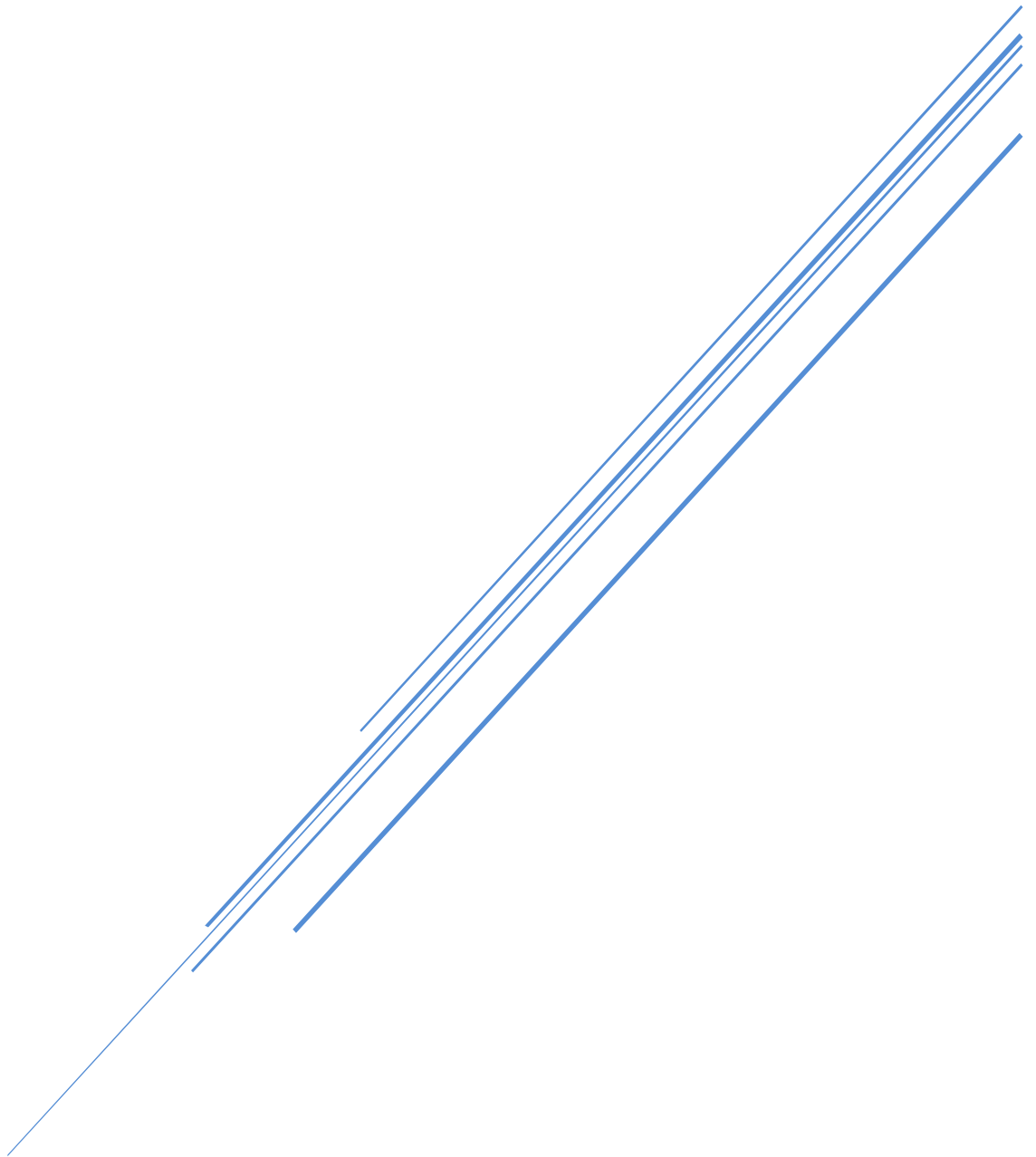


CONFIGURE ASA FIREWALL REPORT

Packet tracer Lab



By
YUNIS MOHAMED

Contents

Introduction.....	2
Part 1: Verify Connectivity and Explore the ASA	2
Step 1: Verify connectivity.....	2
Step 2: Determine the ASA version, interfaces, and license.....	2
Step 3: Determine the file system and contents of flash memory.....	3
Part 2: Configure ASA Settings and Interface Security Using the CLI	4
Step 1: Configure the hostname and domain name.....	4
Step 2: Configure the enable mode password.....	4
Step 3: Set the date and time.	5
Step 4: Configure the INSIDE and OUTSIDE interfaces	5
Step 5: Test connectivity to the ASA.....	7
Part 3: Configure Routing, Address Translation, and Inspection Policy Using the CLI	8
Step 1: Configure a static default route for the ASA.	8
Step 2: Configure address translation using PAT and network objects	9
Part 4: Configure DHCP, AAA, and SSH	10
Step 1: Configure the ASA as a DHCP server.	10
Step 2: Configure AAA to use the local database for authentication.....	11
Step 3: Configure remote access to the ASA.	12
Part 5: Configure a DMZ, Static NAT, and ACLs	13
Step 1: Configure the DMZ interface VLAN 3 on the ASA.	13
Step 2: Configure static NAT to the DMZ server using a network object.....	14
Step 3: Configure an ACL to allow access to the DMZ server from the Internet.....	15
Step 4: Test access to the DMZ server.....	15
Conclusion	16

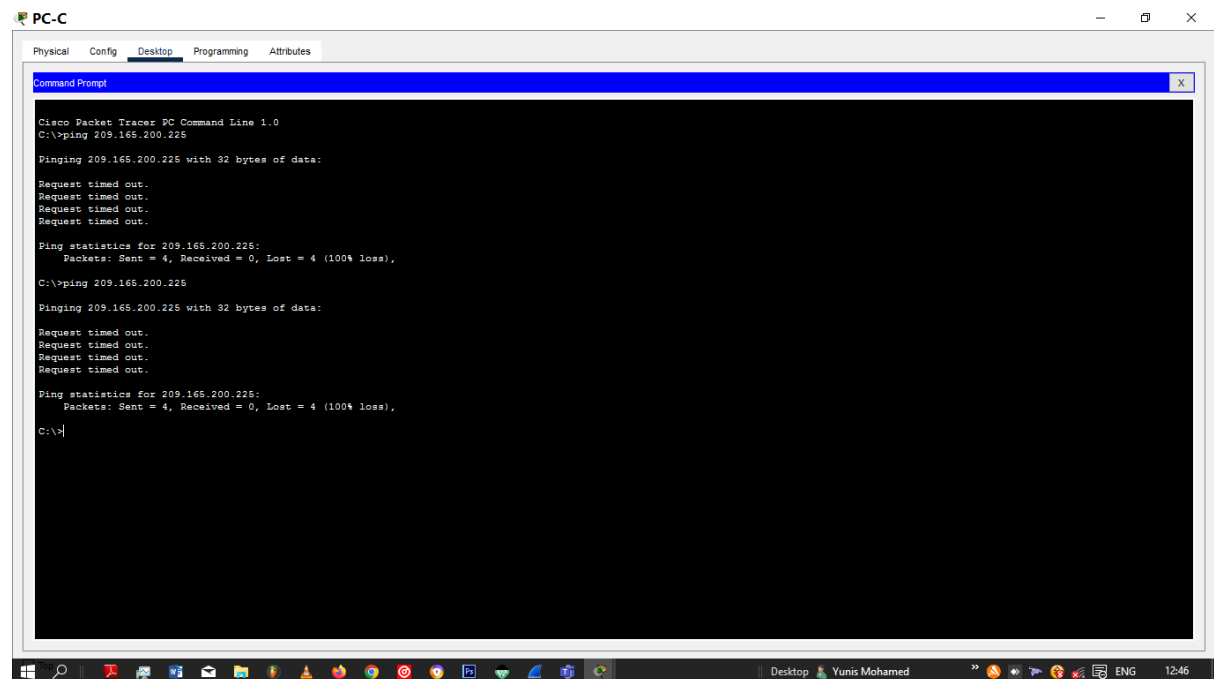
Introduction

The "Configure ASA Basic Settings and Firewall Using the CLI" lab in Packet Tracer offers a hands-on learning experience for configuring and securing a network using a Cisco ASA (Adaptive Security Appliance) firewall. In this lab, I was able to configure and practice the fundamentals of ASA configuration, including setting up basic parameters such as hostname, domain name, and management interface IP address. I also explore the essential firewall functionalities like the Static Network Address Translation (NAT), Access Control Lists (ACLs), and the establishment of firewall policies.

Part 1: Verify Connectivity and Explore the ASA

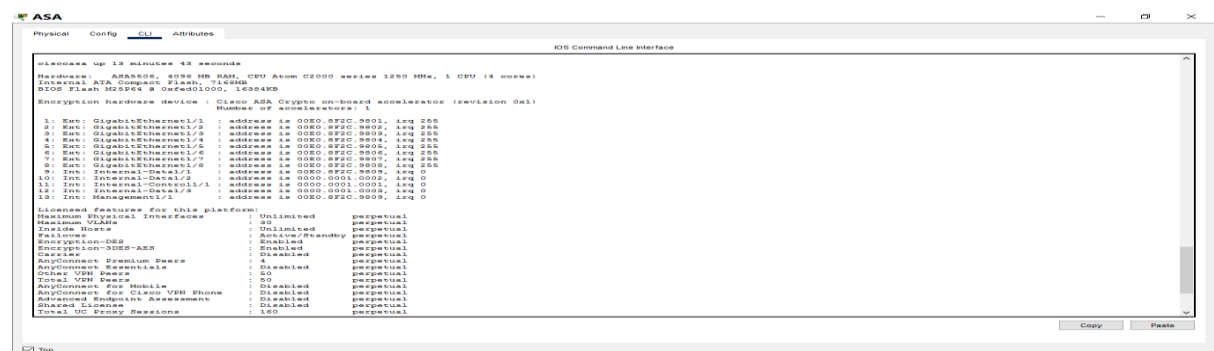
Step 1: Verify connectivity.

The ASA is not currently configured. However, all routers, PCs, and the DMZ server are configured. Verify that PC-C can ping any router interface. PC-C is unable to ping the ASA, PC-B, or the DMZ server.



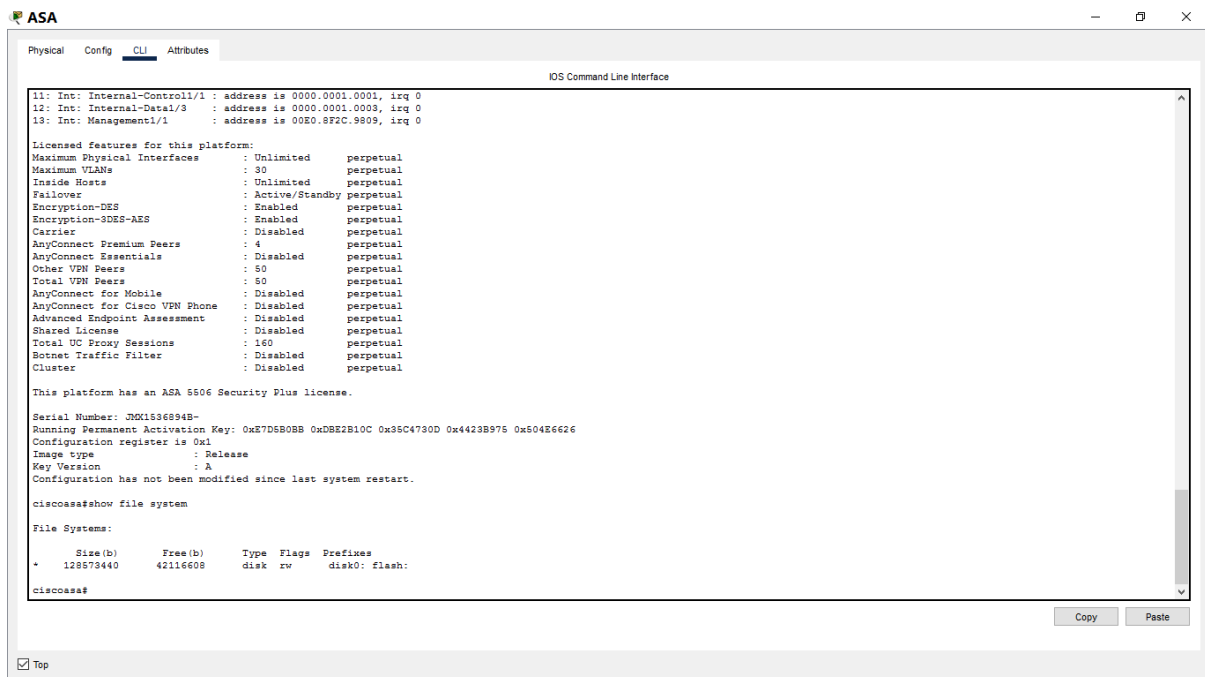
Step 2: Determine the ASA version, interfaces, and license.

Use the **show version** command to determine various aspects of this ASA device



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

Use the **show file system** command to display the ASA file system and determine which prefixes are supported.



The screenshot shows the ASA CLI interface with the 'show file system' command executed. The output displays the file system details for the flash memory.

```
11: Int: Internal-Controll/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3   : address is 0000.0001.0003, irq 0
13: Int: Management1/1     : address is 00E0.8F2C.9809, irq 0

Licensed features for this platform:
Maximum Physical Interfaces   : Unlimited   perpetual
Maximum VLANs                : 30         perpetual
Inside Hosts                 : Unlimited   perpetual
Failover                     : Active/Standby perpetual
Encryption-DES               : Enabled     perpetual
Encryption-3DES-AES          : Enabled     perpetual
Carrier                      : Disabled     perpetual
AnyConnect Premium Peers     : 4         perpetual
AnyConnect Essentials        : Disabled     perpetual
Other VPN Peers              : 50         perpetual
Total VPN Peers              : 50         perpetual
AnyConnect for Mobile        : Disabled     perpetual
AnyConnect for Cisco VPN Phone : Disabled     perpetual
Advanced Endpoint Assessment : Disabled     perpetual
Shared License               : Disabled     perpetual
Total UC Proxy Sessions      : 160        perpetual
Botnet Traffic Filter         : Disabled     perpetual
Cluster                      : Disabled     perpetual

This platform has an ASA 5506 Security Plus license.
Serial Number: JMK1536894B-
Running Permanent Activation Key: 0x7D580BB 0xDBE2B10C 0x35C4730D 0x4423B975 0x504E662E
Configuration register is 0x1
Image type                   : Release
Key Version                   : A
Configuration has not been modified since last system restart.

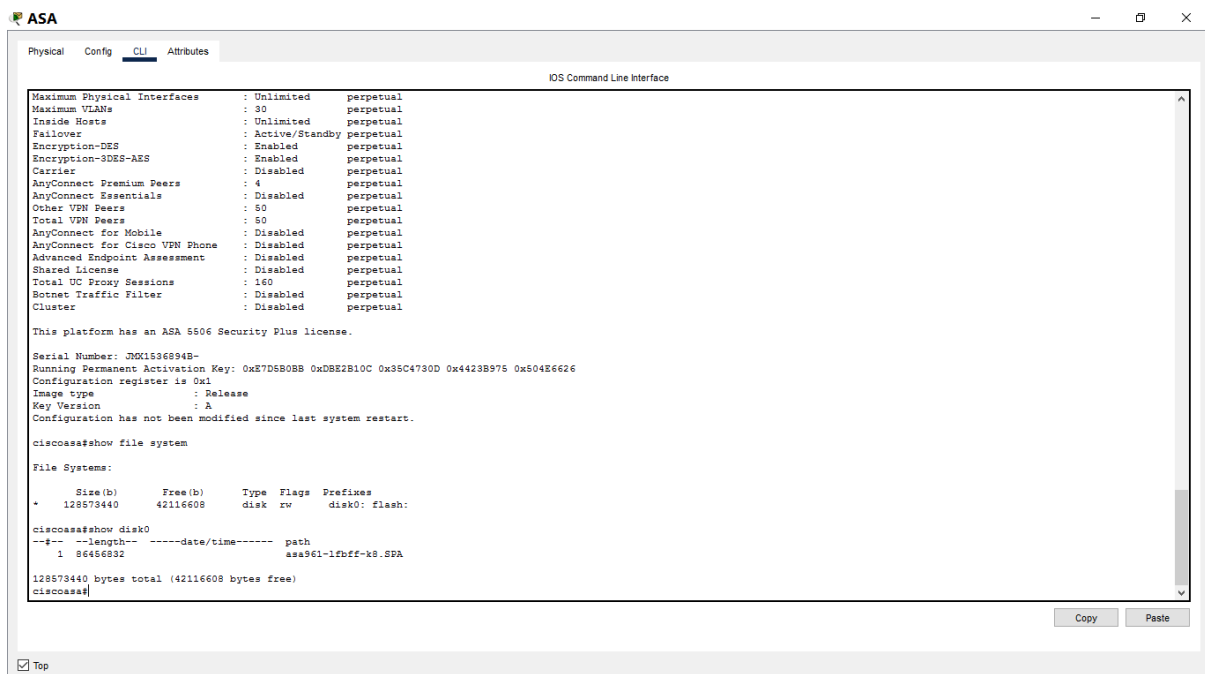
ciscoasa#show file system

File Systems:

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

ciscoasa#
```

c. Use the **show flash:** or **show disk0:** command to display the contents of flash memory.



The screenshot shows the ASA CLI interface with the 'show disk0' command executed. The output displays the contents of the flash memory.

```
Maximum Physical Interfaces   : Unlimited   perpetual
Maximum VLANs                : 30         perpetual
Inside Hosts                 : Unlimited   perpetual
Failover                     : Active/Standby perpetual
Encryption-DES               : Enabled     perpetual
Encryption-3DES-AES          : Enabled     perpetual
Carrier                      : Disabled     perpetual
AnyConnect Premium Peers     : 4         perpetual
AnyConnect Essentials        : Disabled     perpetual
Other VPN Peers              : 50         perpetual
Total VPN Peers              : 50         perpetual
AnyConnect for Mobile        : Disabled     perpetual
AnyConnect for Cisco VPN Phone : Disabled     perpetual
Advanced Endpoint Assessment : Disabled     perpetual
Shared License               : Disabled     perpetual
Total UC Proxy Sessions      : 160        perpetual
Botnet Traffic Filter         : Disabled     perpetual
Cluster                      : Disabled     perpetual

This platform has an ASA 5506 Security Plus license.
Serial Number: JMK1536894B-
Running Permanent Activation Key: 0x7D580BB 0xDBE2B10C 0x35C4730D 0x4423B975 0x504E662E
Configuration register is 0x1
Image type                   : Release
Key Version                   : A
Configuration has not been modified since last system restart.

ciscoasa#show file system

File Systems:

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

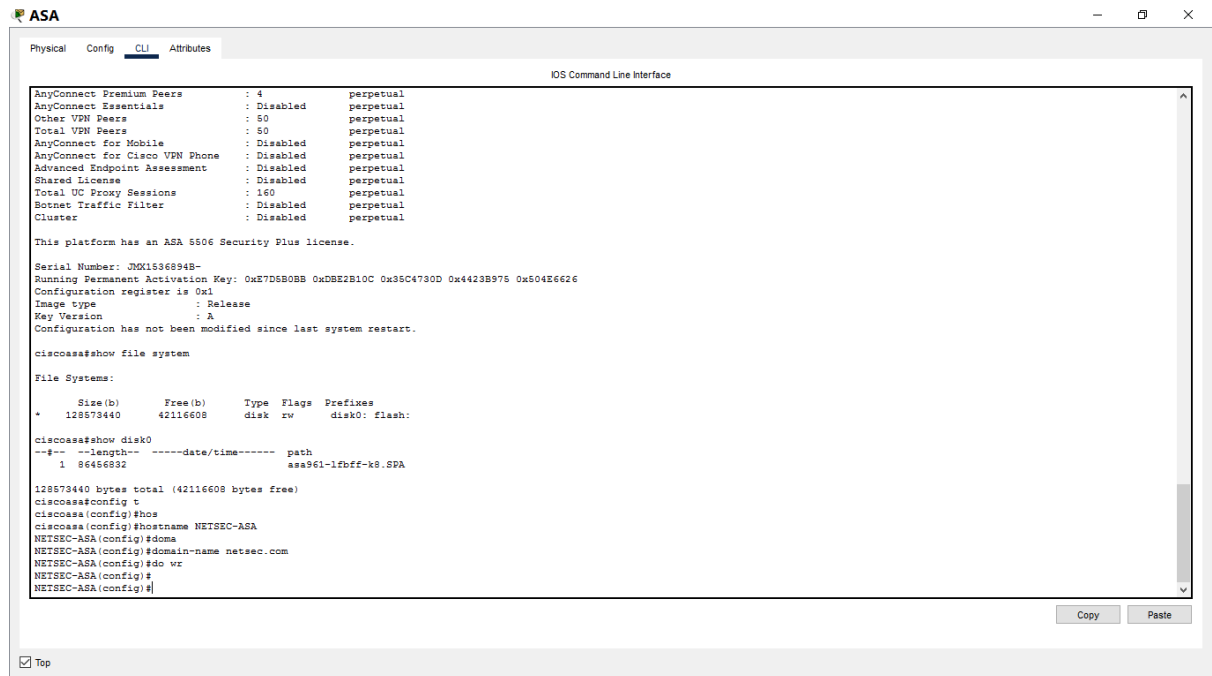
ciscoasa#show disk0
--#--  --length--  -----date/time-----  path
1  86456832                asa961-1fbff-k8.SPA

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

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

Step 1: Configure the hostname and domain name.

- Configure the ASA hostname as **NETSEC-ASA**. Hostname **NETSEC-ASA**
- Configure the domain name as **netsec.com**. Domain-name **netsec.com**



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

```
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 50 perpetual
Total VPN Peers : 50 perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
Shared License : Disabled perpetual
Total UC Proxy Sessions : 160 perpetual
Botnet Traffic Filter : Disabled perpetual
Cluster : Disabled perpetual

This platform has an ASA 5506 Security Plus license.

Serial Number: JMK1536894B-
Running Permanent Activation Key: 0x7D6B0BB 0xDBE2B10C 0x35C4780D 0x4423B975 0x50456626
Configuration register is 0x1
Image type : Release
Key Version : A
Configuration has not been modified since last system restart.

ciscoasa#show file system

File Systems:

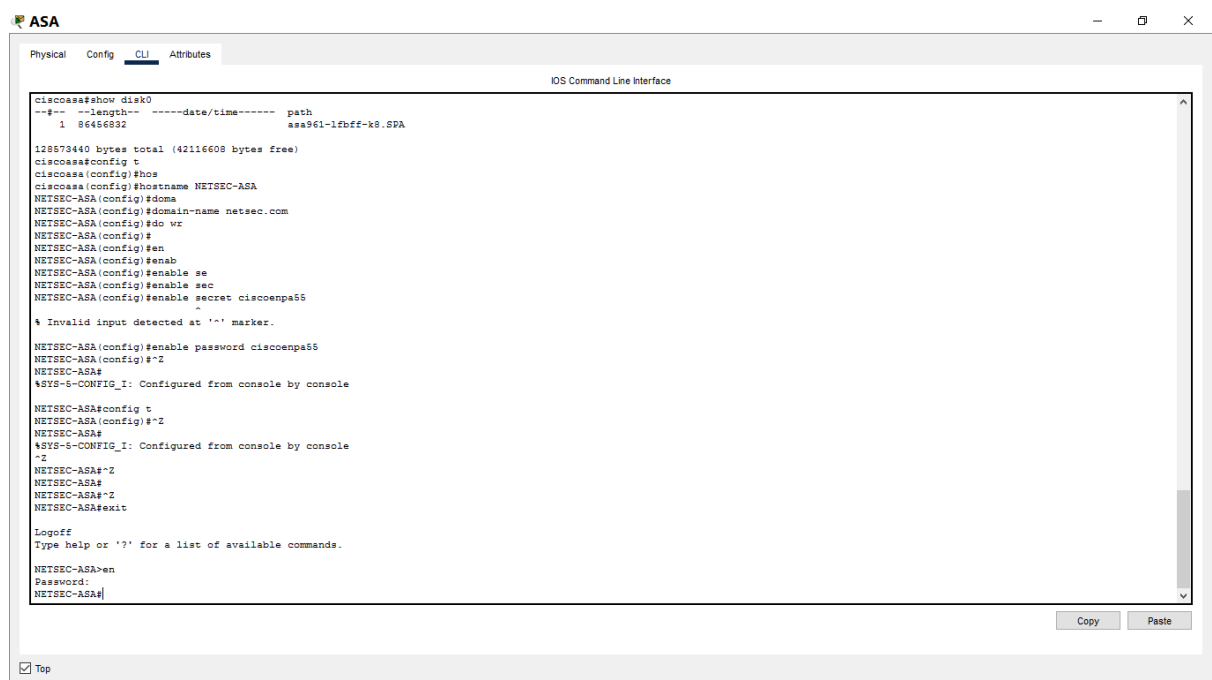
   Size(b)   Free(b)   Type  Flags  Prefixes
*   128573440   42116608   disk  rw     disk0: flash:

ciscoasa#show disk0
--#--  --length--  -----date/time-----  path
   1   86456892                asa961-1fbff-k8.SPA

128573440 bytes total (42116608 bytes free)
ciscoasa#config t
ciscoasa(config)#hos
ciscoasa(config)#hostname NETSEC-ASA
NETSEC-ASA(config)#doma
NETSEC-ASA(config)#domain-name netsec.com
NETSEC-ASA(config)#do wr
NETSEC-ASA(config)#
NETSEC-ASA(config)#
```

Step 2: Configure the enable mode password.

Use the **enable password** command to change the privileged EXEC mode password to **ciscoenpa55**.



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

```
ciscoasa#show disk0
--#--  --length--  -----date/time-----  path
   1   86456892                asa961-1fbff-k8.SPA

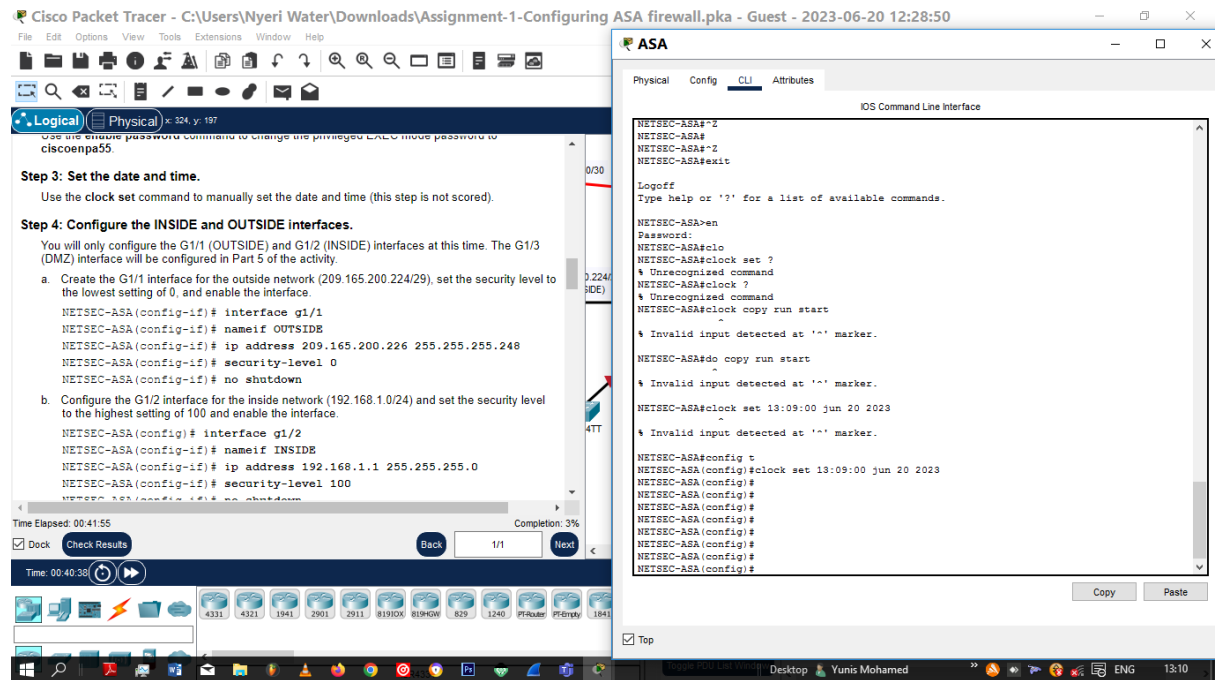
128573440 bytes total (42116608 bytes free)
ciscoasa#config t
ciscoasa(config)#hos
ciscoasa(config)#hostname NETSEC-ASA
NETSEC-ASA(config)#doma
NETSEC-ASA(config)#domain-name netsec.com
NETSEC-ASA(config)#do wr
NETSEC-ASA(config)#
NETSEC-ASA(config)#en
NETSEC-ASA(config)#enab
NETSEC-ASA(config)#enable se
NETSEC-ASA(config)#enable sec
NETSEC-ASA(config)#enable secret ciscoenpa55
% Invalid input detected at '^' marker.
NETSEC-ASA(config)#enable password ciscoenpa55
NETSEC-ASA(config)#^Z
NETSEC-ASA#
%SYS-S-CONFIG_I: Configured from console by console
^Z
NETSEC-ASA#config t
NETSEC-ASA(config)#^Z
NETSEC-ASA#
%SYS-S-CONFIG_I: Configured from console by console
^Z
NETSEC-ASA#^Z
NETSEC-ASA#^Z
NETSEC-ASA#^Z
NETSEC-ASA#exit

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

NETSEC-ASA#en
Password:
NETSEC-ASA#
```

Step 3: Set the date and time.

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



Step 4: Configure the INSIDE and OUTSIDE interfaces

- Create the G1/1 interface for the outside network (209.165.200.224/29), set the security level to the lowest setting of 0, and enable the interface.

```
NETSEC-ASA(config-if)# interface g1/1
```

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

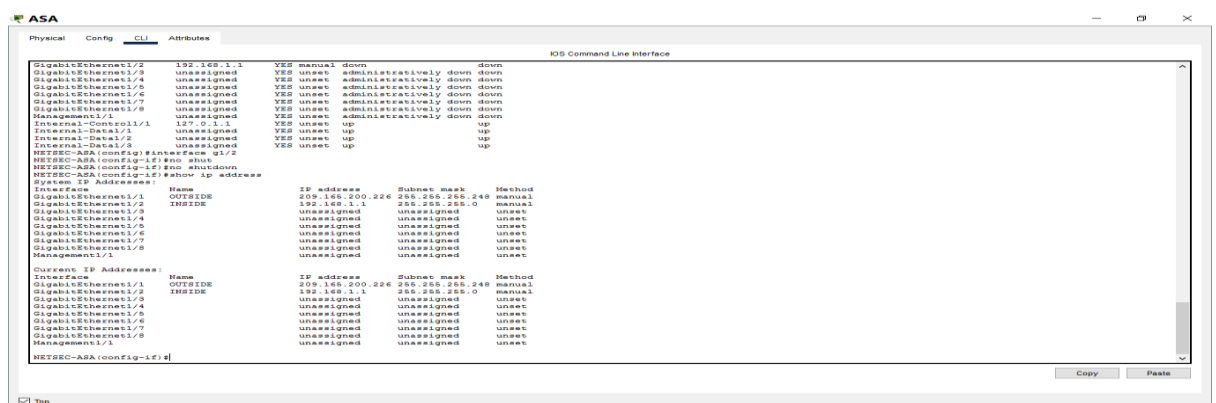
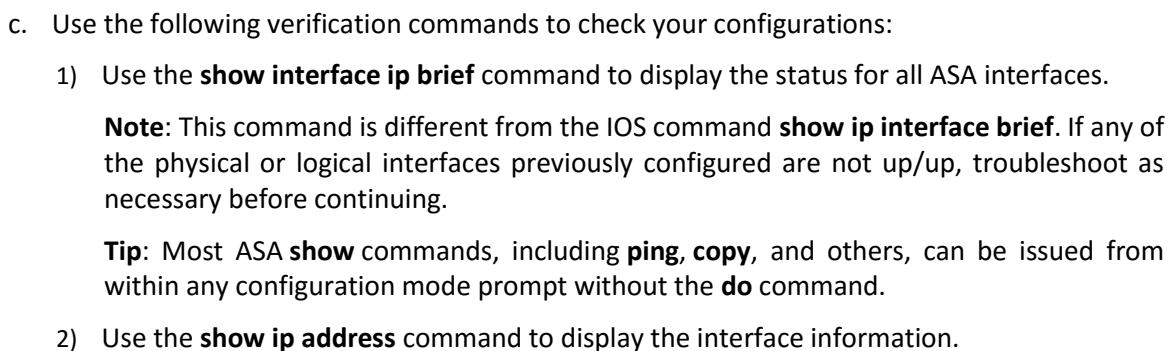
```
NETSEC-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
```

```
NETSEC-ASA(config-if)# security-level 0
```

```
NETSEC-ASA(config-if)# no shutdown
```

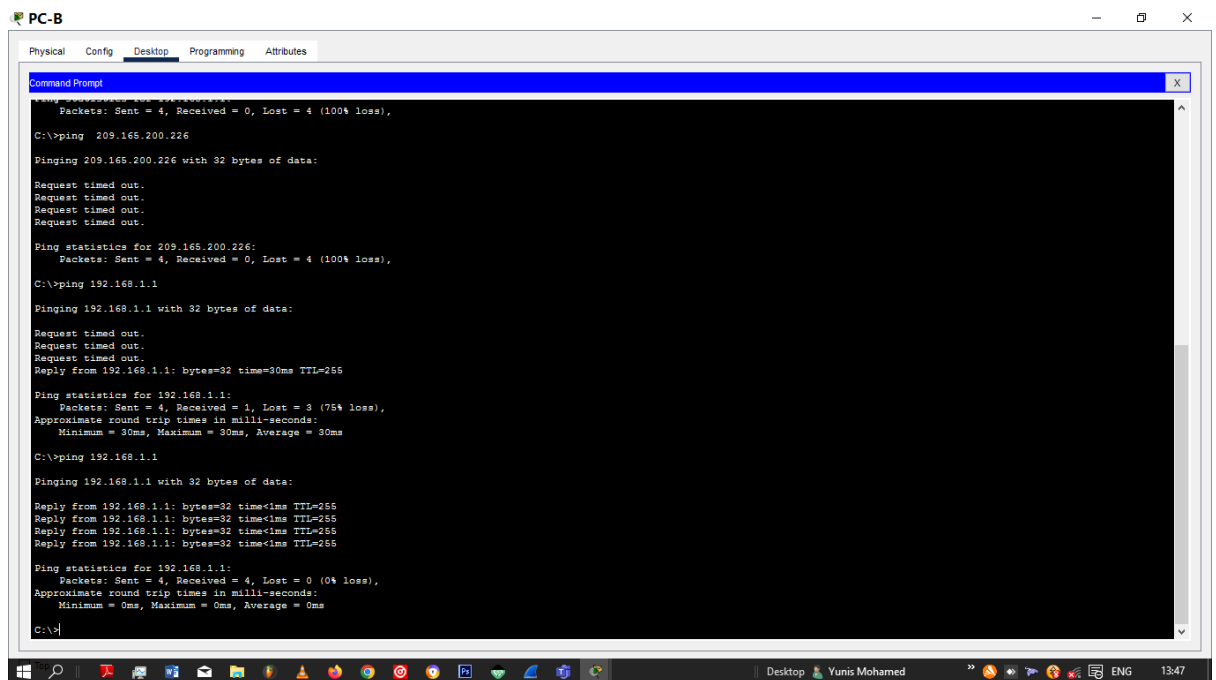


- ```
NETSEC-ASA(config)# interface g1/2
NETSEC-ASA(config-if)# nameif INSIDE
NETSEC-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
NETSEC-ASA(config-if)# security-level 100
NETSEC-ASA(config-if)# no shutdown
```



## Step 5: Test connectivity to the ASA.

- a. You should be able to ping from PC-B to the ASA inside interface address (192.168.1.1). If the pings fail, troubleshoot the configuration as necessary. **The ping is successful**



The screenshot shows a Windows desktop environment with a taskbar at the bottom. The 'PC-B' window is open, displaying a 'Command Prompt' window. The command prompt shows the following output:

```
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:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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=30ms TTL=255

Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 30ms, Maximum = 30ms, Average = 30ms

C:\>ping 192.168.1.1

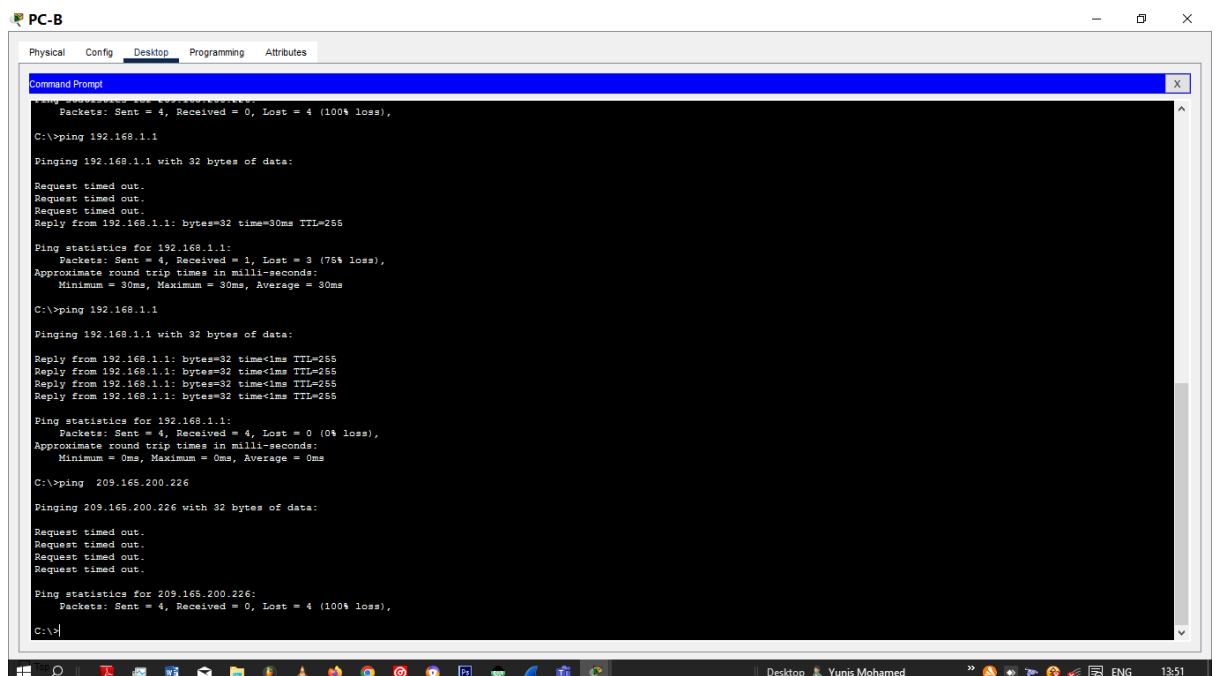
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<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
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 = 0ms, Average = 0ms

C:\>
```

- b. From PC-B, ping the G1/1 (OUTSIDE) interface at IP address 209.165.200.226. You should not be able to ping this address. **The ping is not successful.**



The screenshot shows a Windows desktop environment with a taskbar at the bottom. The 'PC-B' window is open, displaying a 'Command Prompt' window. The command prompt shows the following output:

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 30ms, Maximum = 30ms, Average = 30ms

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<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
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 = 0ms, Average = 0ms

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

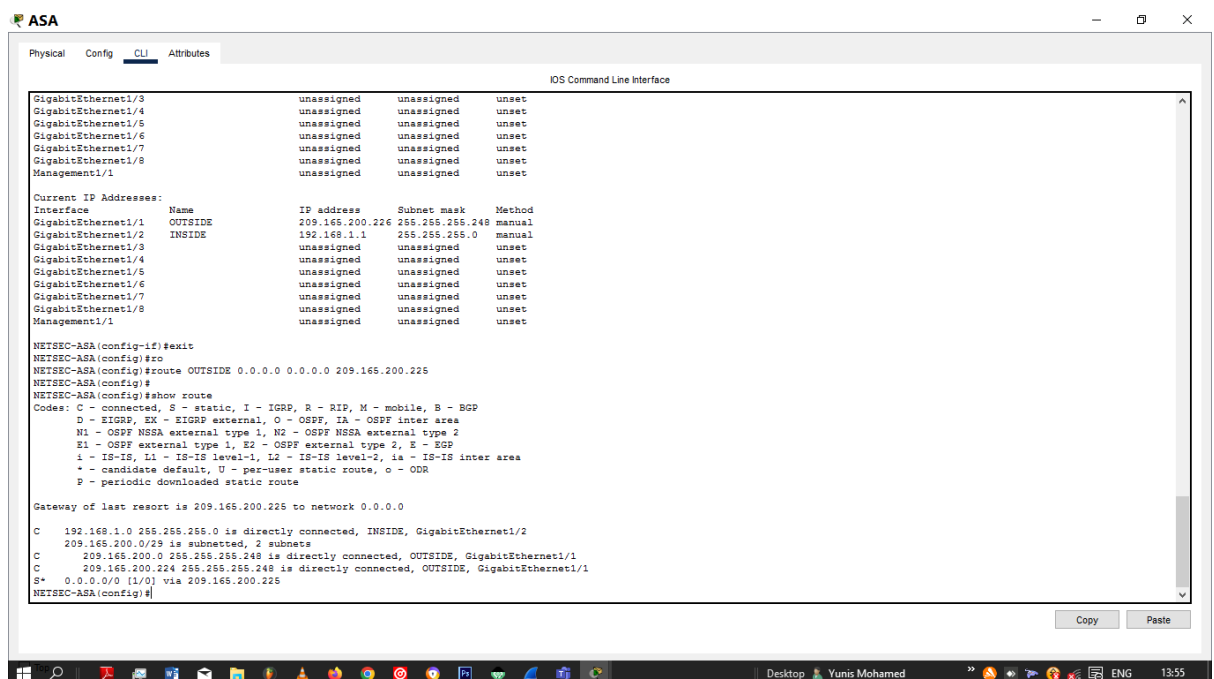
### Step 1: Configure a static default route for the ASA.

Configure a default static route on the ASA OUTSIDE interface to enable the ASA to reach external networks.

- 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.

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

- Issue the **show route** command to verify the static default route is in the ASA routing table. **The default static route is configured successfully.**



```
ASA
Physical Config CLI Attributes
IOS Command Line Interface

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

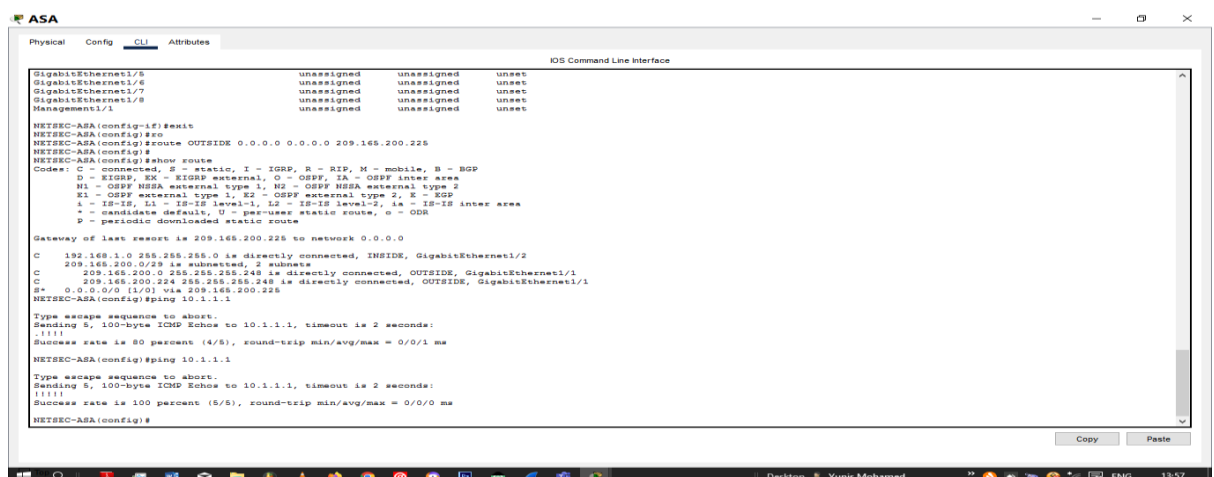
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet1/1 OUTSIDE 209.165.200.226 255.255.255.248 manual
GigabitEthernet1/2 INSIDE 192.168.1.1 255.255.255.0 manual
GigabitEthernet1/3 unassigned unassigned unset
GigabitEthernet1/4 unassigned unassigned unset
GigabitEthernet1/5 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)#exit
NETSEC-ASA(config)#ro
NETSEC-ASA(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
NETSEC-ASA(config)#
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
C 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)#
```

- Verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1. If the ping is unsuccessful, troubleshoot as necessary. **The ping is successful.**



```
ASA
Physical Config CLI Attributes
IOS Command Line Interface

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)#exit
NETSEC-ASA(config)#ro
NETSEC-ASA(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
NETSEC-ASA(config)#
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
C 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 Echoes to 10.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
NETSEC-ASA(config)#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 10.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
NETSEC-ASA(config)#
```

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

- Create network object **INSIDE-NET** and assign attributes to it using the **subnet** and **nat** commands.

```
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
```

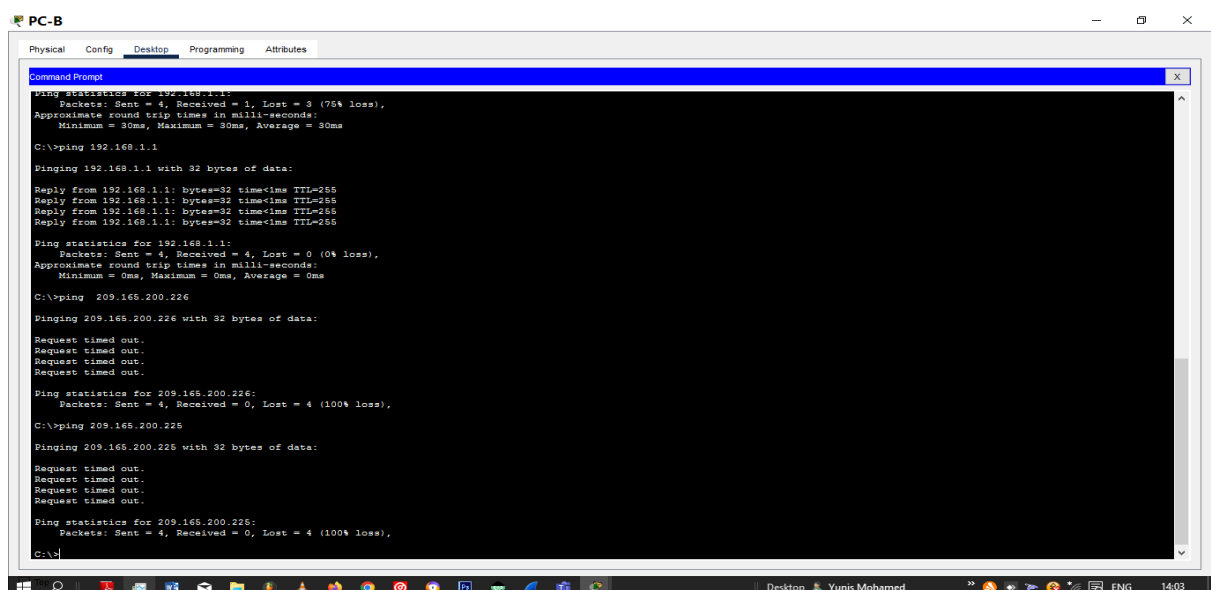
- The ASA splits the configuration into the object portion that defines the network to be translated and the actual **nat** command parameters. These appear in two different places in the running configuration. Display the NAT object configuration using the **show run** command.

A screenshot of the ASA CLI interface. The window title is "ASA". The tabs are "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, showing the "IOS Command Line Interface". The configuration text is as follows:

```
no ip address
shutdown
!
interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown
!
interface GigabitEthernet1/8
no nameif
no security-level
no ip address
shutdown
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
shutdown
!
object network INSIDE-NET
subnet 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
inspect dns preset_dns_map
```

At the bottom right, there are "Copy" and "Paste" buttons. At the bottom left, there is a "Top" button.

- From PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should fail. **The ping is not successful.**

A screenshot of the PC-B Command Prompt window. The window title is "PC-B". The tabs are "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, showing the "Command Prompt". The output of the ping commands is as follows:

```
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 30ms, Maximum = 30ms, Average = 30ms

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<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
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 = 0ms, Average = 0ms

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.

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

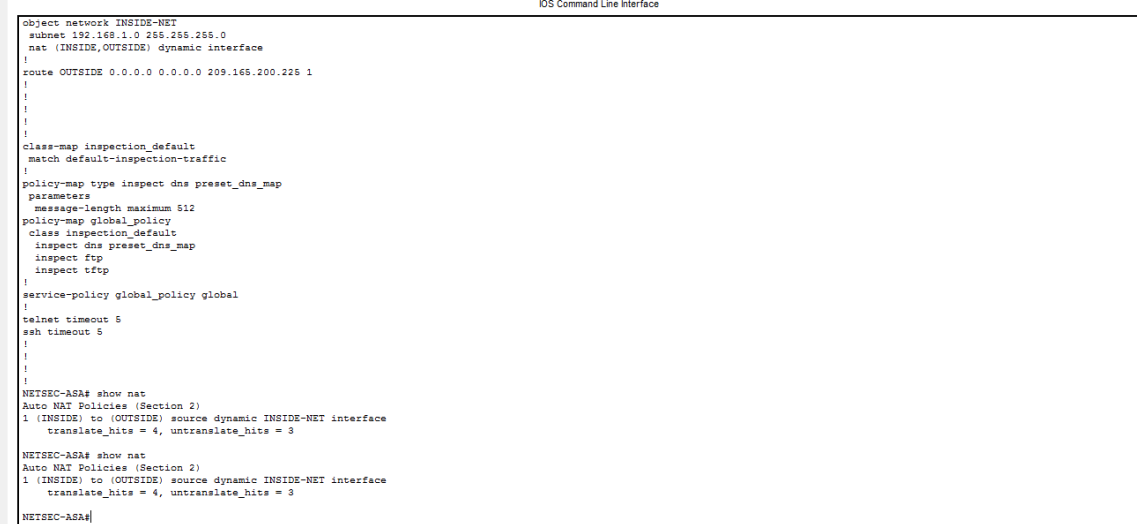
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

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

C:\>
```

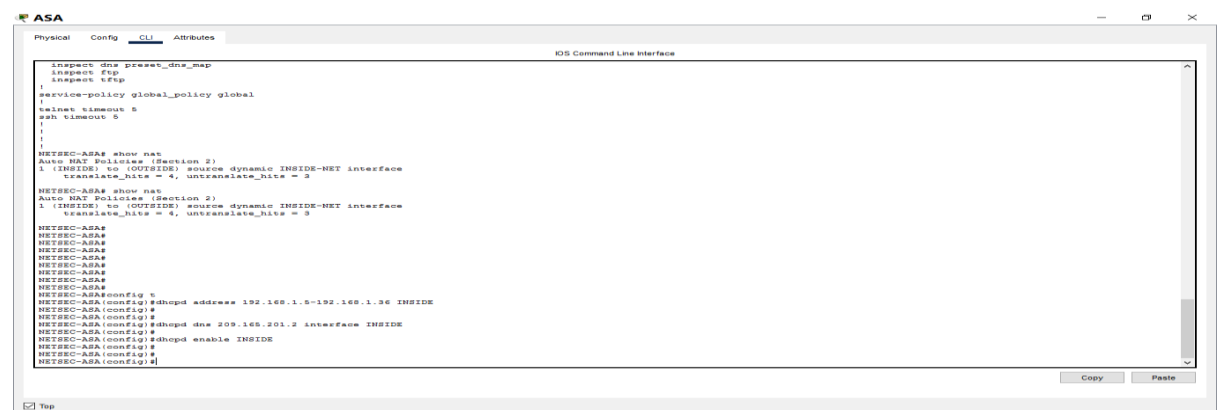
The taskbar at the bottom shows the Windows Start button, several application icons, and the system tray with the date and time "14:03".

- 
- The screenshot shows a Cisco IOS Command Line Interface (CLI) window with the following configuration and verification commands:
- ```

object network INSIDE-NET
  subnet 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
    inspect dns preset_dns_map
    inspect ftp
    inspect tftp
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
!
!
!
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# 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 of the window, there is a "Top" button with a checkmark icon.



-
- The screenshot shows the PC-B configuration window with the following details:
- Physical Tab:**
 - Interface: FastEthernet0
 - IP Configuration:**
 - DHCP (Selected):**
 - IPv4 Address: 192.168.1.5
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - DNS Server: 209.165.201.2
 - Static:** DHCP request successful.
 - IPv6 Configuration:**
 - Static (Selected):**
 - IPv6 Address: [Empty field] / [Empty field]
 - Link Local Address: FE80::201:97FF:FE15:BB76
 - Default Gateway: [Empty field]
 - DNS Server: [Empty field]
 - 802.1X:**
 - ☐ Use 802.1X Security
 - Authentication:**
 - Method: MDS
 - Username: [Empty field]
 - Password: [Empty field]

The image shows a screenshot of the Cisco ASA Command Line Interface (CLI) window. The window has a title bar with the ASA logo and standard window controls. Below the title bar, there are tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' being the active tab. The main area of the window displays the CLI prompt and the following commands and output:

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

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

At the bottom of the window, there is a 'Top' checkbox and two buttons: 'Copy' and 'Paste'.

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.

- a. 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.

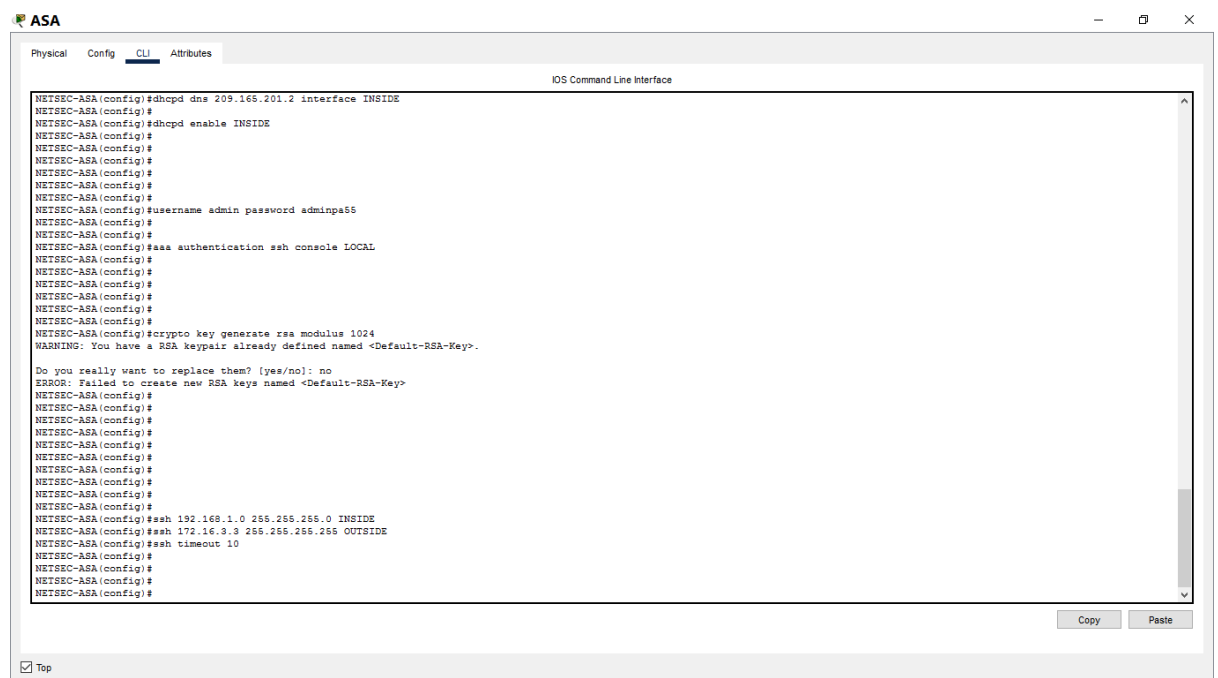
```
NETSEC-ASA(config)# crypto key generate rsa modulus 1024
```

- b. 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)# ssh 192.168.1.0 255.255.255.0 INSIDE
```

```
NETSEC-ASA(config)# ssh 172.16.3.3 255.255.255.255 OUTSIDE
```

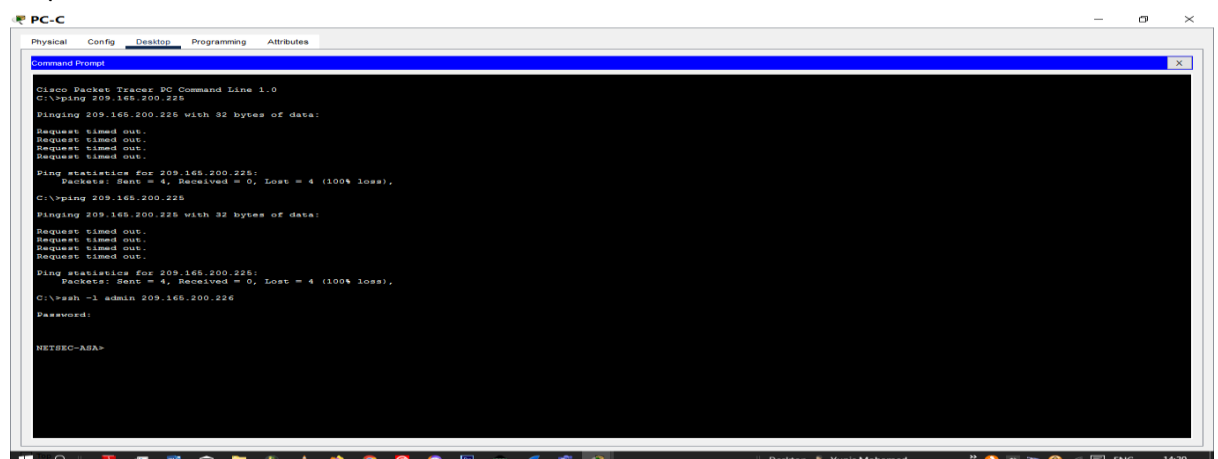
```
NETSEC-ASA(config)# ssh timeout 10
```



```
NETSEC-ASA(config)# dhcpd dns 209.165.201.2 interface INSIDE
NETSEC-ASA(config)#
NETSEC-ASA(config)# dhcpd enable INSIDE
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)# username admin password adminpa55
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)# aaa authentication ssh console LOCAL
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
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)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
NETSEC-ASA(config)#
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)#
NETSEC-ASA(config)#
```

- c. Establish an SSH session from PC-C to the ASA (209.165.200.226). Troubleshoot if it is not successful. **The ssh connection is successful.**

```
C:\> ssh -l admin 209.165.200.226
```



```
Cisco Packet Tracer PC Command Line 1.0
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:\>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:\>ssh -l admin 209.165.200.226
Password:
NETSEC-ASA>
```

- d. Establish an SSH session from PC-B to the ASA (192.168.1.1). Troubleshoot if it is not successful. **The ssh session is successful.**

The screenshot displays a Windows desktop environment. A window titled "PC-B" is open at the top, featuring five tabs: "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is currently selected. Below the tabs, a black Command Prompt window is visible. The text within the Command Prompt reads as follows:

```
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),

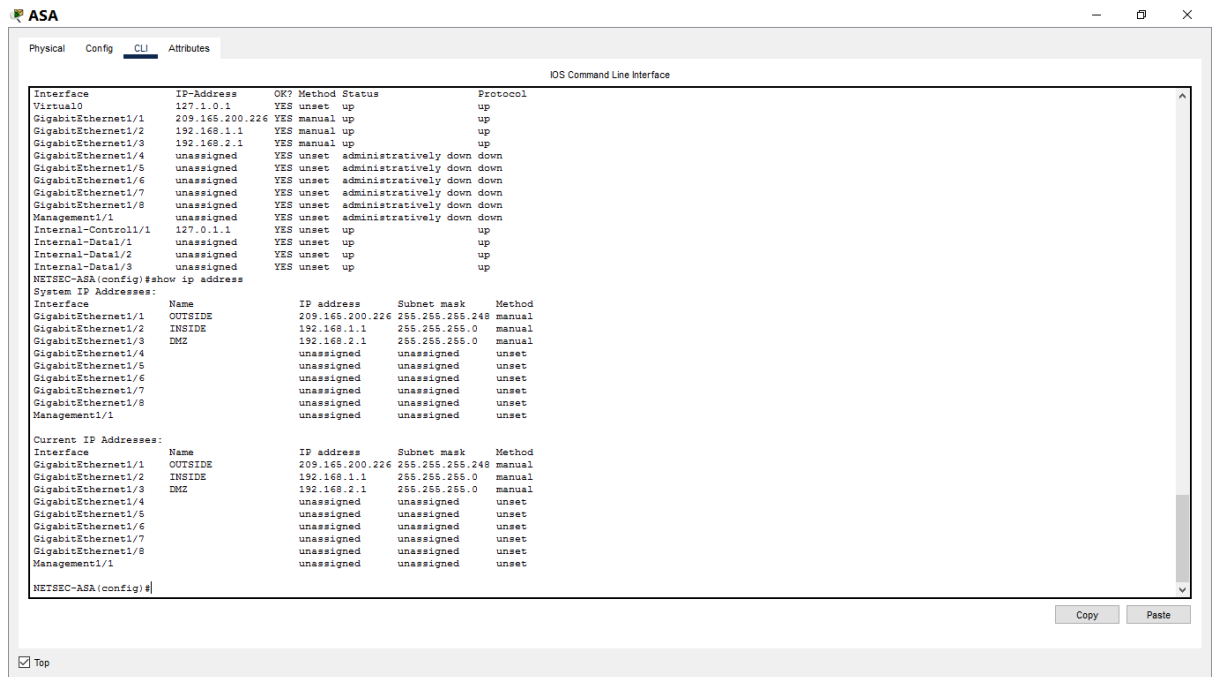
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\> ssh -l admin 192.168.1.1
Invalid Command.

C:\>ssh -l admin 192.168.1.1

Password:

NETSEC-ASA>
```

The taskbar at the bottom of the screen shows various application icons, including File Explorer, Microsoft Edge, and several instances of other applications. The system tray on the right indicates the date and time as "ENG 14:23".



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

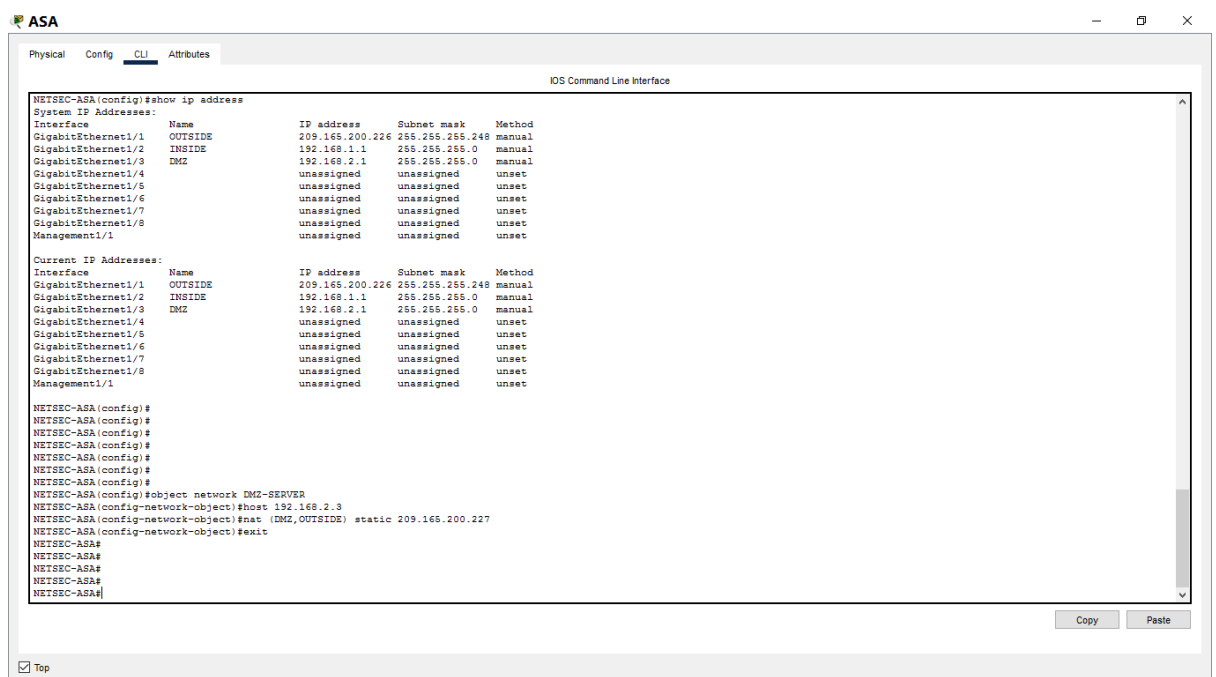
Configure a network object named **DMZ-SERVER** and assign it the static IP address of the DMZ server (192.168.2.3). While in object definition mode, use the **nat** command to specify that this object is used to translate a DMZ address to an OUTSIDE address using static NAT, and specify a public translated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

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

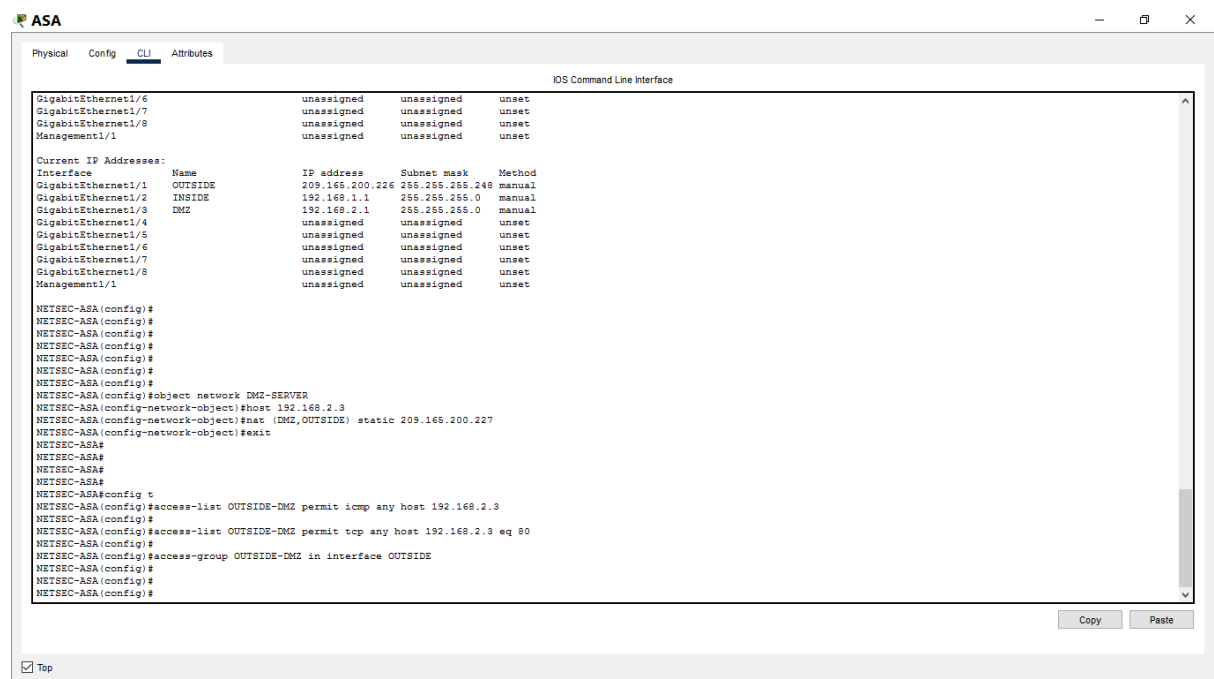


Step 3: Configure an ACL to allow access to the DMZ server from the Internet.

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.

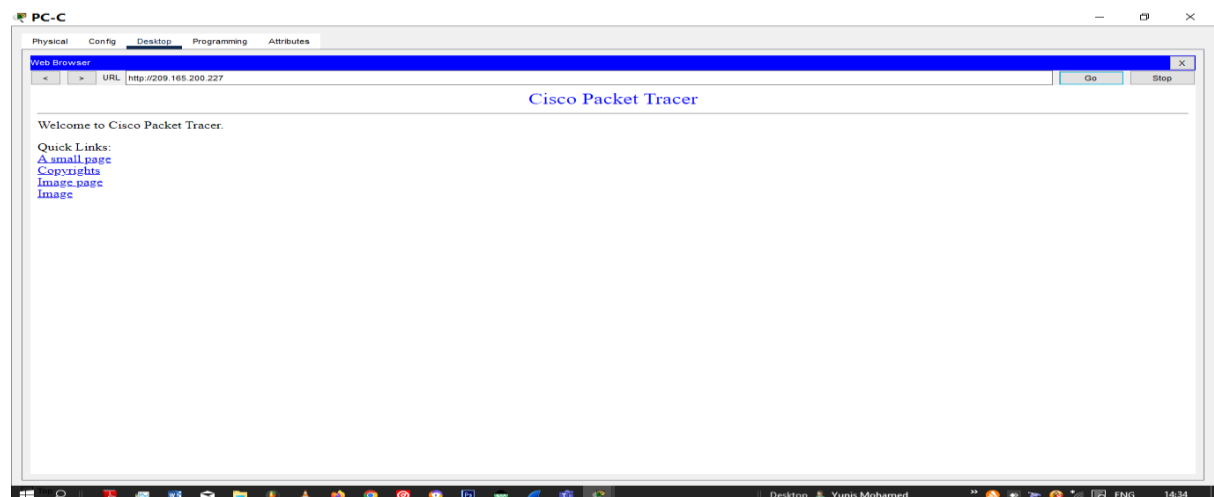
```
NETSEC-ASA(config)# access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
NETSEC-ASA(config)# access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
NETSEC-ASA(config)# access-group OUTSIDE-DMZ in interface OUTSIDE
```

Note: Unlike IOS ACLs, the ASA ACL permit statement must permit access to the internal private DMZ address. External hosts access the server using its public static NAT address, the ASA translates it to the internal host IP address, and then applies the ACL.



Step 4: Test access to the DMZ server.

From a web browser on PC-C, navigate to the DMZ server (209.165.200.227). Troubleshoot if it is not successful. **The connection to the DMZ server is successful.**



Conclusion

In conclusion, the "Configure ASA Basic Settings lab has offered me valuable hands-on experience in setting up and securing a network using a Cisco ASA firewall. Through this lab, I was able to learn crucial skills such as configuring basic settings on the ASA, including hostname, domain name, and management interface IP address. I also gained proficiency in Network Address Translation (NAT) for enabling internet connectivity, as well as in Access Control Lists (ACLs) for filtering and controlling traffic. Additionally, I was able to acquire knowledge on firewall policies and security best practices. I was able to configure the Demilitarized Zone Server (DMZ) which allows for controlled access to specific services while maintaining a higher level of security compared to hosting those services directly on the internal network. Overall, this lab provides a solid foundation for understanding firewall configuration and network security, making it beneficial for network administrators and security professionals in enhancing their knowledge in these areas.