

# ASSIGNMENT TWO WRITE UP:

## CONFIGURE ASA BASIC SETTINGS AND FIREWALL USING THE CLI

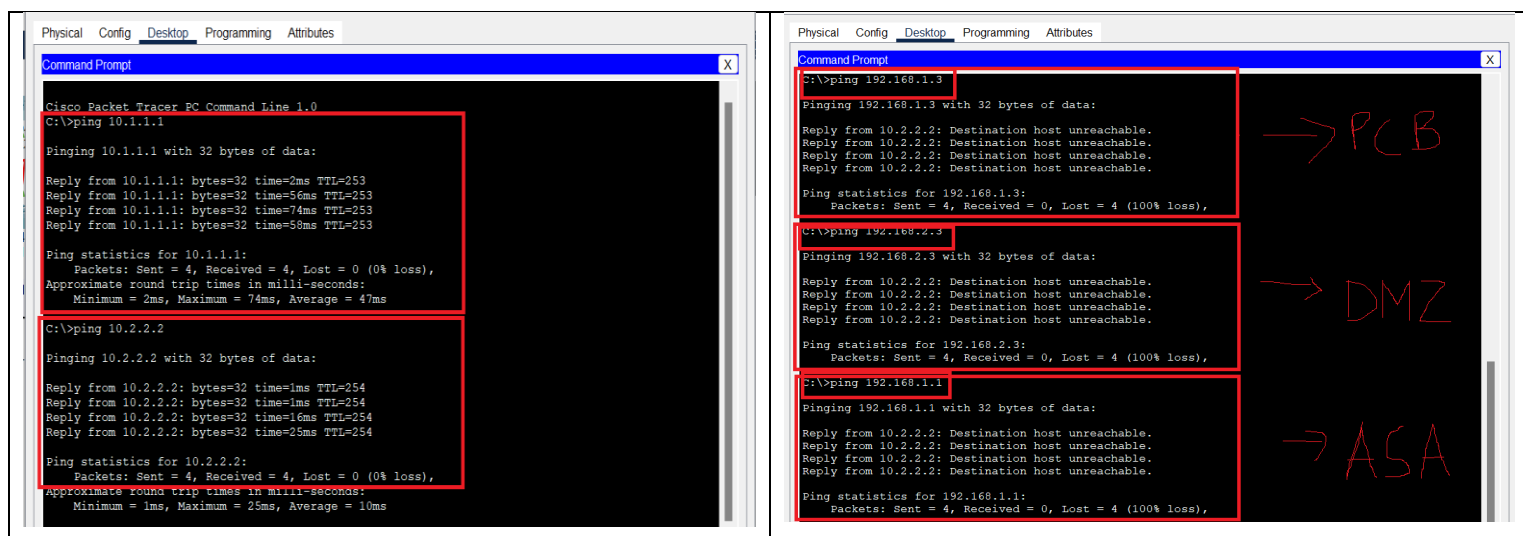
### Introduction

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.

```

ASA
Physical Config CLI Attributes
IOS Command Line Interface

INFO: Power-On Self-Test complete.
INFO: Starting HW-DRBG health test...
INFO: HW-DRBG health test passed.
INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

Type help or '?' for a list of available commands.

ciscoasa show version
Cisco Adaptive Security Appliance Software Version 9.6(1)
Device Manager Version 7.6(1)
Compiled on Fri 18-Mar-16 14:04 EDT by builders
System image file is "disk0:asa961-lfbff-k8.SPA"
Config file at boot was "startup-config"

ciscoasa up 15 minutes 7 seconds

Hardware: ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
Internal ATA Compact Flash, 7168MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
Number of accelerators: 1

1: Ext: GigabitEthernet1/1 : address is 00E0.8F2C.9801, irq 255
2: Ext: GigabitEthernet1/2 : address is 00E0.8F2C.9802, irq 255
3: Ext: GigabitEthernet1/3 : address is 00E0.8F2C.9803, irq 255
4: Ext: GigabitEthernet1/4 : address is 00E0.8F2C.9804, irq 255
5: Ext: GigabitEthernet1/5 : address is 00E0.8F2C.9805, irq 255
6: Ext: GigabitEthernet1/6 : address is 00E0.8F2C.9806, irq 255
7: Ext: GigabitEthernet1/7 : address is 00E0.8F2C.9807, irq 255
8: Ext: GigabitEthernet1/8 : address is 00E0.8F2C.9808, irq 255
9: Int: Internal-Datal/1 : address is 00E0.8F2C.9809, irq 0
10: Int: Internal-Datal/2 : address is 0000.0001.0002, irq 0
11: Int: Internal-Controll/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Datal/3 : address is 0000.0001.0003, irq 0
13: Int: Management1/1 : address is 00E0.8F2C.9809, irq 0
<--- More --->
Copy Paste

```

### 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.

```
NETSEC-ASA(config)#clock set 23:59:00 June 22 2023
NETSEC-ASA(config)#interface g1/1
NETSEC-ASA(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
NETSEC-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
ERROR: % Invalid Hostname
NETSEC-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
NETSEC-ASA(config-if)#security-level 0
NETSEC-ASA(config-if)#no shutdown
^
% Invalid input detected at '^' marker.
NETSEC-ASA(config-if)#no shutdown
NETSEC-ASA(config-if)#exit
NETSEC-ASA(config)#interface g1/2
NETSEC-ASA(config-if)#nameif INSIDE
INFO: Security level for "INSIDE" set to 0 by default.
NETSEC-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
NETSEC-ASA(config-if)#security-level 100
NETSEC-ASA(config-if)#no shutdown
```

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

The first screenshot shows the output of the `show interface ip brief` command. It lists all interfaces with their IP addresses, security levels, and status. The OUTSIDE interface (GigabitEthernet1/1) is highlighted with a red box, showing it is up and has an IP address of 209.165.200.226. The INSIDE interface (GigabitEthernet1/2) is also highlighted, showing it is up and has an IP address of 192.168.1.1.

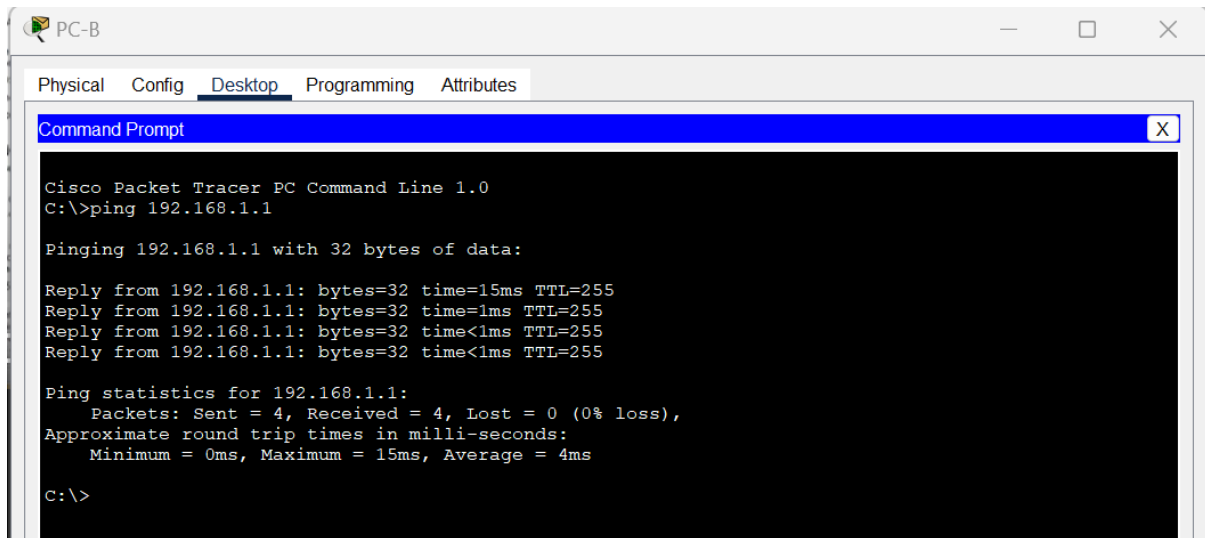
Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.0.0.1	YES	unset	up	up
GigabitEthernet1/1	209.165.200.226	YES	manual	up	up
GigabitEthernet1/2	192.168.1.1	YES	manual	up	up
GigabitEthernet1/3	unassigned	YES	unset	administratively down	down
GigabitEthernet1/4	unassigned	YES	unset	administratively down	down
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down
GigabitEthernet1/6	unassigned	YES	unset	administratively down	down
GigabitEthernet1/7	unassigned	YES	unset	administratively down	down
GigabitEthernet1/8	unassigned	YES	unset	administratively down	down
Management1/1	unassigned	YES	unset	administratively down	down
Internal-Data1/1	127.0.1.1	YES	unset	up	up
Internal-Data1/2	unassigned	YES	unset	up	up
Internal-Data1/3	unassigned	YES	unset	up	up

The second screenshot shows the output of the `show ip address` command. It displays the current IP addresses for all interfaces. The OUTSIDE interface (GigabitEthernet1/1) is highlighted with a red box, showing it has an IP address of 209.165.200.226 and a subnet mask of 255.255.255.248. The INSIDE interface (GigabitEthernet1/2) is also highlighted, showing it has an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0.

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet1/1	OUTSIDE	209.165.200.226	255.255.255.248	manual
GigabitEthernet1/2	INSIDE	192.168.1.1	255.255.255.0	manual
GigabitEthernet1/3		unassigned	unassigned	unset
GigabitEthernet1/4		unassigned	unassigned	unset
GigabitEthernet1/5		unassigned	unassigned	unset
GigabitEthernet1/6		unassigned	unassigned	unset
GigabitEthernet1/7		unassigned	unassigned	unset
GigabitEthernet1/8		unassigned	unassigned	unset
Management1/1		unassigned	unassigned	unset

#### Step 5: Test connectivity to the ASA.

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



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=15ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 4ms

C:\>
```

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.

```
C:\>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

### 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.

The screenshot shows the ASA CLI interface with the following commands and output:

```
NETSEC-ASA#configure terminal
NETSEC-ASA(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
NETSEC-ASA(config)#show route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

```
C    192.168.1.0 255.255.255.0 is directly connected, INSIDE, GigabitEthernet1/2
    209.165.200.0/29 is subnetted, 2 subnets
C      209.165.200.0 255.255.255.248 is directly connected, OUTSIDE,
GigabitEthernet1/1
C      209.165.200.224 255.255.255.248 is directly connected, OUTSIDE,
GigabitEthernet1/1
S*    0.0.0.0/0 [1/0] via 209.165.200.225
NETSEC-ASA(config)#
```

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

The screenshot shows the ASA CLI interface with the following command and output:

```
NETSEC-ASA#ping 10.1.1.1
```

Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:  
.....  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

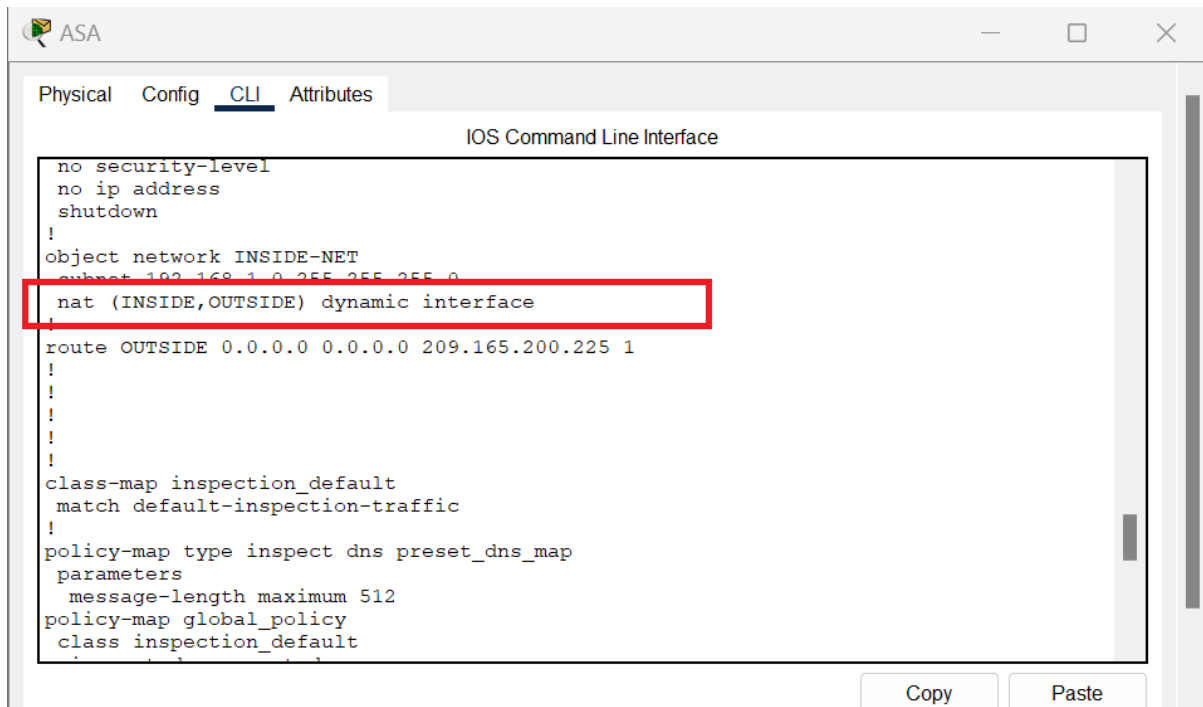
## Step 2: Configure address translation using PAT and network objects.

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.

The screenshot shows the ASA CLI interface with the following commands:

```
NETSEC-ASA#configure terminal
NETSEC-ASA(config)#object network INSIDE-NET
NETSEC-ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
NETSEC-ASA(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
NETSEC-ASA(config-network-object)#exit
```

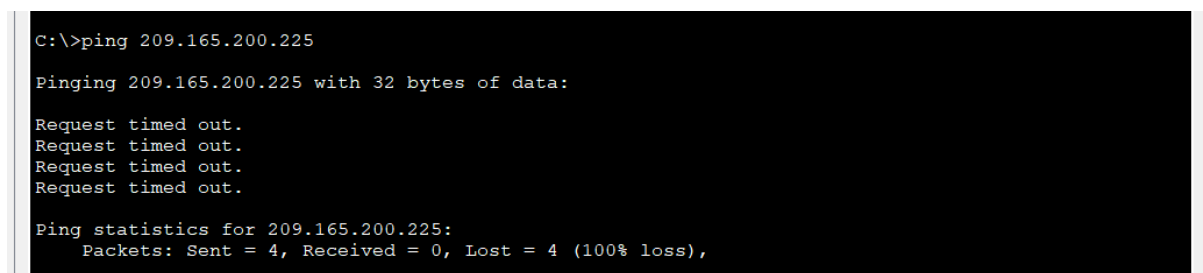
To verify use the show run command.

A screenshot of the ASA configuration window. The 'CLI' tab is selected. The configuration text is as follows:

```
no security-level
no ip address
shutdown
!
object network INSIDE-NET
  subject 192.168.1.0 255.255.255.0
  nat (INSIDE,OUTSIDE) dynamic interface
!
route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225 1
!
!
!
!
class-map inspection_default
  match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
```

The line `nat (INSIDE,OUTSIDE) dynamic interface` is highlighted with a red rectangle. At the bottom right, there are 'Copy' and 'Paste' buttons.

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.

A screenshot of a Windows command prompt window. The command `C:\>ping 209.165.200.225` has been entered. The output shows four 'Request timed out.' messages and ping statistics indicating 100% loss.

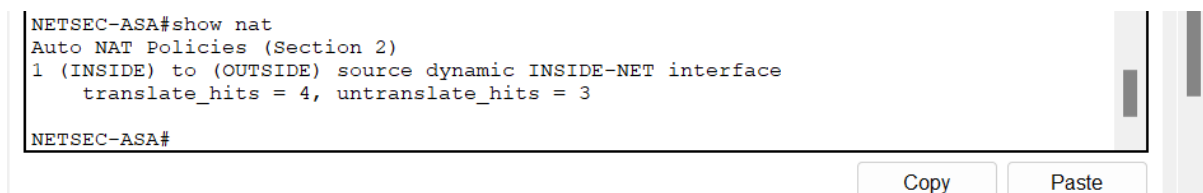
```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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.

A screenshot of the ASA CLI showing the output of the `show nat` command.

```
NETSEC-ASA#show nat
Auto NAT Policies (Section 2)
1 (INSIDE) to (OUTSIDE) source dynamic INSIDE-NET interface
  translate_hits = 4, untranslate_hits = 3
NETSEC-ASA#
```

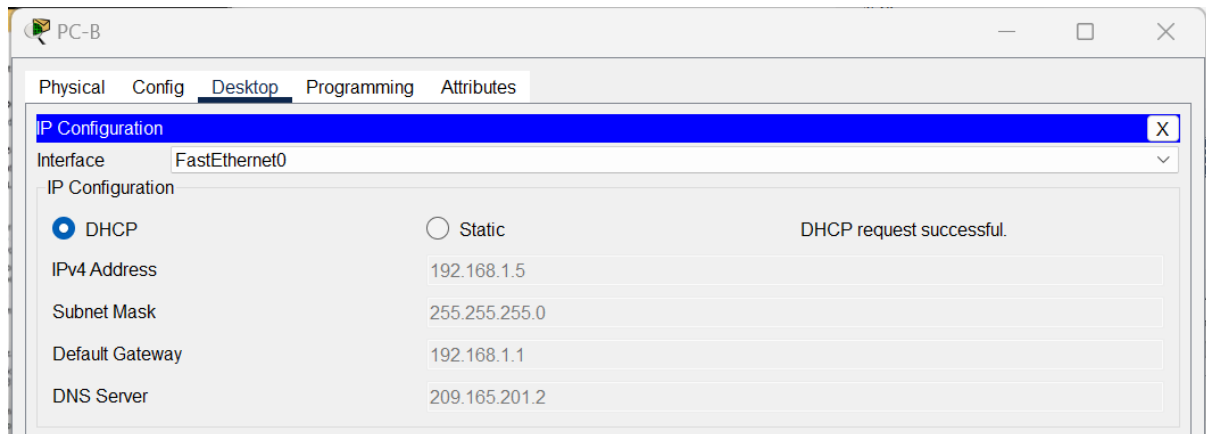
At the bottom right, there are 'Copy' and 'Paste' buttons.

## 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.

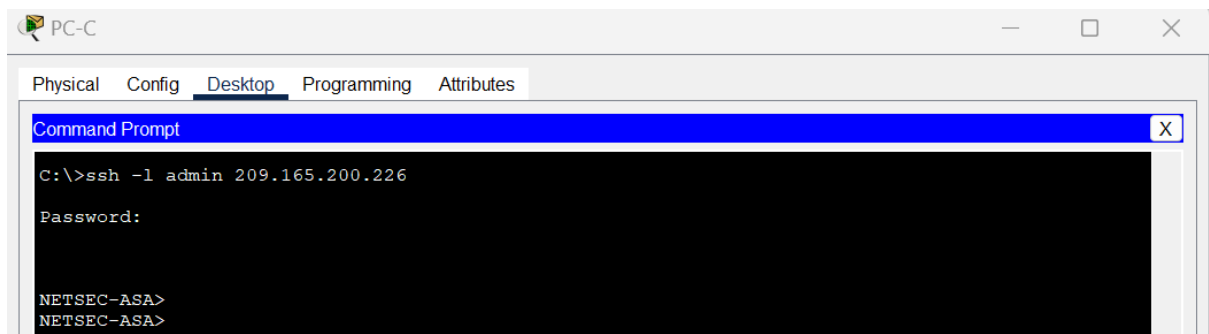
The ASA can be configured to accept connections from a single host or a range of hosts on the INSIDE or OUTSIDE network. In this step, hosts from the OUTSIDE network can only use SSH to communicate with the ASA. SSH sessions can be used to access the ASA from the inside network. To Generate an RSA key 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)#
```

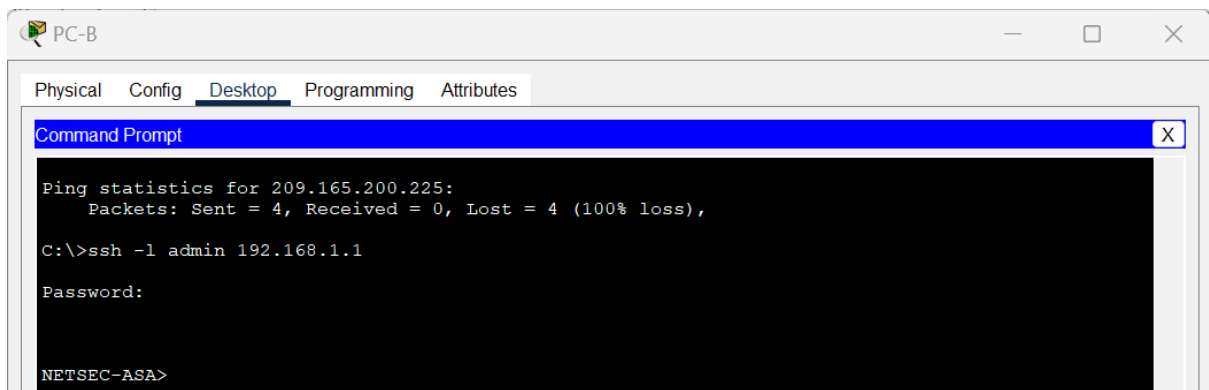
To verify establish an SSH session from PC-C to the ASA (209.165.200.226).i.e this should be successful.



The screenshot shows a window titled 'PC-C' with a 'Command Prompt' tab selected. The command prompt displays the following text:

```
C:\>ssh -l admin 209.165.200.226  
Password:  
  
NETSEC-ASA>  
NETSEC-ASA>
```

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



The screenshot shows a window titled 'PC-B' with a 'Command Prompt' tab selected. The command prompt displays the following text:

```
Ping statistics for 209.165.200.225:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>ssh -l admin 192.168.1.1  
Password:  
  
NETSEC-ASA>  
NETSEC-ASA>
```

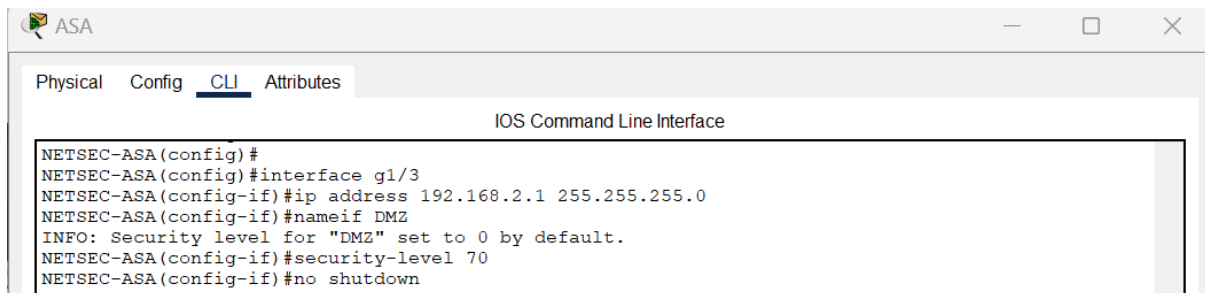


## Part 5: Configure a DMZ, Static NAT, and ACLs

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

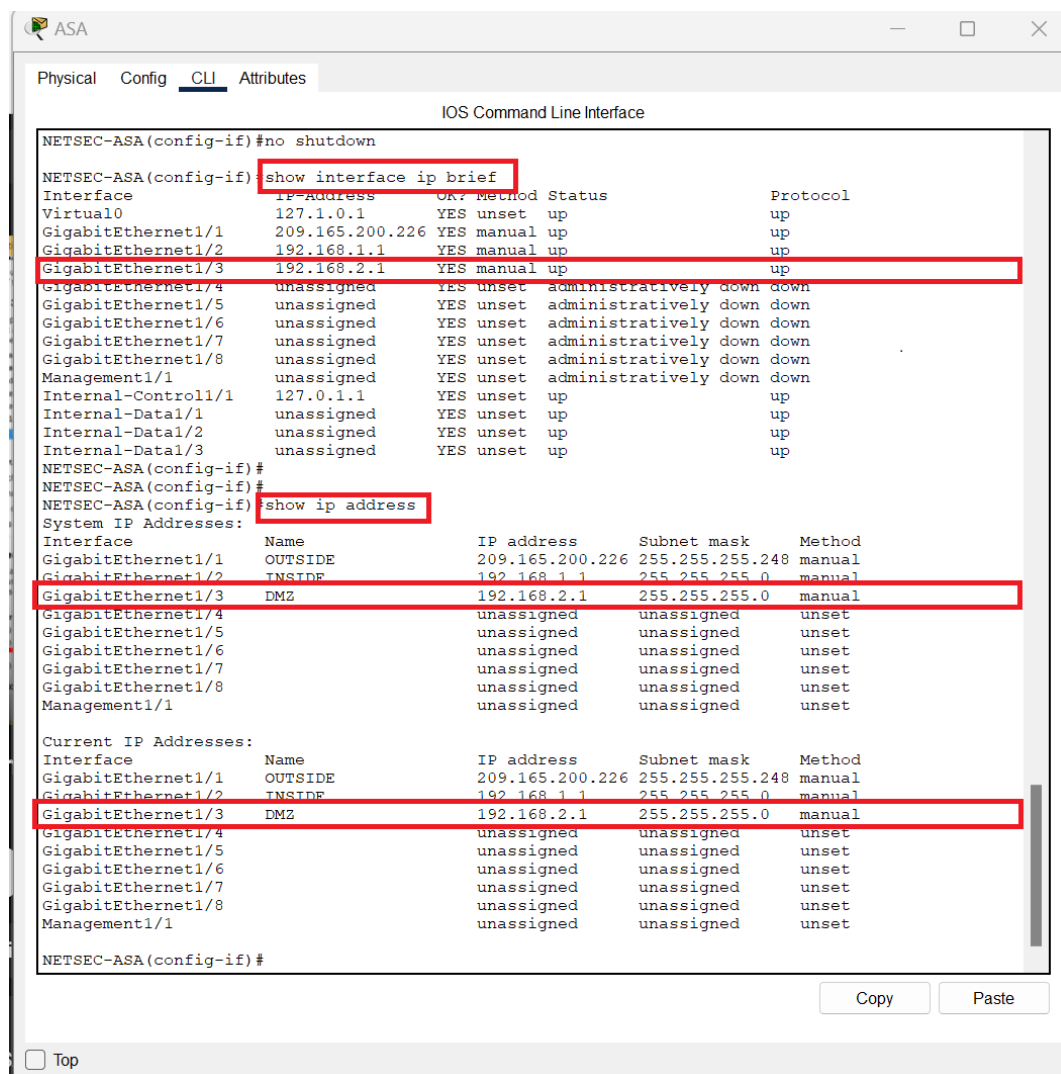
### Step 1: Configure the DMZ interface VLAN 3 on the ASA.

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.



```
NETSEC-ASA(config)#
NETSEC-ASA(config)#interface g1/3
NETSEC-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
NETSEC-ASA(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
NETSEC-ASA(config-if)#security-level 70
NETSEC-ASA(config-if)#no shutdown
```

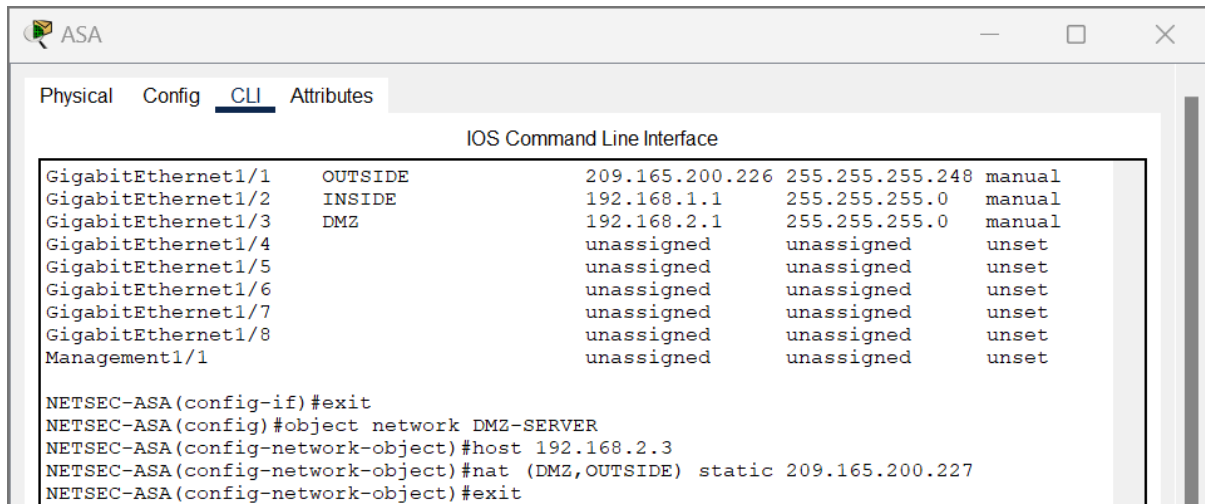
To verify use interface ip brief and show ip address command to check your configurations:



```
NETSEC-ASA(config-if)#no shutdown
NETSEC-ASA(config-if)#show interface ip brief
Interface IP-Address OK? Method Status Protocol
Virtual0 127.1.0.1 YES unset up up
GigabitEthernet1/1 209.165.200.226 YES manual up up
GigabitEthernet1/2 192.168.1.1 YES manual up up
GigabitEthernet1/3 192.168.2.1 YES manual up up
GigabitEthernet1/4 unassigned YES unset administratively down down
GigabitEthernet1/5 unassigned YES unset administratively down down
GigabitEthernet1/6 unassigned YES unset administratively down down
GigabitEthernet1/7 unassigned YES unset administratively down down
GigabitEthernet1/8 unassigned YES unset administratively down down
Management1/1 unassigned YES unset administratively down down
Internal-Controll1/1 127.0.1.1 YES unset up up
Internal-Data1/1 unassigned YES unset up up
Internal-Data1/2 unassigned YES unset up up
Internal-Data1/3 unassigned YES unset up up
NETSEC-ASA(config-if)#
NETSEC-ASA(config-if)#show ip address
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet1/1 OUTSIDE 209.165.200.226 255.255.255.248 manual
GigabitEthernet1/2 INSIDE 192.168.1.1 255.255.255.0 manual
GigabitEthernet1/3 DMZ 192.168.2.1 255.255.255.0 manual
GigabitEthernet1/4 unassigned unassigned unset
GigabitEthernet1/5 unassigned unassigned unset
GigabitEthernet1/6 unassigned unassigned unset
GigabitEthernet1/7 unassigned unassigned unset
GigabitEthernet1/8 unassigned unassigned unset
Management1/1 unassigned unassigned unset
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet1/1 OUTSIDE 209.165.200.226 255.255.255.248 manual
GigabitEthernet1/2 INSIDE 192.168.1.1 255.255.255.0 manual
GigabitEthernet1/3 DMZ 192.168.2.1 255.255.255.0 manual
GigabitEthernet1/4 unassigned unassigned unset
GigabitEthernet1/5 unassigned unassigned unset
GigabitEthernet1/6 unassigned unassigned unset
GigabitEthernet1/7 unassigned unassigned unset
GigabitEthernet1/8 unassigned unassigned unset
Management1/1 unassigned unassigned unset
NETSEC-ASA(config-if)#
```

## 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.

```
NETSEC-ASA#
NETSEC-ASA#configure terminal
NETSEC-ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
NETSEC-ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
NETSEC-ASA(config)#access-group OUTSIDE-DMZ in interface OUTSIDE
NETSEC-ASA(config)#
```

## 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 today's 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.