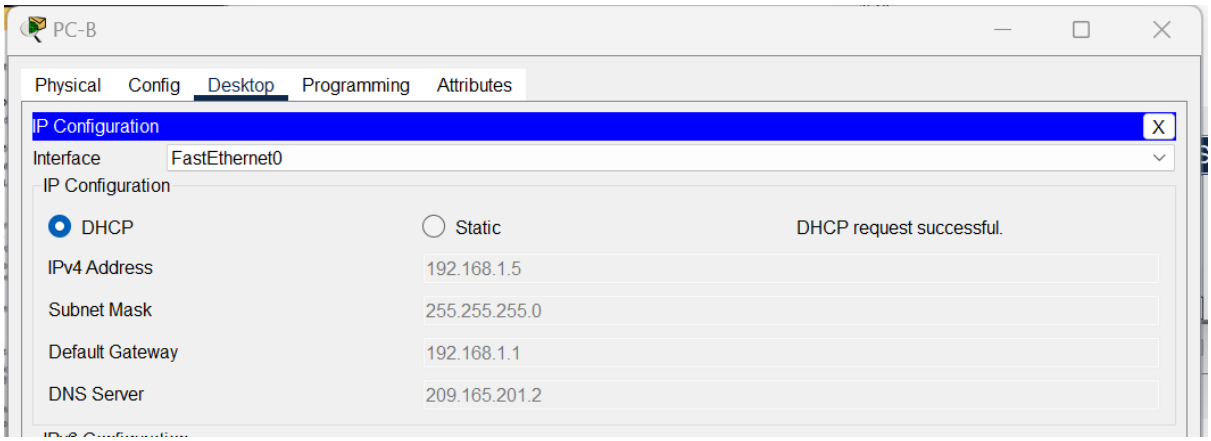


Part 4: Configure DHCP, AAA, and SSH

The following displays a step-by-step process for configuring DHCP, AAA and SSH.

Step 1: Configure the ASA as a DHCP server.

In this step, configure a DHCP address pool and enable it on the ASA INSIDE interface by going to the desktop then Ip configuration.



Step 2: Configure AAA to use the local database for authentication.

To configure the AAA, define a local user named admin by entering the username command. Specify a password of adminpa55 and configure AAA to use the local ASA database for SSH user authentication.

```
NETSEC-ASA(config)#username admin password adminpa55
NETSEC-ASA(config)#aaa authentication ssh console LOCAL
NETSEC-ASA(config)#
```

Step 3: Configure remote access to the ASA.

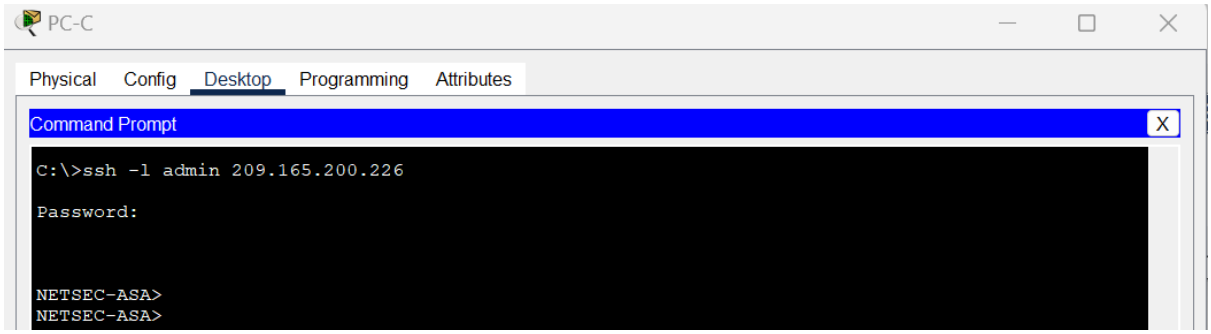
The ASA can be configured to accept connections from a single host or a range of hosts on the INSIDE or OUTSIDE network. In this step, hosts from the OUTSIDE network can only use SSH to communicate with the ASA. SSH sessions can be used to access the ASA from the inside network. To Generate an RSA key pair, which is required to support SSH connections, because the ASA device has RSA keys already in place, enter no when prompted to replace them.

In addition, to Configure the ASA to allow SSH connections from any host on the INSIDE network (192.168.1.0/24) and from the remote management host at the branch office (172.16.3.3) on the OUTSIDE network. Set the SSH timeout to 10 minutes (the default is 5 minutes).

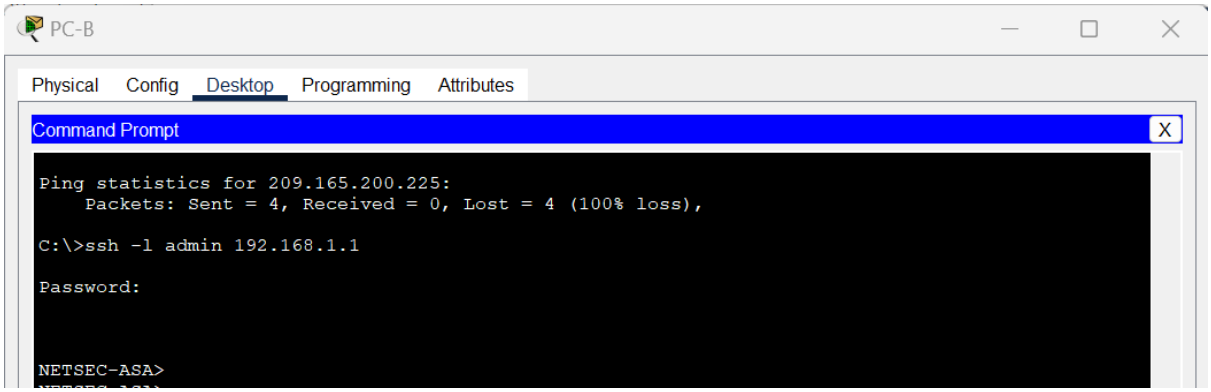
```
NETSEC-ASA(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
NETSEC-ASA(config)#ssh 192.168.1.0 255.255.255.0 INSIDE
NETSEC-ASA(config)#ssh 172.16.3.3 255.255.255.255 OUTSIDE
NETSEC-ASA(config)#ssh timeout 10
NETSEC-ASA(config)#
NETSEC-ASA(config)#
```

Copy Paste

To verify establish an SSH session from PC-C to the ASA (209.165.200.226).i.e this should be successful.



To verify establish an SSH session from PC-B to the ASA (192.168.1.1).i,e this should be successful.

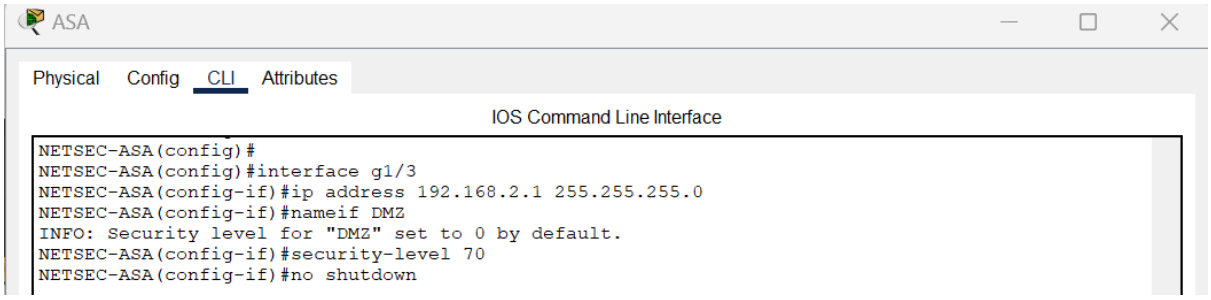


Part 5: Configure a DMZ, Static NAT, and ACLs

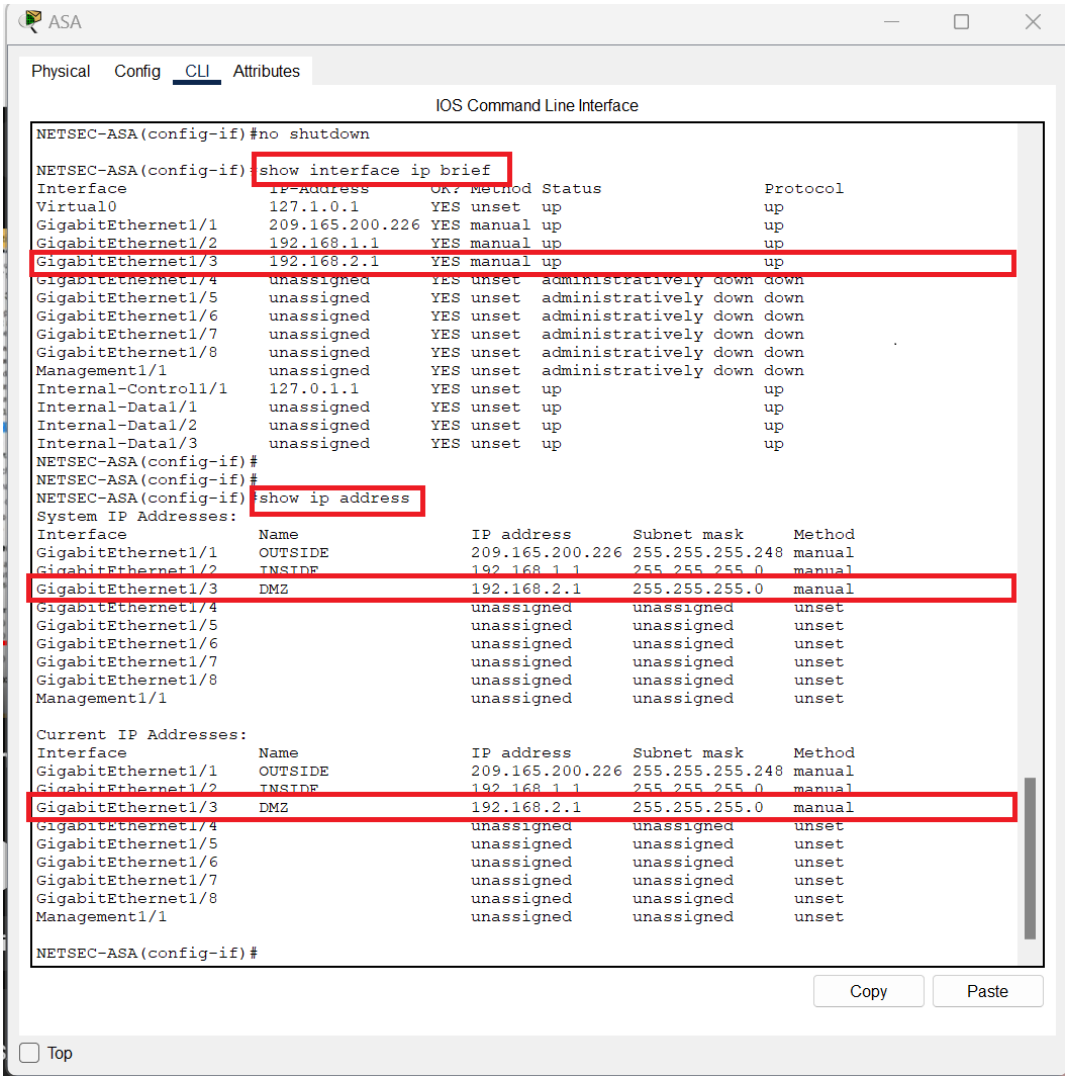
The following section entails a step by step of how to configure the DMZ, Static NAT and ACLs.

Step 1: Configure the DMZ interface VLAN 3 on the ASA.

To Configure the DMZ on the ASA, assign it IP address 192.168.2.1/24, name it DMZ, and assign it a security level of 70 because the server does not need to initiate communication with the inside users, disable forwarding to interface VLAN 1.

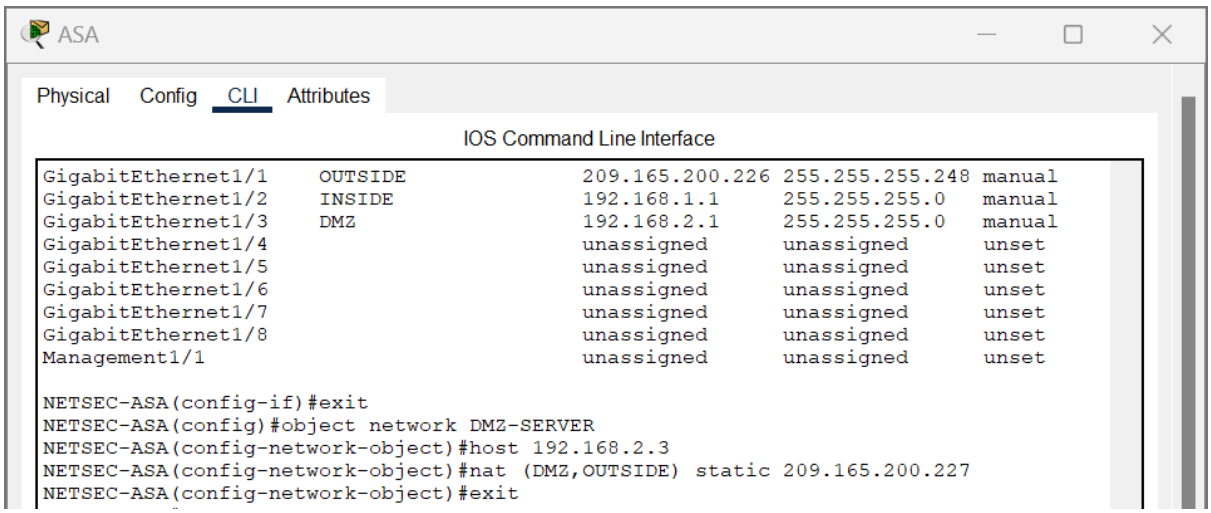


To verify use interface ip brief and show ip address command to check your configurations:



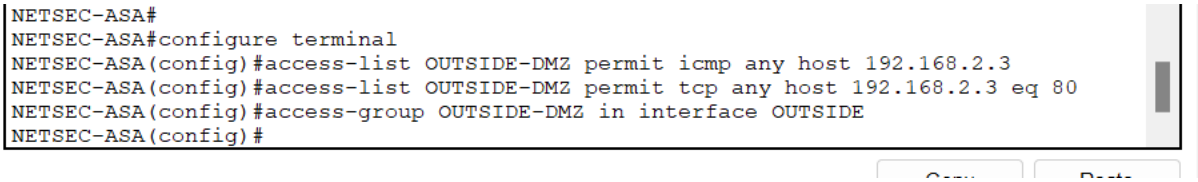
Step 2: Configure static NAT to the DMZ server using a network object.

To configure static NAT to the DMZ server using a network object, configure a network object named DMZ-SERVER and assign it the static IP address of the DMZ server (192.168.2.3). While in object definition mode, use the nat command to specify that this object is used to translate a DMZ address to an OUTSIDE address using static NAT, and specify a public translated address of 209.165.200.227.



Step 3: Configure an ACL to allow access to the DMZ server from the Internet.

To configure an ACL to allow access to the DMZ server from the Internet, configure a named access list OUTSIDE-DMZ that permits the TCP protocol on port 80 from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA OUTSIDE interface in the "IN" direction.



Conclusion

In conclusion, mastering the configuration of ASA basic settings and firewall rules using the CLI is a vital skill for network professionals. Through this assignment, we have explored the essential components of ASA configuration, including network interfaces, IP addressing and access control lists in which has sharpened my technical abilities, deepened my understanding of network security and the role it plays in todays interconnected world. As we continue to advance in our networking careers, the knowledge and proficiency gained from this assignment will most definitely serve as a strong foundation.