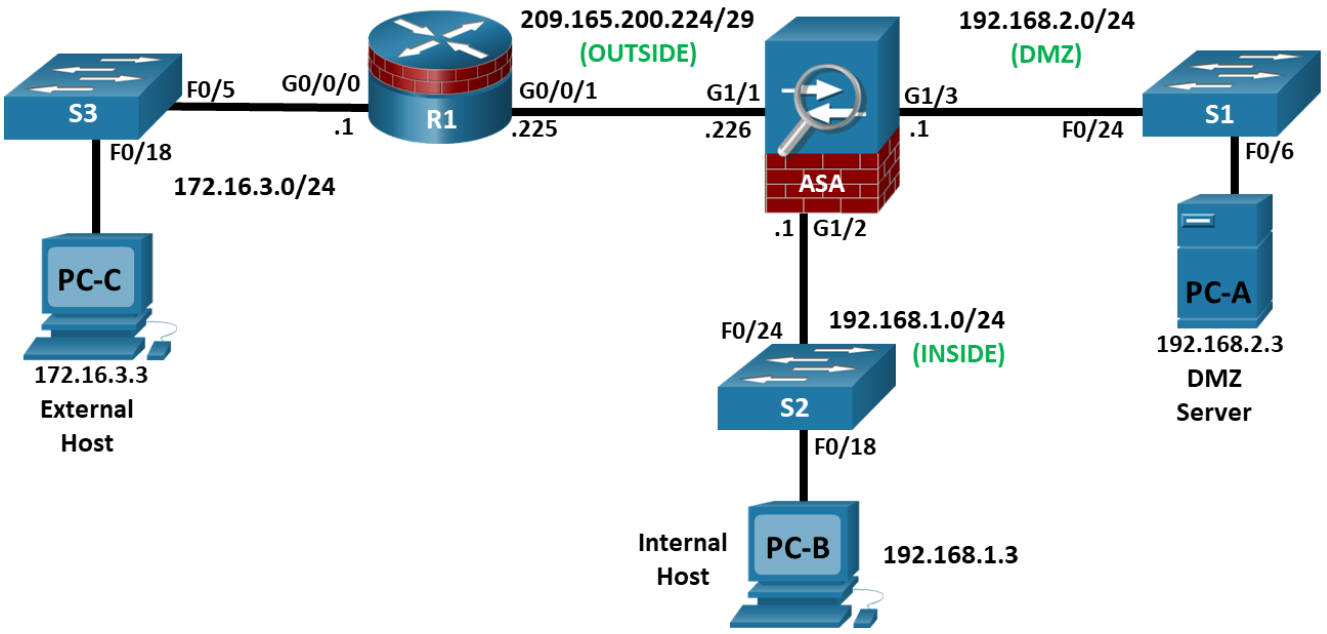
Answers: 21.2.10 Optional Lab - Configure ASA Basic Settings Using CLI

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: Access the ASA Console and Use CLI Setup Mode to Configure Basic Settings

Part 3: Configure Basic ASA Settings and Interface Security Levels

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 the 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. In Part 2, you will explore two ways to configure basic ASA settings. In Part 3, you will configure additional settings, test connectivity, and configure Adaptive Security Device Manager (ASDM) access. ASDM provides an intuitive, GUI-based tool for configuring the ASA.

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.

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

Required Resources

- 3 Routers (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation, such as PuTTY or Tera Term installed)
- 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: Do not configure ASA settings at this time.

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 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 secret algorithm-type scrypt 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 3: Verify connectivity.

Because the ASA is the focal point for the network zones, and it has not yet been configured, there will be no connectivity between devices that are connected to it. However, PC-C should be able to ping the R1 interface. From PC-C, ping the R1 G0/0/1 IP address (209.165.200.225). If these pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Access the ASA Console and Use CLI Setup to Configure Basic Settings

In this part, you will access the ASA via the console and use various **show** commands to determine hardware, software, and configuration settings. You will clear the current configuration and use the CLI interactive setup utility to configure basic ASA settings.

Step 1: Access the ASA console.

a. Accessing the ASA via the console port is the same as with a Cisco router or switch. Connect to the ASA console port with a rollover cable and use a terminal emulation program, such as TeraTerm or PuTTy to open a serial connection and access the CLI.

b. The ASA initially prompts you to pre-configure the firewall using an interactive prompt. We will not be configuring the ASA this way, therefore enter **no** and press **Enter**. If you have inadvertently started the

setup wizard, press **CTRL-Z** to exit it. The terminal screen should display the default ASA user EXEC hostname and prompt ciscoasa>.

c. You will get prompt requesting that you configure an enable password to enter privileged EXEC mode. Enter class to configure the password and then again to confirm it. You will now be in privileged EXEC mode.

```
enable password cannot be removed
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#
```

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

The ASA 5506-X comes with an integrated eight-port Ethernet switch. Ports G1/1 to G1/8 are normal GigabitEthernet ports.

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

```
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 9.15(1)1
SSP Operating System Version 2.9(1.131)
Device Manager Version 7.15(1)

Compiled on Fri 20-Nov-20 18:47 GMT by builders
System image file is "disk0:/asa9-15-1-1-lfbff-k8.SPA"
Config file at boot was "startup-config"

ciscoasa up 2 days 23 hours

Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
Internal ATA Compact Flash, 8000MB
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 00a3.8ecd.0ed2, irq 255
 2: Ext: GigabitEthernet1/2  : address is 00a3.8ecd.0ed3, irq 255
 3: Ext: GigabitEthernet1/3  : address is 00a3.8ecd.0ed4, irq 255
<output omitted>
```

What software version is this ASA running?

What is the name of the system image file and from where was it loaded?

The ASA can be managed using a built-in GUI known as ASDM. What version of ASDM is this ASA running?

What is the Firepower Extension Operating System version?

How much RAM does this ASA have?

How much flash memory does this ASA have?

How many Ethernet ports does this ASA have?

What type of license does this ASA have?

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

a. Display the ASA file system using the **show file system** command. Determine what prefixes are supported.

```
ciscoasa# show file system

File Systems:

     Size(b)     Free(b)      Type      Flags  Prefixes
* 7365472256   3859148800    disk      rw      disk0: flash:
             -            -  disk      rw      disk1:
             -            -  network   rw      tftp:
             -            -  opaque    rw      system:
             -            -  network   ro      http:
             -            -  network   ro      https:
             -            -  network   rw      scp:
             -            -  network   rw      ftp:
             -            -  network   wo      cluster:
             -            -  stub      ro      cluster_trace:
             -            -  network   rw      smb:
```

What is another name for flash:?

b. Display the contents of flash memory using either the **show flash**, **show disk0**, **dir flash:**, or **dir disk0:** command. These commands display similar output.

```
ciscoasa# show flash
--#--  --length--  -----date/time------  path
   28  38925172    Jan 24 2021 20:50:06  asdm-7151.bin
   29  33          Feb 09 2021 11:43:44  .boot_string
    4  4096        Jan 24 2021 20:52:44  log
   35  31000       Oct 28 2020 13:46:04  log/asa-appagent.log
    5  2265        Feb 19 2021 15:25:22  log/asa-cmd-server.log
   14  4096        Aug 29 2017 14:26:24  crypto_archive
   15  4096        Aug 29 2017 14:26:28  coredumpinfo
   16  59          Aug 29 2017 14:26:28  coredumpinfo/coredump.cfg
   31  35209829    Oct 04 2017 03:17:02  anyconnect-win-4.5.02033-webdeploy-k9.pkg
   32  70744710    Oct 28 2020 22:31:52  anyconnect-win-4.9.03049-webdeploy-k9.pkg
```

```
   33  137859680   Jan 24 2021 20:47:30  asa9-15-1-1-lfbff-k8.SPA
    6  39          Feb 19 2021 15:25:23  snortpacketinfo.conf

7365472256 bytes total (3859148800 bytes free)
```

What is the name of the ASDM file in flash:?

Step 4: Determine the current running configuration.

The ASA 5506-X is commonly used as an edge security device that connects a small business or teleworker to an ISP device, such as a DSL or cable modem, for access to the internet.

a. Display the current running configuration using the **show running-config** command.

```
ciscoasa# show running-config
: Saved

:
: Serial Number: JAD21140GC5
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
:
ASA Version 9.15(1)1
!
hostname ciscoasa
enable password ***** pbkdf2
service-module 1 keepalive-timeout 4
service-module 1 keepalive-counter 6
service-module sfr keepalive-timeout 4
service-module sfr keepalive-counter 6
names
no mac-address auto

!
interface GigabitEthernet1/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
<output omitted>
```

Note: To stop the output from a command using the CLI, press **Q**.

You may also see other security features, such as a global policy that inspects selected application traffic, which the ASA inserts by default if the original startup configuration has been erased. The actual output varies depending on the ASA model, version, and configuration status.

b. You can restore the ASA to its factory default settings by using the **configure factory-default** global configuration command. When entering global configuration, you will initially be prompted to enable anonymous error reporting. Enter **N**, otherwise enter **A** to be prompted for this at a later date.

```
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: N

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)# configure factory-default
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 250 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: !
Executing command: interface Management1/1
Executing command:  management-only
Executing command:  no nameif
Executing command:  no security-level
Executing command:  no ip address
Executing command:  no shutdown
Executing command:  exit
Executing command: !
Executing command: interface GigabitEthernet1/1
Executing command:  nameif outside
INFO: Security level for "outside" set to 0 by default.
Executing command:  security-level 0
Executing command:  no shutdown
<output omitted>
Executing command: same-security-traffic permit inter-interface
Executing command: !
Executing command: !
Factory-default configuration is completed
ciscoasa(config)#
```

c. You may want to capture and print the factory-default configuration as a reference. Use the terminal emulation program to copy it from the ASA and paste it into a text document. You can then edit this file if desired, so that it contains only valid commands. You should remove password commands and enter the **no shut** command to enable the desired interfaces.

Step 5: Clear the previous ASA configuration settings.

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

```
ciscoasa(config)# end
ciscoasa# write erase
Erase configuration in flash memory? [confirm] <Enter>
[OK]
ciscoasa# show start
No Configuration
ciscoasa#
```

Note: The IOS command **erase startup-config** is not supported on the ASA.

b. Use the **reload** command to restart the ASA. This causes the ASA to come up in CLI Setup mode. If prompted that the config has been modified and needs to be saved, respond with **N**, and then press **Enter** to proceed with the reload.

```
ciscoasa# reload
System config has been modified. Save? [Y]es/[N]o:  n
Proceed with reload? [confirm] <Enter>
ciscoasa#



***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
<output omitted>
```

Step 6: Use the Setup interactive CLI mode to configure basic settings.

When the ASA completes the reload process, it should detect that the startup-config file is missing and prompt you to pre-configure the firewall using interactive prompts. This presents a series of interactive prompts to configure basic ASA settings.

Note: The interactive prompt mode does not configure the ASA with factory defaults as described in Step 4. This mode can be used to configure minimal basic settings, such as hostname, clock, and passwords. You can also go directly to the CLI to configure the ASA settings, as described in Part 3.

a. Respond to the Setup interactive prompts as shown here, after the ASA reloads.

```
Pre-configure Firewall now through interactive prompts [yes]? <Enter>
Firewall Mode [Routed]: <Enter>
Enable password [<use current password>]: class
Allow password recovery [yes]? <Enter>
Clock (UTC): <Enter>
  Year [2021]: <Enter>
```

```
  Month [Feb]: <Enter>
  Day [22]: <Enter>
  Time [15:16:32]: <Enter>
Management IP address: 192.168.100.1
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com
IP address of host running Device Manager: <Enter>

The following configuration will be used:
Enable password: class
Allow password recovery: yes
Clock (UTC): 07:29:14 Mar 19 2019
Firewall Mode: Routed
Management IP address: 192.168.100.1
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com


Use this configuration and save to flash? [yes] <Enter>
INFO: Security level for "management" set to 0 by default.
Cryptochecksum: d0b22e76 5178e9e6 0a6bc590 5f5e5a3d

3958 bytes copied in 0.80 secs


User enable_1 logged in to ASA-Init
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ASA-Init>
```

Note: In the above configuration, the IP address of the host running ASDM was left blank. It is not necessary to install ASDM on a host. It can be run from the flash memory of the ASA device itself using the browser of the host.

Note: The responses to the prompts are automatically stored in the startup-config and the running config. However, additional security-related commands, such as the **policy-map global_policy** that uses **class inspection_default**, are inserted into the running-config by the ASA OS.

b. Enter privileged EXEC mode with the **enable** command. Enter **class** for the password.

c. Issue the **show run** command to see the additional security-related configuration commands that are inserted by the ASA.

d. Issue the **write memory** command to capture the additional security-related commands in the startup-config file.

Part 3: Configure ASA Settings and Interface Security

In this part, you will configure basic settings by using the ASA CLI, even though some of them were already configured using the Setup mode interactive prompts in the previous part. In this part, you will start with the settings configured in the previous part and then add to or modify them to create a complete basic configuration.

Tip: Many ASA CLI commands are similar to, if not the same, as those used with the Cisco IOS CLI. In addition, the process of moving between configuration modes and sub-modes is essentially the same.

Note: You must complete the previous part before beginning this part.

Step 1: Configure the hostname and domain name.

a. Enter global configuration mode using the **config t** command. The first time you enter configuration mode after running Setup, you will be prompted to enable anonymous reporting. Respond with no.

```
ASA-Init# config t
ASA-Init(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: n

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

Please remember to save your configuration.
```

b. Configure the ASA hostname using the **hostname** command.

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

c. Configure the domain name using the **domain-name** command.

```
NETSEC-ASA(config)# domain-name netsec.com
```

Step 2: Configure the login and enable mode passwords.

a. The login password is used for Telnet connections (and SSH prior to ASA version 8.4). By default, it is set to cisco, but because the default startup configuration was erased you have the option to configure the login password using the **passwd** or **password** command. This command is optional because later in the lab we will configure the ASA for SSH, and not Telnet access.

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

b. Configure the privileged EXEC mode (enable) password using the **enable password** command.

```
NETSEC-ASA(config)# enable password class
```

Step 3: Set the date and time.

The date and time can be set manually using the **clock set** command. The syntax for the **clock set** command is **clock set** *hh:mm:ss* {*month day* | *day month*} *year*. The following example shows how to set the date and time using a 24-hour clock:

```
NETSEC-ASA(config)# clock set 2:23:00 feb 22 2021
```

Step 4: Configure the INSIDE and OUTSIDE interfaces.

In this step, you will configure internal and external interfaces, name them, assign IP addresses, and set the interface security level.

In Part 2, the MGMT interface was configured with an IP address of 192.168.100.1. You will configure another interface as the INSIDE interface for this lab and remove the IP addressing for M1/1. You will only configure the INSIDE and OUTSIDE interfaces at this time. The DMZ interface will be configured in the next lab.

a. Configure interface G1/2 for the INSIDE network, 192.168.1.0/24. Name the interface **INSIDE**, set the security level to the highest setting of **100** and enable it.

```
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
```

b. Configure interface G1/1for the OUTSIDE network, 209.165.200.224/29. Name the interface **OUTSIDE**, set the security level to the lowest setting of **0** and enable it.

```
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
```

c. Remove the configuration from the M1/1 interface and shut it down (if required).

```
NETSEC-ASA(config-if)# interface m1/1
NETSEC-ASA(config-if)# shutdown
NETSEC-ASA(config-if)# no ip address
```

Interface security-level notes:

You may receive a message that the security level for the INSIDE interface was set automatically to 100, and the OUTSIDE interface was set to 0. The ASA uses interface security levels from 0 to 100 to enforce the security policy. Security level 100 (INSIDE) is the most secure and level 0 (OUTSIDE) is the least secure.

By default, the ASA applies a policy where traffic from a higher security level interface to one with a lower level is permitted and traffic from a lower security level interface to one with a higher security level is denied. The ASA default security policy permits outbound traffic, which is inspected, by default. Returning traffic is allowed due to stateful packet inspection. This default “routed mode” firewall behavior of the ASA allows packets to be routed from the INSIDE network to the OUTSIDE network, but not vice-versa. In a latter part of this lab, you will configure NAT to increase the firewall protection.

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

Note: The command syntax is different from the **show ip interface brief** IOS command. If any of the physical or logical interfaces previously configured are not up/up, troubleshoot as necessary before continuing.

Tip: Most ASA **show** commands, as well as **ping**, **copy**, and others, can be issued from within any configuration mode prompt without the **do** command that is required with IOS.

```
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
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
```

e. Display the Layer 3 interface information using the **show ip address** command.

```
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
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
```

f. You may also use the command **show running-config interface** to display the configuration for a particular interface from the running-config.

```
NETSEC-ASA(config-if)# show run interface g1/1
!
interface GigabitEthernet1/1
 nameif OUTSIDE
 security-level 0
 ip address 209.165.200.226 255.255.255.248
```

Step 5: Test connectivity to the ASA.

a. Ensure that PC-B has a static IP address of 192.168.1.3, a subnet mask of 255.255.255.0, and a default gateway of 192.168.1.1.

b. You should be able to ping from PC-B to the ASA INSIDE interface address and ping from the ASA to PC-B. If the pings fail, troubleshoot the configuration as necessary.

```
NETSEC-ASA(config-if)# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

c. From PC-C, ping the OUTSIDE interface IP address **209.165.200.226**. Alternatively, instead of configuring PC-C just for a ping test, you can source a ping from the G0/0/0 interface on R1. You should not be able to ping the OUTSIDE interface.

```
R1# ping 209.165.200.226 source 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
.....
Success rate is 0 percent (0/5)
R1#
```

Step 6: Configure ASDM access to the ASA.

ASDM provides an intuitive, GUI-based tool for configuring the ASA from a PC.

a. Configure the ASA to allow HTTPS connections from any host on the INSIDE network (192.168.1.0/24) using the **http server enable** command in global configuration mode. This allows access to the ASA GUI (ASDM).

```
NETSEC-ASA(config-if)# exit
NETSEC-ASA(config)# http server enable
NETSEC-ASA(config)# http 192.168.1.0 255.255.255.0 INSIDE
```

b. Open a browser on PC-B and test the HTTPS access to the ASA by entering **https://192.168.1.1**. You will be prompted that the connection is not secure. Select the option to allow you to continue to the webpage.

c. You should then see Cisco ASDM Welcome screen that allows you to either **Install ASDM Launcher** or **Install Java Web Start** to run ASDM as a Java Web start application.

Note: If you or your instructor have already installed the **Cisco ASDM-ID Launcher**, open the application.

d. You should then be required to authenticate to the ASA. Because no username was specified, simply enter the enable password **class** in the password field.

e. Close the browser or **Cisco ASDM-ID Launcher**. Using ASDM to configure the ASA is beyond the scope of this course. However, there is an optional topic after the summary for this module with more information about ASDM along with three optional labs. The objective here is not to use the ASDM configuration screens, but to verify HTTP/ASDM connectivity to the ASA. If you are unable to access ASDM, check your configurations. If the configurations are correct contact your instructor for further assistance.

Step 7: Save your ASA configuration for the next lab.

In the next lab, you will extend your current configuration adding a DMZ, routing, NAT, DHCP, AAA, and SSH. If you are ready now, proceed to that lab. If not, save you configurations to load into the next lab.

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)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
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.