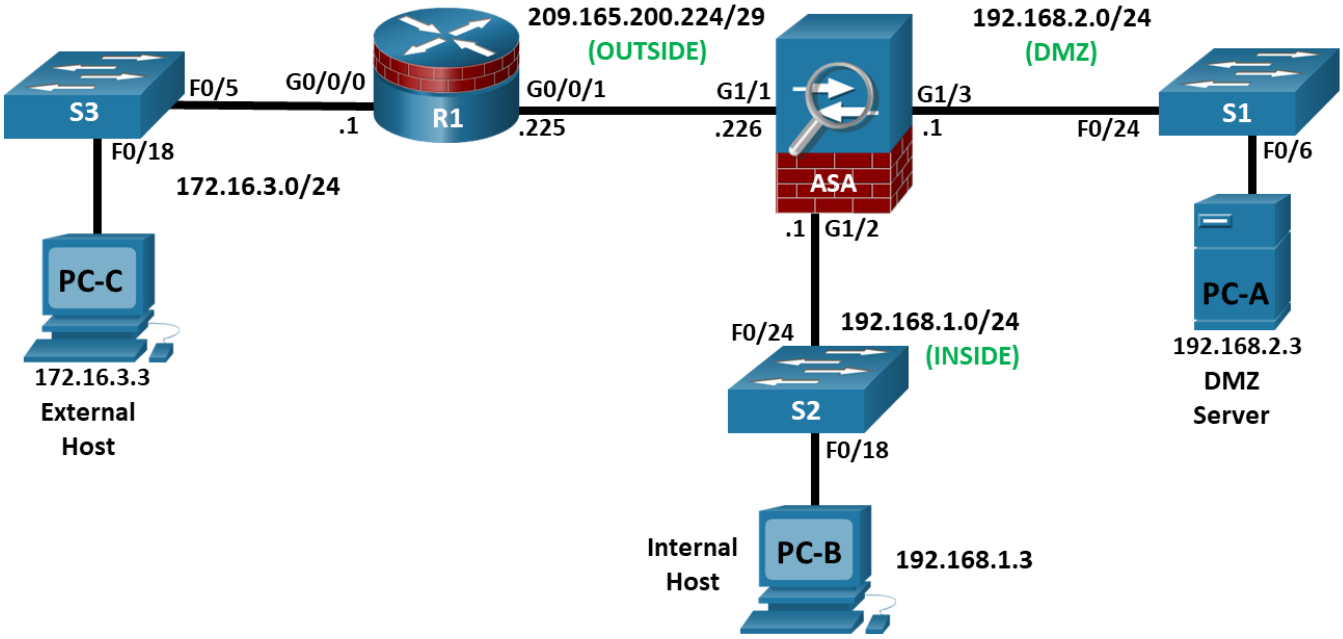
Answers: 21.7.6 Optional Lab - Configure ASA Network Services, Routing, and DMZ withACLsUsing CLI

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	G0/0/1	209.165.200.225	255.255.255.248		ASA G1/1
ASA	G1/1 (OUTSIDE)	209.165.200.226	255.255.255.248	N/A	R1 G0/0/1
	G1/2 (INSIDE)	192.168.1.1	255.255.255.0		S2 F0/24
	G1/3 (DMZ)	192.168.2.1	255.255.255.0		S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure Routing, Address Translation, and Inspection Policy

Part 3: Configure DHCP, AAA, and SSH

Part 4: Configure the DMZ, Static NAT, and ACLs

Background / Scenario

The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall, VPN, and FirePOWER services. This lab employs an ASA 5506-X to create a firewall and protect an internal corporate network from external intruders while allowing internal hosts access to the Internet. The ASA creates three security interfaces: OUTSIDE, INSIDE, and DMZ. It provides outside users limited access to the DMZ and no access to inside resources. Inside users can access the DMZ and outside resources.

The focus of this lab is to configure basic ASA as a basic firewall. Other devices will receive minimal configuration to support the ASA portion of this lab. This lab uses the ASA CLI, which is similar to the IOS CLI, to configure basic device and security settings.

In Part 1 of this lab, you will configure the topology and non-ASA devices. This part can be skipped if your topology is still configured from the previous lab, **Configure ASA 5506-X Basic Settings and Firewall Using CLI**. In Part 2, you will configure routing, NAT, and the firewall between the inside and outside networks. In Part 3, you will configure the ASA for additional services, such as DHCP, AAA, and SSH. In Part 4, you will configure a DMZ on the ASA and provide access to a server in the DMZ.

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

The ASA used with this lab is a Cisco model 5506-X with an 8-port integrated switch, running OS version 9.15(1), Adaptive Security Device Manager (ASDM) version 7.15(1).

Note: Before you begin, ensure that the devices have been erased and have no startup configurations.

Required Resources

- 1 Router (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 3 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 3 PCs (Windows OS with a terminal emulation, such as PuTTY or Tera Term installed)
- 1 ASA 5506-X (OS version 9.15(1) and ASDM version 7.15(1) and Base license or comparable)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

In this part, you will set up the network topology and configure basic settings on the routers, such as interface IP addresses and static routing.

Note: If you proceeded directly to this lab from the previous lab and your configurations have not changed, you can proceed directly to Part 2.

Step 1: Cable the network and clear previous device settings.

Attach the devices that are shown in the topology diagram and cable as necessary. Make sure the router and ASA have been erased and have no startup configuration.

Note: To avoid using the switches, use a cross-over cable to connect the end devices

Step 2: Configure the ASA.

Use the following script to configure the ASA. This will return ASA to the state it was in at the end of the last lab.

a. Use the **write erase** command to remove the startup-config file from flash memory.

b. Use the **reload** command to restart the ASA.

c. Answer no to the following prompt

```
Pre-configure Firewall now through interactive prompts [yes]? No



User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> enable
The enable password is not set.  Please set it now.
Enter  Password: class
Repeat Password: class
Note: Save your configuration so that the password persists across reboots
("write memory" or "copy running-config startup-config").
ciscoasa# conf t
ciscoasa(config)#

***************************** NOTICE *****************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: no

In the future, if you would like to enable this feature,
issue the command "call-home reporting anonymous".

Please remember to save your configuration.

ciscoasa(config)#
```

d. Use the following script to configure the ASA.

ASA Script

```
hostname NETSEC-ASA
domain-name netsec.com
passwd cisco
!
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 209.165.200.226 255.255.255.248
 no shutdown
!
interface GigabitEthernet1/2
 nameif INSIDE
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 no shutdown
!
domain-name netsec.com
!
http server enable
http 192.168.1.0 255.255.255.0 INSIDE
!
end
write mem
```

Step 3: Configure R1 and the end devices.

a. Use the following script to configure R1. No additional configuration for R1 will be required for this lab.

Note: R1 does not need any routing as all inbound packets from the ASA will have 209.165.200.226 as the source IP address.

R1 Script

```
enable
configure terminal
hostname R1
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
ip domain name netsec.com
username admin01 algorithm-type scrypt secret cisco12345
interface GigabitEthernet0/0/0
 ip address 172.16.3.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/0/1
 ip address 209.165.200.225 255.255.255.248
 no shutdown
```

```
crypto key generate rsa general-keys modulus 1024
ip http server
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
end
copy running start
```

b. Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C as shown in the IP Addressing Table.

Step 4: Verify connectivity.

R1 should be able to ping the OUTSIDE interface for the ASA. PC-B should be able to ping the INSIDE interface for the ASA. If these pings are not successful, troubleshoot the basic device configurations before continuing. PC-A and PC-C will not be able to ping the ASA.

Part 2: Configure Routing, Address Translation, and Inspection Policy

In this part of this lab, you will provide a default route for the ASA to reach external networks. You will configure address translation using network objects to enhance firewall security. You will then modify the default application inspection policy to allow specific traffic.

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

The ASA OUTSIDE interface is configured with a static IP address and subnet mask. However, the ASA does not have a gateway of last resort defined. To enable the ASA to reach external networks, you will configure a default static route on the ASA OUTSIDE interface.

Note: If the ASA OUTSIDE interface was configured as a DHCP client, it could obtain a default gateway IP address from the ISP. However, in this lab, the OUTSIDE interface is configured with a static address.

a. Ping from the ASA to R1 G0/0/1 at IP address 209.165.200.225.

Was the ping successful?

b. Ping from the ASA to R1 G0/0/0 at IP address 172.16.3.1.

Was the ping successful?

c. Create a “quad zero” default route using the **route** command, associate it with the ASA **OUTSIDE** interface, and point to the R1 G0/0/1 at IP address 209.165.200.225 as the gateway of last resort. The default administrative distance is one by default.

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

d. Issue the **show route** command to display the ASA routing table and the static default route you just created.

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

```
Codes: L - local, C - connected, S - static, 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, V - VPN
       i - IS-IS, su - IS-IS summary, 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, + - replicated route
Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S*        0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, OUTSIDE
C         192.168.1.0 255.255.255.0 is directly connected, INSIDE
L         192.168.1.1 255.255.255.255 is directly connected, INSIDE
C         209.165.200.224 255.255.255.248 is directly connected, OUTSIDE
L         209.165.200.226 255.255.255.255 is directly connected, OUTSIDE
```

e. Ping from the ASA to R1 G0/0/0 IP address 172.16.3.1.

Was the ping successful?

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

Beginning with ASA version 8.3, network objects are used to configure all forms of NAT. A network object is created, and it is within this object that NAT is configured. In Step 2a, the network object **INSIDE-NET** is used to translate the inside network addresses (192.168.10.0/24) to the global address of the OUTSIDE ASA interface. This type of object configuration is called Auto-NAT.

a. Create the 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)# end
```

b. 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 object** and **show run nat** commands.

```
NETSEC-ASA# show run object
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.0
NETSEC-ASA# show run nat
!
object network INSIDE-NET
 nat (INSIDE,OUTSIDE) dynamic interface
```

c. From PC-B, attempt to ping the R1 G0/0/1 interface at IP address **209.165.200.225**.

Were the pings successful?

d. Issue 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 because ICMP is not being inspected by the global inspection policy. The outgoing pings (echoes) were translated, and the returning echo replies

were blocked by the firewall policy. You will configure the default inspection policy to allow ICMP in the next step.

Note: Depending on the processes and daemons running on the particular computer used as PC-B, you may see more translated and untranslated hits than the four echo requests and echo replies.

```
NETSEC-ASA# show nat

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

e. Ping from PC-B to R1 again and quickly issue the **show xlate** command to see the addresses being translated. However, ICMP is denied, by default, be the firewall inspection policy

```
NETSEC-ASA# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from INSIDE:192.168.1.3/1 to OUTSIDE:209.165.200.226/1 flags ri
idle 0:00:02 timeout 0:00:30
```

Note: The flags (r and i) indicate that the translation was based on a port map (r) and was done dynamically (i).

f. Open a browser on PC-B and enter the IP address of R1 G0/0/1 (https://209.165.200.225). The connection will fail, but you will see a secure connection error message. These means PC-B received a replay from R1.The connection was denied because PC-B does not have a certificate for a Secure Socket Layer (SSL) connection. However, TCP-based HTTP traffic was permitted to egress the OUTSIDE interface on the ASA, by default, by the firewall inspection policy.

g. On the ASA, reissue the **show nat** and **show xlate** commands to see the hits and addresses being translated for the HTTP connection.

```
NETSEC-ASA# show nat

Auto NAT Policies (Section 2)
1 (INSIDE) to (OUTSIDE) source dynamic INSIDE-NET interface
    translate_hits = 17, untranslate_hits = 4
NETSEC-ASA# show xlate
4 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

TCP PAT from INSIDE:192.168.1.3/49503 to OUTSIDE:209.165.200.226/49503 flags ri idle
0:01:24 timeout 0:00:30
TCP PAT from INSIDE:192.168.1.3/49502 to OUTSIDE:209.165.200.226/49502 flags ri idle
0:01:24 timeout 0:00:30
TCP PAT from INSIDE:192.168.1.3/49501 to OUTSIDE:209.165.200.226/49501 flags ri idle
0:01:25 timeout 0:00:30
TCP PAT from INSIDE:192.168.1.3/49500 to OUTSIDE:209.165.200.226/49500 flags ri idle
0:01:25 timeout 0:00:30
NETSEC-ASA#
```

Step 3: Modify the default MPF application inspection global service policy.

For application layer inspection, as well as other advanced options, the Cisco Modular Policy Framework (MPF) is available on ASAs. Cisco MPF uses three configuration objects to define modular, object-oriented, and hierarchical policies:

- **Class maps** - Define a match criterion.
- **Policy maps** - Associate actions to the match criteria.
- **Service policies** - Attach the policy map to an interface, or globally to all interfaces of the appliance.

a. Display the default MPF policy map that performs the inspection on inside-to-outside traffic. Only traffic that was initiated from the inside is allowed back in to the OUTSIDE interface. Notice that the ICMP protocol is missing.

```
NETSEC-ASA# show run | begin class
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect snmp
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
!
service-policy global_policy global
<output omitted>
```

b. Add the inspection of ICMP traffic to the policy map list using the following commands:

```
NETSEC-ASA# configure terminal
NETSEC-ASA(config)# policy-map global_policy
NETSEC-ASA(config-pmap)# class inspection_default
NETSEC-ASA(config-pmap-c)# inspect icmp
```

c. Display the default MPF polich map to verify ICMP is now listed in the inspection rules.

```
NETSEC-ASA(config-pmap-c)# show run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect snmp
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect icmp
!
```

d. From PC-B, attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should be successful this time because ICMP traffic is now being inspected and legitimate return traffic is being allowed.

Part 3: Configure DHCP, AAA, and SSH

In this part, you will configure ASA features, such as DHCP and enhanced login security, using AAA and SSH.

Step 1: Configure the ASA as a DHCP server.

The ASA can be both a DHCP server and a DHCP client. In this step, you will configure the ASA as a DHCP server to dynamically assign IP addresses for DHCP clients on the inside network.

a. Configure a DHCP address pool and enable it on the ASA INSIDE interface. This is the range of addresses to be assigned to inside DHCP clients. Set the range from 192.168.1.5 through 192.168.1.100.

```
NETSEC-ASA(config-pmap-c)# exit
NETSEC-ASA(config-pmap)# exit
NETSEC-ASA(config)# dhcpd address 192.168.1.5-192.168.1.100 INSIDE
```

b. (Optional) Specify the IP address of the DNS server to be given to clients.

```
NETSEC-ASA(config)# dhcpd dns 209.165.201.2
```

Note: Other parameters can be specified for clients, such as WINS server, lease length, and domain name. By default, the ASA sets its own IP address as the DHCP default gateway, so there is no need to

configure it. However, to manually configure the default gateway, or set it to a different networking device's IP address, use the following command:

```
NETSEC-ASA(config)# dhcpd option 3 ip 192.168.1.1
```

c. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (INSIDE).

```
NETSEC-ASA(config)# dhcpd enable INSIDE
```

d. Verify the DHCP daemon configuration by using the **show run dhcpd** command.

```
NETSEC-ASA(config)# show run dhcpd
dhcpd dns 209.165.201.2
dhcpd option 3 ip 192.168.1.1
!
dhcpd address 192.168.1.5-192.168.1.100 INSIDE
dhcpd enable INSIDE
```

e. Access the Network Connection IP Properties for PC-B, and change it from a static IP address to a DHCP client so that it obtains an IP address automatically from the ASA DHCP server. The procedure to do this varies depending on the PC operating system. It may be necessary to issue the **ipconfig /renew** command on PC-B to force it to obtain a new IP address from the ASA.

Verify that PC-B was assigned an IP address from 192.168.1.5 to 192.168.1.100, which will most likely be 192.168.1.5. PC-B should still be able to ping the G0/0/1 interface for R1 at 209.165.200.225.

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

a. Define a local user named admin by entering the **username** command. Specify a password of **cisco12345**.

```
NETSEC-ASA(config)# username admin password cisco12345
```

b. Configure AAA to use the local ASA database for SSH user authentication.

```
NETSEC-ASA(config)# aaa authentication ssh console LOCAL
```

Note: For added security, starting with ASA version 8.4(2), configure AAA authentication to support SSH connections. The Telnet/SSH default login is not supported. You can no longer connect to the ASA using SSH with the default username and the login password.

Step 3: Configure SSH remote access to the ASA.

You can configure the ASA to accept SSH connections from a single host or a range of hosts on the inside or outside network.

a. Generate an **RSA** key pair, which is required to support SSH connections. The modulus (in bits) can be 512, 768, 1024, or 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA. Specify a modulus of **2048** using the **crypto key** command.

```
NETSEC-ASA(config)# crypto key generate rsa modulus 2048
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

Note: You may receive a message that a RSA key pair is already defined. To replace the RSA key pair enter **yes** at the prompt.

b. Save the RSA keys to persistent flash memory using the **write mem** command. Your "Cryptochecksum" values will be different

```
NETSEC-ASA(config)# write mem
Building configuration...
```

```
Cryptochecksum: 3c845d0f b6b8839a f9e43be0 33feb4ef
3270 bytes copied in 0.890 secs
[OK]
```

c. 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
```

d. On PC-C, use an SSH client (such as PuTTY) to connect to the ASA OUTSIDE interface at the IP address **209.165.200.226**. The first time you connect you may be prompted by the SSH client to accept the RSA host key of the ASA SSH server. Log in as user **admin** and provide the password **cisco12345**.

e. You can also connect to the ASA INSIDE interface from a PC-B SSH client using the IP address **192.168.1.1**.

Part 4: Configure DMZ, Static NAT, and ACLs

Previously, you configured address translation using PAT for the inside network. In this part of the lab, you will create a DMZ on the ASA, configure static NAT to a DMZ server, and apply ACLs to control access to the server.

To accommodate the addition of a DMZ and a web server, you will use another address from the ISP range assigned 209.165.200.224/29 (.224-.231). Router R1 G0/0 and the ASA OUTSIDE interface are already using 209.165.200.225 and .226. You will use the public address 209.165.200.227 and static NAT to provide address translation access to the server.

Step 1: Configure the DMZ interface G1/3 on the ASA.

a. Configure DMZ interface G1/3 which is on the LAN where the public access web server will reside. Assign the interface IP address **192.168.2.1/24**, name it **DMZ**, assign it a security level of **70** and enable the interface.

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

b. Display the status for all ASA interfaces using the **show interface ip brief** command.

```
NETSEC-ASA # 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
Internal-Control1/1        unassigned      YES unset  down                  down
Internal-Data1/1           unassigned      YES unset  down                  down
Internal-Data1/2           unassigned      YES unset  down                  down
Internal-Data1/3           unassigned      YES unset  up                    up
Internal-Data1/4           169.254.1.1     YES unset  up                    up
Management1/1              unassigned      YES unset  administratively down down
```

c. Display the information for the interfaces using the **show ip address** command.

```
NETSEC-ASA # 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
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
```

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

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

Configure a named access list (**OUTSIDE-DMZ**) that permits any IP protocol 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 ip any host 192.168.2.3
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.

You can modify this ACL to allow only services that you want to be exposed to external hosts, such as web (HTTP) or file transfer (FTP).

Step 4: Test access to the DMZ server.

a. Source a ping from the G0/0/0 interface on R1 (172.16.3.1) to the public IP address for the DMZ server. The pings should be successful.

```
R1# ping 209.165.200.227 source g0/0/0
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

b. Clear the NAT counters using the **clear nat counters** command.

```
NETSEC-ASA# clear nat counters
```

c. Ping from PC-C to the DMZ server at the public address **209.165.200.227**. The pings should be successful.

d. Issue the **show nat** and **show xlate** commands on the ASA to see the effect of the pings. Both the PAT (INSIDE to OUTSIDE) and static NAT (DMZ to OUTSIDE) policies are shown.

```
NETSEC-ASA# show nat

Auto NAT Policies (Section 2)
1 (DMZ) to (OUTSIDE) source static DMZ-server 209.165.200.227
    translate_hits = 0, untranslate_hits = 4
2 (INSIDE) to (OUTSIDE) source dynamic INSIDE-NET interface
    translate_hits = 1, untranslate_hits = 3
```

Note: Pings from inside to outside are translated hits. Pings from outside host PC-C to the DMZ are considered untranslated hits.

```
NETSEC-ASA# show xlate
1 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from DMZ:192.168.2.3 to OUTSIDE:209.165.200.227
    flags s idle 0:22:58 timeout 0:00:00
```

Note: This time the flag is "**s**", which indicates a static translation.

e. You can also access the DMZ server from a host on the inside network because the ASA INSIDE interface (G1/2) is set to a security level of 100 (the highest) and the DMZ interface (G1/3) is set to 70. The ASA acts like a router between the two networks. Ping the DMZ server (PC-A) internal address (**192.168.2.3**) from inside network host PC-B (192.168.1.X). The pings should be successful because of the interface security level and the fact that ICMP is being inspected on the INSIDE interface by the global inspection policy. The pings from PC-B to PC-A will not affect the NAT translation counts because both PC-B and PC-A are behind the firewall, and no translation takes place.

The DMZ server cannot ping PC-B on the inside network because the DMZ interface has a lower security level. Try to ping from the DMZ server PC-A to PC-B at IP address **192.168.1.3**. The pings should not be successful.

Use the **show run** command to display the configuration for G1/3.

```
NETSEC-ASA# show run interface g1/3
!
interface g1/3
nameif DMZ
 security-level 70
 ip address 192.168.2.1 255.255.255.0
```

Note: An access list can be applied to the INSIDE interface to control the type of access to be permitted or denied to the DMZ server from inside hosts.

Reflection Questions

1. How does the configuration of the ASA firewall differ from that of an ISR?

2. What does the ASA use to define address translation and what is the benefit?

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.