Assignment 2: Configure ASA Basic Settings and Firewall Using the CLI

Report by: Tonny Odhiambo, CS-CNS06-24028

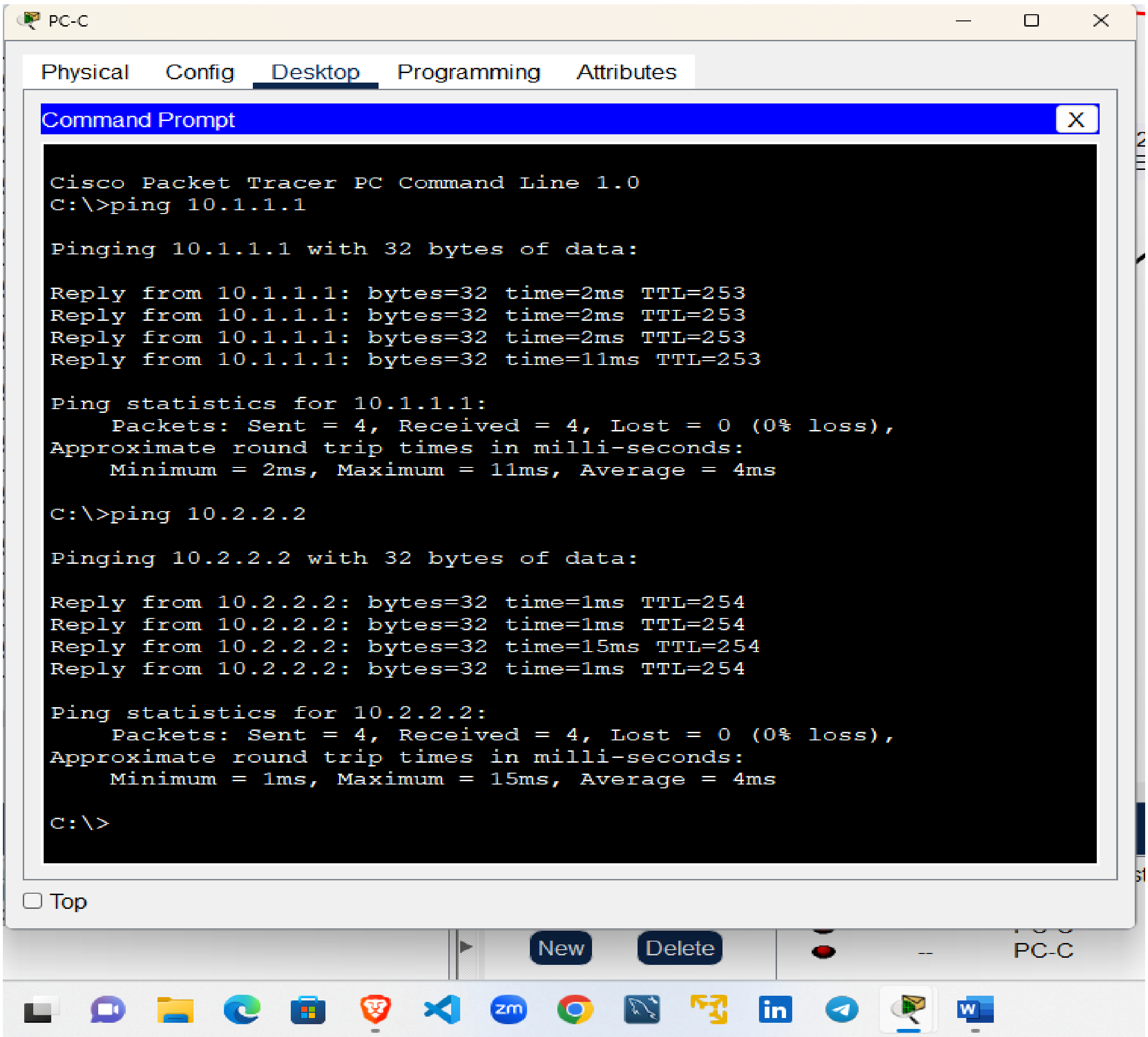
Introduction

This report details the configuration of an Adaptive Security Appliance (ASA) using the Command-Line Interface (CLI) in Cisco Packet Tracer. The configuration includes interface settings, routing, address translation, inspection policies, DHCP, AAA, SSH, DMZ setup, static NAT, and ACLs. The ASA acts as the edge security device for a corporate network connected to an ISP.

Part 1: Verify Connectivity and Explore the ASA

Step 1: Verify Connectivity

To verify connectivity, from PC-C, we open the Command Prompt and use the ping command to test connectivity to router interfaces. Here, we ping R1 and R2 from PC-C and verified its connectivity.

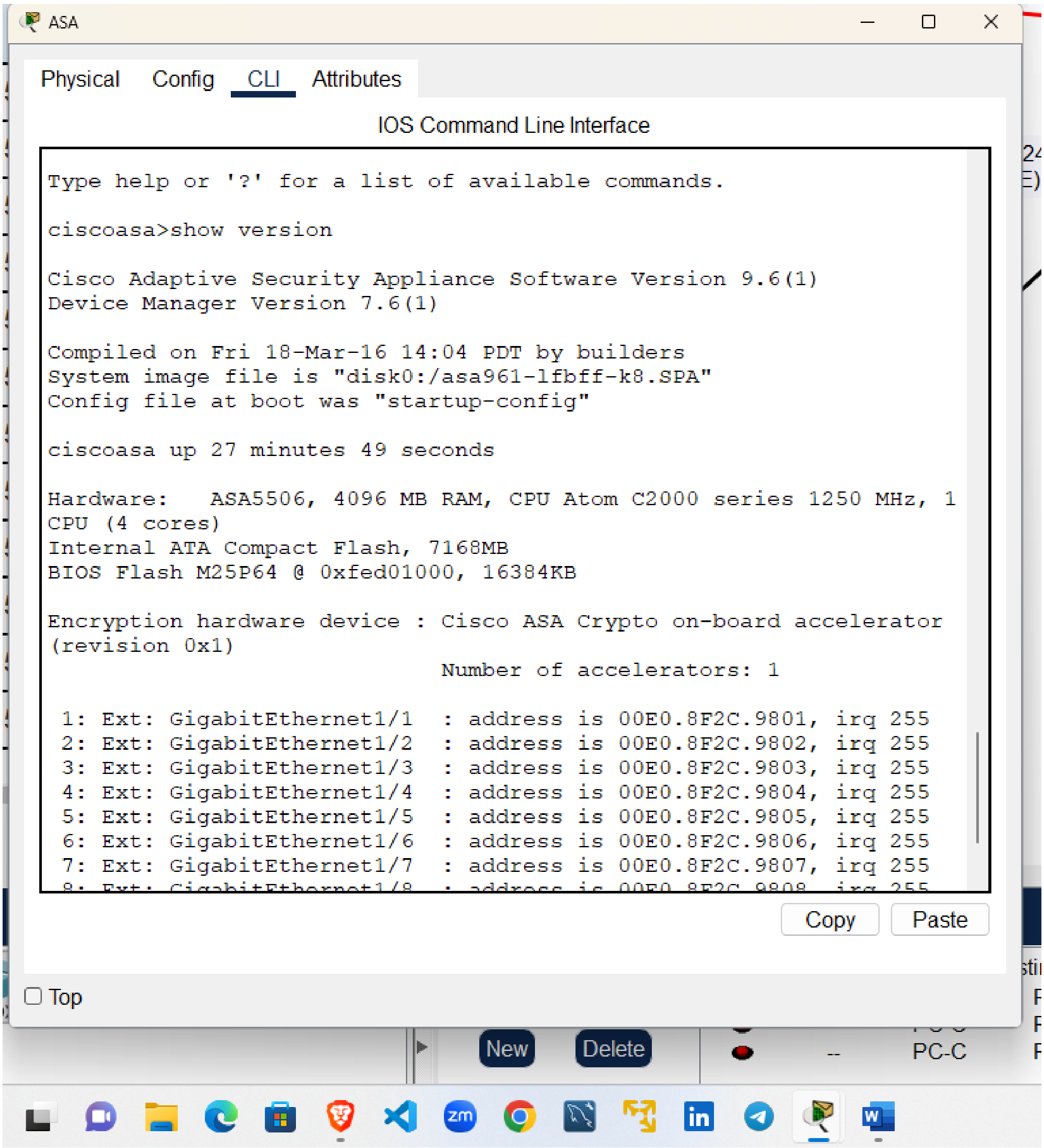


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=2ms TTL=253
Reply from 10.1.1.1: bytes=32 time=2ms TTL=253
Reply from 10.1.1.1: bytes=32 time=2ms TTL=253
Reply from 10.1.1.1: bytes=32 time=11ms TTL=253

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 4ms

C:\>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
Reply from 10.2.2.2: bytes=32 time=15ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254

Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 4ms

C:\>
```

This verifies that the network is set up correctly and the routers are responding to pings.

Step 2: Determine the ASA Version, Interfaces, and License

I accessed the ASA console and entered privileged EXEC mode by pressing Enter (no password needed). I used the show version command to check the ASA version, interface details, and license information.

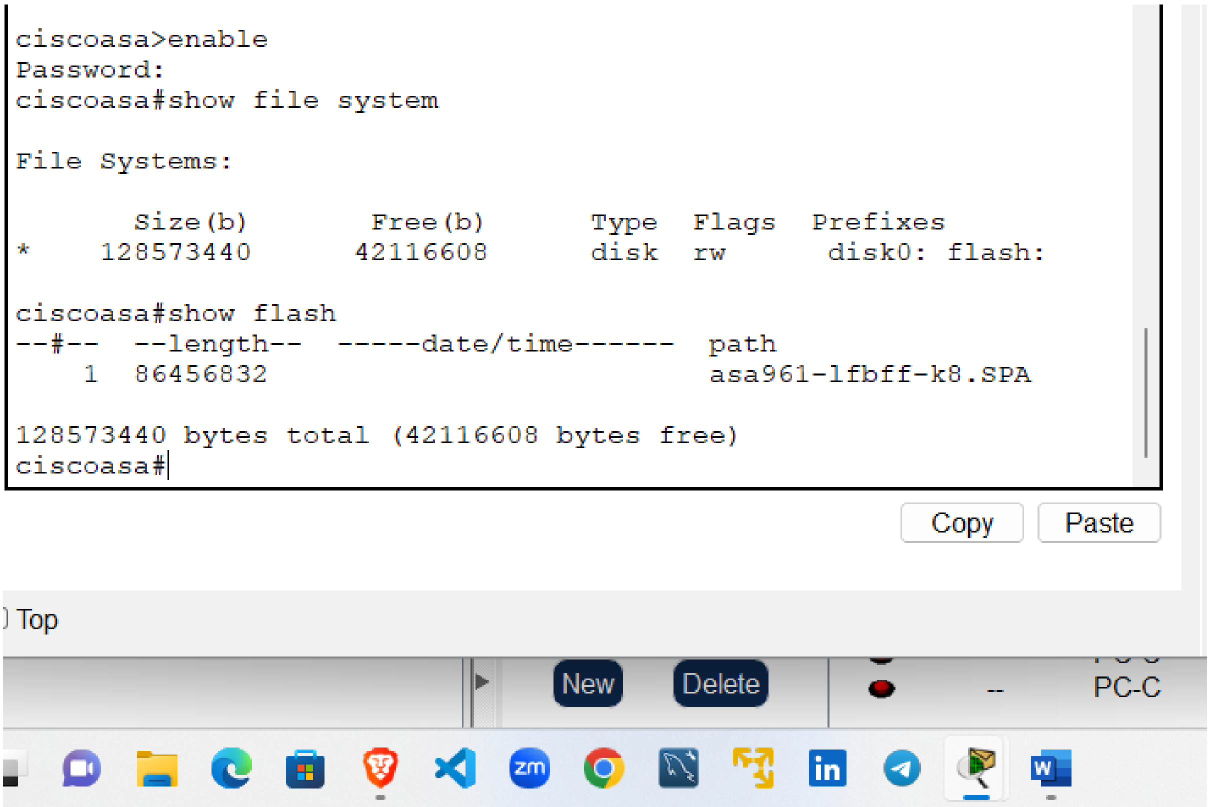


```
Type help or '?' for a list of available commands.

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 PDT by builders
System image file is "disk0:/asa961-lfbff-k8.SPA"
Config file at boot was "startup-config"

ciscoasa up 27 minutes 49 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
```

This helps understand the current configuration and capabilities of the ASA device.

Step 3: Determine the File System and Contents of Flash Memory

In privileged EXEC mode, I used the show file system command to display the supported file system prefixes. Then, I used the show flash: or show disk0: command to view the contents of the flash memory.

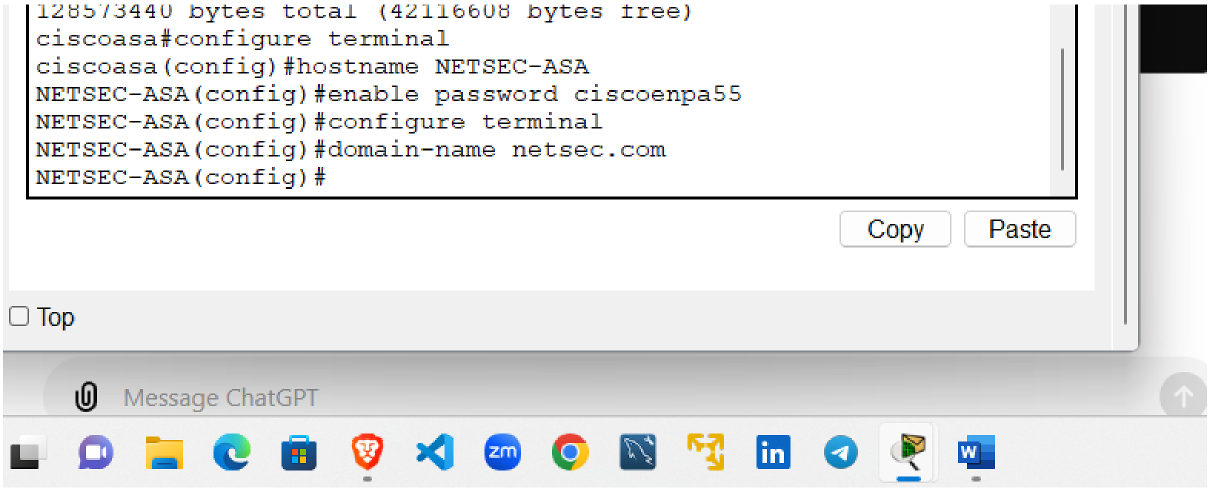


```
ciscoasa>enable
Password:
ciscoasa#show file system

File Systems:

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

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

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

This helps identify available storage and files on the ASA.

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

Step 1: Configure the Hostname and Domain Name

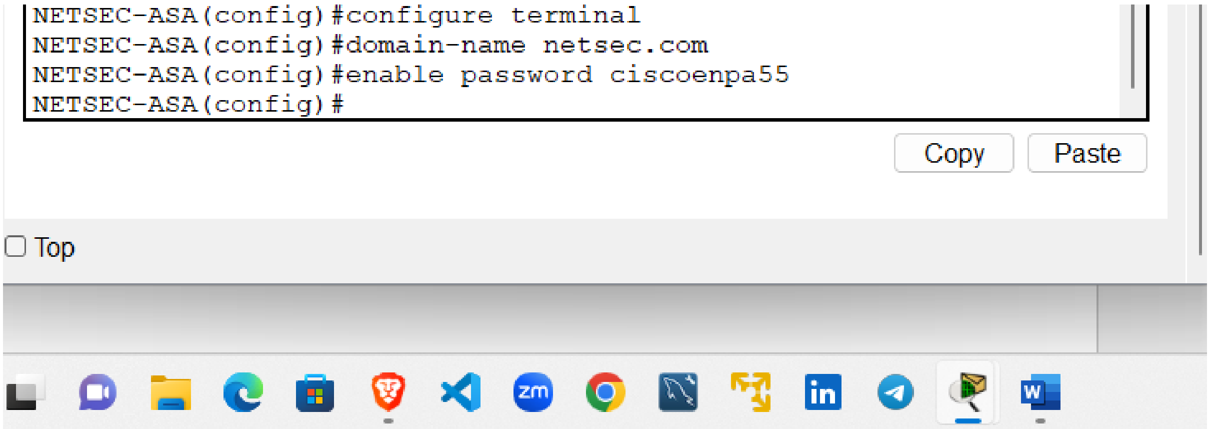


```
128573440 bytes total (42116608 bytes free)
ciscoasa#configure terminal
ciscoasa(config)#hostname NETSEC-ASA
NETSEC-ASA(config)#enable password ciscoenpa55
NETSEC-ASA(config)#configure terminal
NETSEC-ASA(config)#domain-name netsec.com
NETSEC-ASA(config)#
```

This establishes a unique identity for the ASA on the network**.**

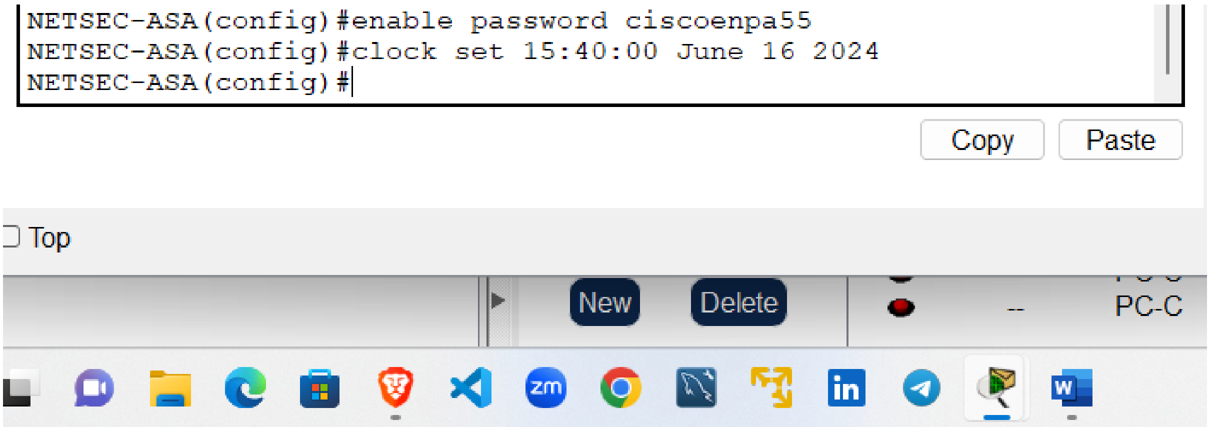
Step 2: Configure the Enable Mode Password

This ensures only authorized users can access privileged EXEC mode.



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

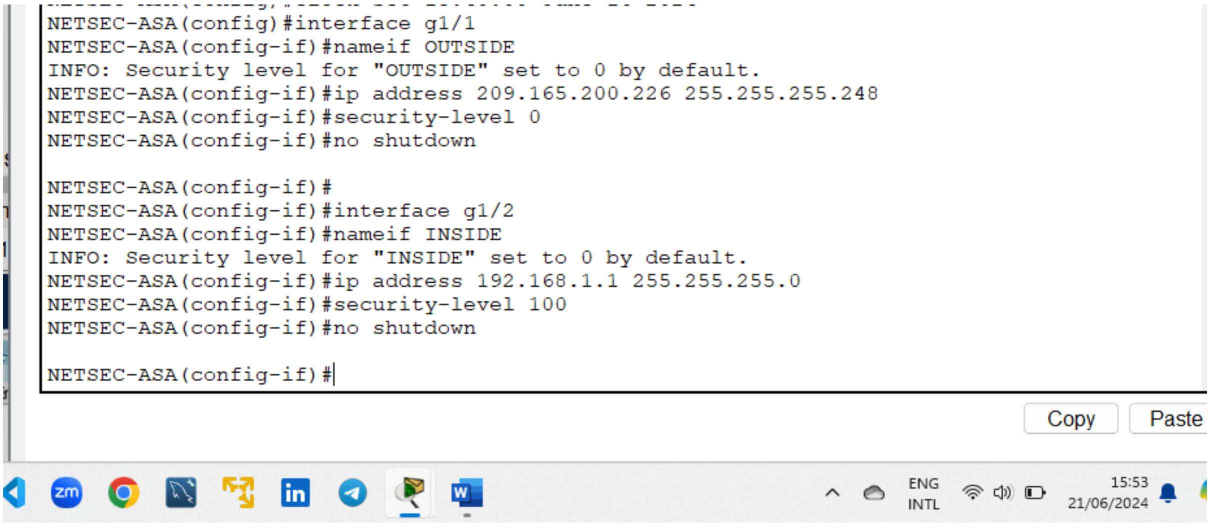
Step 3: Set the Date and Time



```
NETSEC-ASA(config)#enable password ciscoenpa55
NETSEC-ASA(config)#clock set 15:40:00 June 16 2024
NETSEC-ASA(config)#
```

Accurate date and time settings are crucial for logging and event tracking.

Step 4: Configure the INSIDE and OUTSIDE Interfaces



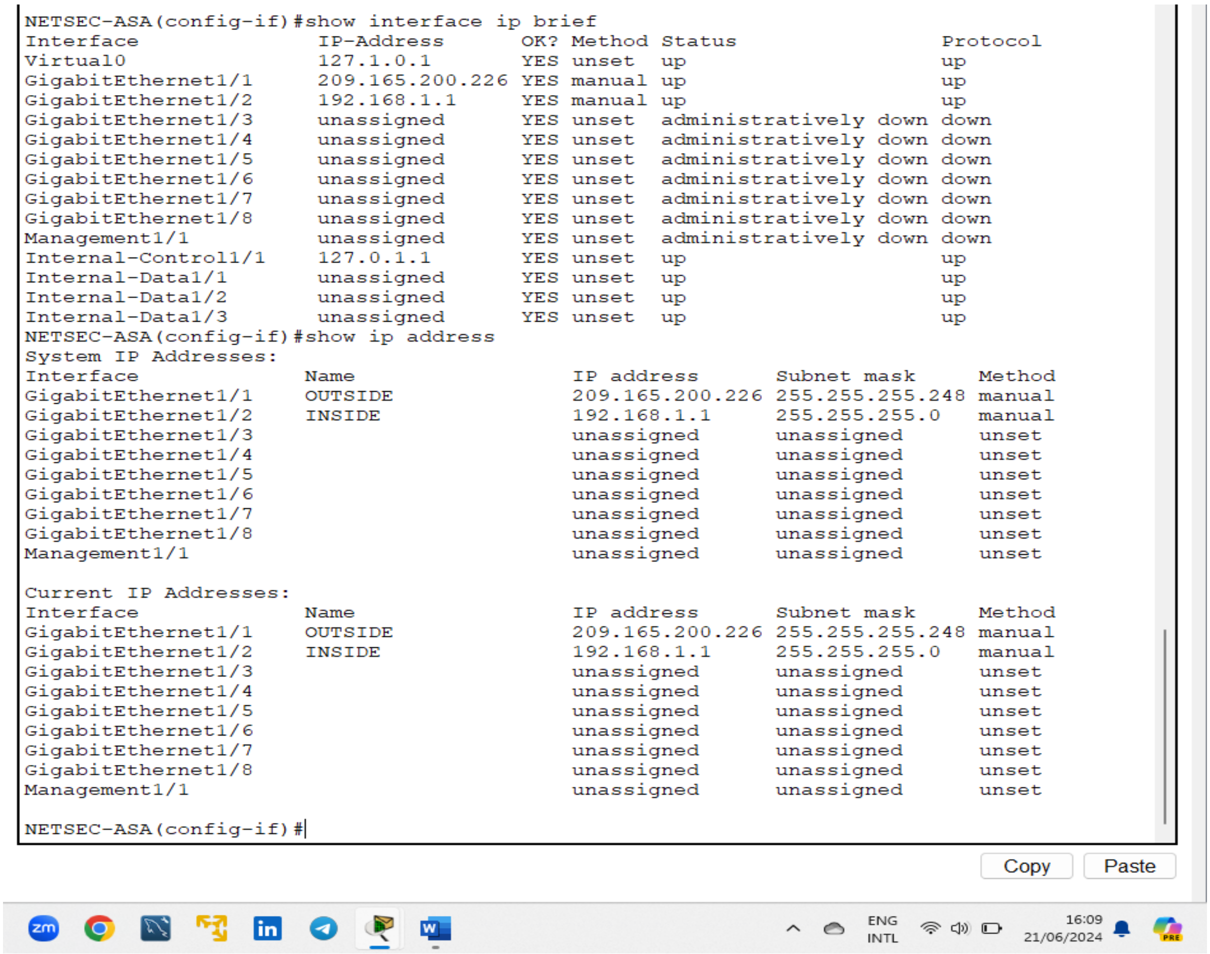
```
NETSEC-ASA(config)#interface g1/1
NETSEC-ASA(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
NETSEC-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
NETSEC-ASA(config-if)#security-level 0
NETSEC-ASA(config-if)#no shutdown

NETSEC-ASA(config-if)#
NETSEC-ASA(config-if)#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

NETSEC-ASA(config-if)#
```

These configurations set up the ASA's internal and external network interfaces.

I verified the ASA configurations using the following commands:

1. Utilized show interface ip brief to check the status of all ASA interfaces, ensuring they were up/up.

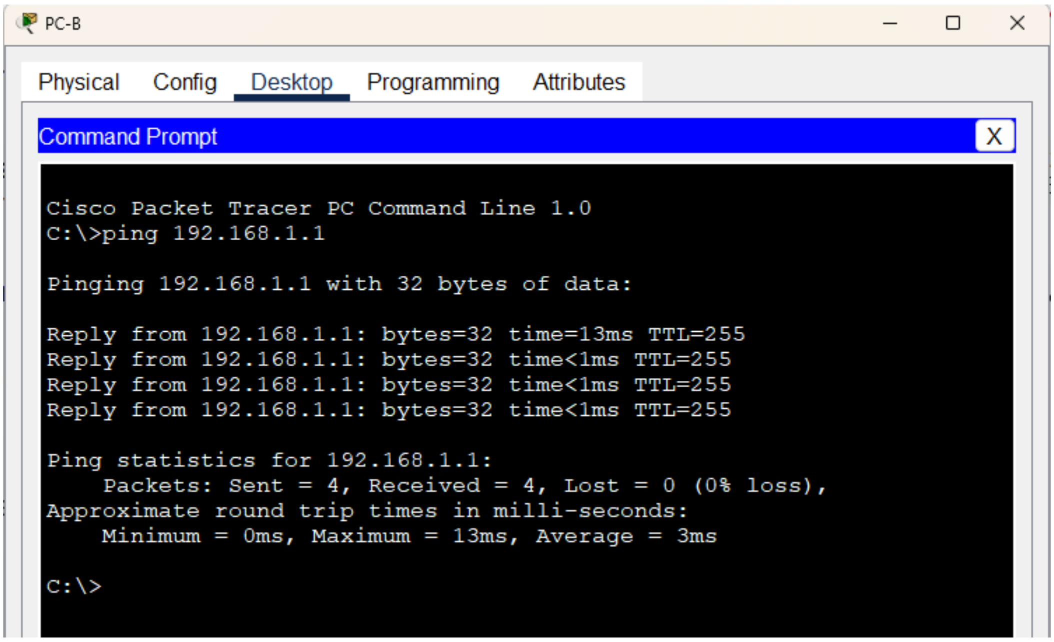
2. Used show ip address to confirm the correct assignment of IP addresses to ASA interfaces, validating network connectivity and configuration alignment.



```
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     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-Control1/1    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)#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                          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

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                          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

NETSEC-ASA(config-if)#
```

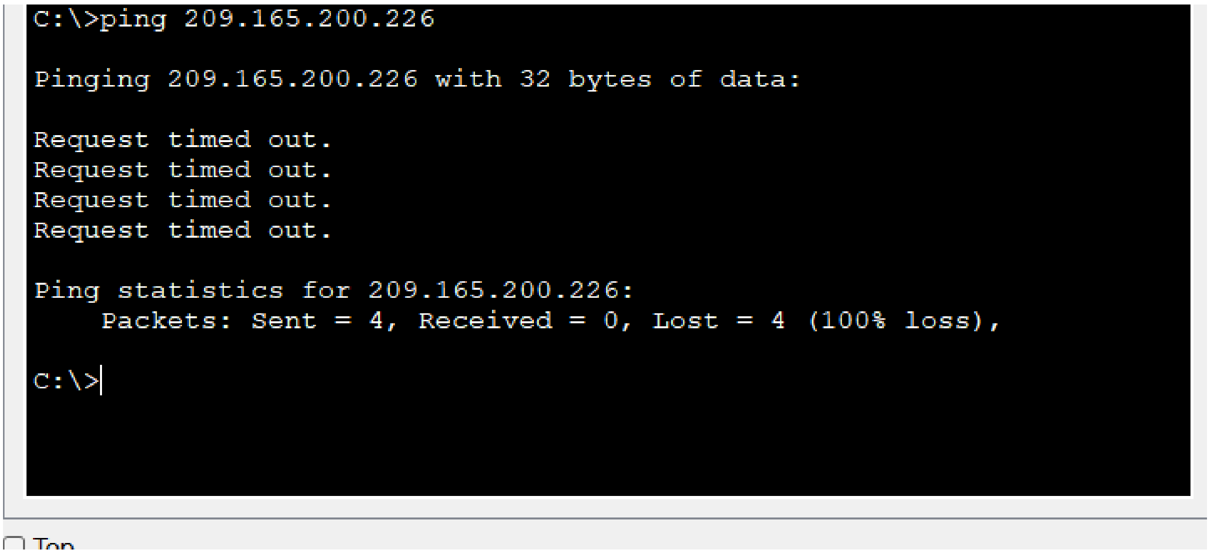
Step 5: Test Connectivity to the ASA

I initiated a ping from PC-B to the ASA inside interface using the command **ping 192.168.1.1**, confirming internal network accessibility.



```
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=13ms 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 = 13ms, Average = 3ms

C:\>
```

Additionally, I performed a ping from PC-B to the ASA outside interface using ping 209.165.200.226, verifying external network connectivity through the firewall.



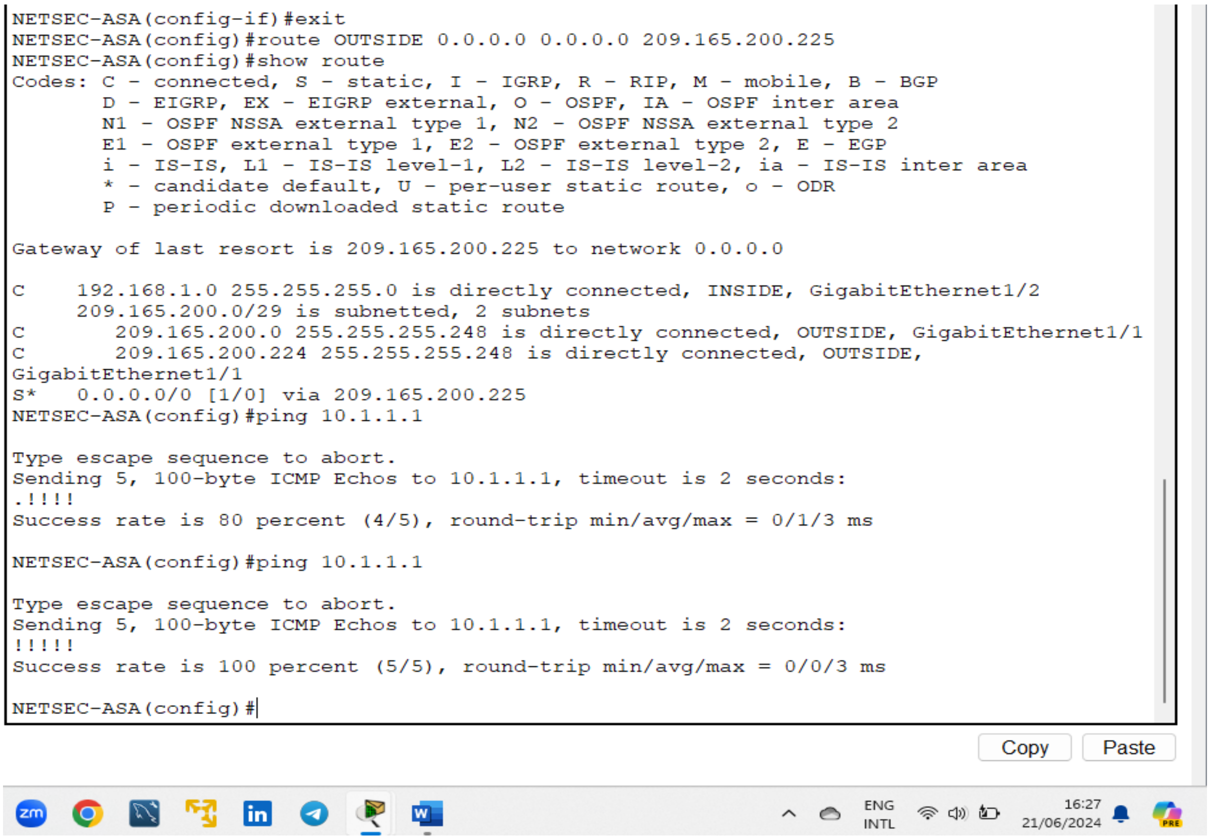
```
C:\>ping 209.165.200.226

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:\>
```

These tests ensured both internal and external reachability to the ASA, validating its role in network traffic management and security.

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

Step 1: Configure a Static Default Route for the ASA

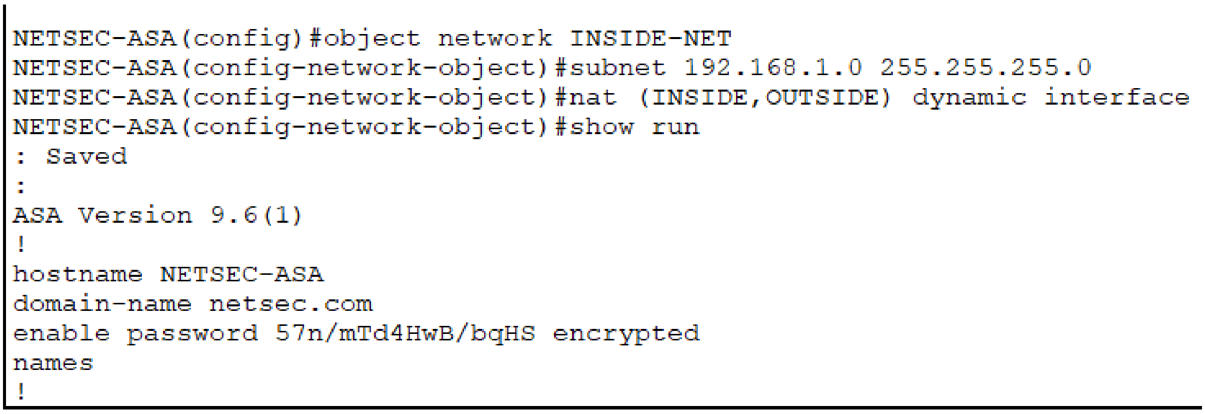
In configuring the ASA to reach external networks, I entered global configuration mode, created a static default route, verified the route, and tested connectivity with a ping to the R1 S0/0/0 interface.



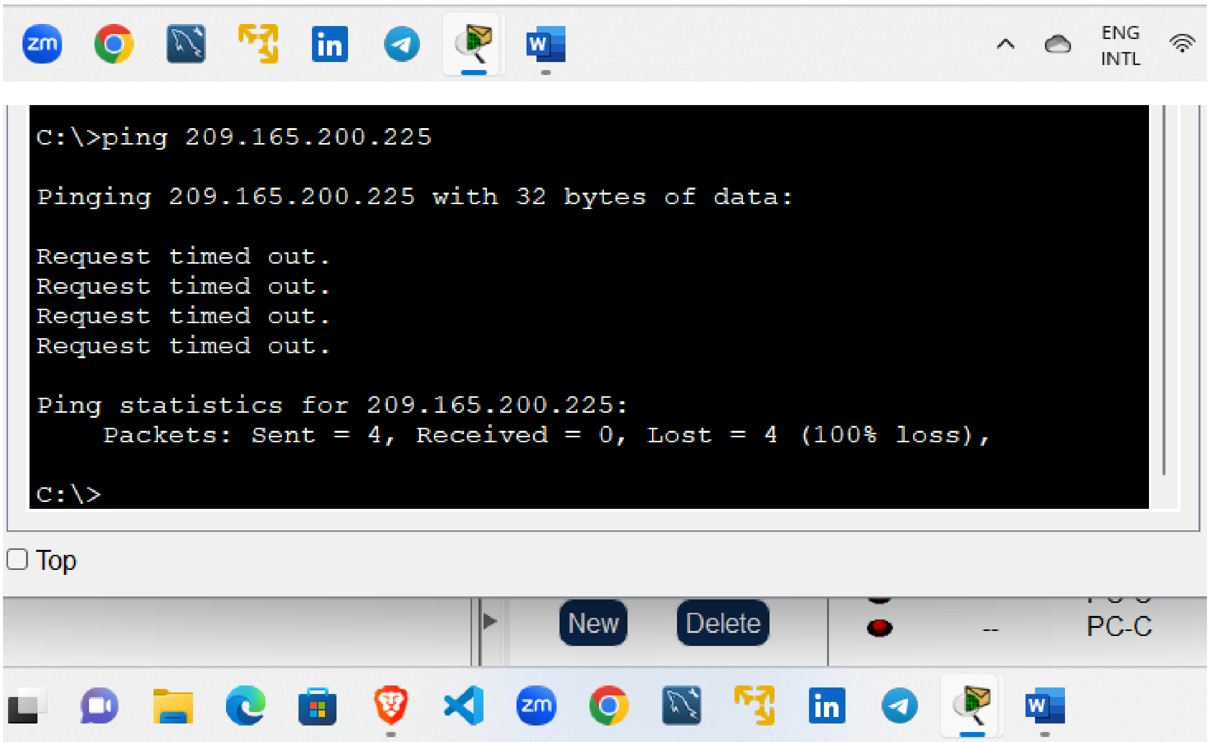
```
NETSEC-ASA(config-if)#exit
NETSEC-ASA(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
NETSEC-ASA(config)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 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)#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 = 0/1/3 ms

NETSEC-ASA(config)#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 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

NETSEC-ASA(config)#
```

Step 2: Configure Address Translation Using PAT and Network Objects

I configured NAT on the ASA to translate internal IP addresses to external addresses, verified the configuration with show run and show nat, and tested connectivity by pinging the R1 G0/0 interface from PC-B.



```
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)#show run
: Saved
:
ASA Version 9.6(1)
!
hostname NETSEC-ASA
domain-name netsec.com
enable password 57n/mTd4HwB/bqHS encrypted
names
!
```



```
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),

C:\>
```

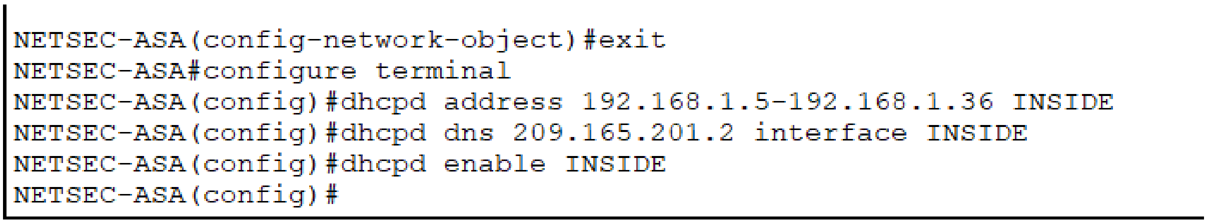
This sets up address translation for internal devices, allowing them to communicate with external networks.

Part 4: Configure DHCP, AAA, and SSH

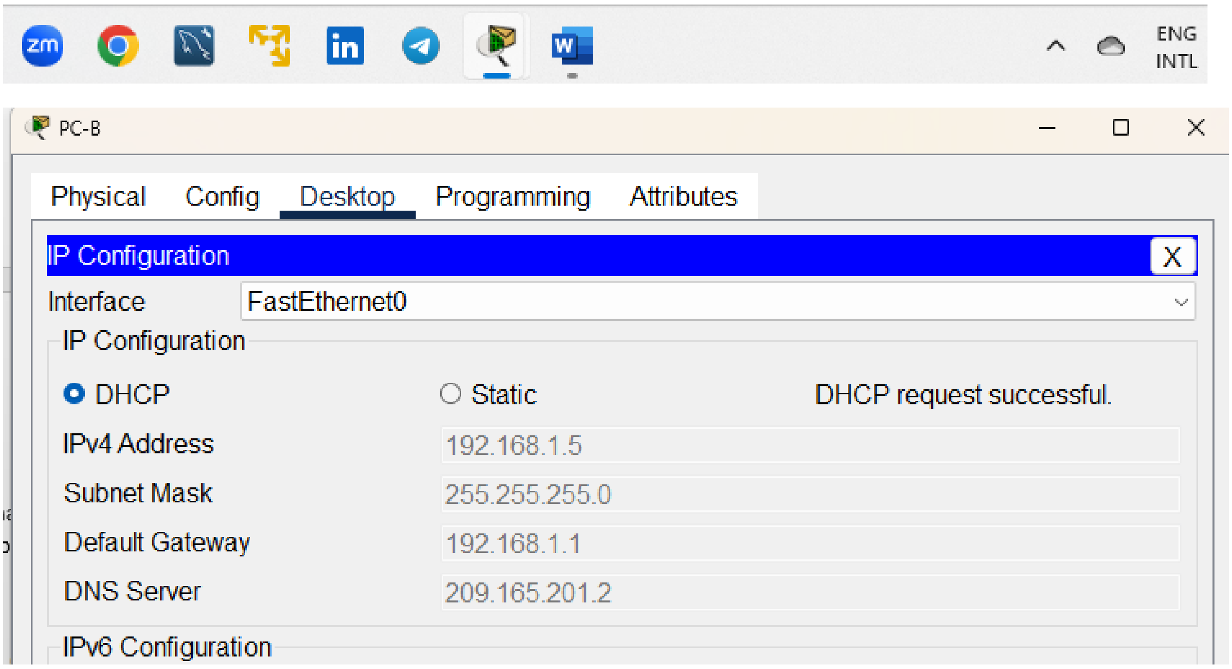
Step 1: Configure the ASA as a DHCP Server

I configured the ASA to provide IP addresses to internal hosts via DHCP by defining a DHCP address pool (dhcpd address 192.168.1.5-192.168.1.36 INSIDE), specifying the DNS server (dhcpd dns

209.165.201.2 interface INSIDE), enabling the DHCP daemon (dhcpd enable INSIDE), and verified IP assignment by changing PC-B to a DHCP client.



```
NETSEC-ASA(config-network-object)#exit
NETSEC-ASA#configure terminal
NETSEC-ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 INSIDE
NETSEC-ASA(config)#dhcpd dns 209.165.201.2 interface INSIDE
NETSEC-ASA(config)#dhcpd enable INSIDE
NETSEC-ASA(config)#
```



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.1.5

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

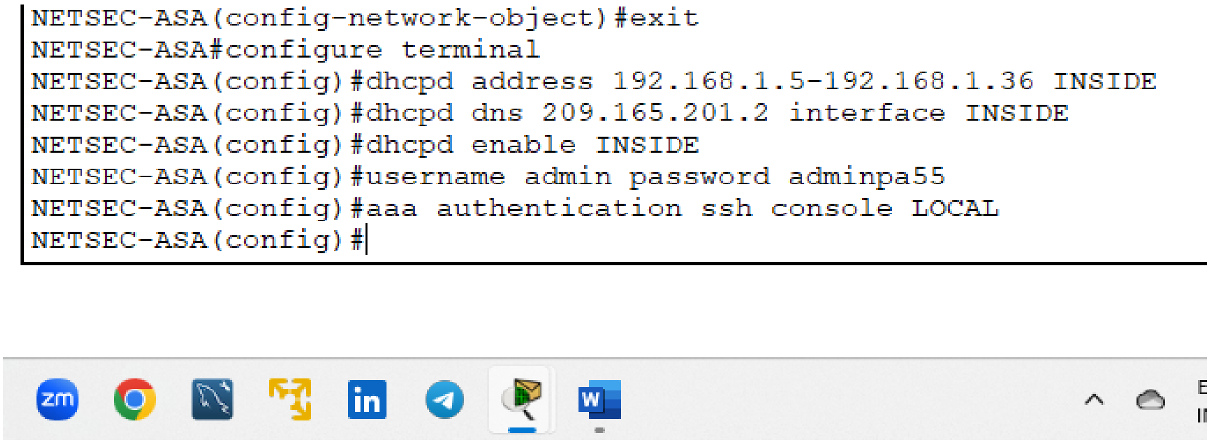
DNS Server: 209.165.201.2

IPv6 Configuration

This allows internal hosts to automatically receive IP configuration from the ASA.

Step 2: Configure AAA to Use the Local Database for Authentication

I secured remote access using local authentication on the ASA by creating a user account (username admin password adminpa55) and configuring AAA authentication for SSH (aaa authentication ssh console LOCAL).

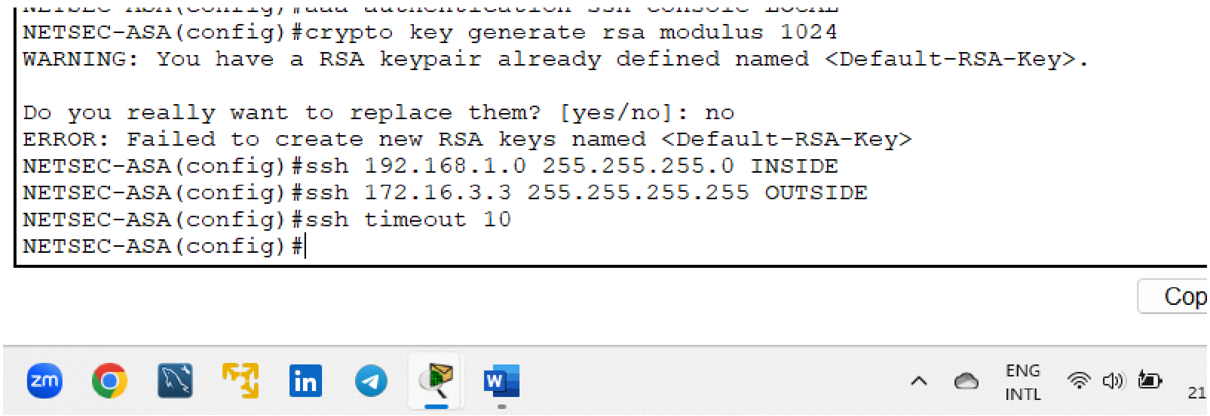


```
NETSEC-ASA(config-network-object)#exit
NETSEC-ASA#configure terminal
NETSEC-ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 INSIDE
NETSEC-ASA(config)#dhcpd dns 209.165.201.2 interface INSIDE
NETSEC-ASA(config)#dhcpd enable INSIDE
NETSEC-ASA(config)#username admin password adminpa55
NETSEC-ASA(config)#aaa authentication ssh console LOCAL
NETSEC-ASA(config)#
```

This ensures that remote access is authenticated using locally configured accounts.

Step 3: Configure Remote Access to the ASA

I enabled SSH access on the ASA by generating RSA keys, allowing SSH from specific subnets (192.168.1.0/24 on the INSIDE interface and 172.16.3.3 on the OUTSIDE interface), and setting the SSH timeout to 10 minutes.



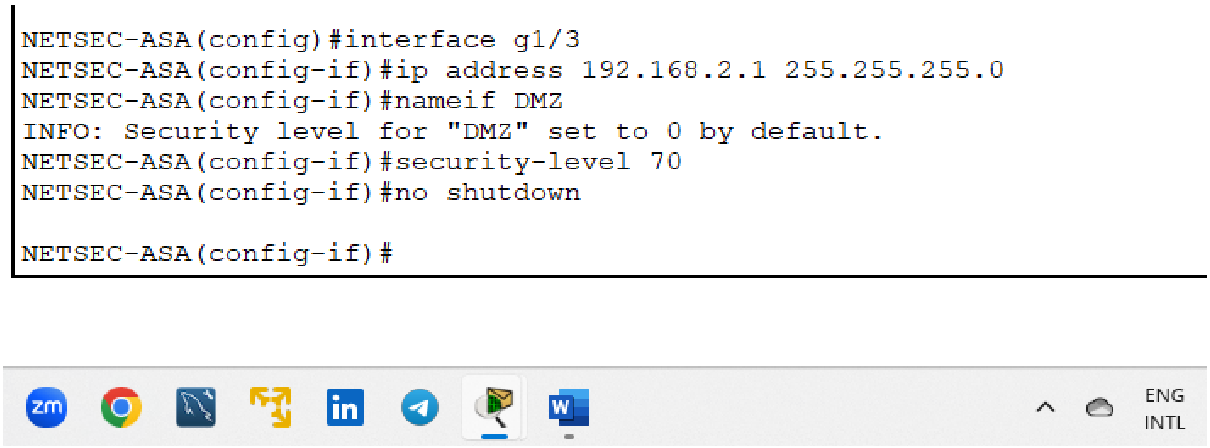
```
NETSEC-ASA(config)#aaa authentication ssh console LOCAL
NETSEC-ASA(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

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)#
```

This secures remote management of the ASA via SSH.

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

Step 1: Configure the DMZ Interface VLAN 3 on the ASA

I set up a DMZ interface on the ASA by configuring interface G1/3 with IP address 192.168.2.1/24, assigning it the nameif DMZ, setting security level to 70, and enabling the interface with no shutdown.



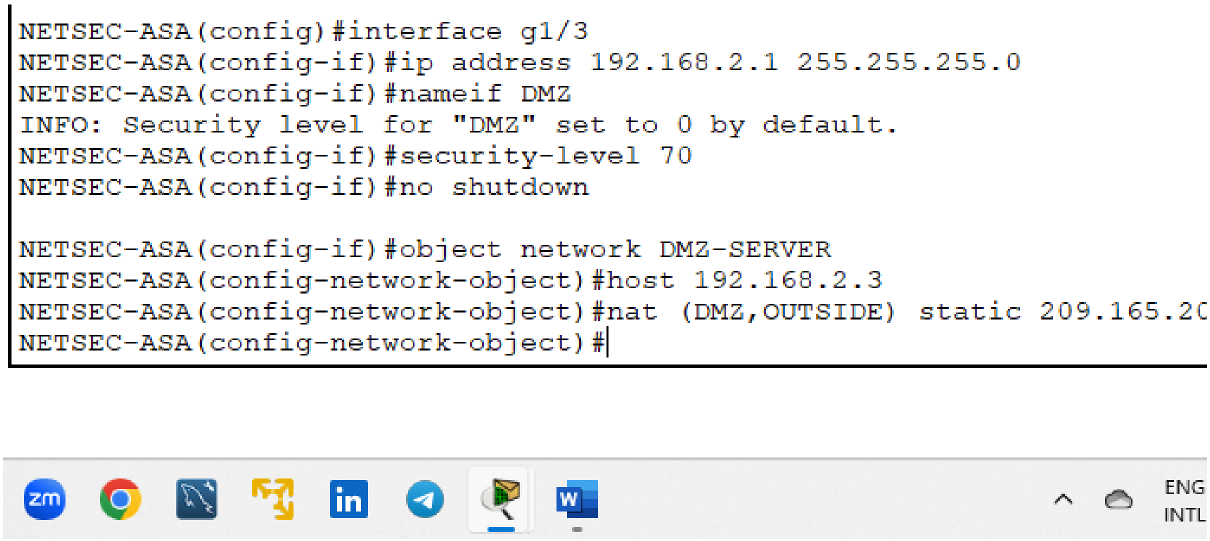
```
NETSEC-ASA(config)#interface g1/3
NETSEC-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
NETSEC-ASA(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
NETSEC-ASA(config-if)#security-level 70
NETSEC-ASA(config-if)#no shutdown

NETSEC-ASA(config-if)#
```

The DMZ provides a separate security zone for public-facing servers.

Step 2: Configure Static NAT to the DMZ Server Using a Network Object

I mapped the external IP address 209.165.200.227 to the DMZ server with internal IP address 192.168.2.3 using NAT configuration (object network DMZ-SERVER host 192.168.2.3 nat (DMZ,OUTSIDE) static 209.165.200.227).

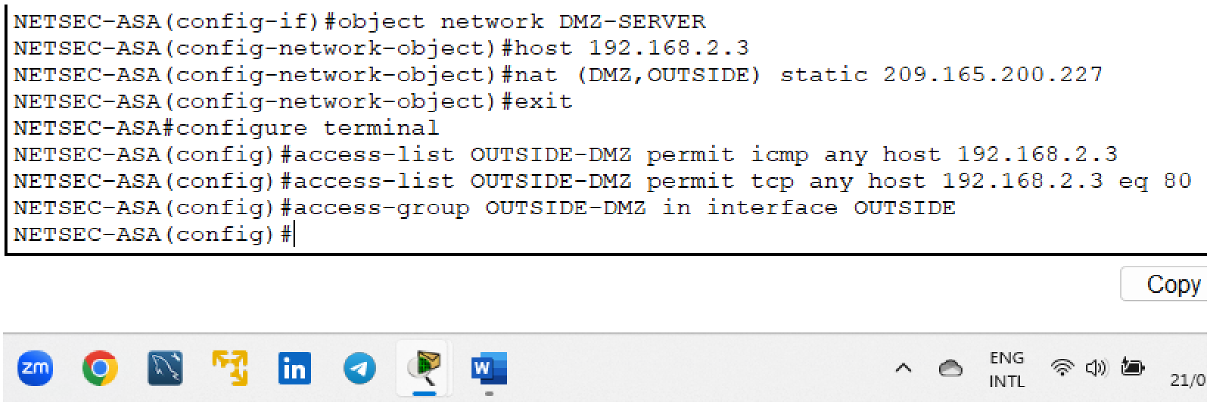
This allows external users to access the DMZ server using a public IP.



```
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

NETSEC-ASA(config-if)#object network DMZ-SERVER
NETSEC-ASA(config-network-object)#host 192.168.2.3
NETSEC-ASA(config-network-object)#nat (DMZ,OUTSIDE) static 209.165.20
NETSEC-ASA(config-network-object)#
```

Step 3: Configure an ACL to Allow Access to the DMZ Server from the Internet

I permitted specific traffic to the DMZ server by creating an access list (access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3 and access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80) and applying it inbound on the OUTSIDE interface with access-group OUTSIDE-DMZ in interface OUTSIDE.



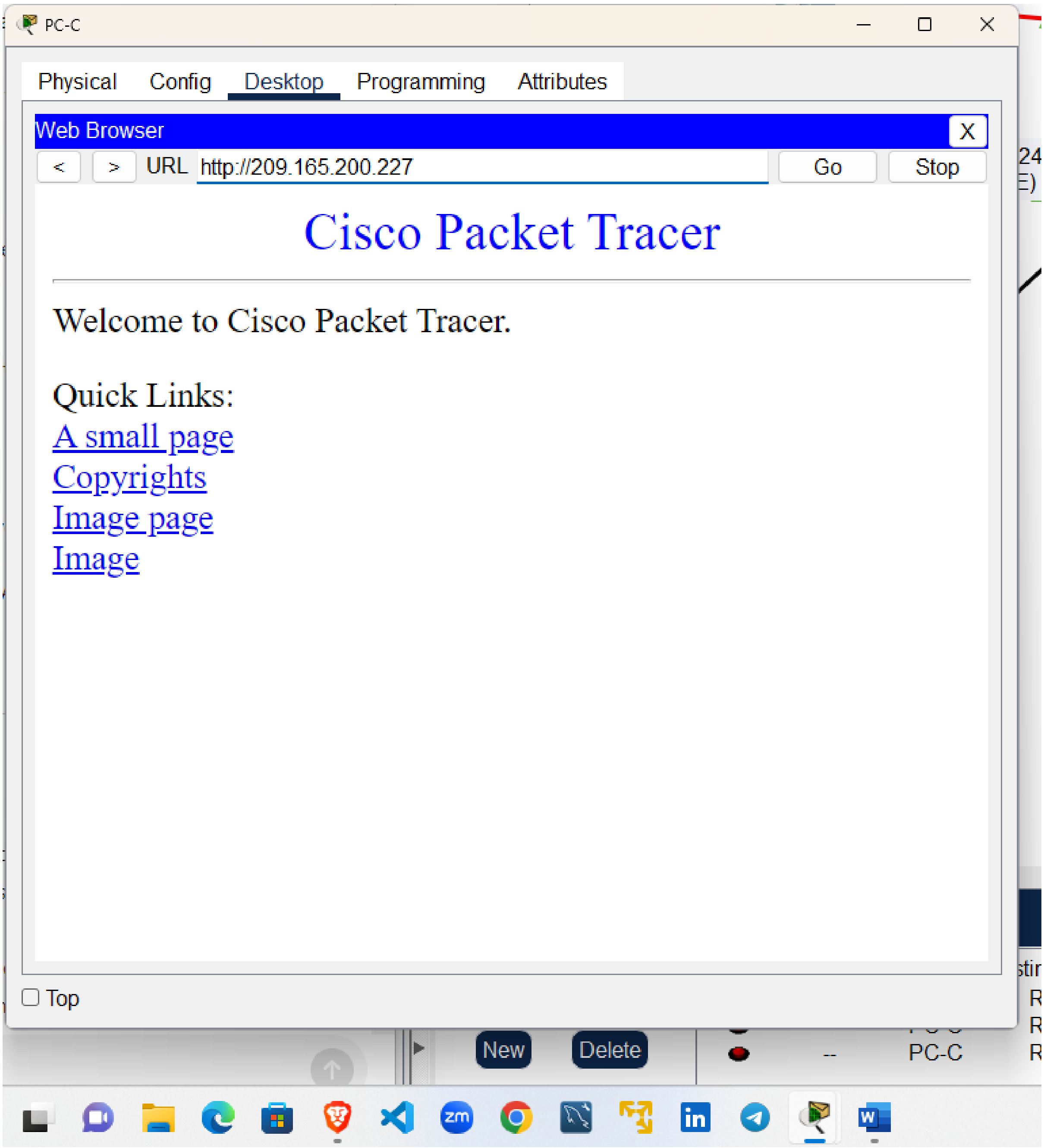
```
NETSEC-ASA(config-if)#object network DMZ-SERVER
NETSEC-ASA(config-network-object)#host 192.168.2.3
NETSEC-ASA(config-network-object)#nat (DMZ,OUTSIDE) static 209.165.200.227
NETSEC-ASA(config-network-object)#exit
NETSEC-ASA#configure terminal
NETSEC-ASA(config)#access-list OUTSIDE-DMZ permit icmp 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)#
```

This restricts access to the DMZ server to specific protocols, enhancing security.

Step 4: Test Access to the DMZ Server

I verified accessibility of the DMZ server by accessing it from PC-C using the URL http://209.165.200.227 in a web browser.

The web page hosted on the DMZ server is displayed. This confirms that the static NAT and ACL configurations are correct.



http://209.165.200.227

Cisco Packet Tracer

Welcome to Cisco Packet Tracer.

Quick Links:
A small page
Copyrights
Image page
Image

Conclusion

This report provides a comprehensive guide to configuring basic settings and firewall rules on a Cisco ASA using the CLI. The steps include interface settings, routing, address translation, inspection policies, DHCP, AAA, SSH, DMZ setup, static NAT, and ACLs. Proper execution of these steps ensures that the ASA is correctly configured to provide network security and management capabilities.