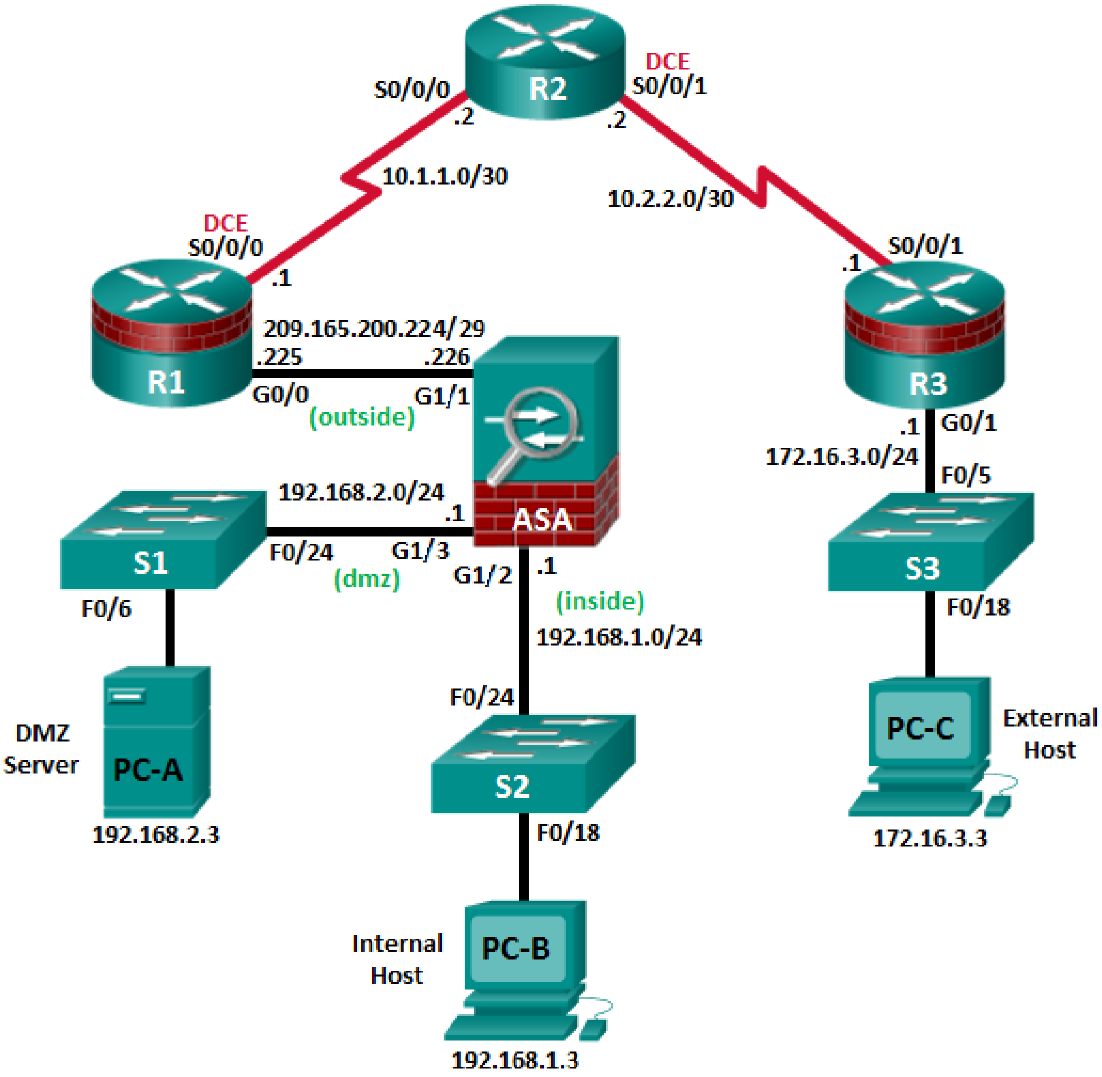
CCNA Security

Chapter 10 - Configure ASA Basic Settings and Firewall using ASDM

This lab has been updated for use on NETLAB+

Topology



Note: ISR G1 devices use FastEthernet interfaces instead of GigabitEthernet interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA G1/1
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	VLAN 1 G1/2	192.168.1.1	255.255.255.0	NA	S2 F0/24
	G1/1	209.165.200.226	255.255.255.248	NA	R1 G0/0
	VLAN 3 G1/3	192.168.2.1	255.255.255.0	NA	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

- Configure basic settings for routers and switches.
- Configure static routing, including default routes, between R1, R2, and R3.
- Enable the HTTP server on R1 and set the enable and VTY passwords.
- Configure PC host IP settings.
- Verify connectivity.

Part 2: Access the ASA Console and ASDM

- Access the ASA console and view hardware, software, and configuration settings.
- Clear previous ASA configuration settings.
- Bypass Setup mode and configure the ASDM VLAN interfaces.
- Configure ASDM and verify access to the ASA.
- Access ASDM and explore the GUI.

Part 3: Configure ASA Settings and Firewall Using the ASDM Startup Wizard

- Access the Configuration menu and launch the Startup wizard.
- Configure the hostname, domain name, and enable the password.
- Configure the inside and outside VLAN interfaces.
- Configure DHCP, address translation, and administrative access.
- Review the summary and deliver the commands to the ASA.
- Test access to an external website from PC-B.

- Test access to an external website using the ASDM Packet Tracer utility.

Part 4: Configure ASA Settings from the ASDM Configuration Menu

- Set the ASA date and time.
- Configure a static default route for the ASA.
- Configure AAA user authentication using the local ASA database.
- Test SSH access to the ASA.
- Test connectivity using ASDM Ping and Traceroute.
- Modify the MPF application inspection policy.

Part 5: Configure DMZ, Static NAT, and ACLs

- Configure the ASA DMZ VLAN 3 interface.
- Configure the DMZ server and static NAT.
- View the DMZ Access Rule generated by ASDM.
- Test access to the DMZ server from the outside network.

Background/Scenario

The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall, a VPN, and other capabilities. This lab employs an ASA 5506 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 with limited access to the DMZ and no access to internal resources. Inside users can access the DMZ and outside resources.

The focus of this lab is the configuration of the ASA as a basic firewall. Other devices will receive minimal configuration to support the ASA portion of the lab. This lab uses the ASA GUI interface ASDM 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 prepare the ASA for Adaptive Security Device Manager (ASDM) access. In Part 3, you will use the ASDM Startup wizard to configure basic ASA settings and the firewall between the inside and outside networks. In Part 4, you will configure additional settings via the ASDM configuration menu. In Part 5, you will configure a DMZ on the ASA and provide access to a server in the DMZ.

Your company has one location connected to an ISP. R1 represents a customer-premise equipment (CPE) device managed by the ISP. R2 represents an intermediate Internet router. R3 connects an administrator from a network management company, who has been hired to remotely manage your network. The ASA is an edge security device that connects the internal corporate network and DMZ to the ISP while providing NAT and DHCP services to inside hosts. The ASA will be configured for management by an administrator on the internal network and the remote administrator. Layer 3 VLAN interfaces provide access to the three areas created in the lab: Inside, Outside, and DMZ. The ISP has assigned the public IP address space of 209.165.200.224/29, which will be used for address translation on the ASA.

Note: The router commands and output in this lab are from a Cisco 1941 router with Cisco IOS Release 15.4(3)M2 (with a Security Technology Package license). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and the output produced might vary from what is shown in this lab.

The ASA used with this lab is a Cisco model 5506 with an 8-port integrated router, running OS version 9.8(1), Adaptive Security Device Manager (ASDM) version 7.8(1), and comes with a Base license.

Part 1: Configure Basic Device Settings

In Part 1, 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: Configure basic settings for routers and switches.

a. Configure hostnames, as shown in the topology, for each router.

b. Configure router interface IP addresses, as shown in the IP Addressing table.

c. Configure a clock rate for routers with a DCE serial cable attached to the serial interface. R1 is shown here as an example.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 128000
```

d. Configure the hostname for the switches. With the exception of the hostname, the switches can be left in their default configuration state. Configuring the VLAN management IP address for the switches is optional.

Step 2: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

b. Configure a static route from R2 to the R1 Fa0/0 subnet (connected to ASA interface E0/0) and a static route from R2 to the R3 LAN.

```
R2(config)# ip route 209.165.200.224 255.255.255.248 10.1.1.1
R2(config)# ip route 172.16.3.0 255.255.255.0 10.2.2.1
```

Step 3: Configure and encrypt passwords on R1.

Note: Passwords in this task are set to a minimum of 10 characters and are relatively simple for the purposes of performing the lab. More complex passwords are recommended in a production network.

a. Configure a minimum password length. Use the **security passwords** command to set a minimum password length of 10 characters.

b. Configure the enable secret password on both routers with a password of **cisco12345**. Use the type 9 (SCRYPT) hashing algorithm.

c. Create a local **admin01** account using **admin01pass** for the password. Use the type 9 (SCRYPT) hashing algorithm and set privilege level to 15

d. Configure the Console and VTY lines to use the local database for login. For additional security, configure the lines to log out after five minutes of inactivity. Issue the **logging synchronous** command to prevent console messages from interrupting command entry.

e. Enable HTTP server access on R1. Use the local database for HTTP authentication.

Note: HTTP server access will be used to demonstrate ASDM tools in Part 3.

Step 4: Configure PC host IP settings.

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 5: Verify connectivity.

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

Note: If you can ping from PC-C to R1 G0/0 and S0/0/0, you have demonstrated that addressing has been configured properly, and static routing is configured and functioning correctly.

Step 6: Save the basic running configuration for each router and switch.

Part 2: Access the ASA Console and ASDM

In Part 2, you will access the ASA via the console and use various **show** commands to determine hardware, software, and configuration settings. You will prepare the ASA for ASDM access and explore ASDM screens and options.

Step 1: Access the ASA console.

a. If prompted to enter Interactive Firewall configuration (Setup mode), answer **No**.

b. Enter privileged mode with the **enable** command and password (if set). The password is blank by default, so press **Enter**. If the password has been changed to one that is specific to this lab, enter the password **cisco12345**. The default ASA hostname and prompt is **ciscoasa>**.

```
ciscoasa> enable
Password: cisco12345 (or press Enter if no password is set)
```

Step 2: Clear previous ASA configuration settings.

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

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm]
[OK]
ciscoasa#

ciscoasa# show start
No Configuration
```

Note: The **erase startup-config** IOS command 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 you see the message: "`System config has been modified. Save? [Y]es/[N]o:`" Type **N** and then press **Enter**.

```
CCNAS-ASA# reload
Proceed with reload? [confirm]
CCNAS-ASA#

***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
*** --- SHUTDOWN NOW ---
Process shutdown finished
```

Step 3: Bypass Setup mode and configure the ASDM VLAN interfaces.

When the ASA completes the reload process, it should detect that the **startup-config** file is missing and present a series of interactive prompts to configure basic ASA settings. If it does not come up in this mode, repeat Step 2.

a. When prompted to pre-configure the firewall through interactive prompts (Setup mode), respond with **no**.

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

b. Enter privileged EXEC mode with the **enable** command. The password should be blank (no password) at this point.

c. Enter global configuration mode using the **conf t** command. The first time you enter configuration mode after reloading, you will be prompted to enable anonymous reporting. Respond with **no**.

d. Configure the inside interface Gi1/2 to prepare for ASDM access. The Security Level should be automatically set to the highest level of **100**. The Gi1/2l interface will be used by PC-B to access ASDM on the ASA.

```
ciscoasa(config)# interface gi1/2
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# exit
```

PC-B is connected to switch S2. Switch S2 is connected to ASA port Gi1/2. Why is it unnecessary to add physical interface Gi1/2 to a VLAN?

____

____

ASA 5506 interface notes:

The 5506 is different from the 5505 series ASA model. Like a Cisco router, the 5506 ASA physical ports can be directly assigned a Layer 3 IP address. The ASA 5505 has eight integrated switch ports that are Layer 2 ports.

By default, all ASA physical interfaces are administratively down unless the Setup utility has been run, or the factory defaults have been reset. Use the **show interface ip brief** command to verify this.

```
ciscoasa# show interface ip brief
Interface                  IP-Address      OK? Method Status
Protocol
Virtual0                   127.1.0.1       YES unset  up
up
GigabitEthernet1/1         unassigned      YES unset  administratively down
down
GigabitEthernet1/2         192.168.1.1     YES manual administratively down
down
```

```
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        127.0.1.1       YES unset  up
up
Internal-Data1/1           unassigned      YES unset  down
up
Internal-Data1/2           unassigned      YES unset  up
up
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
up
```

e. Enable the Gi1/2 interface using the **no shutdown** command and verify the interface status. The status and protocol for interface Gi1/2 should be up/up.

```
ciscoasa(config)# interface Gi1/2
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit



ciscoasa# show interface ip brief
Interface                  IP-Address      OK? Method Status
Protocol
Virtual0                   127.1.0.1       YES unset  up
up
GigabitEthernet1/1         unassigned      YES unset  administratively down
down
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        127.0.1.1       YES unset  up
up
Internal-Data1/1           unassigned      YES unset  down
up
Internal-Data1/2           unassigned      YES unset  up
up
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
up
```

f. Pre-configure outside interface Gi1/1and bring up the interface. You will assign the IP address using ASDM.

```
ciscoasa(config)# interface Gi1/1
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
```

g. Test connectivity to the ASA by pinging from PC-B to ASA interface Gi1/2 IP address **192.168.1.1**. The pings should be successful.

Step 4: Configure ASDM and verify access to the ASA.

a. Configure the ASA to accept HTTPS connections by using the **http** command to allow access to ASDM from any host on the inside network 192.168.1.0/24.

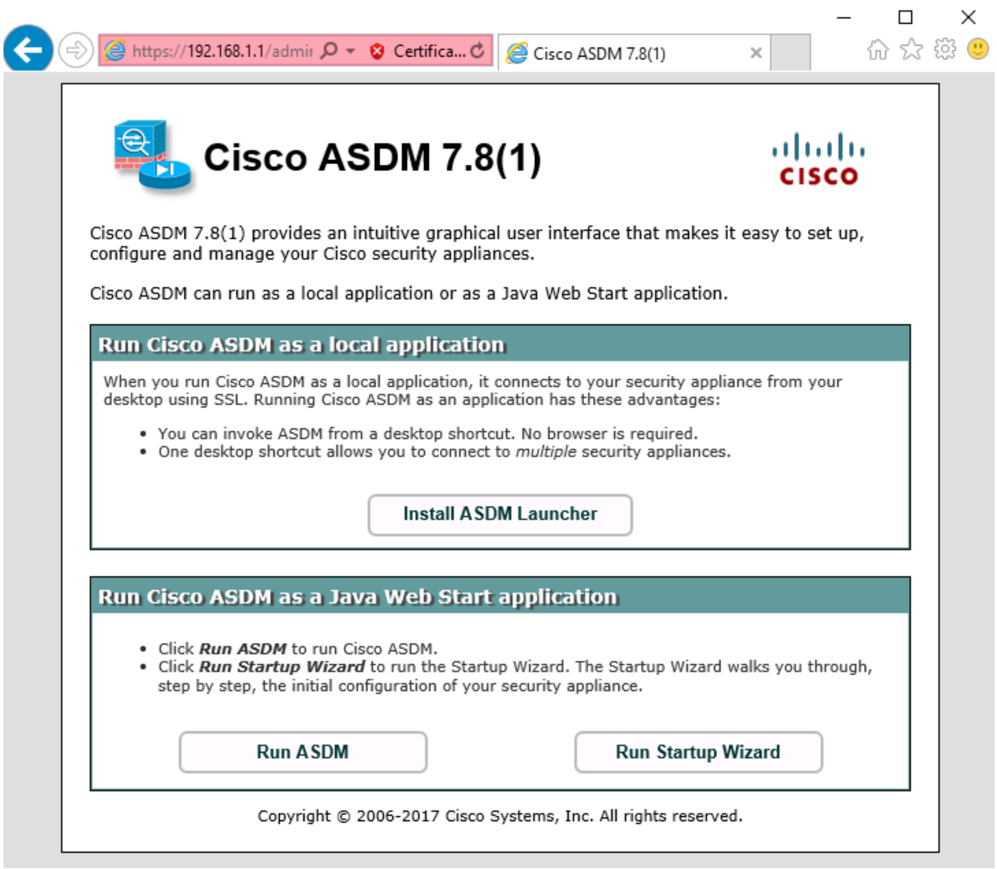
```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

b. Open a browser on PC-B and test the HTTPS access to the ASA by entering **https://192.168.1.1**.

Note: Be sure to specify the HTTPS protocol in the URL.

Step 5: Access ASDM and explore the GUI.

a. After entering the URL above, you should see a security warning about the website security certificate. Click **Continue to this website**. The ASDM Welcome page will display. From this screen, you can run ASDM as a local application on the PC (installs ASDM on the PC), run ASDM as a browser-based Java applet directly from the ASA, or run the Startup wizard.



Cisco ASDM 7.8(1)

Cisco ASDM 7.8(1) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

Run Cisco ASDM as a Java Web Start application

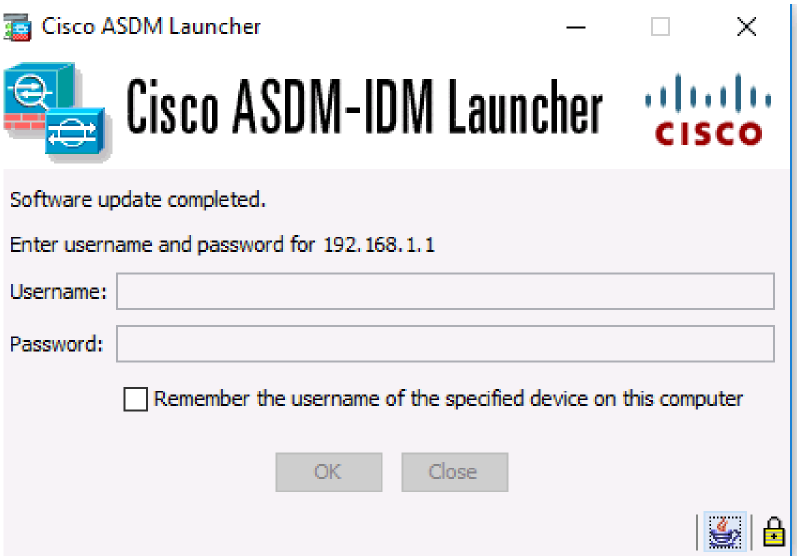
- Click ***Run ASDM*** to run Cisco ASDM.
- Click ***Run Startup Wizard*** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

Copyright © 2006-2017 Cisco Systems, Inc. All rights reserved.

b. Click **Run ASDM**.

c. Click **Yes/Continue/Run** in response to any other security warnings.

d. You should see the **Cisco ASDM-IDM Launcher** dialog box within which you can enter a username and password. Leave these fields **blank** and click **OK** as they have not yet been configured.



Software update completed.

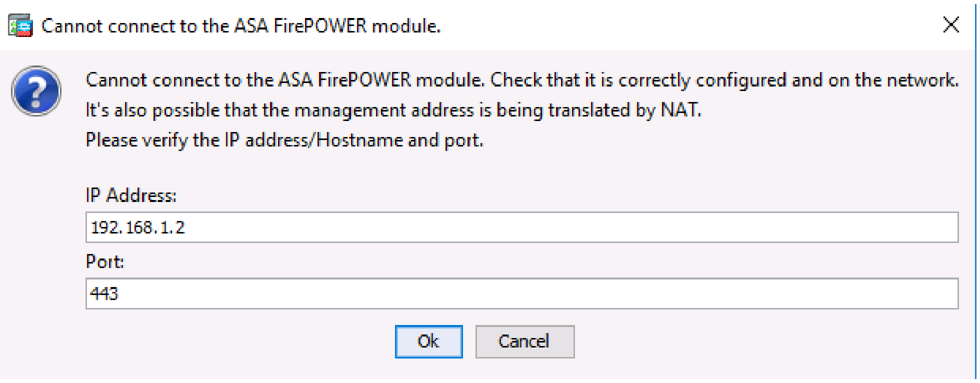
Enter username and password for 192.168.1.1

Username:

Password:

□ Remember the username of the specified device on this computer

e. Click **OK** to continue. ASDM will load the current configuration into the GUI.



Cannot connect to the ASA FirePOWER module.

Cannot connect to the ASA FirePOWER module. Check that it is correctly configured and on the network.
It's also possible that the management address is being translated by NAT.
Please verify the IP address/Hostname and port.

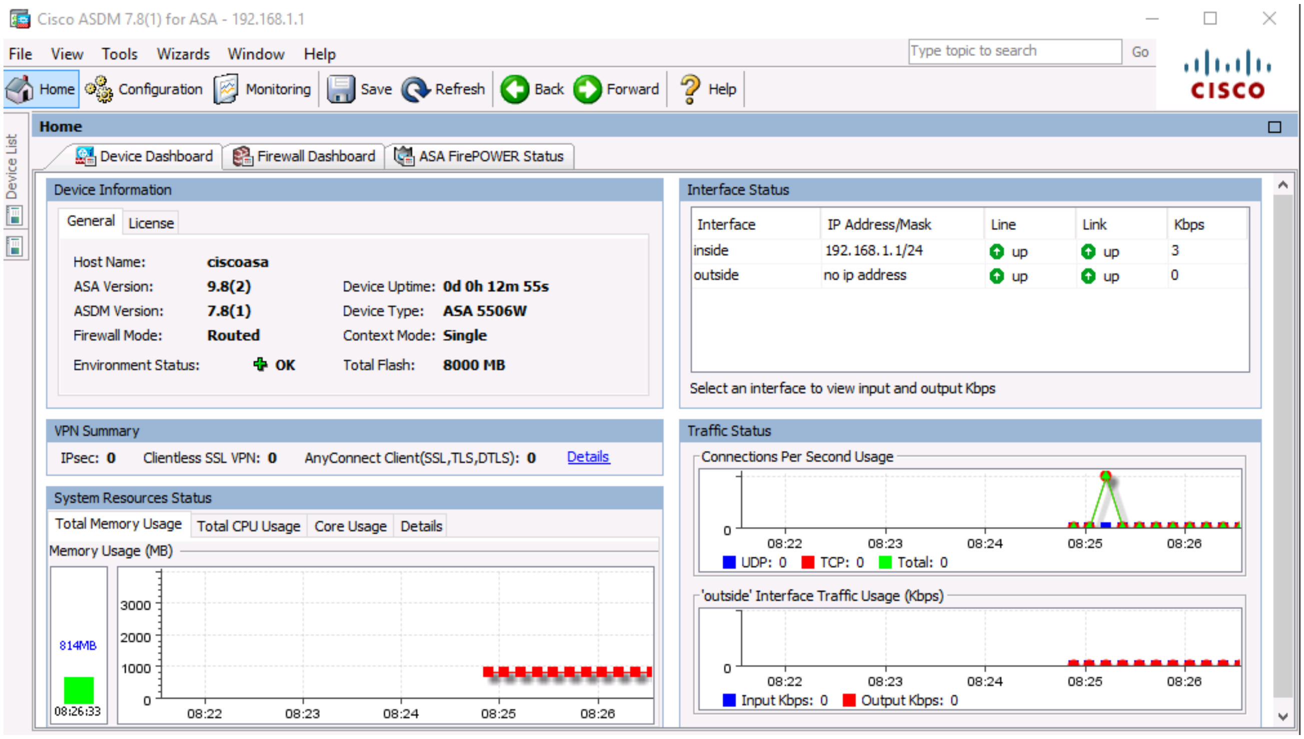
IP Address:
192.168.1.2

Port:
443

f. Click **Cancel** on the “**Cannot Connect**” FirePOWER module window to continue.

g. The initial GUI screen is displayed with various areas and options. The menu at the top left of the screen contains three main sections: Home, Configuration, and Monitoring. The Home section is the default and has three dashboards: Device,Firewall, and ASA FirewPOWER status. The Device dashboard is the default screen and shows device information, such as Type (ASA 5506), ASA and ASDM version, the amount of memory, and firewall mode (routed). There are five areas on the Device dashboard:

- Device Information
- Interface Status
- VPN Summary
- System Resources Status
- Traffic Status



Cisco ASDM 7.8(1) for ASA - 192.168.1.1

Device Information

General License

Host Name: **ciscoasa**
ASA Version: **9.8(2)** Device Uptime: **0d 0h 12m 55s**
ASDM Version: **7.8(1)** Device Type: **ASA 5506W**
Firewall Mode: **Routed** Context Mode: **Single**
Environment Status: **OK** Total Flash: **8000 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	3
outside	no ip address	up	up	0

Select an interface to view input and output Kbps

VPN Summary

IPsec: **0** Clientless SSL VPN: **0** AnyConnect Client(SSL,TLS,DTLS): **0** Details

System Resources Status

Traffic Status

h. Click the **Configuration** and **Monitoring** buttons to become familiar with their layout and to see what options are available.

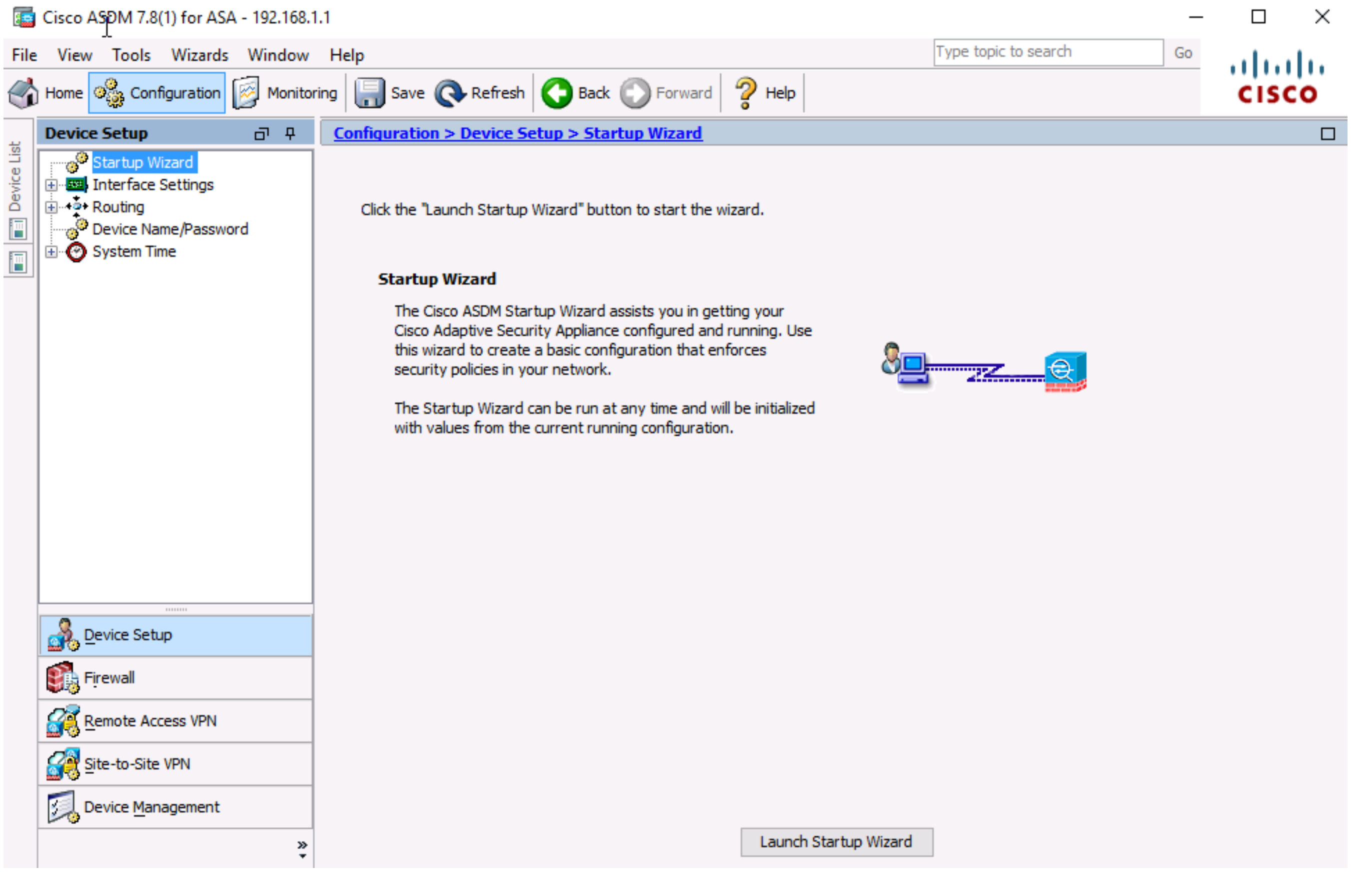
Part 3: Configure Basic ASA Settings and Firewall Using the ASDM Startup Wizard

Step 1: Access the Configuration menu and launch the Startup wizard.

a. On the menu bar, click **Configuration.** There are five main configuration areas:

- Device Setup
- Firewall
- Remote Access VPN
- Site-to-Site VPN
- Device Management

b. The Device Setup Startup wizard is the first option available and displays by default. Read through the on-screen text describing the Startup wizard, and then click **Launch Startup Wizard**.



Click the "Launch Startup Wizard" button to start the wizard.

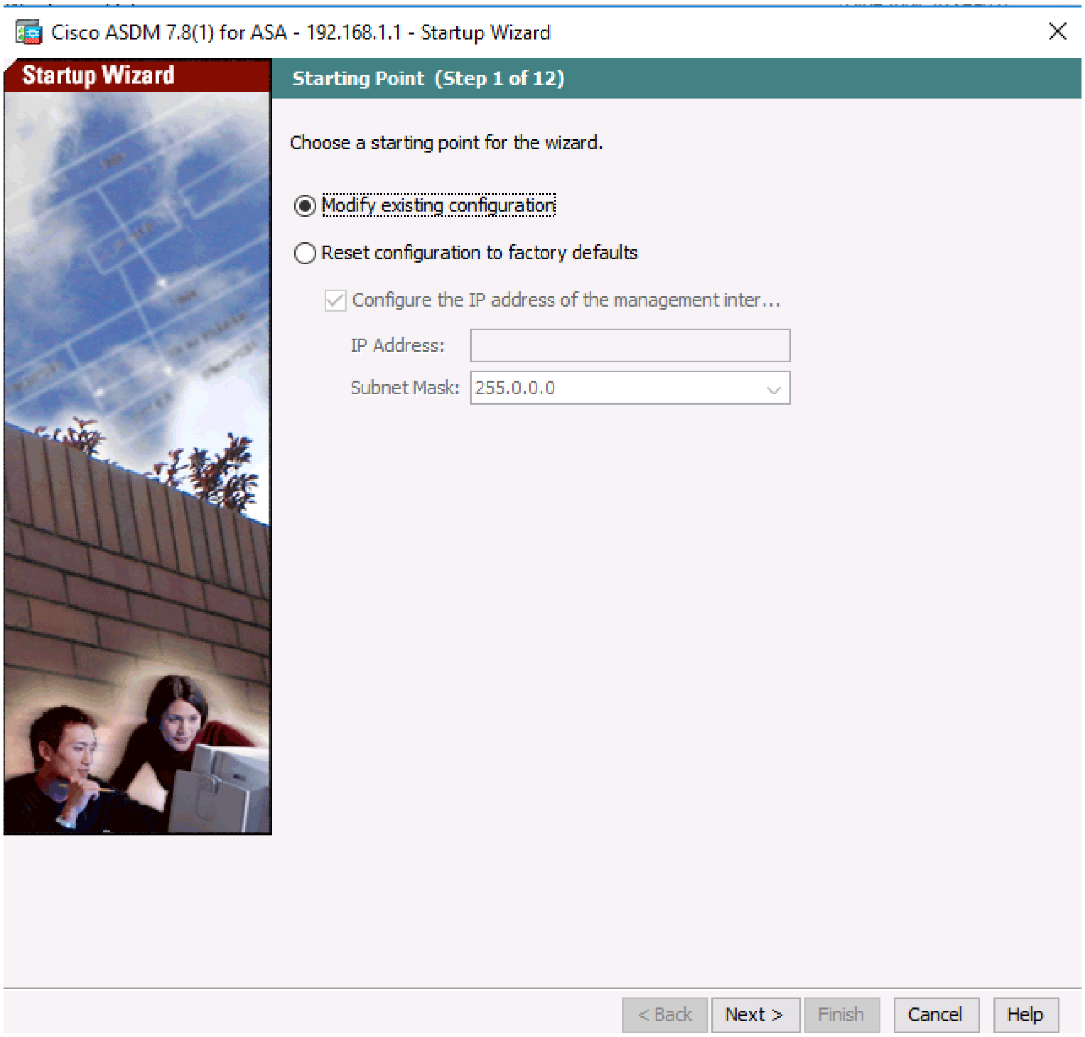
Startup Wizard

The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

Step 2: Configure hostname, domain name, and the enable password.

a. On the first Startup Wizard screen, modify the existing configuration or reset the ASA to the factory defaults. Ensure that the **Modify Existing Configuration** option is selected, and click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Starting Point (Step 1 of 12)

Choose a starting point for the wizard.

● Modify existing configuration

○ Reset configuration to factory defaults

☑ Configure the IP address of the management inter...

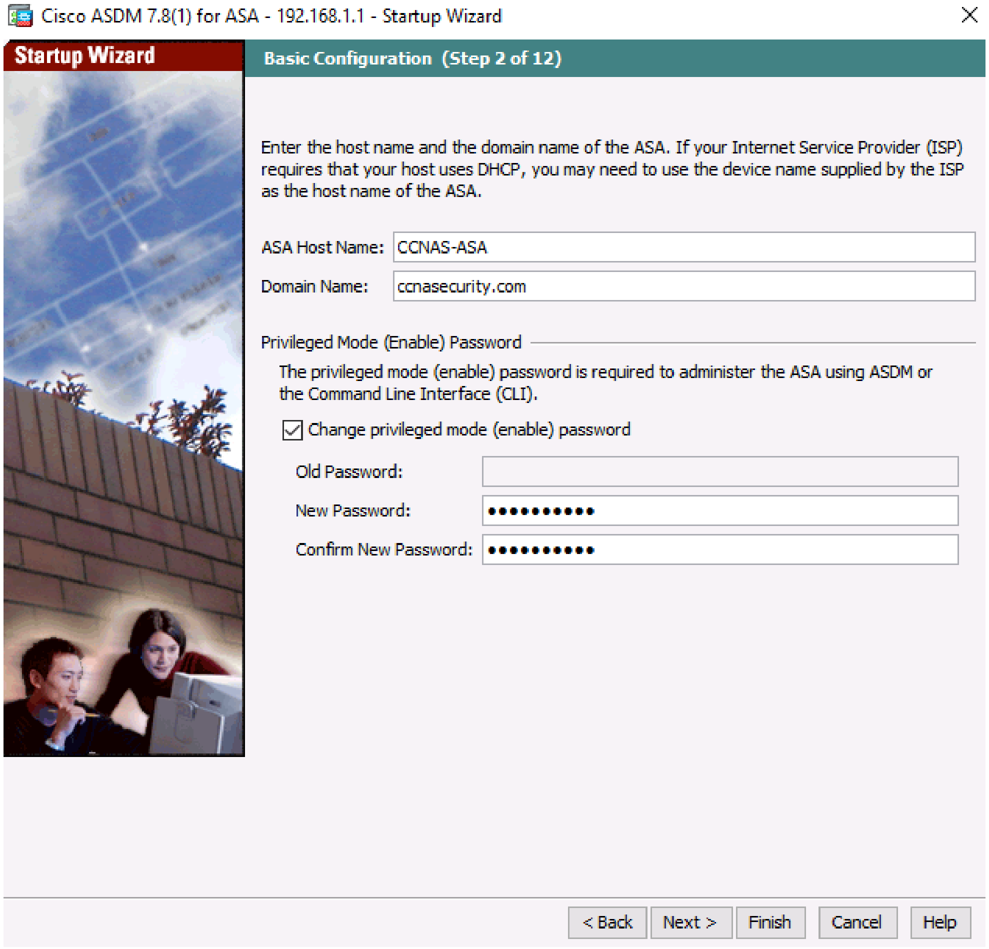
IP Address:

Subnet Mask: 255.0.0.0

b. On the Startup Wizard Step 2 screen, configure the ASA hostname **CCNAS-ASA** and domain name **ccnasecurity.com**.

c. Click the check box for changing the enable mode password, change it from blank (no password) to **cisco12345**, and enter it again to confirm.

d. When the entries are completed, click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Basic Configuration (Step 2 of 12)

Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.

ASA Host Name: CCNAS-ASA

Domain Name: ccnasecurity.com

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).

☑ Change privileged mode (enable) password

Old Password:

New Password: ●●●●●●●●●●

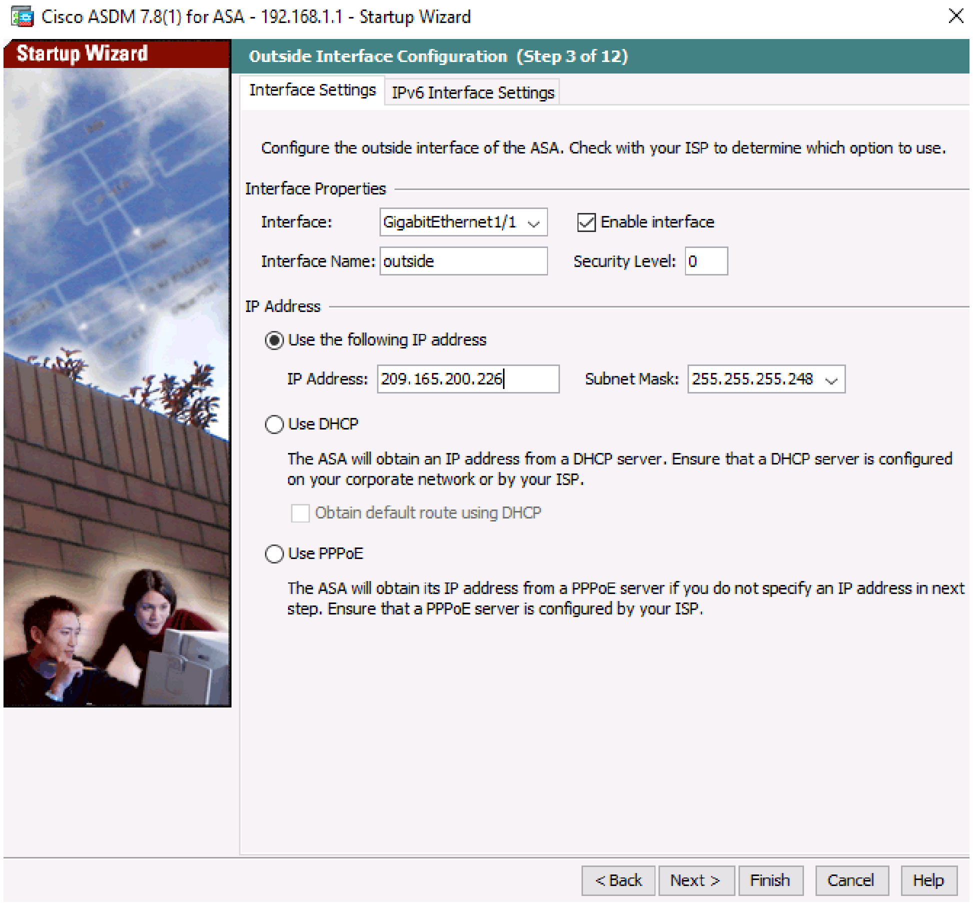
Confirm New Password: ●●●●●●●●●●

Step 3: Configure the inside and outside interfaces.

a. On the Startup Wizard Step 3 screen for the Outside and Inside Interfaces, do not change the current settings because these were previously defined using the CLI.
The inside Gi1/2 interface is named **inside,** and the security level is set to 100 (highest).
The Outside interface Gi1/1 is named **outside,** and the security level is set to 0 (lowest).

b. Enter an Outside IP Address of **209.165.200.226** and a Mask of **255.255.255.248**. You can use the pull-down menu to select the mask.
Leave the inside interface IP address as **192.168.1.1** with a mask of **255.255.255.0**.

c. Click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Outside Interface Configuration (Step 3 of 12)

Configure the outside interface of the ASA. Check with your ISP to determine which option to use.

Interface Properties

Interface: GigabitEthernet1/1 ☑ Enable interface

Interface Name: outside Security Level: 0

IP Address

● Use the following IP address

IP Address: 209.165.200.226 Subnet Mask: 255.255.255.248

○ Use DHCP

The ASA will obtain an IP address from a DHCP server. Ensure that a DHCP server is configured on your corporate network or by your ISP.

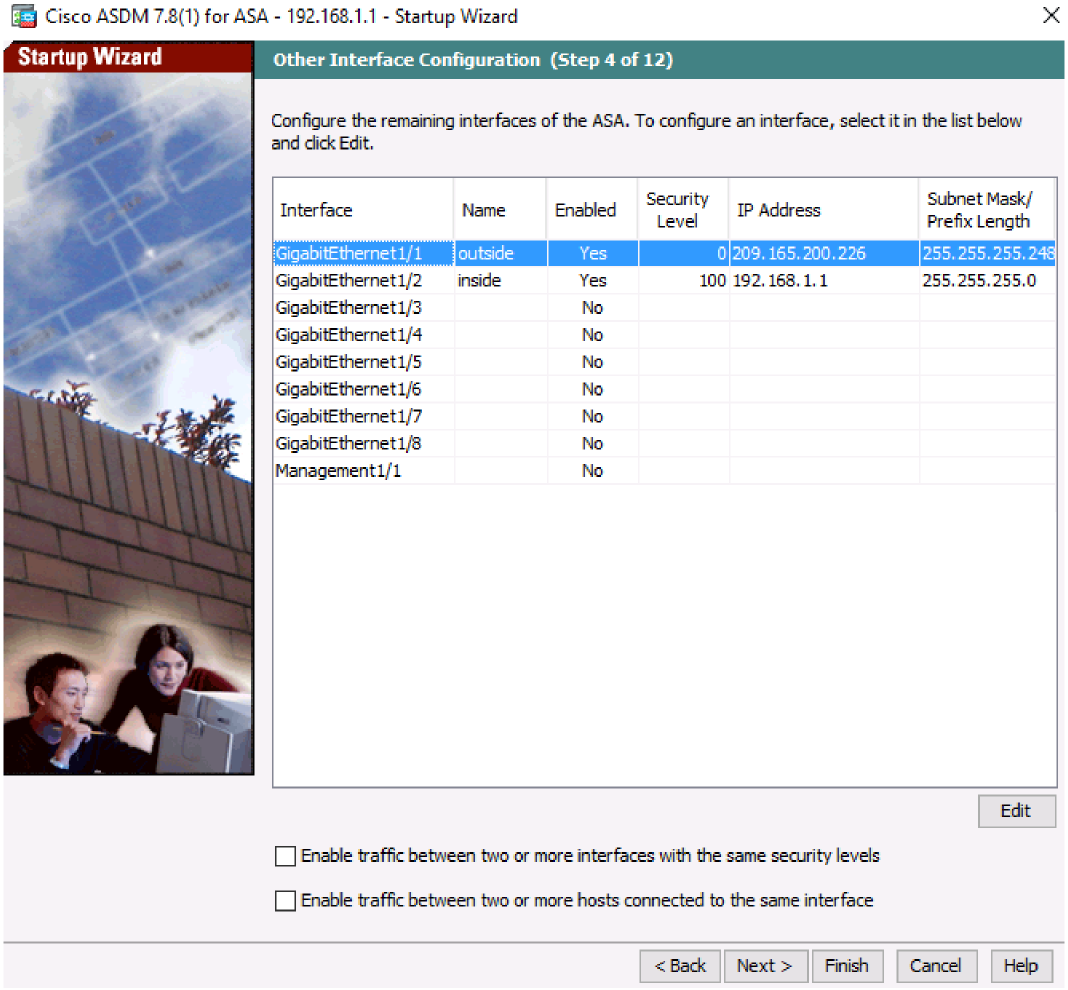
□ Obtain default route using DHCP

○ Use PPPoE

The ASA will obtain its IP address from a PPPoE server if you do not specify an IP address in next step. Ensure that a PPPoE server is configured by your ISP.

Step 4: Configure Other Interface Configurations.

a. On the Startup Wizard Step 4 screen – view the current ASA 5506 interface configurations. Click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Other Interface Configuration (Step 4 of 12)

Configure the remaining interfaces of the ASA. To configure an interface, select it in the list below and click Edit.

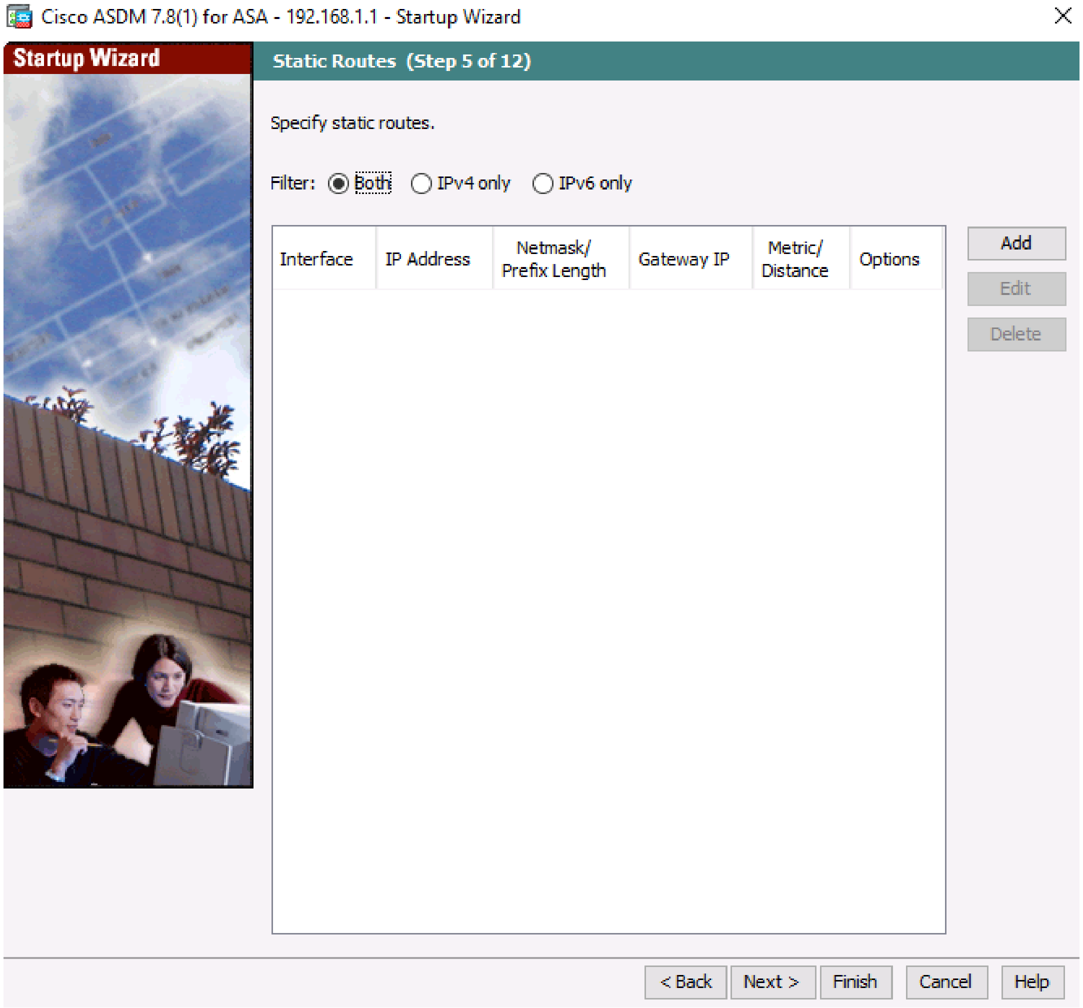
Interface	Name	Enabled	Security Level	IP Address	Subnet Mask/ Prefix Length
GigabitEthernet1/1	outside	Yes	0	209.165.200.226	255.255.255.248
GigabitEthernet1/2	inside	Yes	100	192.168.1.1	255.255.255.0
GigabitEthernet1/3		No			
GigabitEthernet1/4		No			
GigabitEthernet1/5		No			
GigabitEthernet1/6		No			
GigabitEthernet1/7		No			
GigabitEthernet1/8		No			
Management1/1		No			

□ Enable traffic between two or more interfaces with the same security levels

□ Enable traffic between two or more hosts connected to the same interface

Step 5: View Static Routes

a. On the Startup Wizard Step 5 screen – view the configuration screen for IPv4 and IPv6 Static Routes. Click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Static Routes (Step 5 of 12)

Specify static routes.

Filter: ● Both ○ IPv4 only ○ IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options

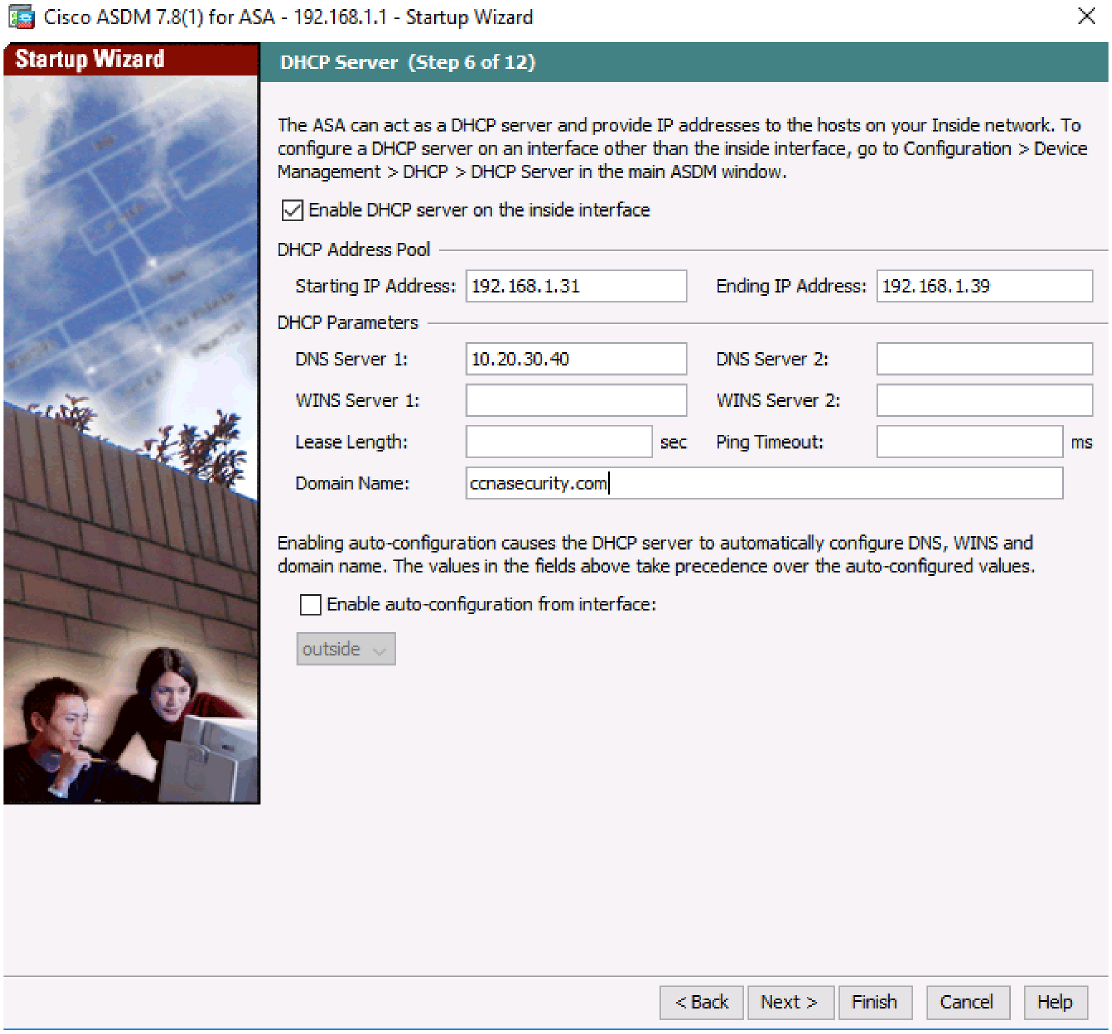
Step 6: Configure DHCP, address translation, and administrative access.

a. On the Startup Wizard Step 6 screen – DHCP Server, click the **Enable DHCP server on the inside interface** check box.

b. Enter a Starting IP Address of **192.168.1.31** and an Ending IP Address of **192.168.1.39**.

c. Enter the DNS Server 1 address of **10.20.30.40** and the Domain Name **ccnasecurity.com**. Do **NOT** check the box to enable auto-configuration from interface.

d. Click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

DHCP Server (Step 6 of 12)

The ASA can act as a DHCP server and provide IP addresses to the hosts on your Inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

☑ Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 192.168.1.31 Ending IP Address: 192.168.1.39

DHCP Parameters

DNS Server 1: 10.20.30.40 DNS Server 2:

WINS Server 1: WINS Server 2:

Lease Length: sec Ping Timeout: ms

Domain Name: ccnasecurity.com

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

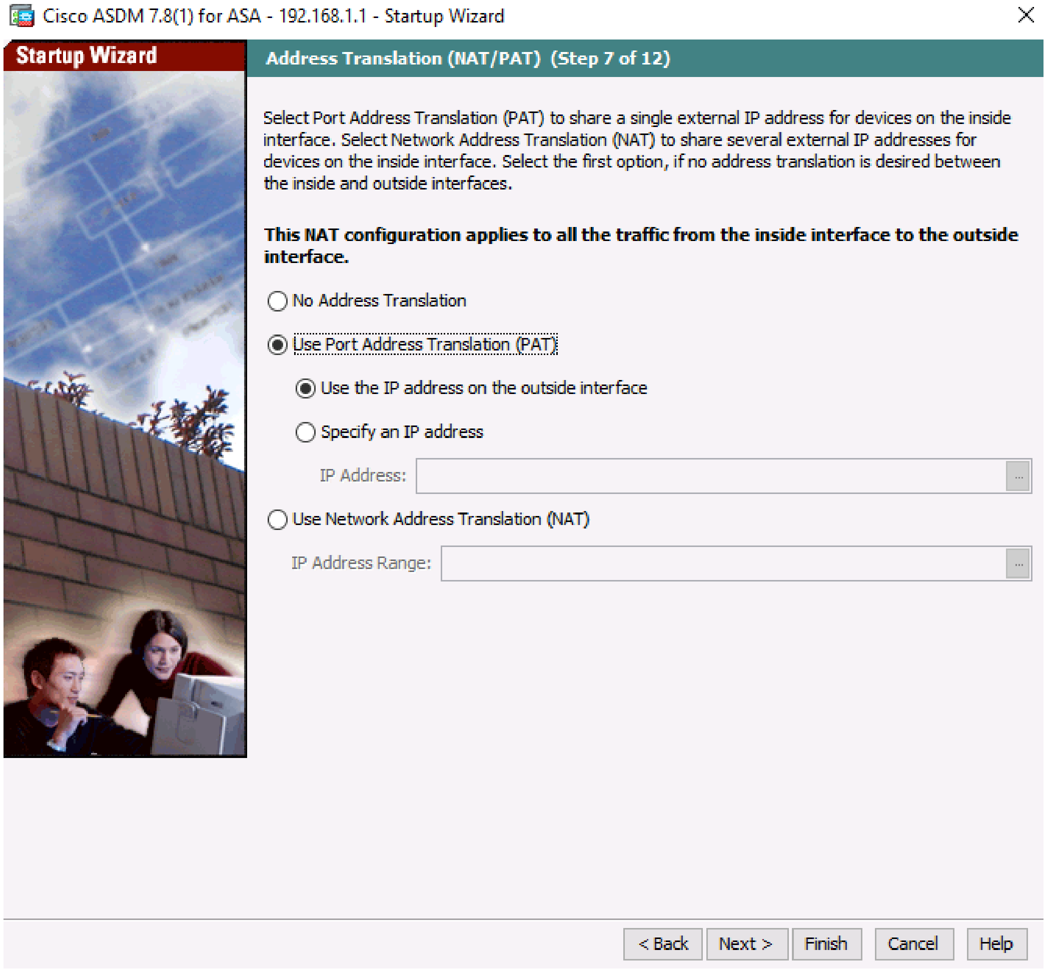
☐ Enable auto-configuration from interface:

outside

e. On the **Startup Wizard Step 7 of 12– Address Translation (NAT/PAT)**

Click **Use Port Address Translation (PAT)**.
The default is to use the IP address of the outside interface.

Note: You can also specify a particular IP address for PAT or a range of addresses with NAT.
Click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Address Translation (NAT/PAT) (Step 7 of 12)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

This NAT configuration applies to all the traffic from the inside interface to the outside interface.

○ No Address Translation

● Use Port Address Translation (PAT)

● Use the IP address on the outside interface

○ Specify an IP address

IP Address:

○ Use Network Address Translation (NAT)

IP Address Range:

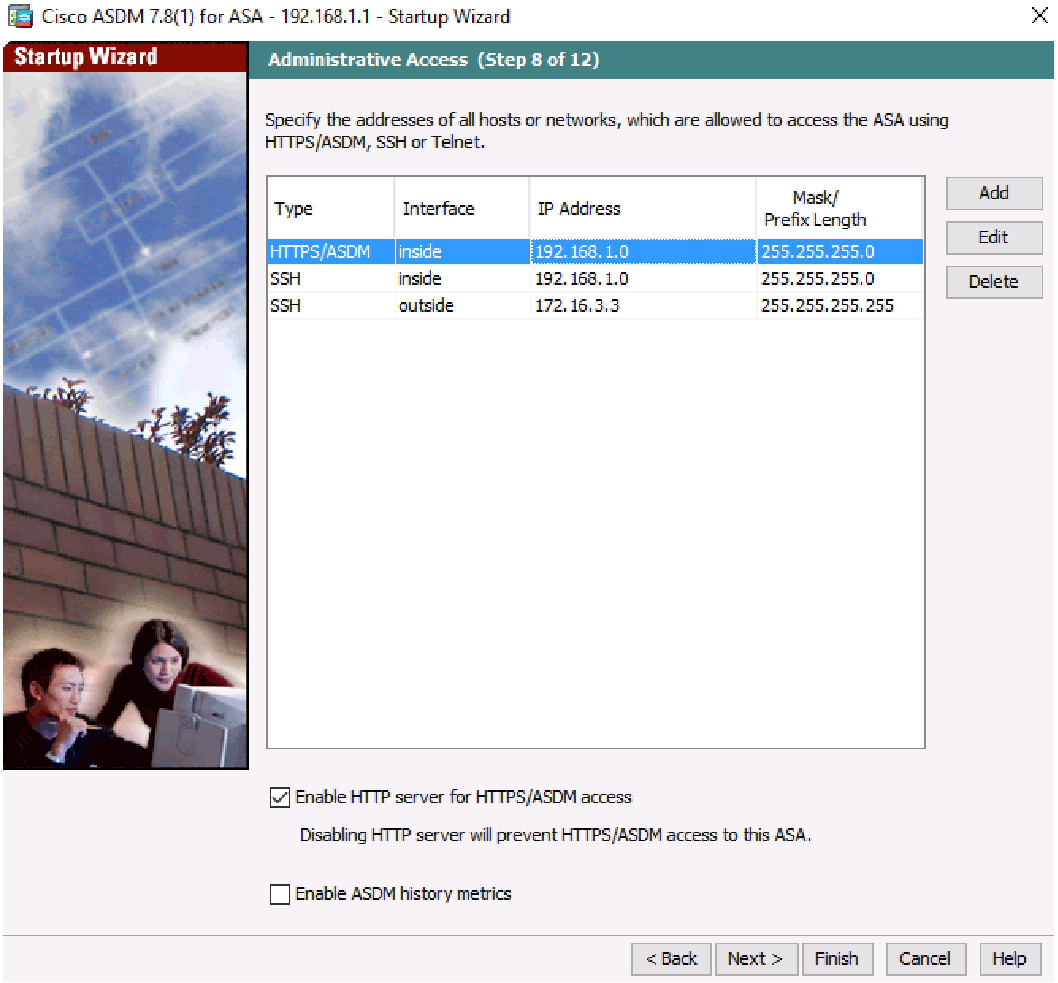
f. On the **Startup Wizard Step 8 of 12– Administrative Access**, HTTPS/ASDM access is currently configured for hosts on the inside network 192.168.1.0/24.

-Add **SSH** access to the ASA for the inside network **192.168.1.0** with a subnet mask of **255.255.255.0**.

-Add **SSH** access to the ASA from host **172.16.3.3** on the outside network.

-Ensure that the **Enable HTTP server for HTTPS/ASDM access** check box is selected.

-Click **Next** to continue.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Administrative Access (Step 8 of 12)

Specify the addresses of all hosts or networks, which are allowed to access the ASA using HTTPS/ASDM, SSH or Telnet.

Type	Interface	IP Address	Mask/ Prefix Length
HTTPS/ASDM	inside	192.168.1.0	255.255.255.0
SSH	inside	192.168.1.0	255.255.255.0
SSH	outside	172.16.3.3	255.255.255.255

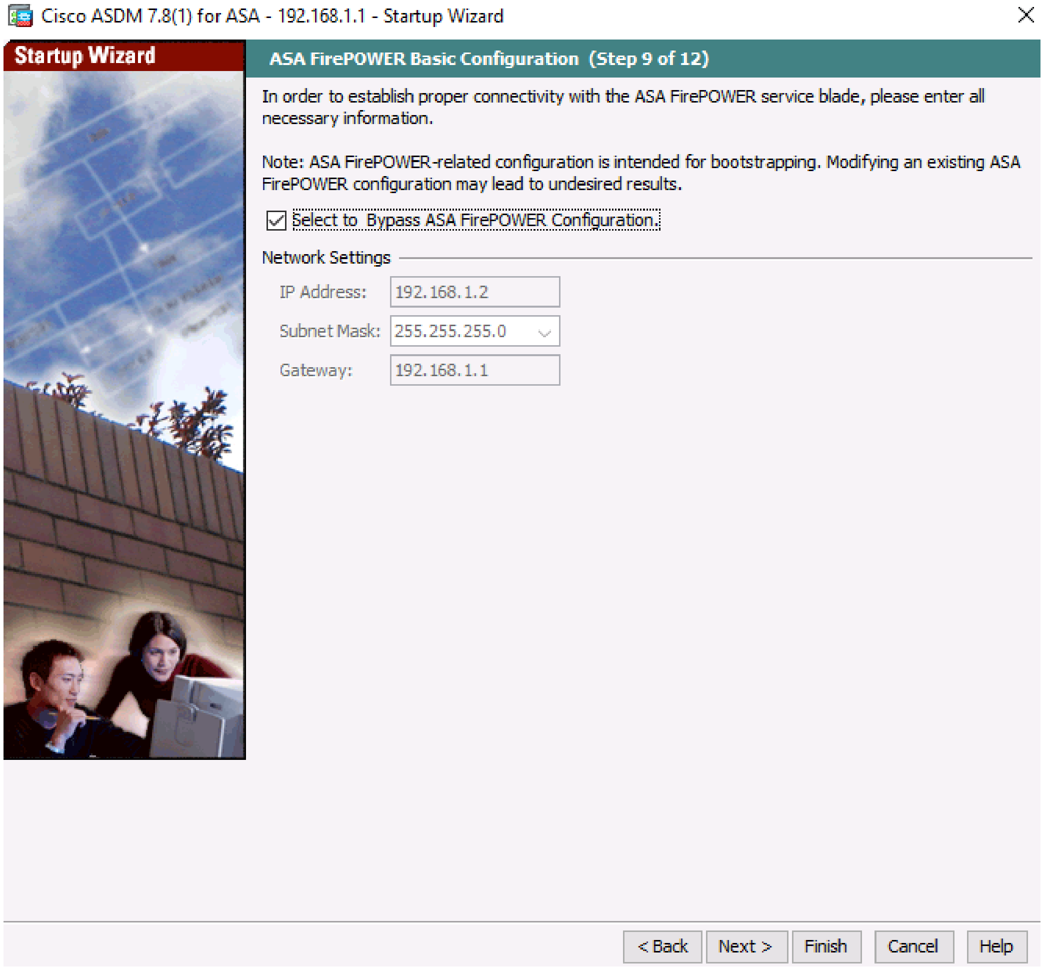
☑ Enable HTTP server for HTTPS/ASDM access

Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

☐ Enable ASDM history metrics

Step 7: Bypass the ASA FirePOWER Configuration

a. On the **Startup Wizard Step 9 of 12 – ASA FirePower Basic Configuration**, click the checkbox “Select to Bypass ASA FirePOWER Configuration and click **Next**.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

ASA FirePOWER Basic Configuration (Step 9 of 12)

In order to establish proper connectivity with the ASA FirePOWER service blade, please enter all necessary information.

Note: ASA FirePOWER-related configuration is intended for bootstrapping. Modifying an existing ASA FirePOWER configuration may lead to undesired results.

☑ Select to Bypass ASA FirePOWER Configuration.

Network Settings

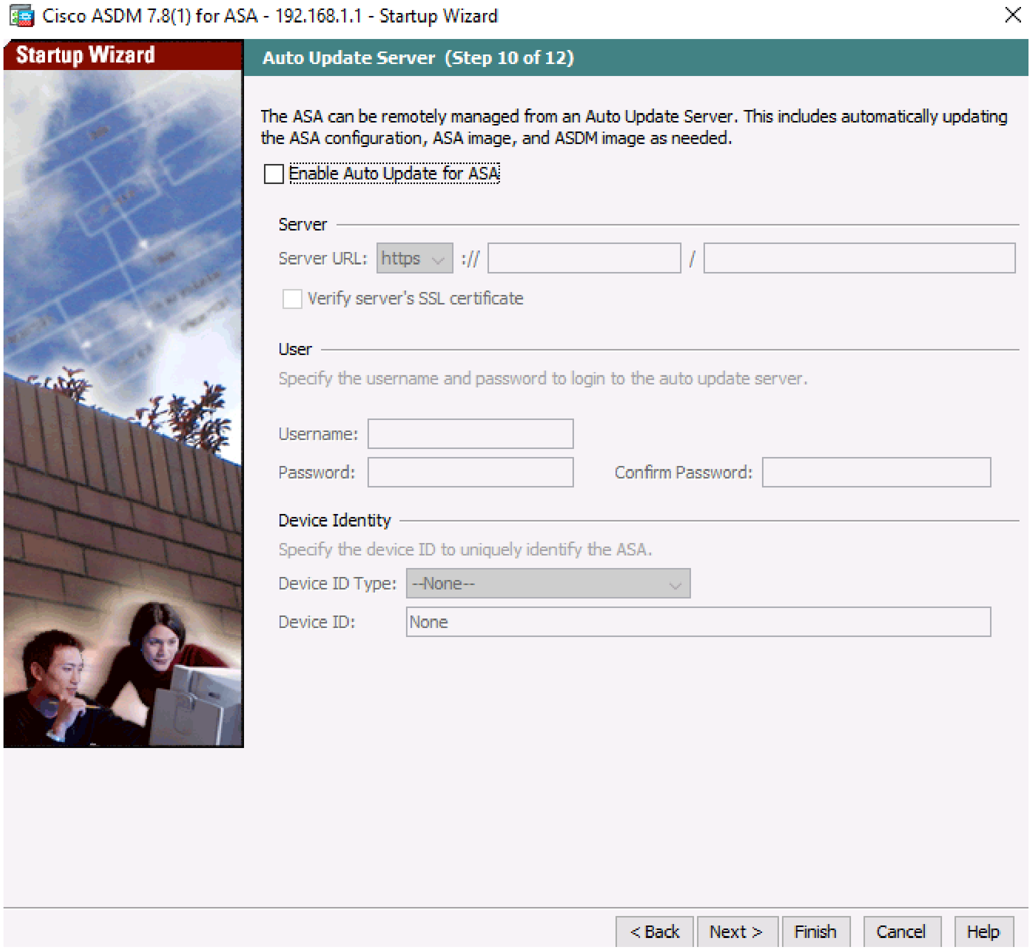
IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Step 8: View the Auto Update Server settings.

a. On the **Startup Wizard Step 10– Auto Update Server**, review the **options** and click **Next.** Do not modify any settings here.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard

Auto Update Server (Step 10 of 12)

The ASA can be remotely managed from an Auto Update Server. This includes automatically updating the ASA configuration, ASA image, and ASDM image as needed.

☐ Enable Auto Update for ASA

Server

Server URL: https :// /

☐ Verify server's SSL certificate

User

Specify the username and password to login to the auto update server.

Username:

Password: Confirm Password:

Device Identity

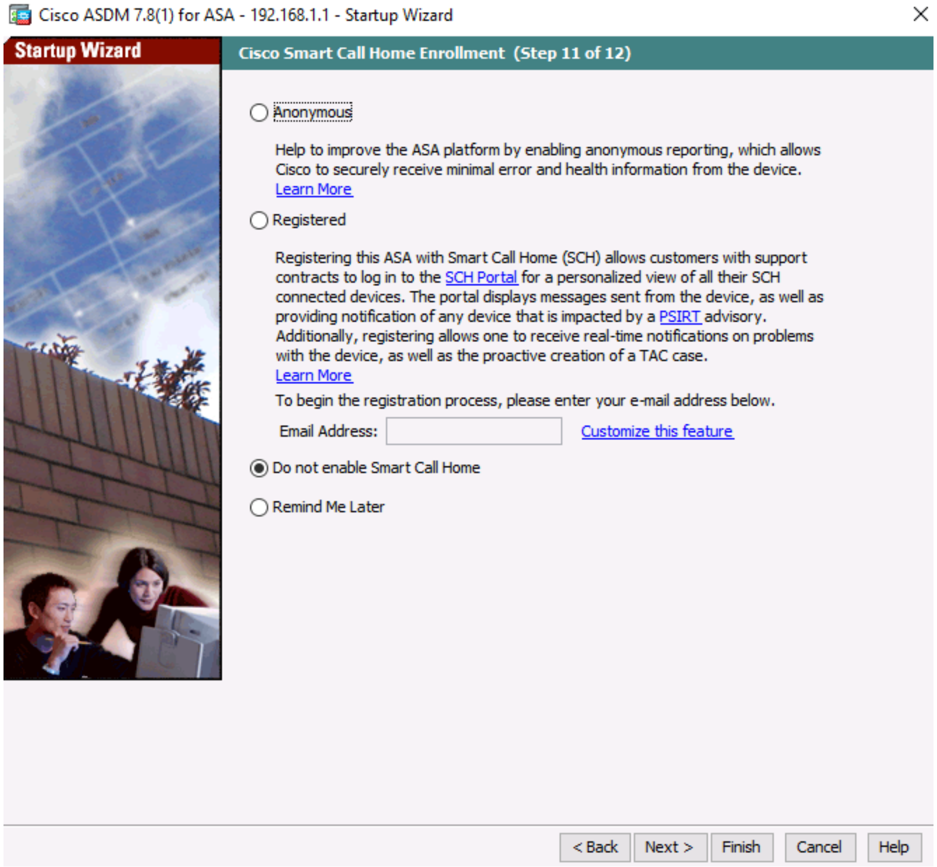
Specify the device ID to uniquely identify the ASA.

Device ID Type: --None--

Device ID: None

Step 9: Cisco Smart Call Home Enrollment

a. On the **Cisco Smart Call Home Enrollment Step 11**, review the **options** and click **Next.**
Do not modify any settings here.


Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Cisco Smart Call Home Enrollment (Step 11 of 12)

○ Anonymous

Help to improve the ASA platform by enabling anonymous reporting, which allows Cisco to securely receive minimal error and health information from the device.
Learn More

○ Registered

Registering this ASA with Smart Call Home (SCH) allows customers with support contracts to log in to the SCH Portal for a personalized view of all their SCH connected devices. The portal displays messages sent from the device, as well as providing notification of any device that is impacted by a PSIRT advisory. Additionally, registering allows one to receive real-time notifications on problems with the device, as well as the proactive creation of a TAC case.
Learn More

To begin the registration process, please enter your e-mail address below.

Email Address: Customize this feature

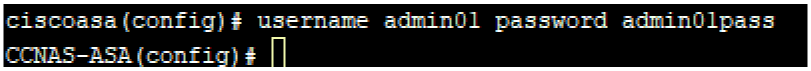
● Do not enable Smart Call Home

○ Remind Me Later

Step 10: Review the summary and deliver the commands to the ASA.

a. On the **Startup Wizard Step 12– Startup Wizard Summary**, review the **Configuration Summary** and click **Finish.**
ASDM will deliver the commands to the ASA device and then reload the modified configuration.

Note: If a GUI dialogue box appears requesting a username and password, go to the command line on the ASA and create a username of **admin01** with password **admin01pass**.
Use this to authenticate in the GUI dialogue box.

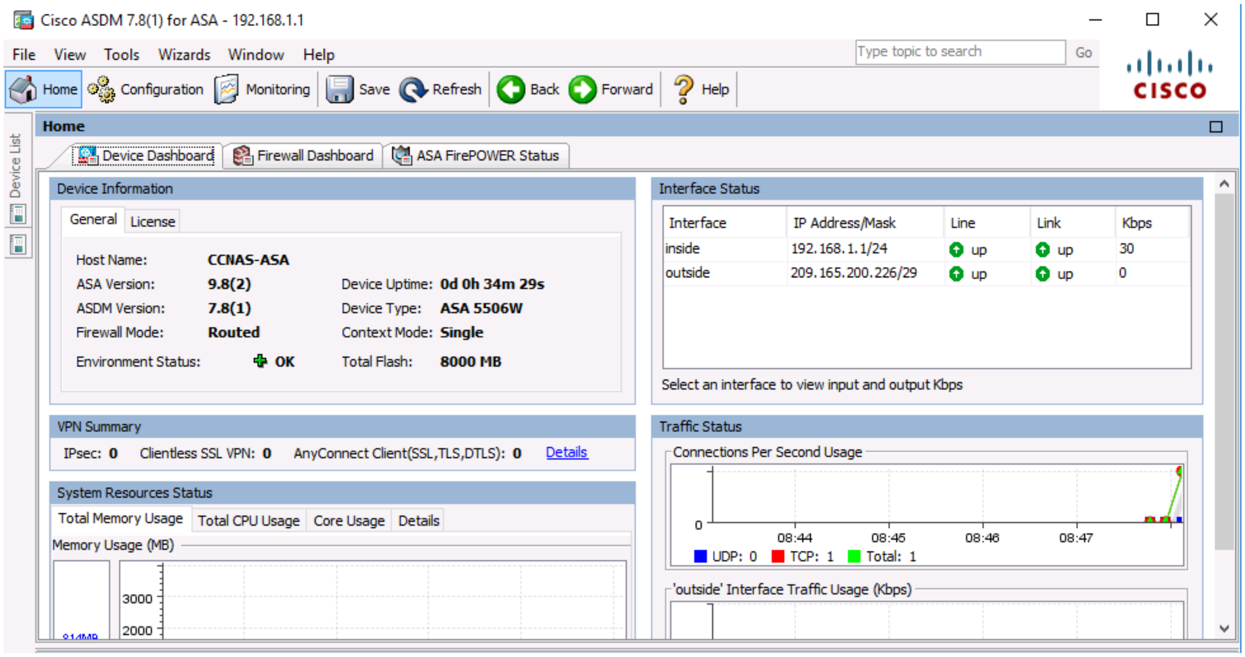


```
ciscoasa(config)# username admin01 password admin01pass
CCNAS-ASA(config)#
```

b. Close the ASDM and if asked, **save** the configuration.

c. Run ASDM again from the web browser on PC-B.
The new enable password is **cisco12345** with no username to access ASDM.

d. Return to the Device dashboard and check the Interface Status window.
You should see the inside and outside interfaces with IP address and status.
The inside interface should show a number of Kb/s.


Cisco ASDM 7.8(1) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device List
Device Dashboard Firewall Dashboard ASA FirePOWER Status
Device Information
General License

Host Name: **CCNAS-ASA**
ASA Version: **9.8(2)** Device Uptime: **0d 0h 34m 29s**
ASDM Version: **7.8(1)** Device Type: **ASA 5506W**
Firewall Mode: **Routed** Context Mode: **Single**
Environment Status: **OK** Total Flash: **8000 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	30
outside	209.165.200.226/29	up	up	0

Select an interface to view input and output Kbps

VPN Summary

IPsec: **0** Clientless SSL VPN: **0** AnyConnect Client(SSL,TLS,DTLS): **0** Details

System Resources Status
Total Memory Usage Total CPU Usage Core Usage Details
Memory Usage (MB)
3000
2000
814MB
Traffic Status
Connections Per Second Usage
0
08:44
08:45
08:46
08:47
UDP: 0 TCP: 1 Total: 1
'outside' Interface Traffic Usage (Kbps)

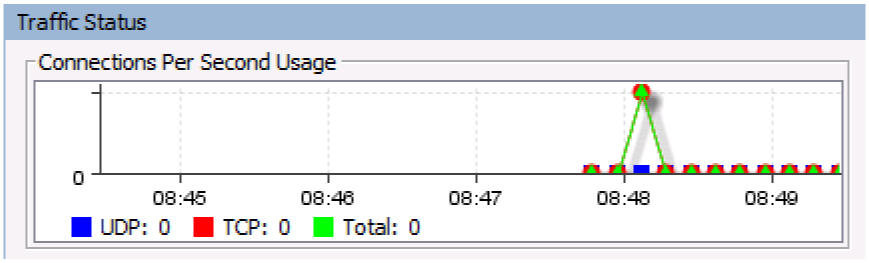
Step 11: Test access to an external website from PC-B.

a. Open a browser on PC-B and enter the IP address of the R1 G0/0 interface (**209.165.200.225**) to simulate access to an external website.

b. The R1 HTTP server was enabled in Part 1. You should be prompted with a user authentication login dialog box from the R1 GUI device manger.

c. Enter the username **admin01** and the password **admin01pass**.

d. Exit the browser.
You should see TCP activity in the ASDM Device Dashboard Traffic Status window on the Home page.



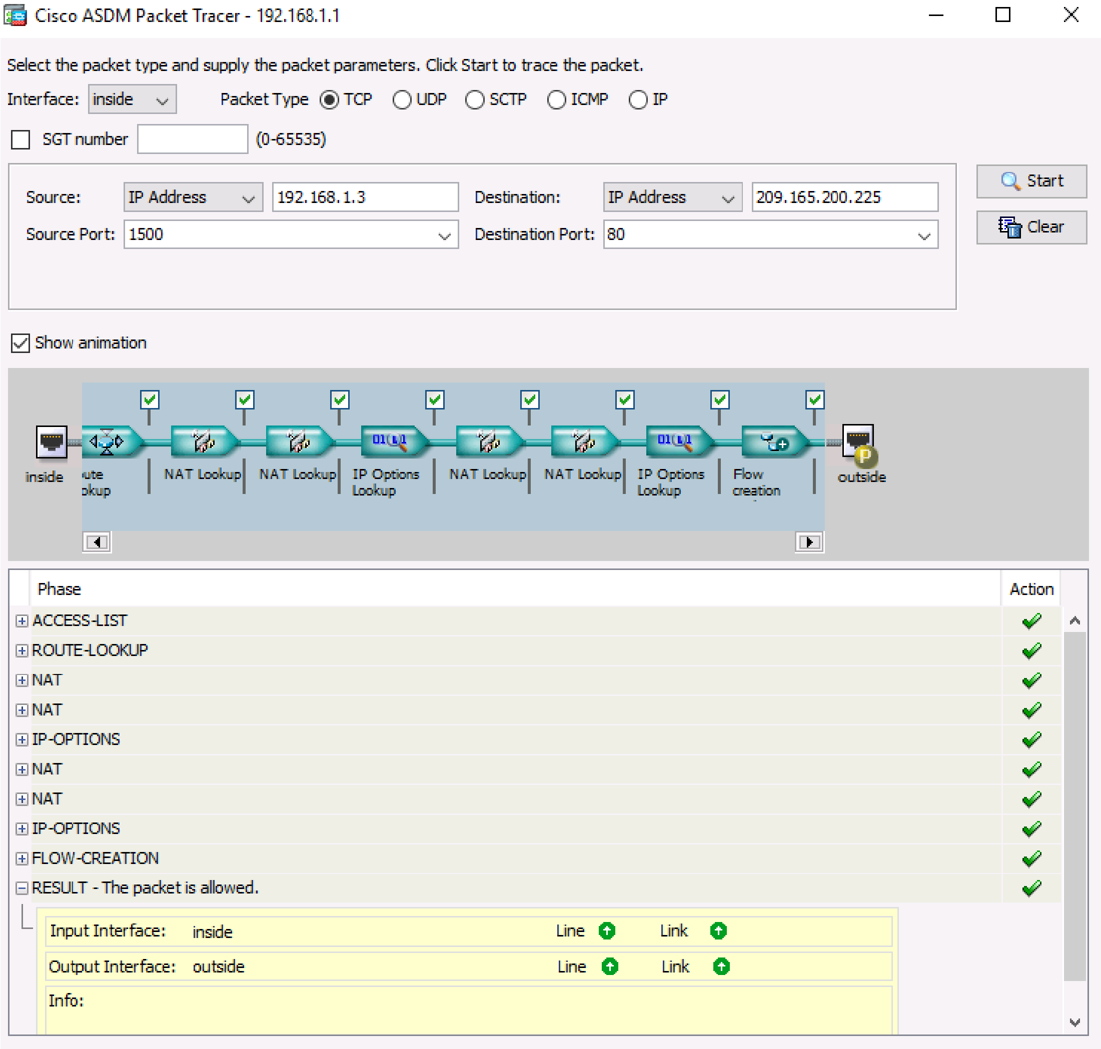
Step 12: Test access to an external website using the ASDM Packet Tracer utility.

a. Within the ASDM Device, click **Tools** > **Packet Tracer**.

b. Select the **inside** interface from the Interface drop-down list and click **TCP** from the Packet Type radio buttons.

c. From the Source drop-down list, select **IP Address** and enter the address **192.168.1.3** (PC-B) with a Source Port of **1500**. From the Destination drop-down list, select **IP Address**, and enter **209.165.200.225** (R1 Gi0/0) with a Destination Port of **80**.

d. Click **Start** to begin the trace of the packet. The packet should be permitted.



Cisco ASDM Packet Tracer - 192.168.1.1

Select the packet type and supply the packet parameters. Click Start to trace the packet.

Interface: inside   Packet Type ● TCP ○ UDP ○ SCTP ○ ICMP ○ IP

□ SGT number (0-65535)

Source: IP Address 192.168.1.3   Destination: IP Address 209.165.200.225

Source Port: 1500   Destination Port: 80

☑ Show animation

Phase	Action
⊞ ACCESS-LIST	✓
⊞ ROUTE-LOOKUP	✓
⊞ NAT	✓
⊞ NAT	✓
⊞ IP-OPTIONS	✓
⊞ NAT	✓
⊞ NAT	✓
⊞ IP-OPTIONS	✓
⊞ FLOW-CREATION	✓
⊟ RESULT - The packet is allowed.	✓

Input Interface: inside   Line ●   Link ●

Output Interface: outside   Line ●   Link ●

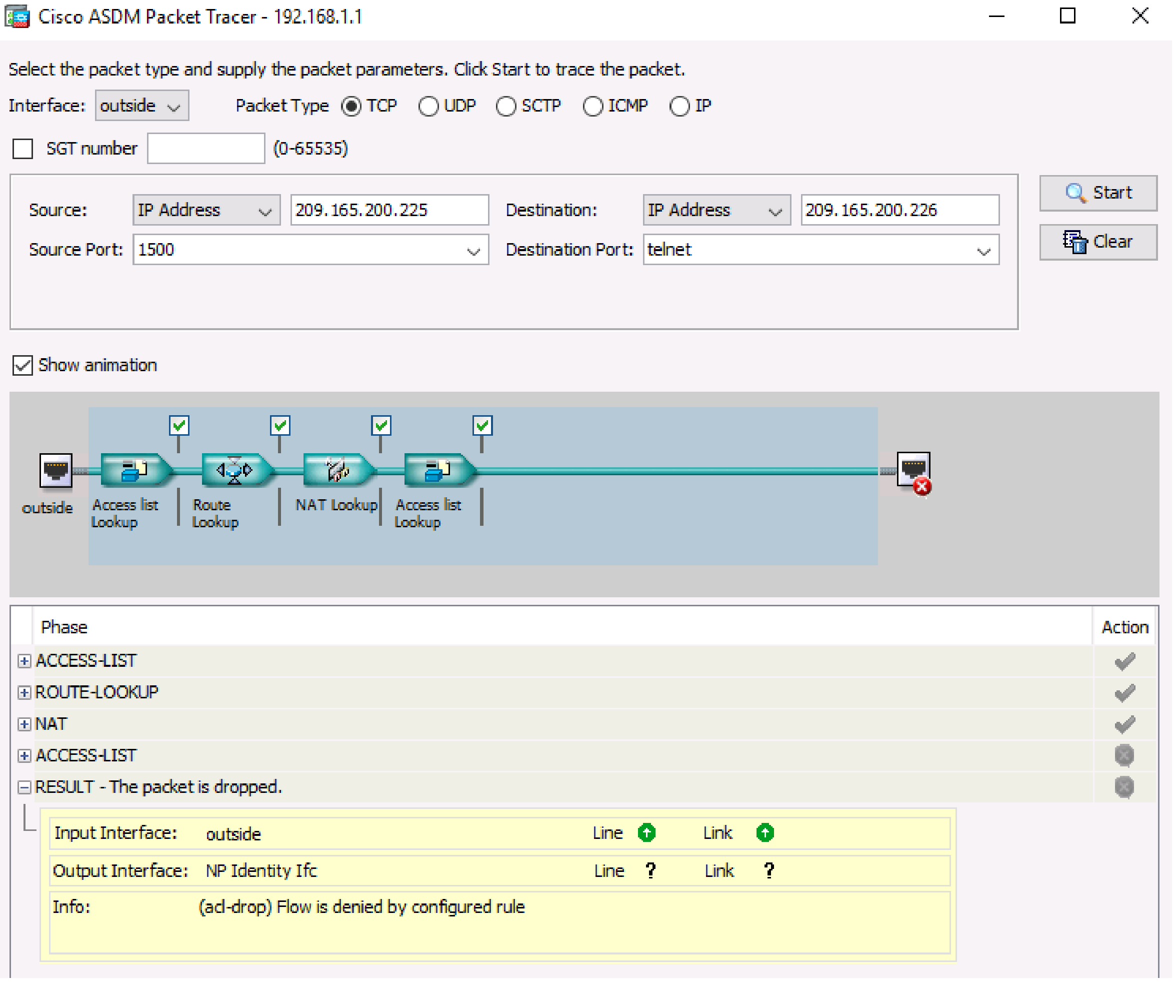
Info:

e. Click **Clear** to reset the entries.

f. Try another trace and select **outside** from the **Interface** drop-down list and leave **TCP** as the packet type.

g. From the **Sources** drop-down list, select **IP Address**, and enter **209.165.200.225** (R1 G0/0) and a Source Port of 1500. From the **Destination** drop-down list, select **IP Address** and enter the address **209.165.200.226** (ASA outside interface) with a Destination Port of **telnet**.

h. Click **Start** to begin the trace of the packet. The packet should be dropped. Click **Close** to continue.



Cisco ASDM Packet Tracer - 192.168.1.1

Select the packet type and supply the packet parameters. Click Start to trace the packet.

Interface: outside   Packet Type ● TCP ○ UDP ○ SCTP ○ ICMP ○ IP

□ SGT number (0-65535)

Source: IP Address 209.165.200.225   Destination: IP Address 209.165.200.226

Source Port: 1500   Destination Port: telnet

☑ Show animation

Phase	Action
⊞ ACCESS-LIST	✓
⊞ ROUTE-LOOKUP	✓
⊞ NAT	✓
⊞ ACCESS-LIST	✗
⊟ RESULT - The packet is dropped.	✗

Input Interface:	outside	Line	●	Link	●
Output Interface:	NP Identity Ifc	Line	?	Link	?
Info:	(acl-drop) Flow is denied by configured rule				

Part 4: Configure ASA Settings from the ASDM Configuration Menu

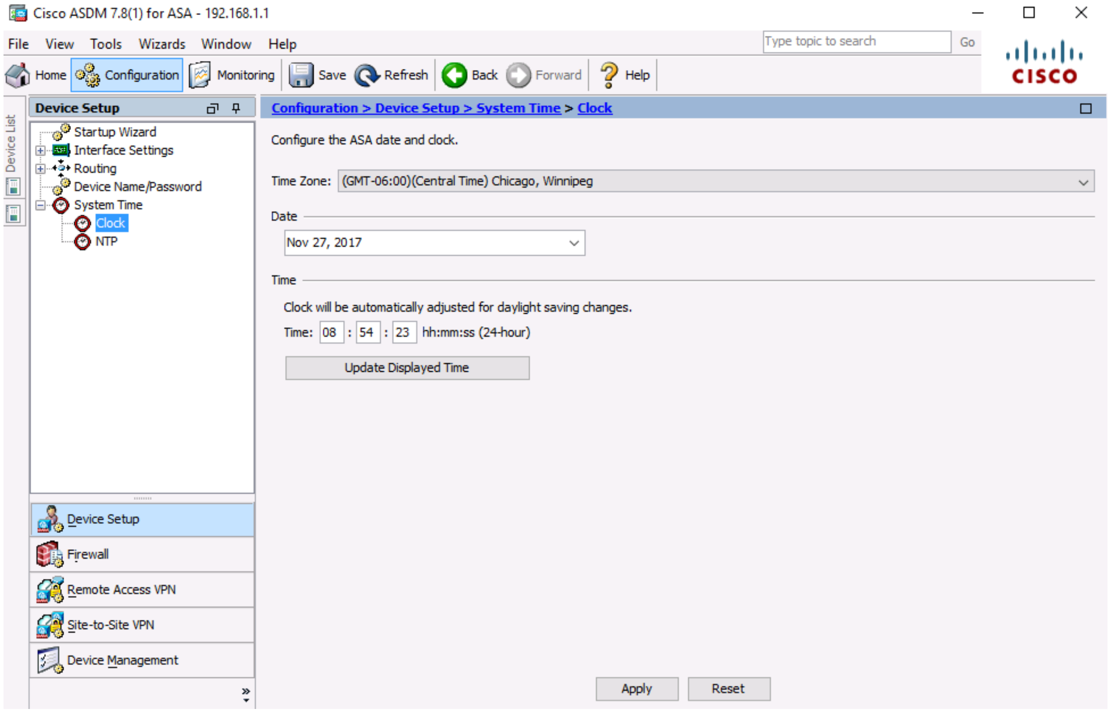
In Part 4, you will set the ASA clock, configure a default route, test connectivity using the ASDM tools ping and traceroute, configure local AAA user authentication, test SSH access, and modify the MPF application inspection policy.

Step 1: Set the ASA date and time.

a. On the **Configuration** screen > **Device Setup** menu, click **System Time** > **Clock**.

b. Select your **Time Zone** from the drop-down list and enter the current date and time in the fields provided. (The clock is a 24-hour clock.)

c. Click **Apply** to send the commands to the ASA.



Configuration > Device Setup > System Time > Clock

Configure the ASA date and clock.

Time Zone: (GMT-06:00)(Central Time) Chicago, Winnipeg

Date

Nov 27, 2017

Time

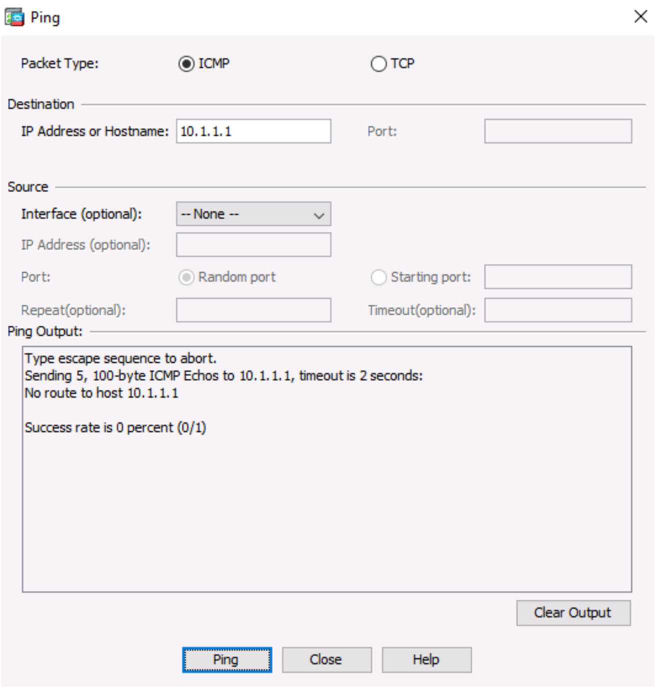
Clock will be automatically adjusted for daylight saving changes.

Time: 08 : 54 : 23 hh:mm:ss (24-hour)

Step 2: Configure a static default route for the ASA.

a. On the **ASDM Tools** menu, select **Ping** and enter the IP address of router R1 S0/0/0 (**10.1.1.1**).

b. Click **Ping**



Packet Type: ● ICMP ○ TCP

IP Address or Hostname: 10.1.1.1 Port:

Interface (optional): -- None --

IP Address (optional):

Port: ● Random port ○ Starting port:

Repeat(optional): Timeout(optional):

Ping Output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
No route to host 10.1.1.1

Success rate is 0 percent (0/1)
```

c. The ASA does not have a default route to unknown external networks. The ping should fail because the ASA does not have a route to 10.1.1.1.

d. Click **Close** to continue.

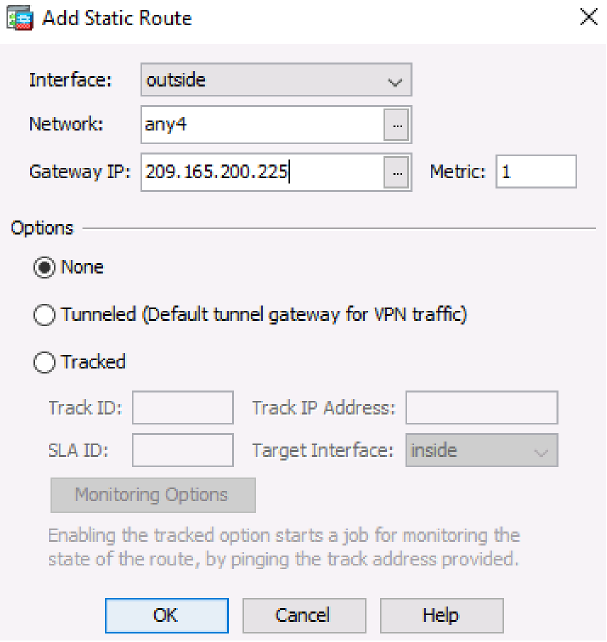
e. From the **Configuration** screen > **Device Setup** menu, click **Routing** > **Static Routes**.

f. Click **IPv4 Only** and click **Add** to add a new static route.

g. On the Add Static Route dialog box, select the **outside** interface from the drop-down list.

h. Click the ellipsis button to the right of **Network and** select **any4** from the list of network objects andd click **OK**. The selection of **any4** translates to a "quad zero" route.

i. For the Gateway IP, enter **209.165.200.225** (R1 G0/0).



Add Static Route

Interface: outside

Network: any4

Gateway IP: 209.165.200.225 Metric: 1

Options

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

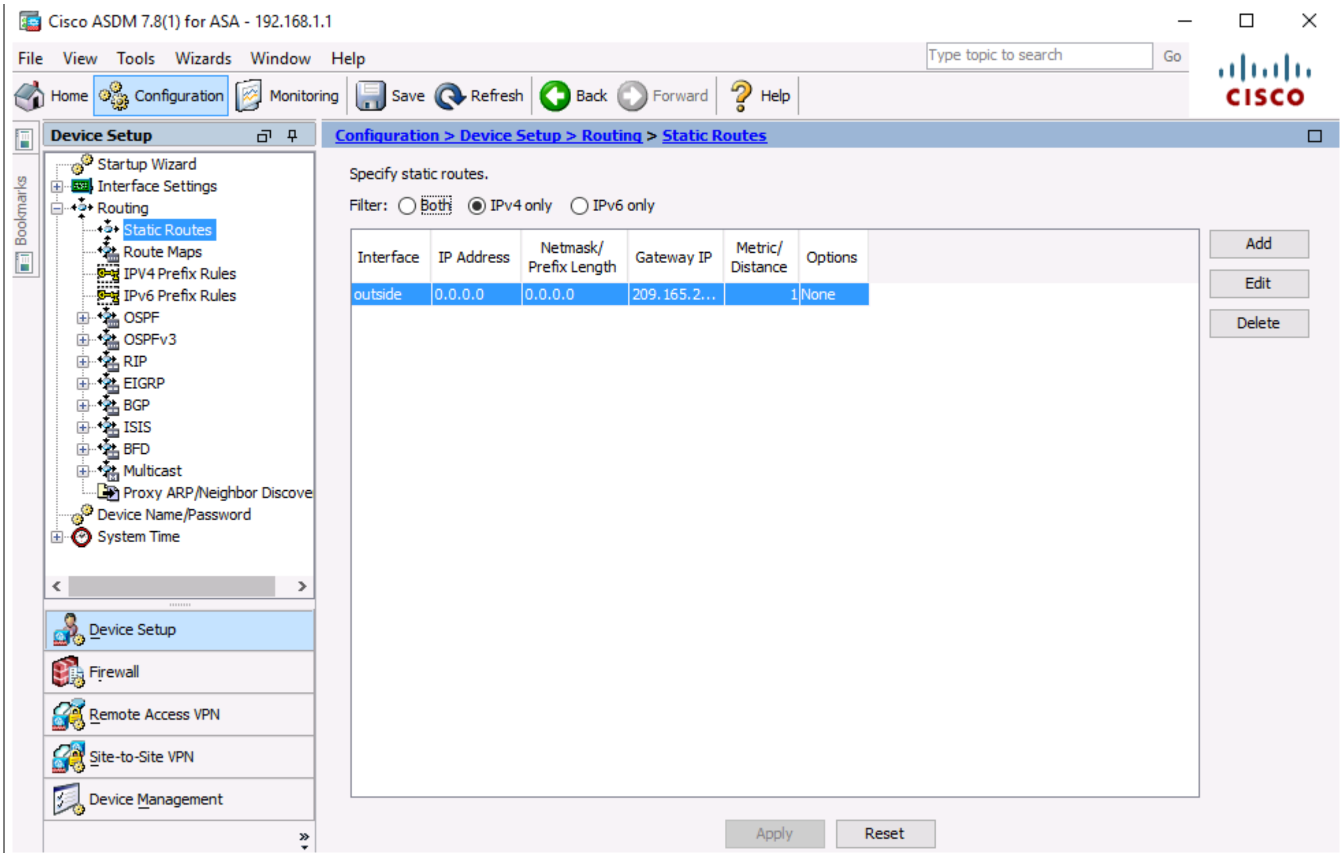
○ Tracked

Track ID: Track IP Address:

SLA ID: Target Interface: inside

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

j. Click **OK** and then **Apply** to send the commands to the ASA.

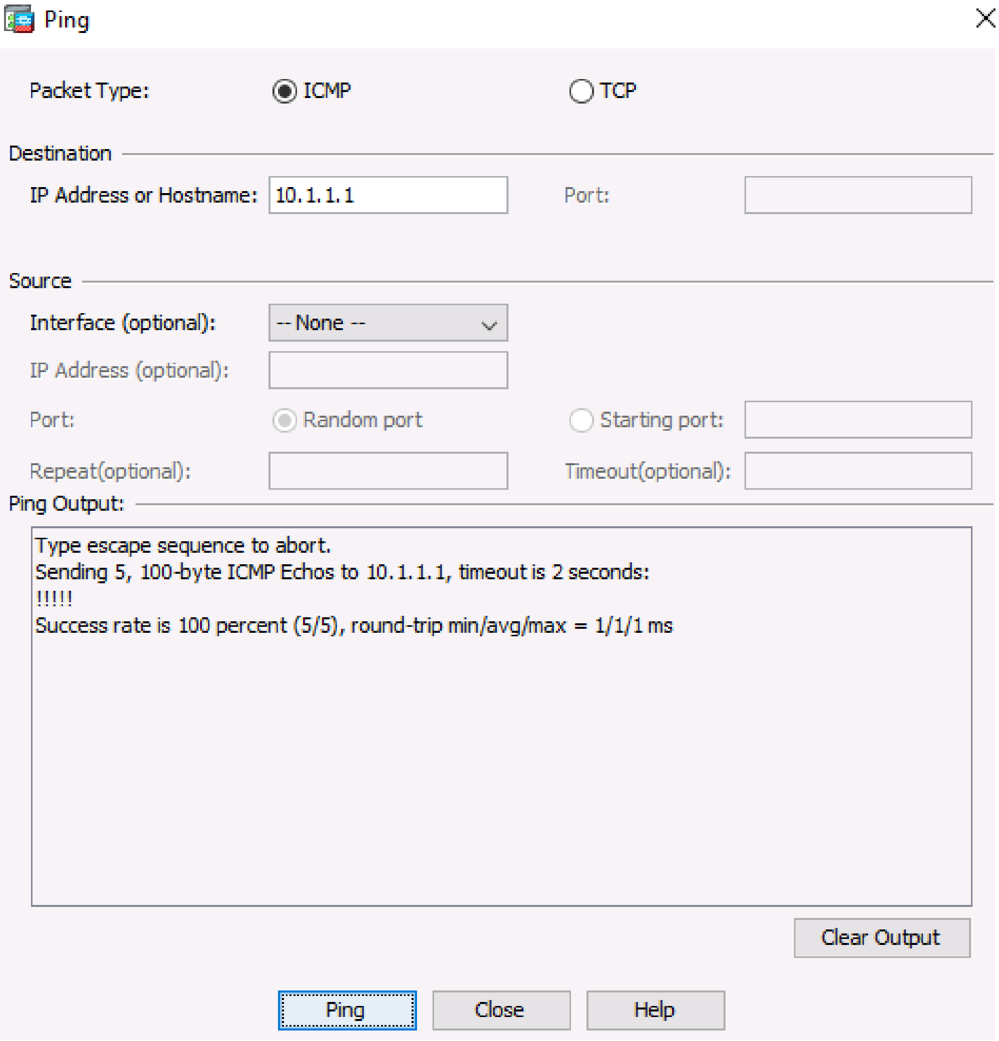


Specify static routes.

Filter: ○ Both ● IPv4 only ○ IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
outside	0.0.0.0	0.0.0.0	209.165.2...	1	None

k. On the ASDM **Tools** menu, select **Ping** and enter the IP address of router R1 S0/0/0 (**10.1.1.1**). The ping should succeed this time. Click **Close** to continue.



IP Address or Hostname: 10.1.1.1

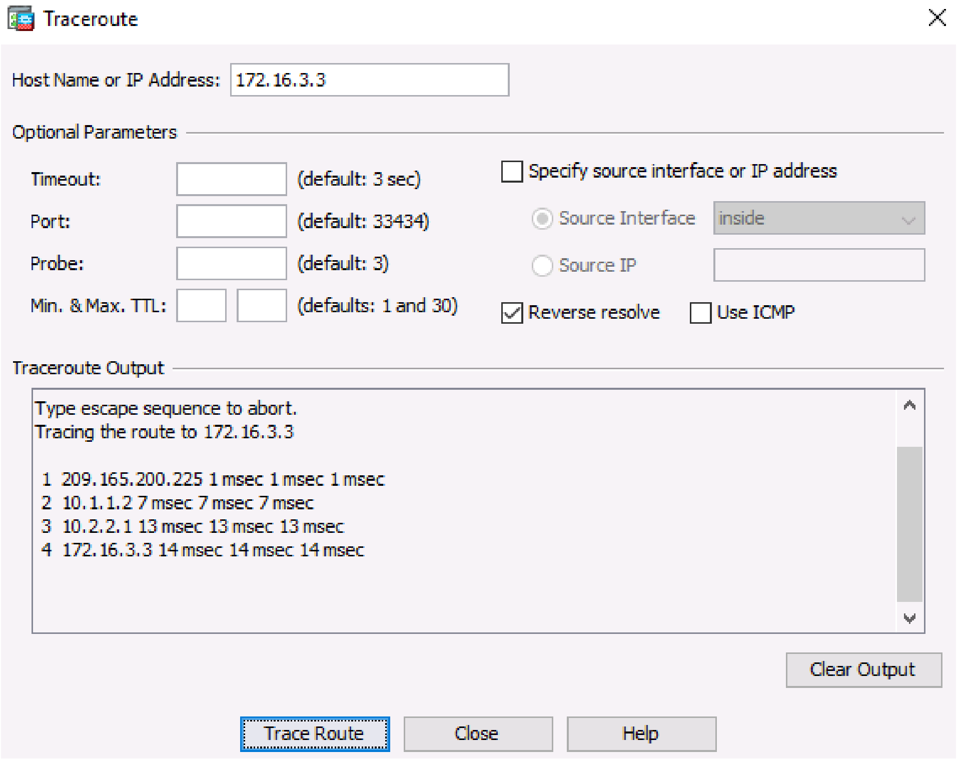
Interface (optional): -- None --

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

l. On the ASDM **Tools** menu, select **Traceroute** and enter the IP address of external host PC-C (**172.16.3.3**).

m. Click **Trace Route**. The traceroute should succeed and show the hops from the ASA through R1, R2, and R3 to host PC-C.

n. Click **Close** to continue.



Traceroute

Host Name or IP Address: 172.16.3.3

Optional Parameters

Timeout: (default: 3 sec)

Port: (default: 33434)

Probe: (default: 3)

Min. & Max. TTL: (defaults: 1 and 30)

□ Specify source interface or IP address

● Source Interface inside

○ Source IP

☑ Reverse resolve □ Use ICMP

Traceroute Output

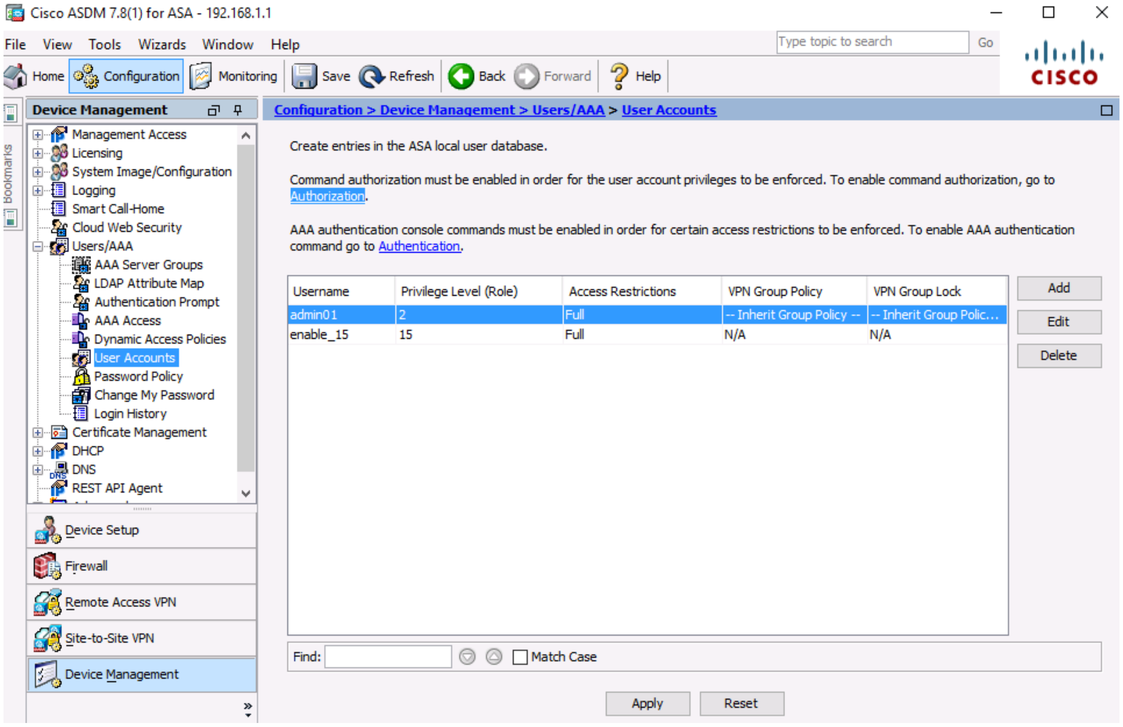
```
Type escape sequence to abort.
Tracing the route to 172.16.3.3

 1  209.165.200.225 1 msec 1 msec 1 msec
 2  10.1.1.2 7 msec 7 msec 7 msec
 3  10.2.2.1 13 msec 13 msec 13 msec
 4  172.16.3.3 14 msec 14 msec 14 msec
```

Step 3: Configure AAA user authentication using the ASA local database.

Enable AAA user authentication to access the ASA using SSH. You allowed SSH access to the ASA from the inside network and the outside host PC-C when the **Startup wizard** was run. To allow the administrator to have SSH access to the ASA, you will create a user in the local database.

a. On the **Configuration** screen > **Device Management** area, click **Users/AAA**.

b. Click **User Accounts**



Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to Authorization.

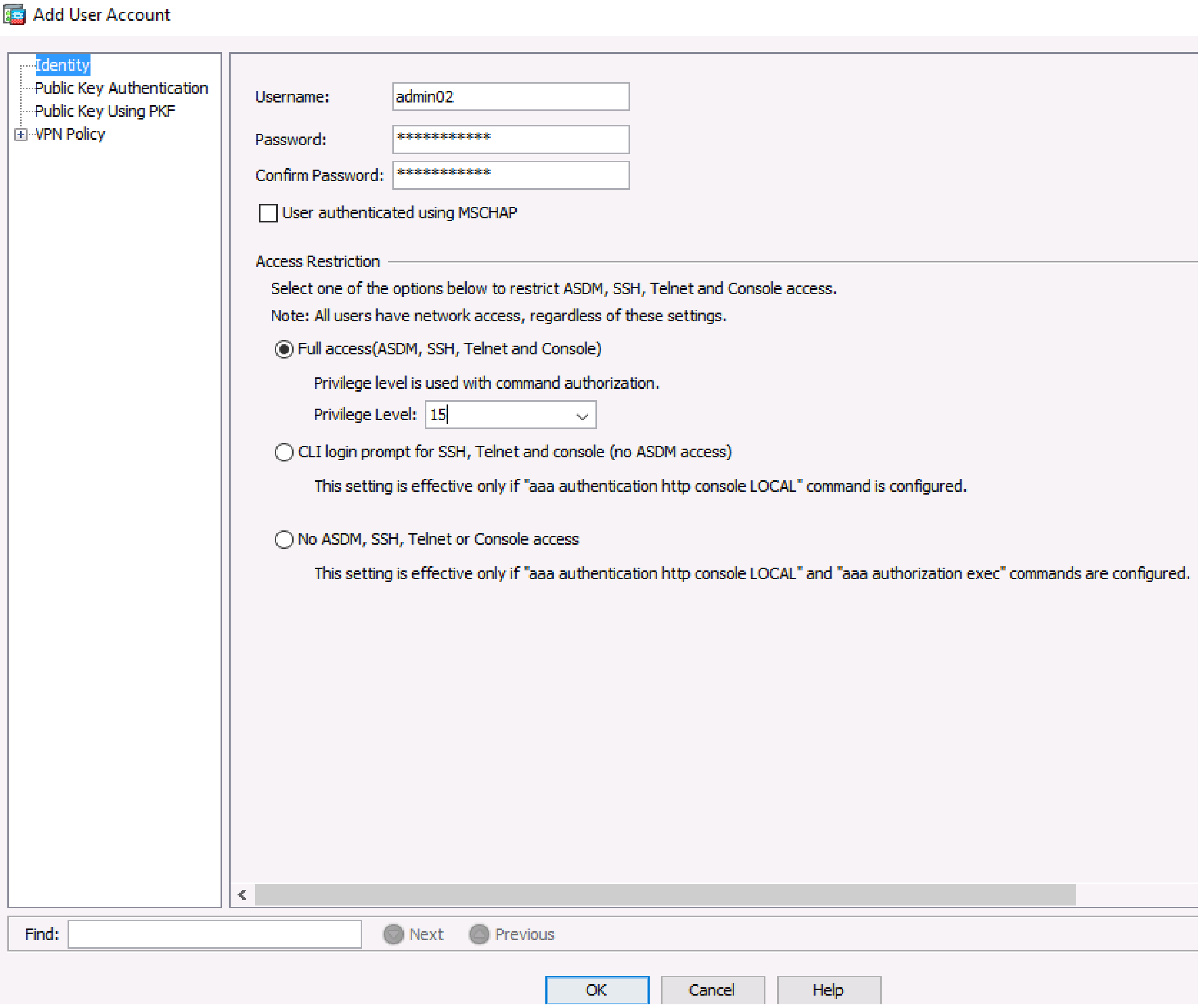
AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to Authentication.

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
admin01	2	Full	-- Inherit Group Policy --	-- Inherit Group Polic...
enable_15	15	Full	N/A	N/A

c. Click **Add**.

d. Create a new user named **admin02** with a password of **admin02pass** and enter the password again to confirm it. Allow this user **Full access** (ASDM, SSH, Telnet, and console) and set the privilege level to **15**.

e. Click **OK** to add the user and click **Apply** to send the command to the ASA.



Add User Account

Username: admin02

Password: ************

Confirm Password: ************

□ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 15

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if "aaa authentication http console LOCAL" command is configured.

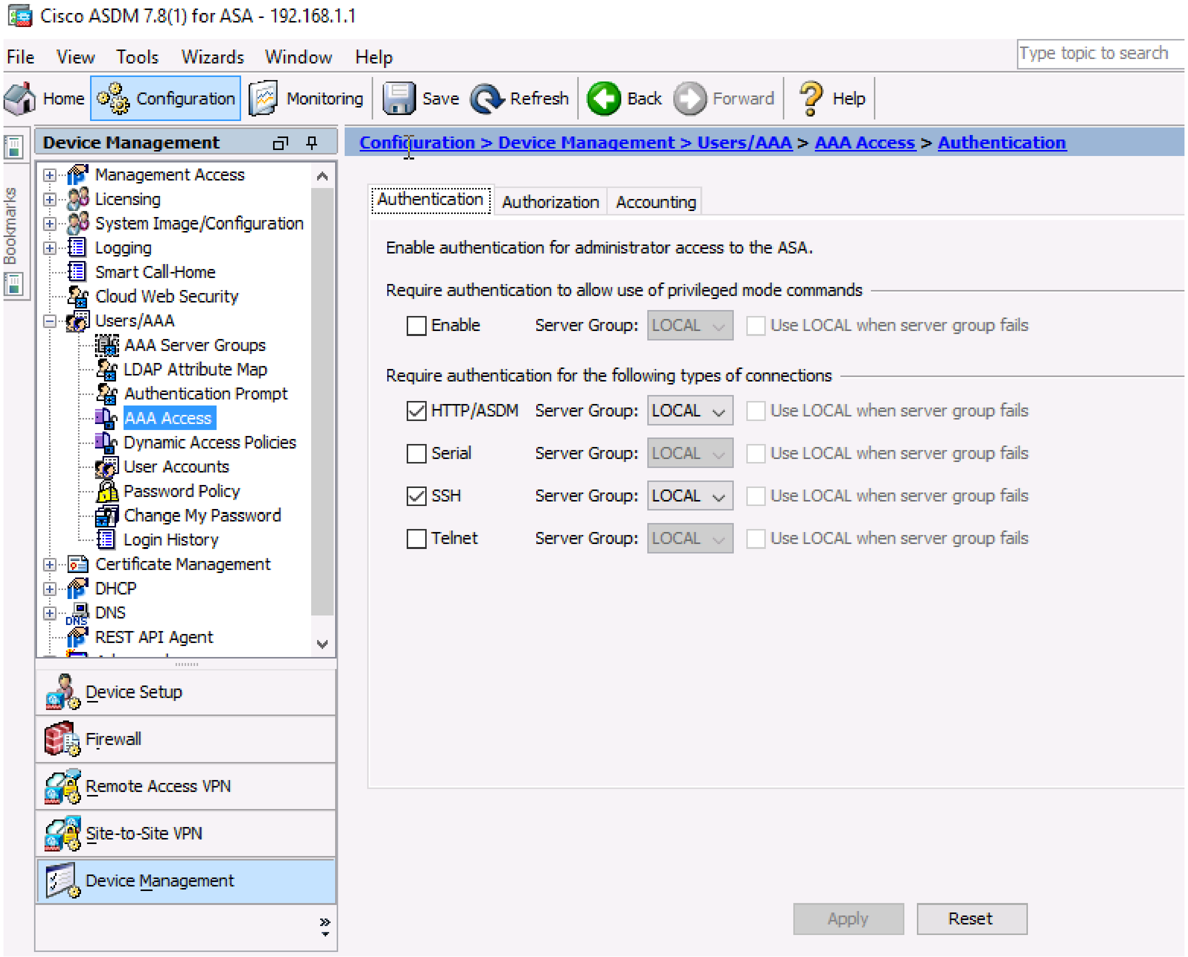
○ No ASDM, SSH, Telnet or Console access

This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

f. On the **Configuration** screen > **Device Management** area, click **Users/AAA**. Click **AAA Access**.

g. On the **Authentication** tab, click the check box to require authentication for **HTTP/ASDM** and **SSH** connections and specify the **LOCAL** server group for each connection type.

h. Click **Apply** to send the commands to the ASA.



Configuration > Device Management > Users/AAA > AAA Access > Authentication

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

□ Enable Server Group: LOCAL □ Use LOCAL when server group fails

Require authentication for the following types of connections

☑ HTTP/ASDM Server Group: LOCAL □ Use LOCAL when server group fails

□ Serial Server Group: LOCAL □ Use LOCAL when server group fails

☑ SSH Server Group: LOCAL □ Use LOCAL when server group fails

□ Telnet Server Group: LOCAL □ Use LOCAL when server group fails

Note: The next action you attempt within ASDM will require that you log in as **admin02** with the password **admin02pass**.

Step 4: Test SSH access to the ASA.

a. Open a SSH client on PC-B, such as PuTTY and connect to the ASA inside interface at IP address **192.168.1.1**. When prompted to log in, enter the user name **admin02** and the password **admin02pass**.

b. From **PC-C**, open an SSH client, such as PuTTY, and attempt to access the ASA outside interface at **209.165.200.226**. When prompted to log in, enter the user name **admin02** and the password **admin02pass**.

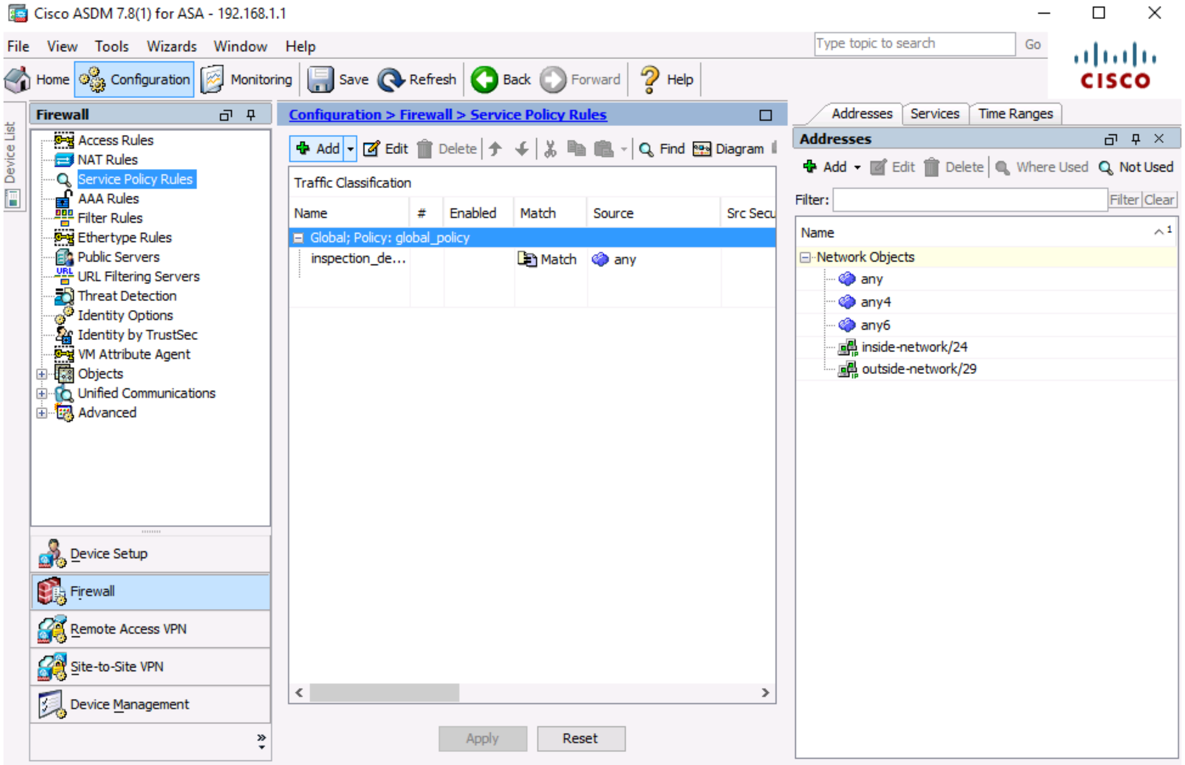
c. After logging in to the ASA using SSH, enter the **enable** command and provide the password **cisco12345**. Issue the **show run** command to display the current configuration that you have created using ASDM.

Step 5: Modify the MPF application inspection policy.

For application layer inspection, and other advanced options, the Cisco Modular Policy Framework (MPF) is available on ASAs.

a. The default global inspection policy does not inspect ICMP. To enable hosts on the internal network to ping external hosts and receive replies, ICMP traffic must be inspected.

b. Within the ASDM on **PC-B**, access the **Configuration** tab > **Firewall** area menu, click **Service Policy Rules**.

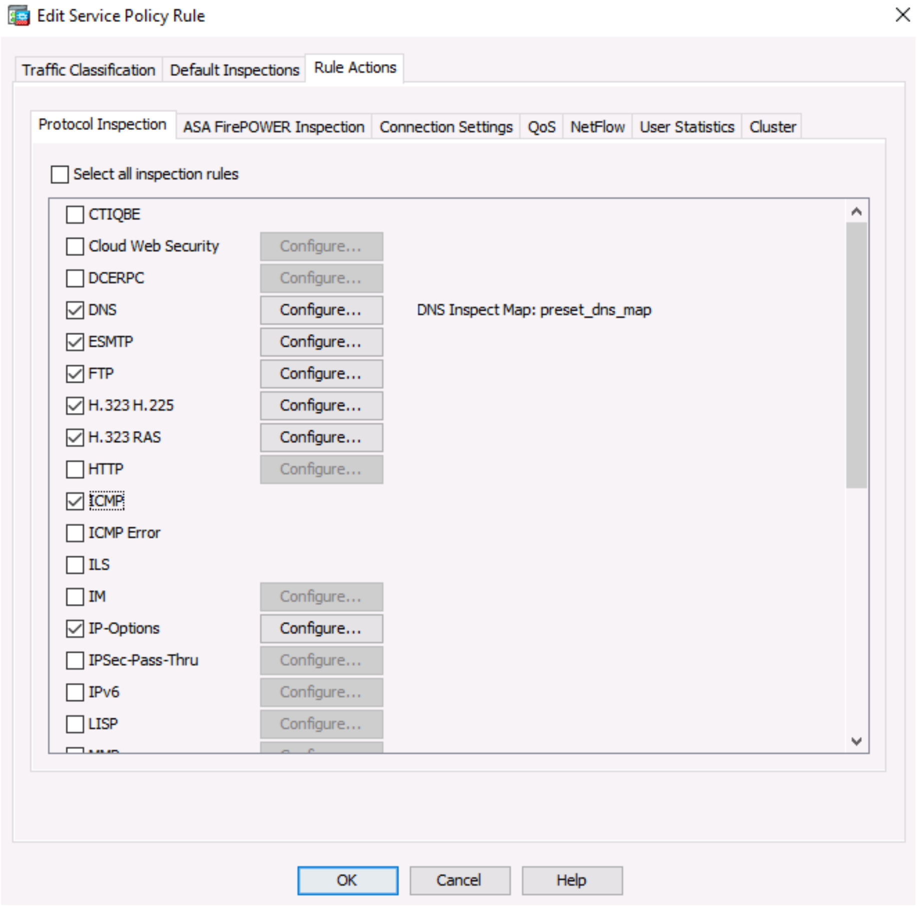


Traffic Classification

Name	#	Enabled	Match	Source	Src Secu
Global; Policy: global_policy					
inspection_de...			Match	any	

c. Select the **inspection_default** policy and click **Edit** to modify the default inspection rules.

d. On the Edit Service Policy Rule window, click the **Rule Actions** tab and select the **ICMP** check box. Do not change the other default protocols that are checked.



Edit Service Policy Rule

☐ Select all inspection rules

☐ CTIQBE
☐ Cloud Web Security Configure...
☐ DCERPC Configure...
☑ DNS Configure... DNS Inspect Map: preset_dns_map
☑ ESMTP Configure...
☑ FTP Configure...
☑ H.323 H.225 Configure...
☑ H.323 RAS Configure...
☐ HTTP Configure...
☑ ICMP
☐ ICMP Error
☐ ILS
☐ IM Configure...
☑ IP-Options Configure...
☐ IPSec-Pass-Thru Configure...
☐ IPv6 Configure...
☐ LISP Configure...

e. Click **OK** > **Apply** to send the commands to the ASA.
If prompted, log in as **admin02** with the password **admin02pass**.

f. From PC-B, **ping** the external interface of R1 S0/0/0 (**10.1.1.1**). The pings should be successful.

Part 5: Configure DMZ, Static NAT, and ACLs

In this part, you will create a DMZ on the ASA, configure static NAT to a DMZ server, and apply an ACL to control access to the server.

Step 1: Configure the ASA DMZ VLAN 3 interface.

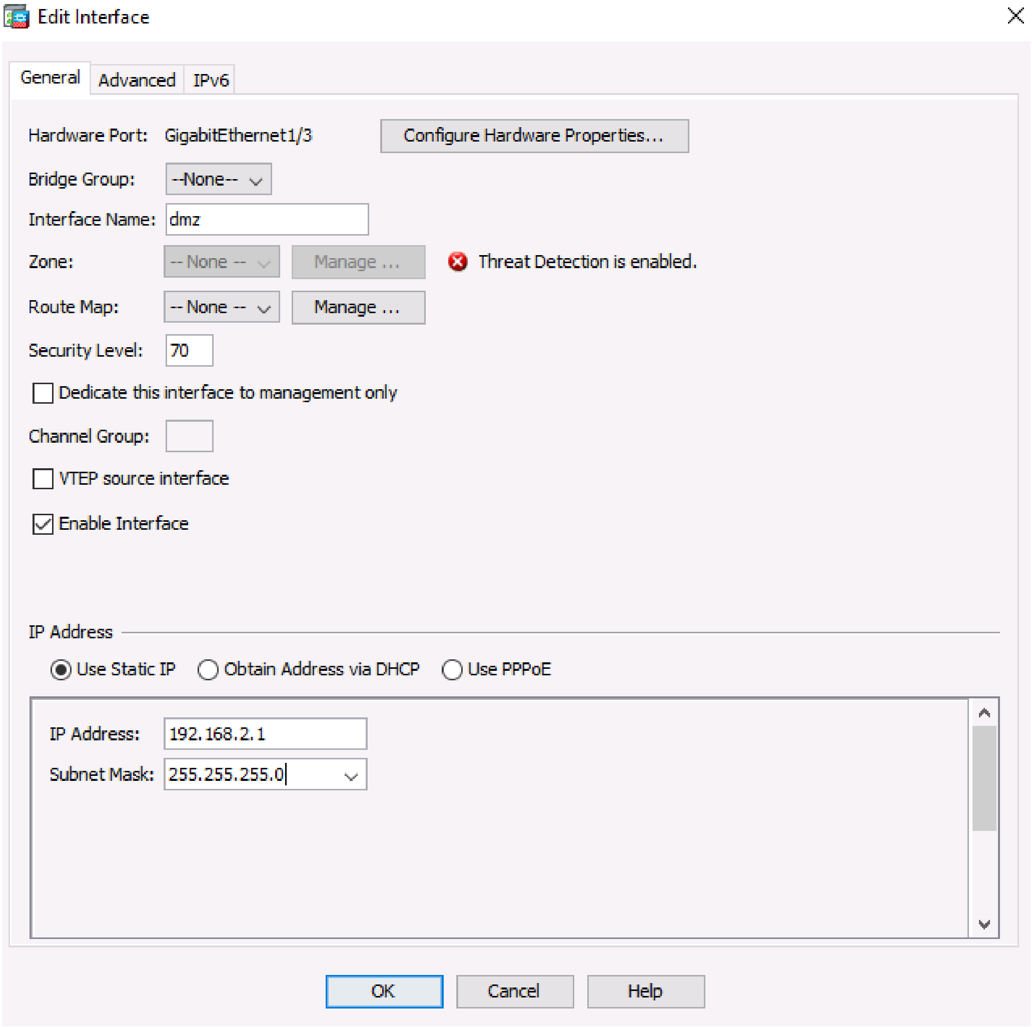
In this step, you will configure interface Gi1/3 named **dmz**, set the security level to **70**, and limit communication from this interface to the inside (Gi1/2) interface.

a. On the **Configuration** screen > **Device Setup** menu, click **Interface Settings > Interfaces**. The currently defined inside and outside interfaces are listed.

b. **Double**-click **GigabitEthernet1/3** to configure the dmz interface.

c. The Edit Interface dialog box will open. In the Interface Name box, name the interface **dmz**, assign it a security level of **70**, and make sure the **Enable Interface** checkbox is checked.

d. Ensure that the **Use Static IP** option is selected and enter an IP address of **192.168.2.1** with a subnet mask of **255.255.255.0**.



Hardware Port: GigabitEthernet1/3

Bridge Group: --None--

Interface Name: dmz

Zone: -- None --

Threat Detection is enabled.

Route Map: -- None --

Security Level: 70

☐ Dedicate this interface to management only

Channel Group:

☐ VTEP source interface

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 192.168.2.1

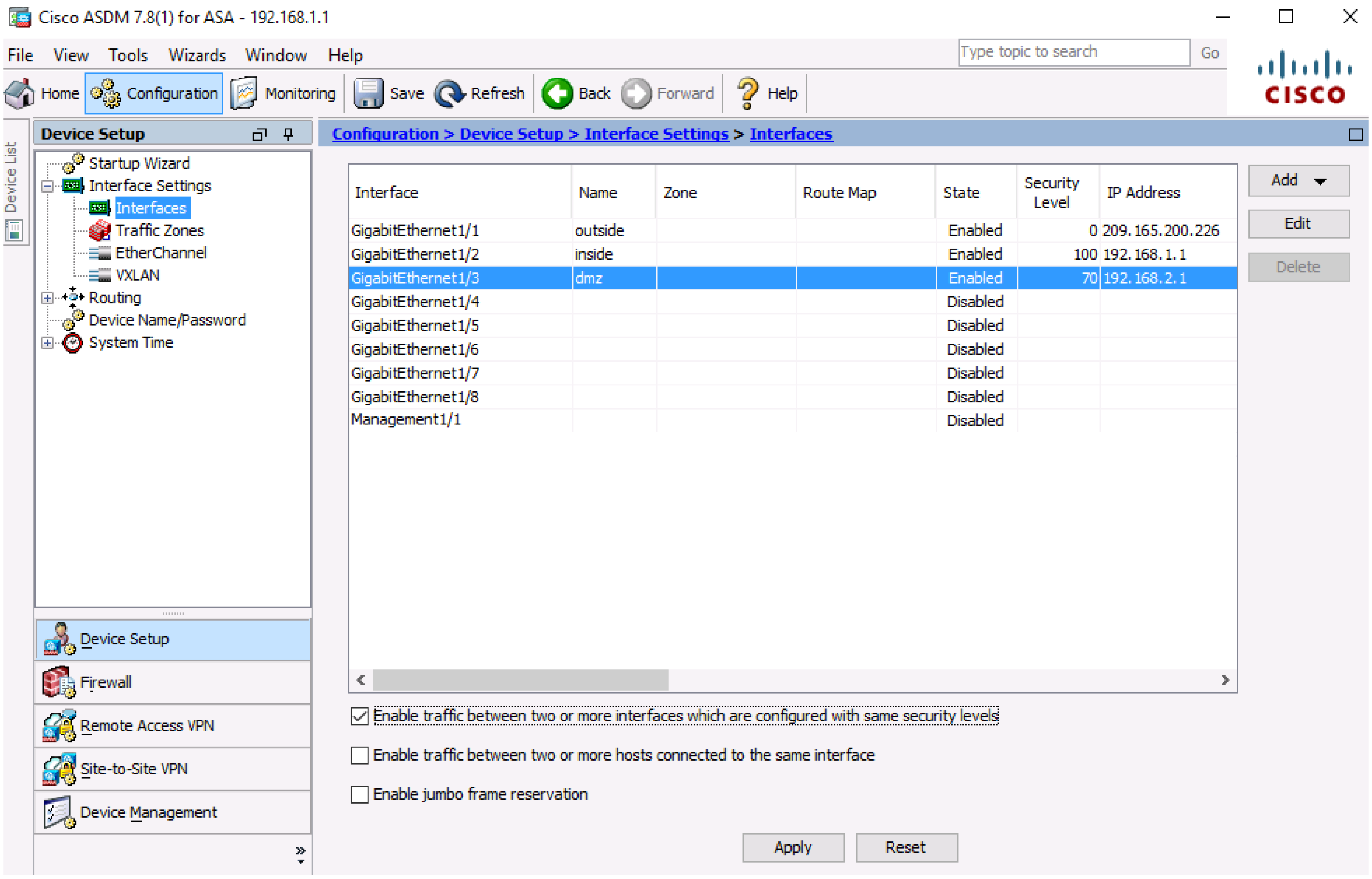
Subnet Mask: 255.255.255.0

e. Click **OK** to close the window.
When prompted on the Security Level Change, click **OK**.

f. You should see the new interface named **dmz**, in addition to the inside and outside interfaces.

g. Check the box **Enable traffic between two or more interfaces which are configured with the same security levels**.

h. Click **Apply** to send the commands to the ASA.



Interface	Name	Zone	Route Map	State	Security Level	IP Address
GigabitEthernet1/1	outside			Enabled	0	209.165.200.226
GigabitEthernet1/2	inside			Enabled	100	192.168.1.1
GigabitEthernet1/3	dmz			Enabled	70	192.168.2.1
GigabitEthernet1/4				Disabled		
GigabitEthernet1/5				Disabled		
GigabitEthernet1/6				Disabled		
GigabitEthernet1/7				Disabled		
GigabitEthernet1/8				Disabled		
Management1/1				Disabled		

☑ Enable traffic between two or more interfaces which are configured with same security levels

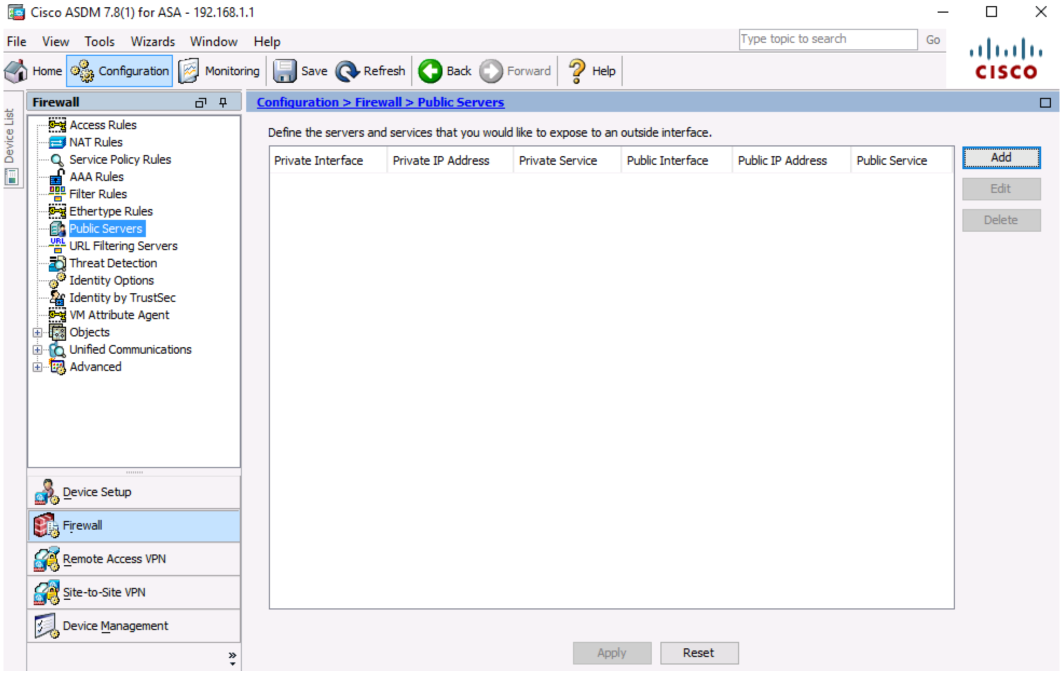
□ Enable traffic between two or more hosts connected to the same interface

□ Enable jumbo frame reservation

Step 2: Configure the DMZ server and static NAT.

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). R1 G0/0 and the ASA outside interface are already using 209.165.200.225 and .226. You will use public address **209.165.200.227** and static NAT to provide address translation access to the server.

a. On the **Firewall** menu, click the **Public Servers** option and click **Add** to define the DMZ server and services offered.



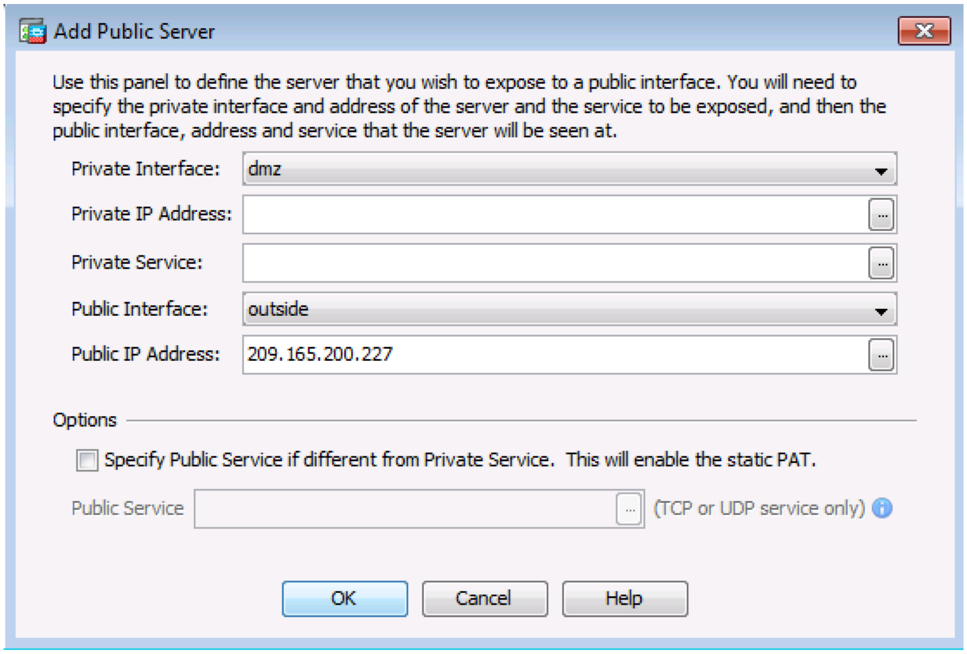
Cisco ASDM 7.8(1) for ASA - 192.168.1.1

Configuration > Firewall > Public Servers

Define the servers and services that you would like to expose to an outside interface.

Private Interface	Private IP Address	Private Service	Public Interface	Public IP Address	Public Service

b. In the Add Public Server dialog box, specify the Private Interface as **dmz**, the Public Interface as **outside**, and the Public IP address as **209.165.200.227**.



Add Public Server

Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface and address of the server and the service to be exposed, and then the public interface, address and service that the server will be seen at.

Private Interface: dmz

Private IP Address:

Private Service:

Public Interface: outside

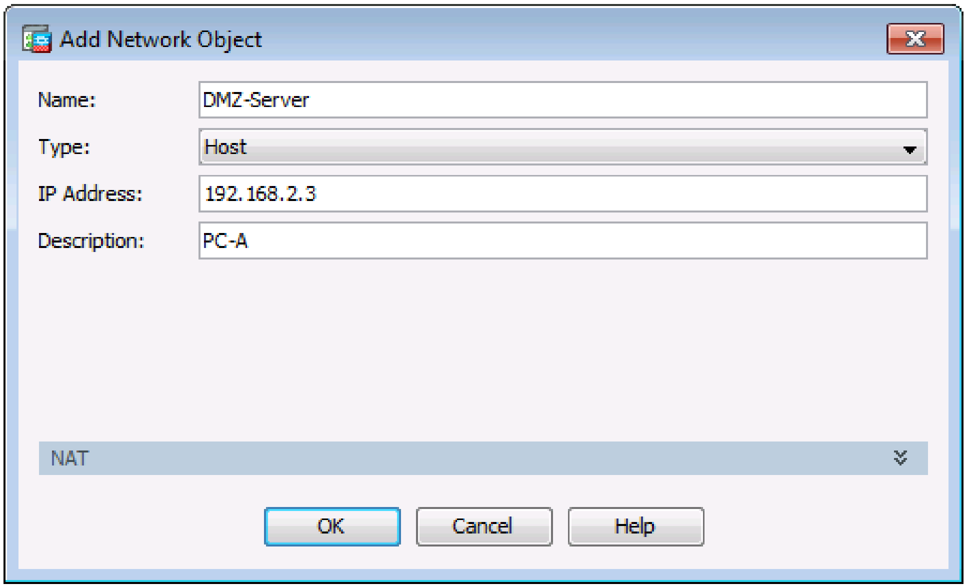
Public IP Address: 209.165.200.227

Options

□ Specify Public Service if different from Private Service. This will enable the static PAT.

Public Service (TCP or UDP service only)

c. Click the ellipsis button to the right of Private IP Address. In the Browse Private IP Address window, click **Add** to define the server as a **Network Object**. Enter the name **DMZ-Server**, select **Host** from the Type pull-down menu**,** enter the IP Address **192.168.2.3**, and a Description of **PC-A**.

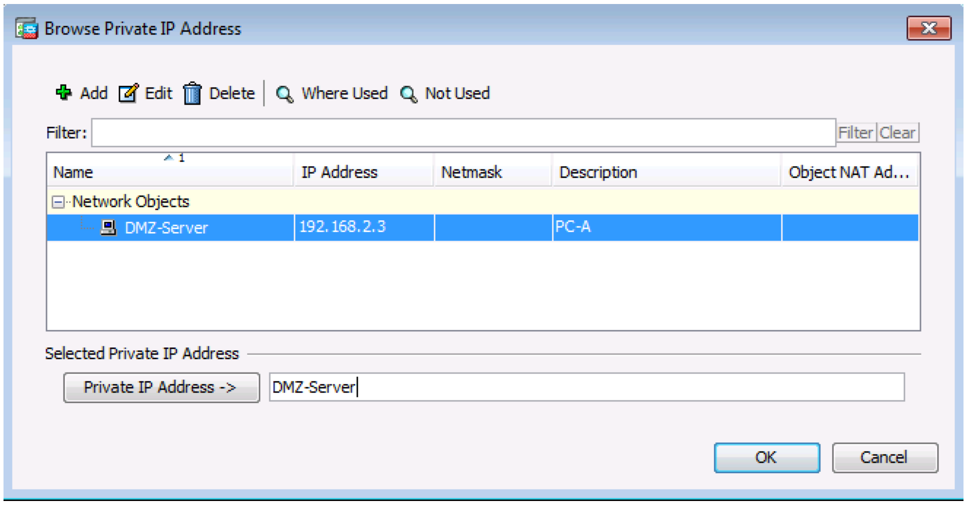


Add Network Object

Name:	DMZ-Server
Type:	Host
IP Address:	192.168.2.3
Description:	PC-A

d. Click **OK**

e. From the Browse Private IP Address window, verify that the DMZ-Server appears in the Selected Private IP Address field and click **OK**. You will return to the Add Public Server dialog box.



Browse Private IP Address

Name	IP Address	Netmask	Description	Object NAT Ad...
Network Objects				
DMZ-Server	192.168.2.3		PC-A	

Selected Private IP Address

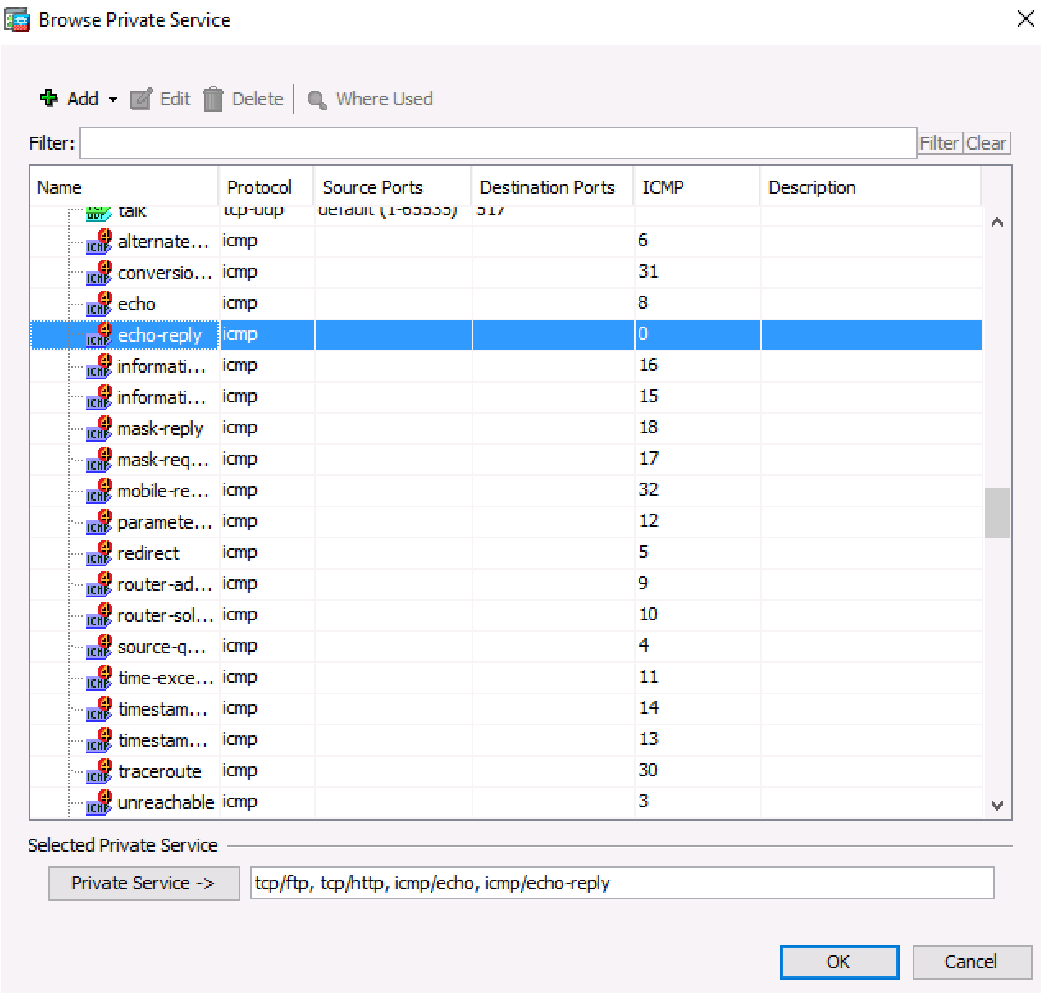
Private IP Address -> DMZ-Server

f. Click the ellipsis button to the right of **Private Service**.

g. Double-click to select the following services: **tcp/ftp**, **tcp/http**, **icmp/echo,** and **icmp/echo-reply**

h. Click **OK** to continue and return to the Add Public Server dialog.

Note: You can specify Public services if they are different from the Private services, using the option on this screen.

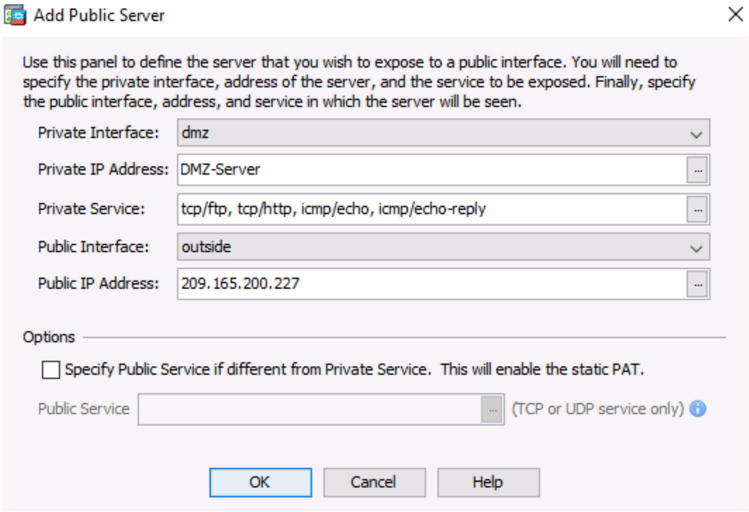


Name	Protocol	Source Ports	Destination Ports	ICMP	Description
talk	tcp-udp	default (1-65535)	517		
alternate…	icmp			6	
conversio…	icmp			31	
echo	icmp			8	
echo-reply	icmp			0	
informati…	icmp			16	
informati…	icmp			15	
mask-reply	icmp			18	
mask-req…	icmp			17	
mobile-re…	icmp			32	
paramete…	icmp			12	
redirect	icmp			5	
router-ad…	icmp			9	
router-sol…	icmp			10	
source-q…	icmp			4	
time-exce…	icmp			11	
timestam…	icmp			14	
timestam…	icmp			13	
traceroute	icmp			30	
unreachable	icmp			3	

Selected Private Service

Private Service -> tcp/ftp, tcp/http, icmp/echo, icmp/echo-reply

i. When you have completed all the information in the Add Public Server dialog box, it should look like the one shown below. Click **OK** to add the server.



Add Public Server

Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface, address of the server, and the service to be exposed. Finally, specify the public interface, address, and service in which the server will be seen.

Private Interface: dmz

Private IP Address: DMZ-Server

Private Service: tcp/ftp, tcp/http, icmp/echo, icmp/echo-reply

Public Interface: outside

Public IP Address: 209.165.200.227

Options

□ Specify Public Service if different from Private Service. This will enable the static PAT.

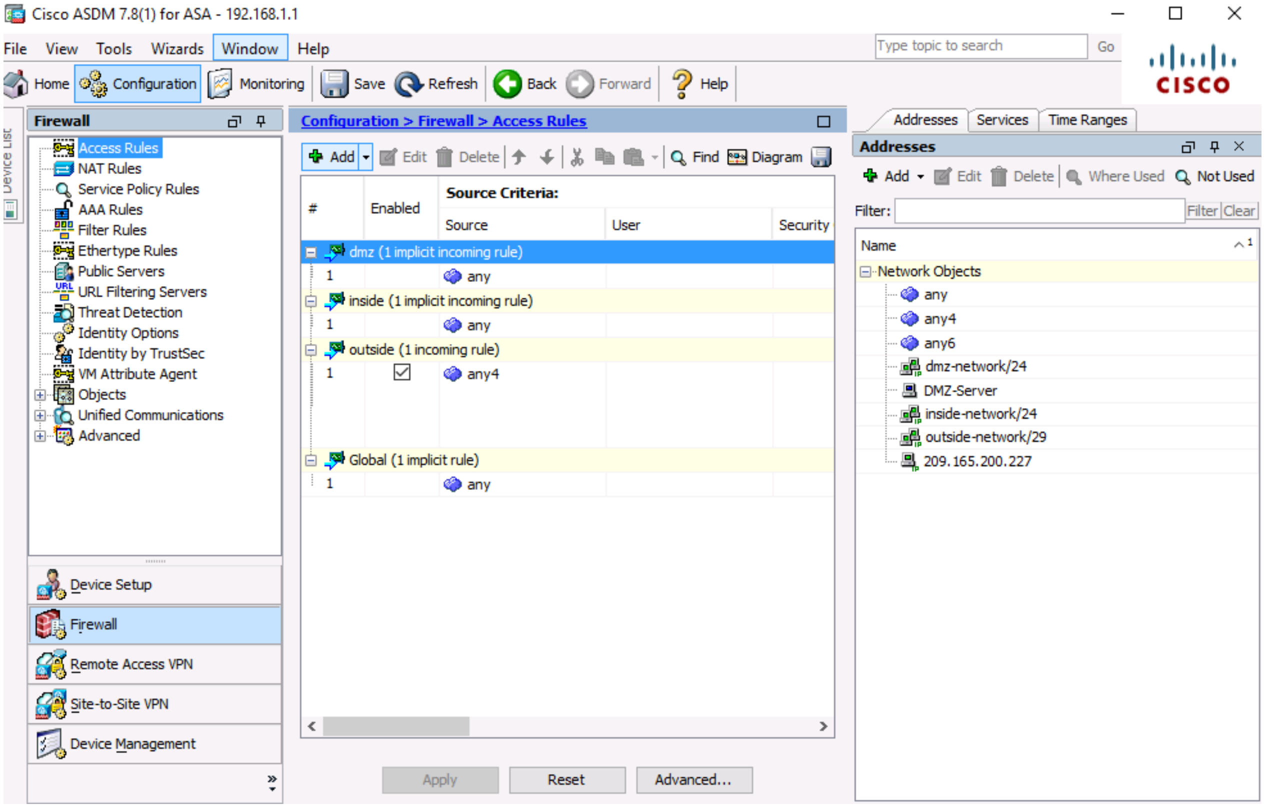
Public Service (TCP or UDP service only)

j. Click **Apply** at the Public Servers screen to send the commands to the ASA.

Step 3: View the DMZ Access Rule generated by ASDM.

a. After the creation of the DMZ server object and selection of services, ASDM automatically generates an Access Rule (ACL) to permit the appropriate access to the server and applies it to the outside interface in the incoming direction.

b. View this ACL in ASDM by clicking **Configuration** > **Firewall** > **Access Rules**. It appears as an outside incoming rule. You can select the rule and use the horizontal scroll bar to see all of the components.



Cisco ASDM 7.8(1) for ASA - 192.168.1.1

Configuration > Firewall > Access Rules

#	Enabled	Source Criteria: Source	User	Security
dmz (1 implicit incoming rule)				
1		any		
inside (1 implicit incoming rule)				
1		any		
outside (1 incoming rule)				
1	☑	any4		
Global (1 implicit rule)				
1		any		

Addresses

Name

Network Objects
- any
- any4
- any6
- dmz-network/24
- DMZ-Server
- inside-network/24
- outside-network/29
- 209.165.200.227

Note: You can also see the commands generated by using the **Tools** > **Command Line Interface** and entering the **show run** command.

Step 4: Test access to the DMZ server from the outside network.

a. From PC-C, ping the IP address of the static NAT public server address (**209.165.200.227**). The pings should be successful.

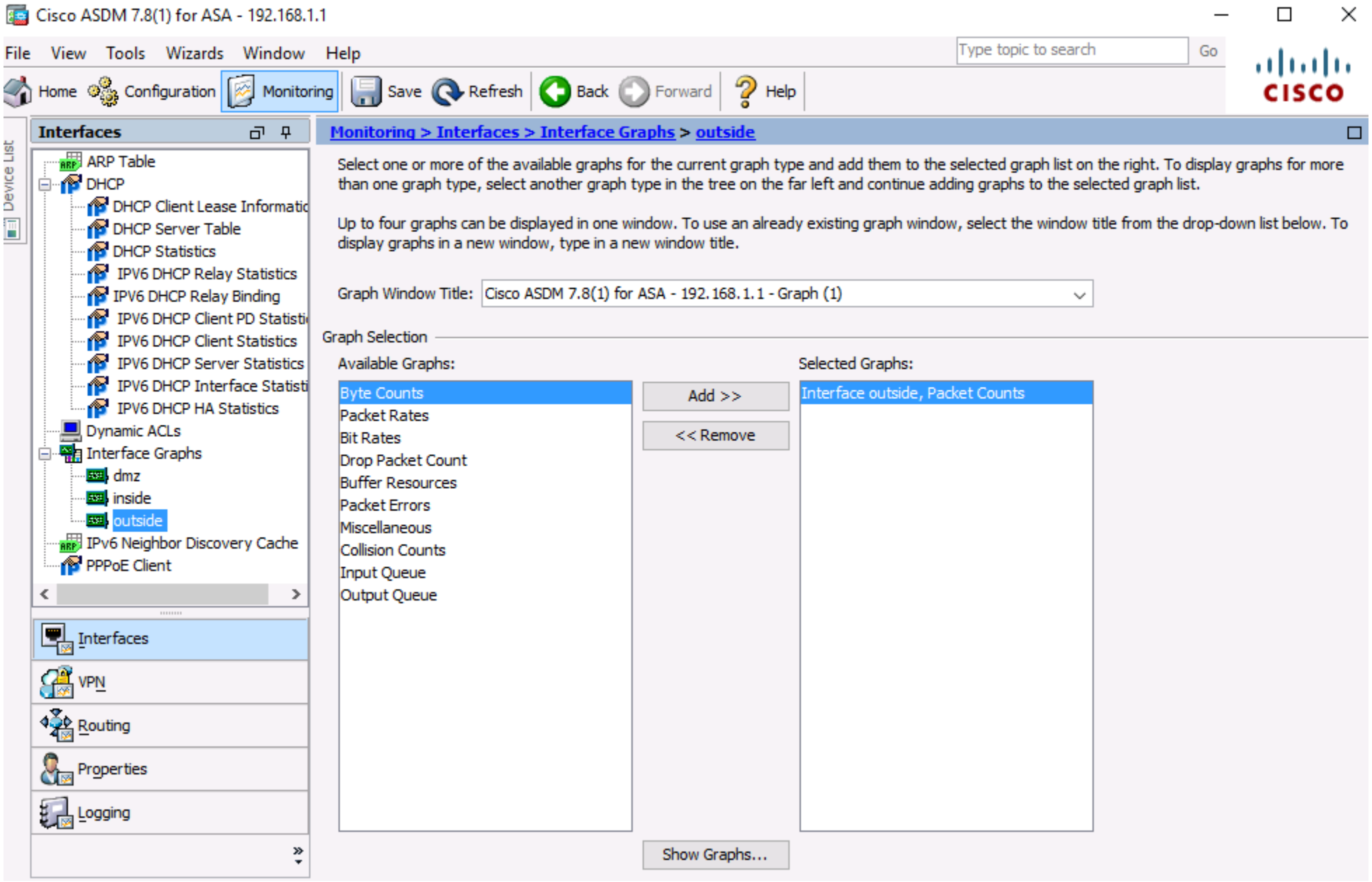
b. Because the ASA inside interface Gi1/2 is set to security level 100 (the highest) and the DMZ interface Gi1/3 is set to 70, you can also access the DMZ server from a host on the inside network. The ASA acts like a router between the two networks. Ping the DMZ server (PC-A) internal address (**192.168.2.3**) from inside network host PC-B (192.168.1.X). The pings should be successful due to the interface security level and the fact that ICMP is being inspected on the inside interface by the global inspection policy.

c. The DMZ server cannot ping PC-B on the inside network. This is because the DMZ interface Gi1/3 has a lower security level. Try to ping from the DMZ server PC-A to PC-B at the IP address 192.168.1.3. The pings should **Not** be successful.

Step 5: Use ASDM Monitoring to graph packet activity.

There are a number of aspects of the ASA that can be monitored using the **Monitoring** screen. The main categories on this screen are **Interfaces**, **VPN**, **Routing**, **Properties**, and **Logging**. In this step, you will create a graph to monitor packet activity for the outside interface.

a. On the **Monitoring** screen > **Interfaces** menu, click **Interface Graphs** > **outside**. Select **Packet Counts** and click **Add** to add the graph. The exhibit below shows Packet Counts added.


Cisco ASDM 7.8(1) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search Go
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Interfaces
ARP Table
DHCP
DHCP Client Lease Informatic
DHCP Server Table
DHCP Statistics
IPV6 DHCP Relay Statistics
IPV6 DHCP Relay Binding
IPV6 DHCP Client PD Statisti
IPV6 DHCP Client Statistics
IPV6 DHCP Server Statistics
IPV6 DHCP Interface Statisti
IPV6 DHCP HA Statistics
Dynamic ACLs
Interface Graphs
dmz
inside
outside
IPv6 Neighbor Discovery Cache
PPPoE Client
Interfaces
VPN
Routing
Properties
Logging
Monitoring > Interfaces > Interface Graphs > outside

Select one or more of the available graphs for the current graph type and add them to the selected graph list on the right. To display graphs for more than one graph type, select another graph type in the tree on the far left and continue adding graphs to the selected graph list.

Up to four graphs can be displayed in one window. To use an already existing graph window, select the window title from the drop-down list below. To display graphs in a new window, type in a new window title.

Graph Window Title: Cisco ASDM 7.8(1) for ASA - 192.168.1.1 - Graph (1)

Graph Selection

Available Graphs: Byte Counts, Packet Rates, Bit Rates, Drop Packet Count, Buffer Resources, Packet Errors, Miscellaneous, Collision Counts, Input Queue, Output Queue

Selected Graphs: Interface outside, Packet Counts

b. Click **Show Graphs** to display the graph. Initially, there is no traffic displayed.

c. From a privileged mode command prompt on R2, simulate Internet traffic to the ASA by pinging the DMZ server's public address with a repeat count of **1000**. You can increase the number of pings if desired.

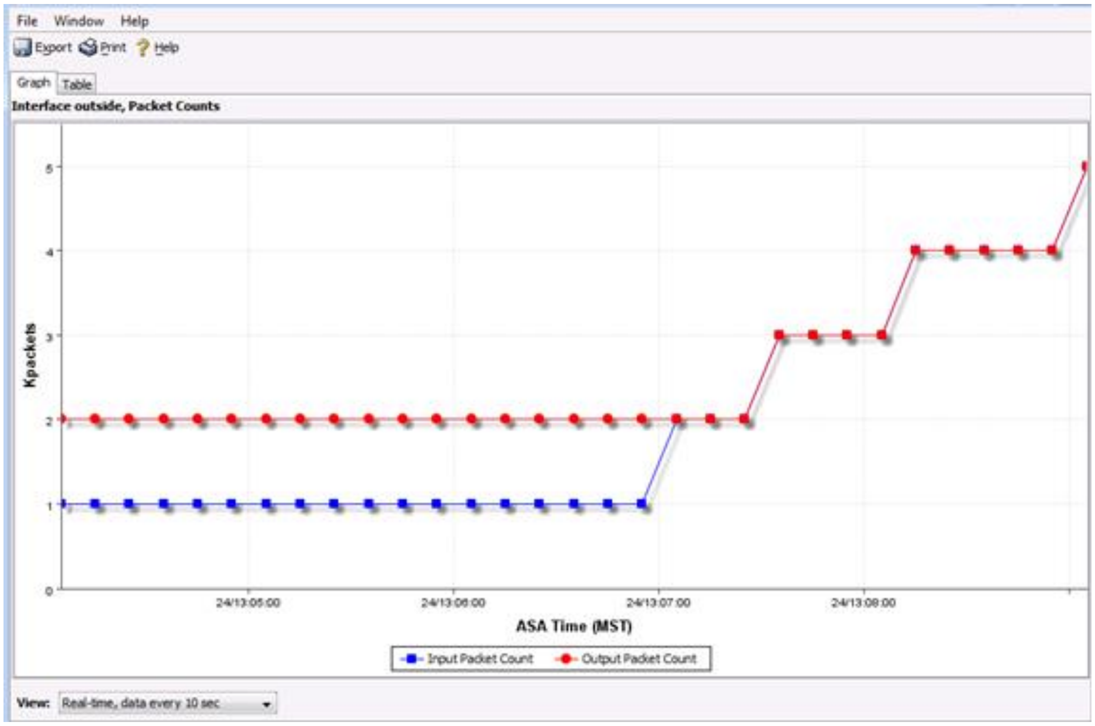
```
R2# ping 209.165.200.227 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/12 ms
```

d. You should see the results of the pings from R2 on the graph. The scale of the graph is automatically adjusted depending on the volume of traffic. You can also view the data in tabular form by clicking the **Table** tab. Notice that the **View** selected at the bottom left of the Graph screen is Real-time, data every 10 seconds. Click the pull-down list to see the other available options.

e. Ping from PC-B to R1 S0/0/0 at **10.1.1.1** using the **–n** option (number of packets) to specify **100** packets.

```
C:>\ ping 10.1.1.1 -n 100
```

Note: The response from the PC is relatively slow, and it may take a while to show up on the graph as Output Packet Count. The graph below shows an additional 4000 input packets and both input and output packet counts.



View: Real-time, data every 10 sec

Reflection

1. What are some of the benefits of using ASDM over the CLI?

____

____

____

____

____

____

2. What are some of the benefits of using the CLI over ASDM?

____

____

____

____

____

____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
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)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	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)
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.				