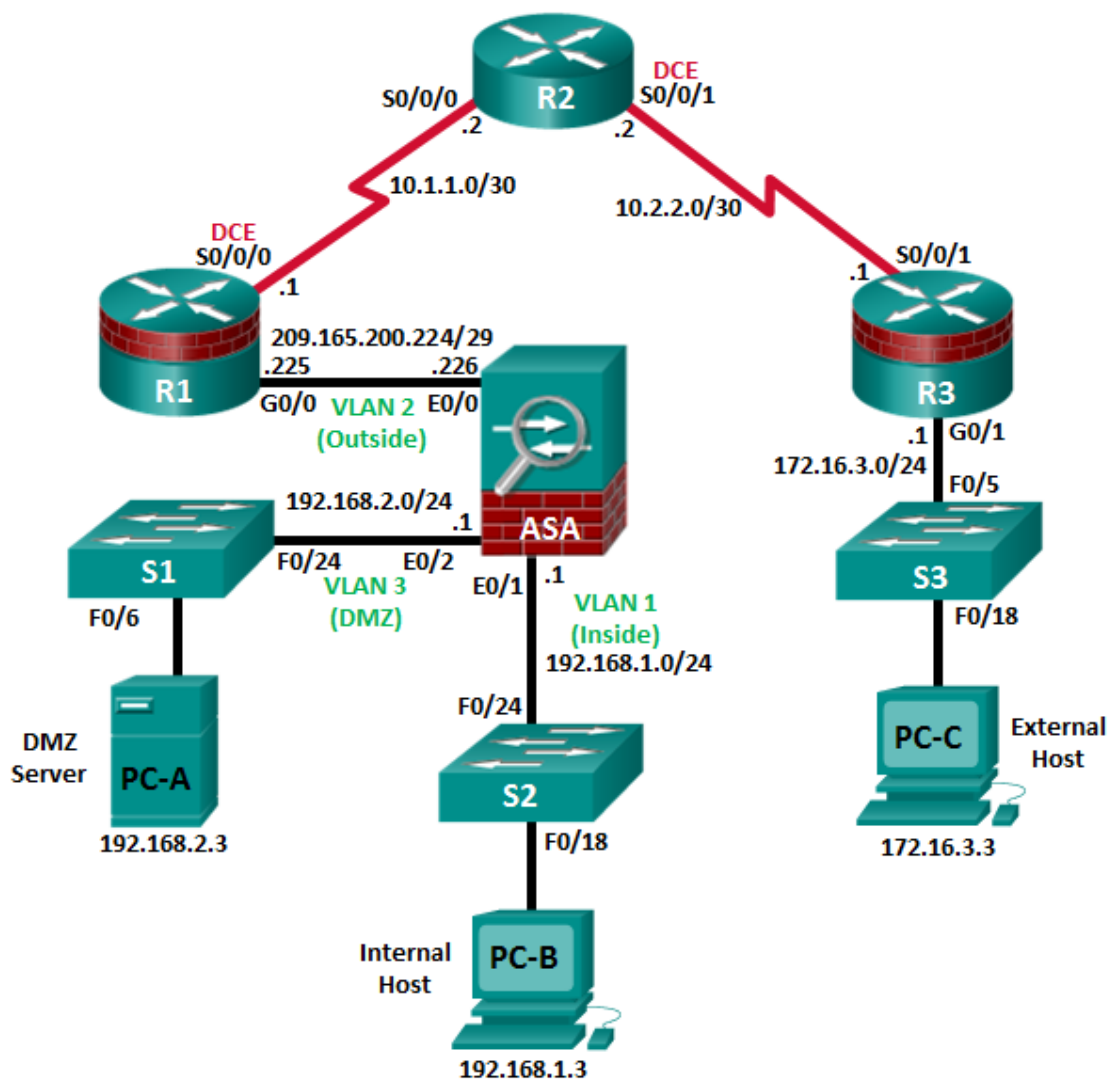


## CCNA Security

# Chapter 10 - Configure ASA Basic Settings and Firewall using ASDM

## 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 E0/0    |
|        | 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 (E0/1) | 192.168.1.1     | 255.255.255.0   | NA              | S2 F0/24    |
|        | VLAN 2 (E0/0) | 209.165.200.226 | 255.255.255.248 | NA              | R1 G0/0     |
|        | VLAN 3 (E0/2) | 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

- Cable the network and clear previous 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 5505 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 5505 with an eight-port integrated switch, running OS version 9.2(3) and ASDM version 7.4(1), and comes with a Base license that allows a maximum of three VLANs.

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

## Required Resources

- 1 ASA 5505 (OS version 9.2(3) and ASDM version 7.4(1) and Base license or comparable)
- 3 routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology package license)
- 3 switches (Cisco 2960 or comparable) (not required)
- 3 PCs (Windows 7 or Windows 8.1, SSH Client, and WinRadius)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

## 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: Cable the network and clear previous device settings.

Attach the devices shown in the topology diagram and cable as necessary. Ensure that the routers and switches have been erased and have no startup configurations.

### Step 2: Configure basic settings for routers and switches.

- Configure hostnames, as shown in the topology, for each router.
- Configure router interface IP addresses, as shown in the IP Addressing table.
- 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 64000
```

- 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 3: Configure static routing on the routers.

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

```
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

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 4: 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.

- Configure a minimum password length. Use the **security passwords** command to set a minimum password length of 10 characters.
- Configure the enable secret password on both routers with a password of **cisco12345**. Use the type 9 (SCRYPT) hashing algorithm.
- Create a local **admin01** account using **admin01pass** for the password. Use the type 9 (SCRYPT) hashing algorithm and set privilege level to 15
- 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.
- 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 5: 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 6: 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 7: 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.**

- Accessing the ASA via the console port is the same as accessing it with a Cisco router or switch. Connect to the ASA console port with a rollover cable.
- Use a terminal emulation program to access the CLI. Use the serial port settings of 9600 baud, 8 data bits, no parity, one stop bit, and no flow control.
- If prompted to enter Interactive Firewall configuration (Setup mode), answer **no**.
- 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**.

```
ciscoasa# reload
Proceed with reload? [confirm] <Enter>
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
CISCO SYSTEMS
Embedded BIOS Version 1.0(12)13 08/28/08 15:50:37.45
<output omitted>
```

**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 VLAN 1 to prepare for ASDM access. The Security Level should be automatically set to the highest level of **100**. The VLAN 1 logical interface will be used by PC-B to access ASDM on ASA physical interface E0/1.

```
ciscoasa(config)# interface vlan 1
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 E0/1. Why is it unnecessary to add physical interface E0/1 to this VLAN?

#### ASA 5505 interface notes:

The 5505 is different from the other 5500 series ASA models. On the other ASAs, like a Cisco router, the physical port can be directly assigned a Layer 3 IP address. The ASA 5505 has eight integrated switch ports that are Layer 2 ports. To assign Layer 3 parameters, you must create a switch virtual interface (SVI) or logical VLAN interface and then assign one or more of the physical Layer 2 ports to it.

By default, all ASA physical interfaces are administratively down unless the Setup utility has been run, or the factory defaults have been reset. Because no physical interface in VLAN 1 has been enabled, the VLAN 1 status is down/down. Use the **show interface ip brief** command to verify this.

```
ciscoasa(config)# show interface ip brief
```

| Interface        | IP-Address  | OK? | Method | Status                | Protocol |
|------------------|-------------|-----|--------|-----------------------|----------|
| Ethernet0/0      | unassigned  | YES | unset  | administratively down | up       |
| Ethernet0/1      | unassigned  | YES | unset  | administratively down | up       |
| Ethernet0/2      | unassigned  | YES | unset  | administratively down | up       |
| Ethernet0/3      | unassigned  | YES | unset  | administratively down | up       |
| Ethernet0/4      | unassigned  | YES | unset  | administratively down | down     |
| Ethernet0/5      | unassigned  | YES | unset  | administratively down | down     |
| Ethernet0/6      | unassigned  | YES | unset  | administratively down | down     |
| Ethernet0/7      | unassigned  | YES | unset  | administratively down | down     |
| Internal-Data0/0 | unassigned  | YES | unset  | up                    | up       |
| Internal-Data0/1 | unassigned  | YES | unset  | up                    | up       |
| Vlan1            | 192.168.1.1 | YES | manual | down                  | down     |
| Virtual0         | 127.0.0.1   | YES | unset  | up                    | up       |

- e. Enable the E0/1 interface using the **no shutdown** command and verify the E0/1 and VLAN 1 interface status. The status and protocol for interface E0/1 and VLAN 1 should be up/up.

```
ciscoasa(config)# interface e0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
```

```
ciscoasa(config)# show interface ip brief
```

| Interface   | IP-Address | OK? | Method | Status                | Protocol |
|-------------|------------|-----|--------|-----------------------|----------|
| Ethernet0/0 | unassigned | YES | unset  | administratively down | up       |
| Ethernet0/1 | unassigned | YES | unset  | up                    | up       |
| Ethernet0/2 | unassigned | YES | unset  | administratively down | up       |

|                  |             |     |        |                       |      |
|------------------|-------------|-----|--------|-----------------------|------|
| Ethernet0/3      | unassigned  | YES | unset  | administratively down | up   |
| Ethernet0/4      | unassigned  | YES | unset  | administratively down | down |
| Ethernet0/5      | unassigned  | YES | unset  | administratively down | down |
| Ethernet0/6      | unassigned  | YES | unset  | administratively down | down |
| Ethernet0/7      | unassigned  | YES | unset  | administratively down | down |
| Internal-Data0/0 | unassigned  | YES | unset  | up                    | up   |
| Internal-Data0/1 | unassigned  | YES | unset  | up                    | up   |
| Vlan1            | 192.168.1.1 | YES | manual | up                    | up   |
| Virtual0         | 127.0.0.1   | YES | unset  | up                    | up   |

- f. Pre-configure outside interface VLAN 2, add physical interface E0/0 to VLAN 2 and bring up the E0/0 interface. You will assign the IP address using ASDM.

```
ciscoasa(config)# interface vlan 2
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# interface e0/0
ciscoasa(config-if)# switchport access vlan 2
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
```

- g. Test connectivity to the ASA by pinging from PC-B to ASA interface VLAN 1 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
```

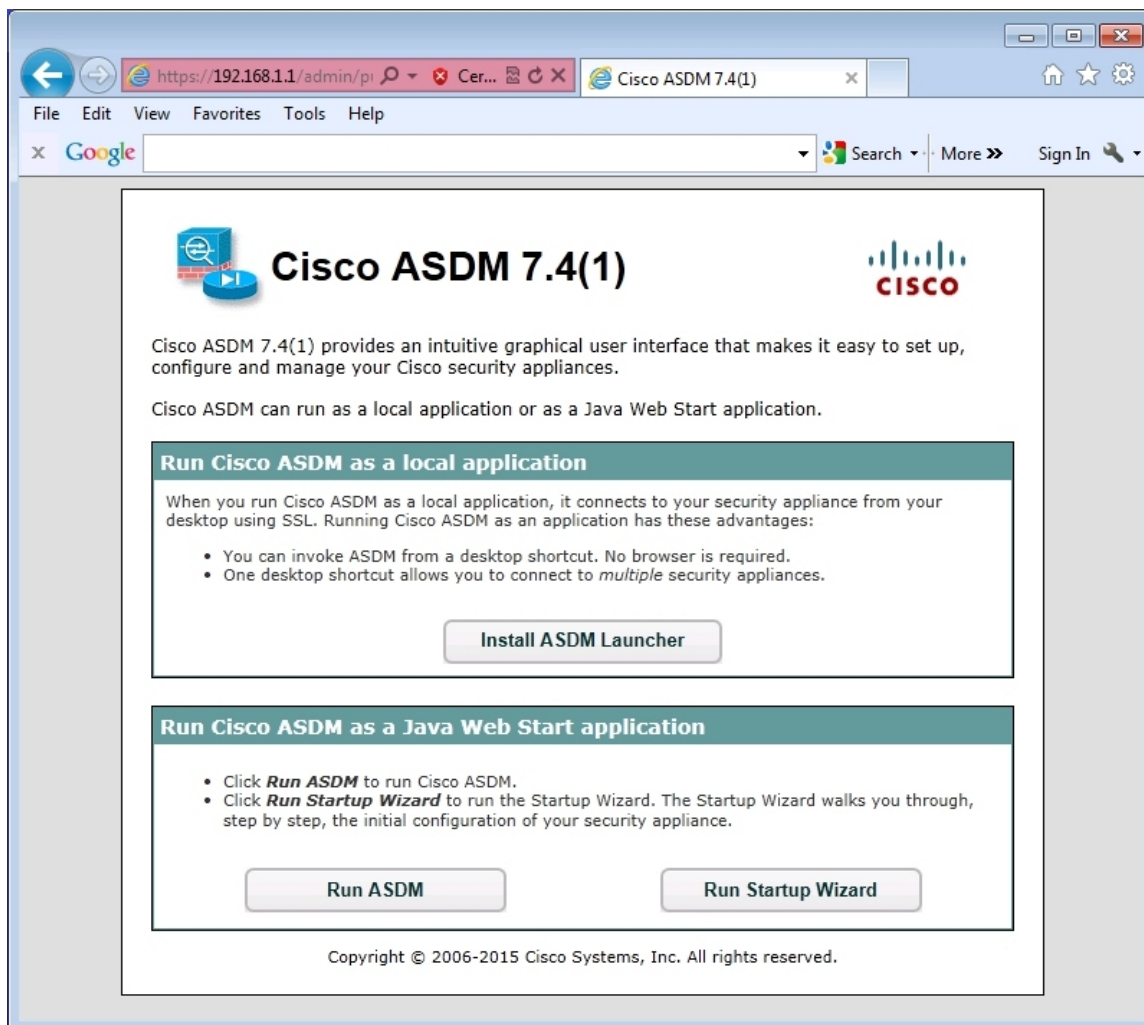
- b. Open a browser on PC-B and test the HTTPS access to the ASA by entering **https://192.168.1.1**.

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

#### Step 5: Access ASDM and explore the GUI.

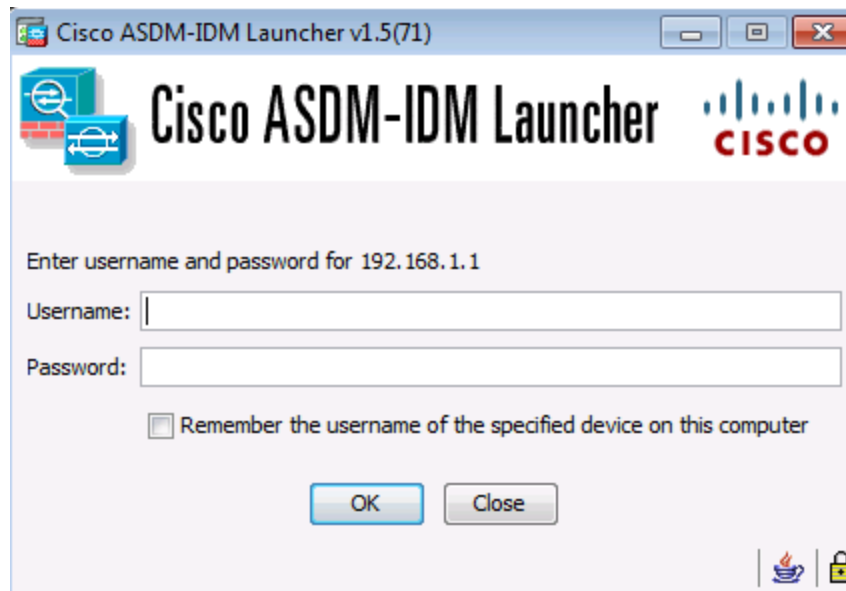


- a. After entering the URL above, you should see a security warning about the website security certificate. Click **Continue to this website**. The ASDM Welcome page will display. From this screen, you can run ASDM as a local application on the PC (installs ASDM on the PC), run ASDM as a browser-based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



- b. Click **Run ASDM**.

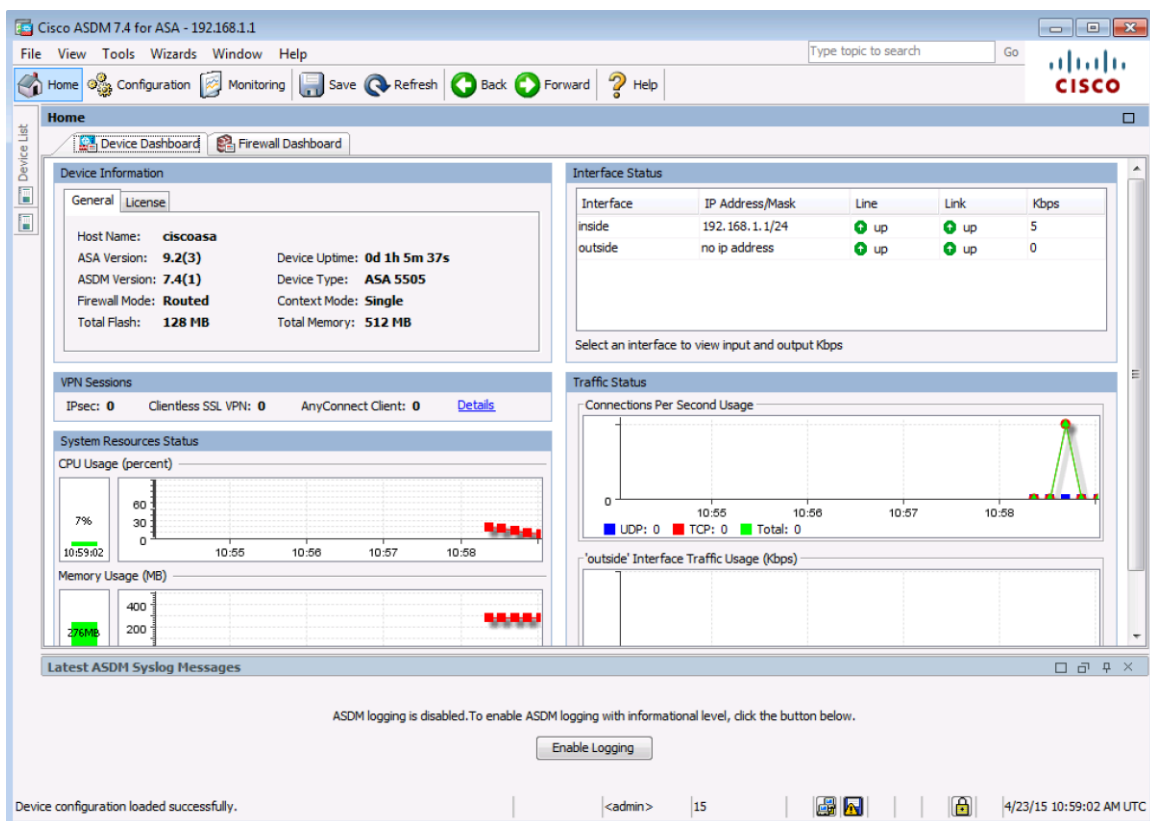
- c. Click **Yes** in response to any other security warnings. You should see the **Cisco ASDM-IDM Launcher** dialog box within which you can enter a username and password. Leave these fields blank as they have not yet been configured.



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

- e. 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 two dashboards: Device and Firewall. The Device dashboard is the default screen and shows device information, such as Type (ASA 5505), 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 Sessions
  - System Resources Status
  - Traffic Status

**Note:** If the Cisco Smart Call Home window appears, click **Do not enable Smart Call Home** and click **OK**.

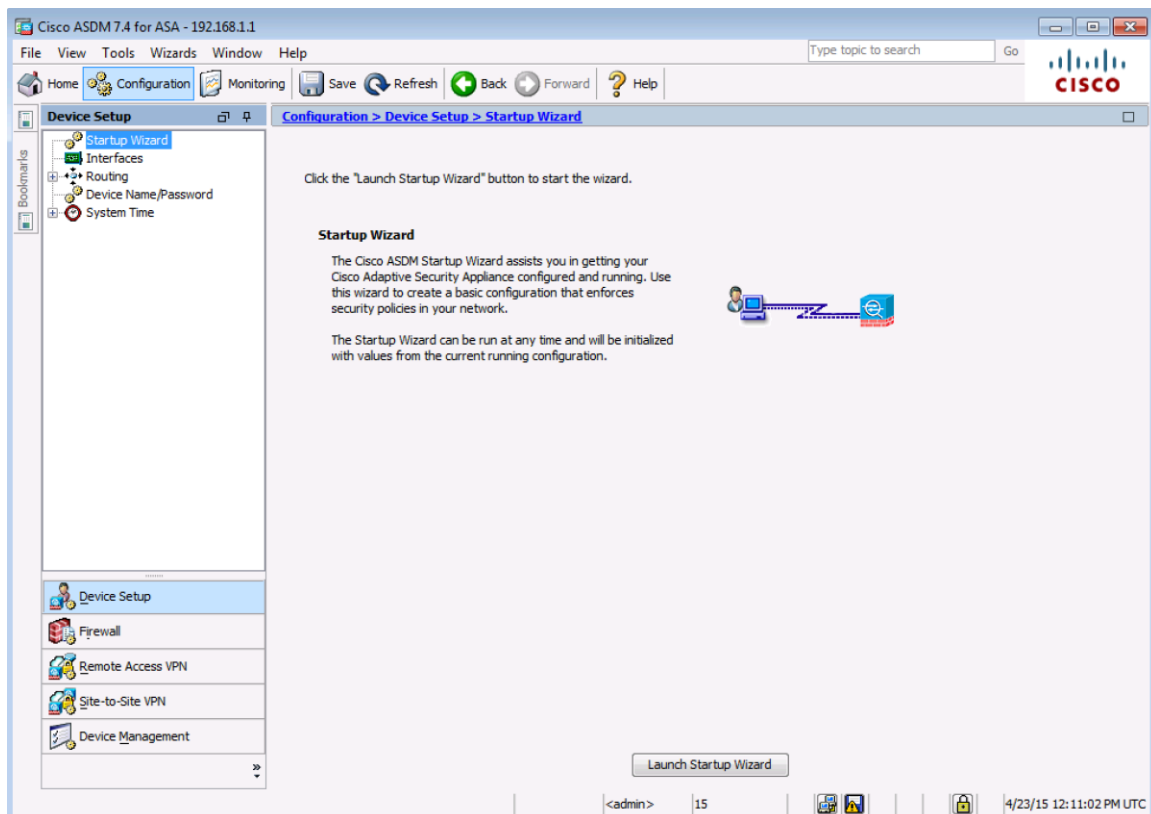


- f. Click the **Configuration** and **Monitoring** buttons to become familiar with their layout and to see what options are available.

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

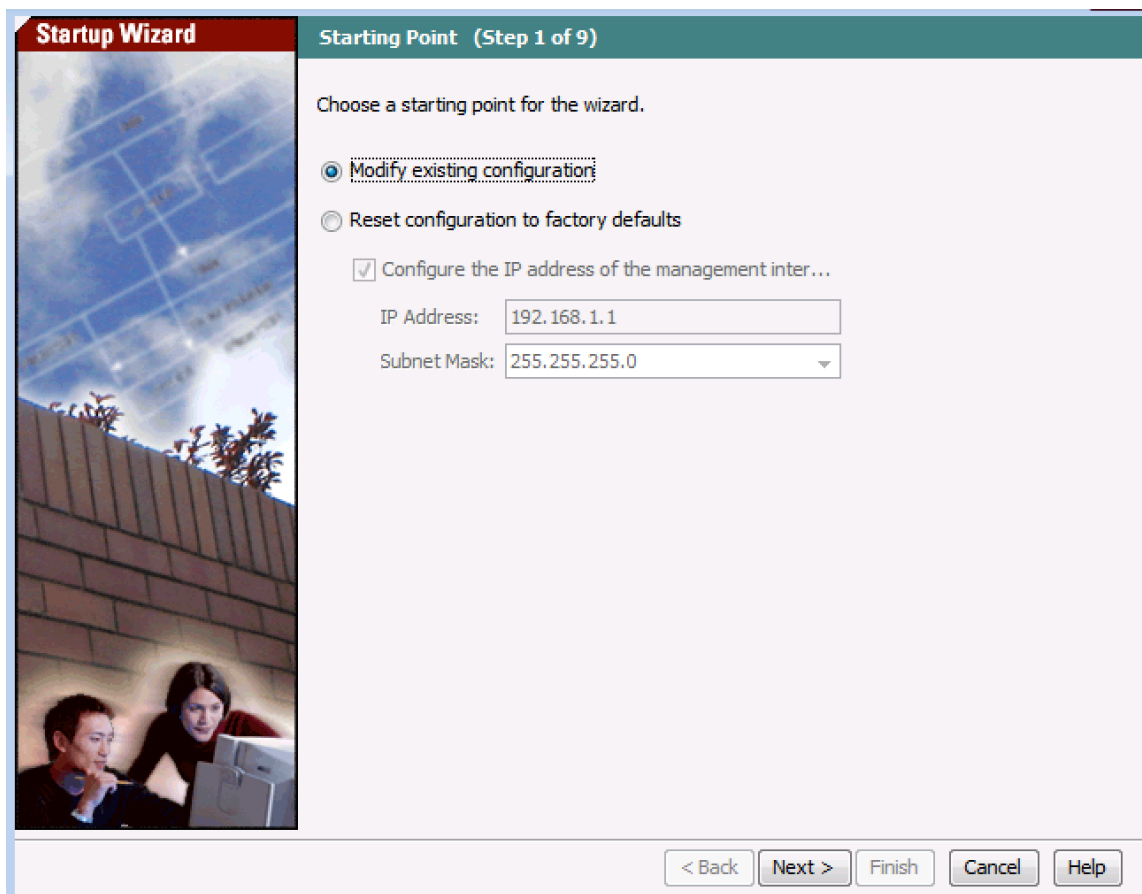
### Step 1: Access the Configuration menu and launch the Startup wizard.

- 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**.



**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.



The screenshot shows the 'Startup Wizard' interface. On the left is a vertical banner image showing a network diagram and two people working on a laptop. The main area is titled 'Starting Point (Step 1 of 9)' and contains the instruction 'Choose a starting point for the wizard.' There are two radio button options: 'Modify existing configuration' (which is selected) and 'Reset configuration to factory defaults'. Below these is a checked checkbox for 'Configure the IP address of the management inter...'. Under this checkbox are two input fields: 'IP Address' with the value '192.168.1.1' and 'Subnet Mask' with the value '255.255.255.0'. At the bottom right are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

**Startup Wizard**

**Starting Point (Step 1 of 9)**

Choose a starting point for the wizard.

☒ **Modify existing configuration**

☐ Reset configuration to factory defaults

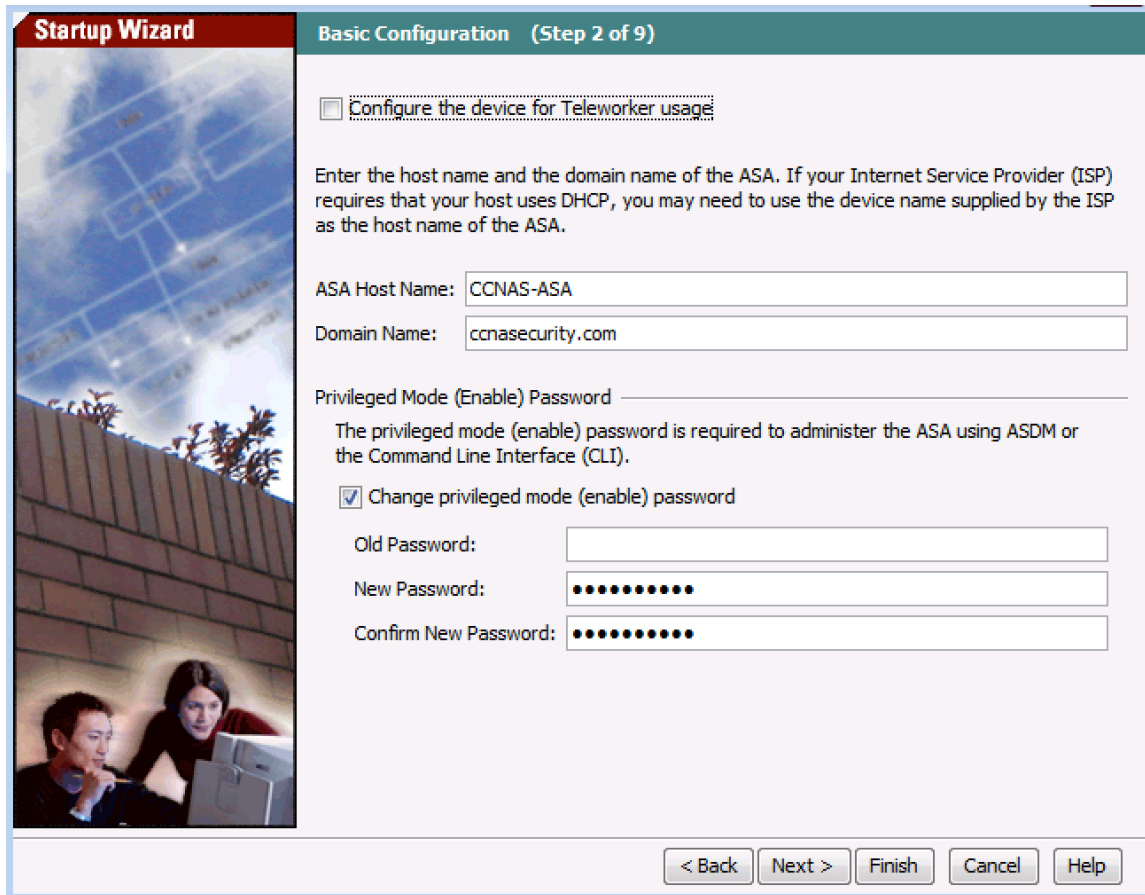
☒ Configure the IP address of the management inter...

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

< Back   Next >   Finish   Cancel   Help

- b. On the Startup Wizard Step 2 screen, configure the ASA hostname **CCNAS-ASA** and domain name **ccnasecurity.com**. Click the check box for changing the enable mode password, change it from blank (no password) to **cisco12345**, and enter it again to confirm. When the entries are completed, click **Next** to continue.



**Startup Wizard**

**Basic Configuration (Step 2 of 9)**

☐ Configure the device for Teleworker usage

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:

Domain Name:

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:

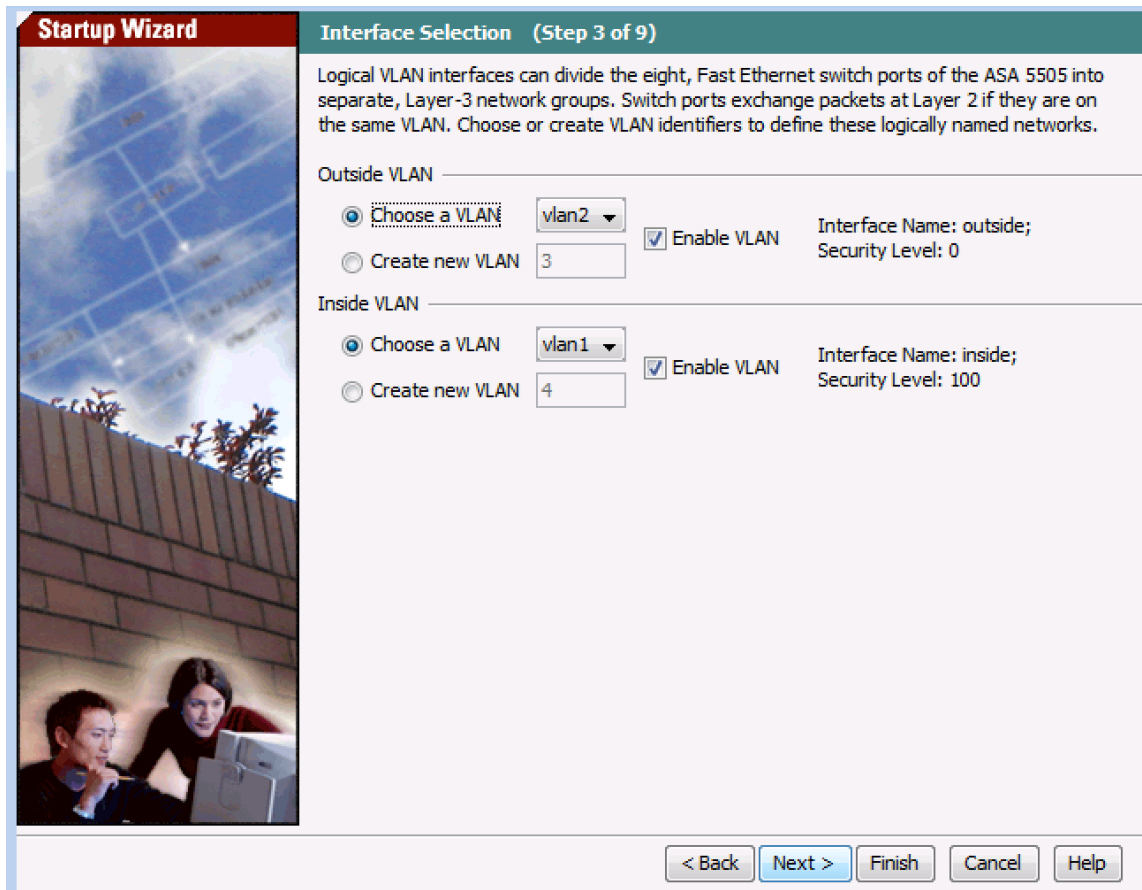
New Password:

Confirm New Password:

< Back   Next >   Finish   Cancel   Help

**Step 3: Configure the inside and outside VLAN interfaces.**

- a. On the Startup Wizard Step 3 screen for the Outside and Inside VLANs, do not change the current settings because these were previously defined using the CLI. The inside VLAN is named **inside**, and the security level is set to 100 (highest). The Outside VLAN interface is named **outside**, and the security level is set to 0 (lowest). Click **Next** to continue.



**Startup Wizard**

**Interface Selection (Step 3 of 9)**

Logical VLAN interfaces can divide the eight, Fast Ethernet switch ports of the ASA 5505 into separate, Layer-3 network groups. Switch ports exchange packets at Layer 2 if they are on the same VLAN. Choose or create VLAN identifiers to define these logically named networks.

**Outside VLAN**

☒ Choose a VLAN vlan2 ☒ Enable VLAN Interface Name: outside; Security Level: 0

☐ Create new VLAN 3

**Inside VLAN**

☒ Choose a VLAN vlan1 ☒ Enable VLAN Interface Name: inside; Security Level: 100

☐ Create new VLAN 4

< Back Next > Finish Cancel Help

- b. On the Startup Wizard Step 4 screen – Switch Port Allocation, verify that port **Ethernet0/1** is allocated for Inside VLAN 1 and that port **Ethernet0/0** is allocated for Outside VLAN 2. Click **Next** to continue.

**Startup Wizard**

**Switch Port Allocation (Step 4 of 9)**

Allocate physical switch ports to each logically named VLAN.

Switch Ports for Outside VLAN (vlan2)

| Available Ports | Allocated Ports |
|-----------------|-----------------|
| Ethernet0/1     | Ethernet0/0     |
| Ethernet0/2     |                 |
| Ethernet0/3     |                 |
| Ethernet0/4     |                 |
| Ethernet0/5     |                 |
| Ethernet0/6     |                 |
| Ethernet0/7     |                 |

Buttons: Add >> << Remove

Switch Ports for Inside VLAN (vlan1)

| Available Ports | Allocated Ports |
|-----------------|-----------------|
| Ethernet0/0     | Ethernet0/1     |
|                 | Ethernet0/2     |
|                 | Ethernet0/3     |
|                 | Ethernet0/4     |
|                 | Ethernet0/5     |
|                 | Ethernet0/6     |
|                 | Ethernet0/7     |

Buttons: Add >> << Remove

Navigation: < Back Next > Finish Cancel Help



- c. On the Startup Wizard Step 5 screen – Interface IP Address Configuration, 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**. Click **Next** to continue.

**Startup Wizard**

**Interface IP Address Configuration (Step 5 of 9)**

Assign IP addresses to each named VLAN.

Outside IP Address

☒ Use the following IP address

IP Address: 209.165.200.226 Mask: 255.255.255.248

☐ Use DHCP ☐ Obtain default route using DHCP

☐ Use PPPoE

Inside IP Address

☒ Use the following IP address

IP Address: 192.168.1.1 Mask: 255.255.255.0

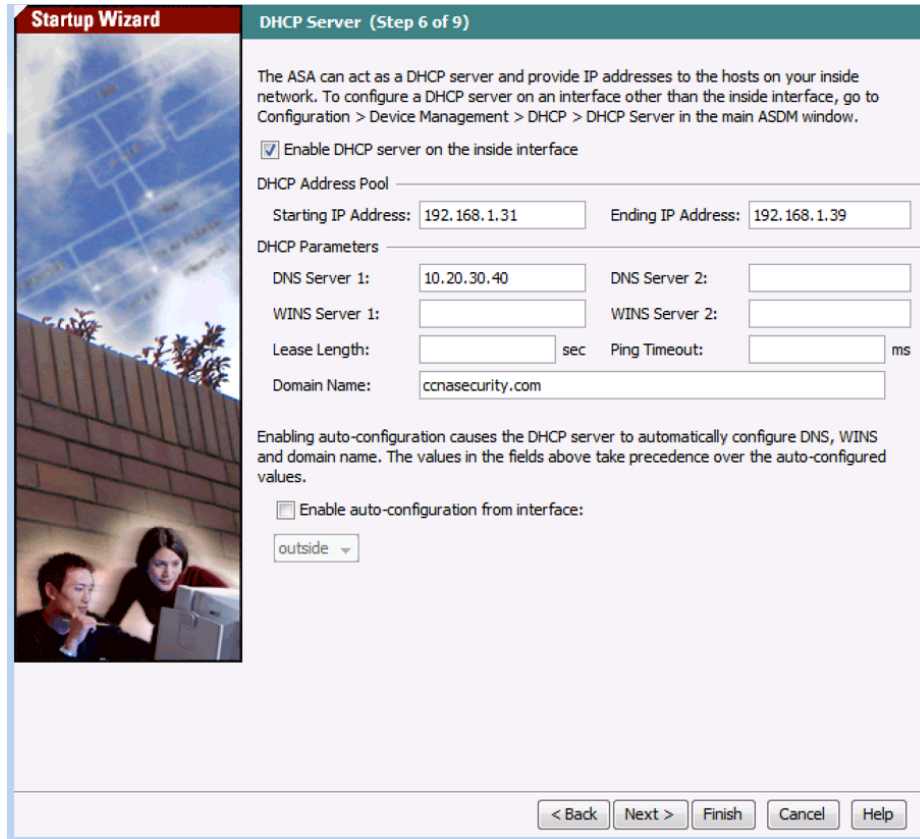
☐ Use DHCP ☐ Obtain route using DHCP

☐ Use PPPoE

< Back Next > Finish Cancel Help

**Step 4: 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. Enter a Starting IP Address of **192.168.1.31** and an Ending IP Address of **192.168.1.39**. 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. Click **Next** to continue.



**Startup Wizard** **DHCP Server (Step 6 of 9)**

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:  Ending IP Address:

DHCP Parameters

DNS Server 1:  DNS Server 2:

WINS Server 1:  WINS Server 2:

Lease Length:  sec Ping Timeout:  ms

Domain Name:

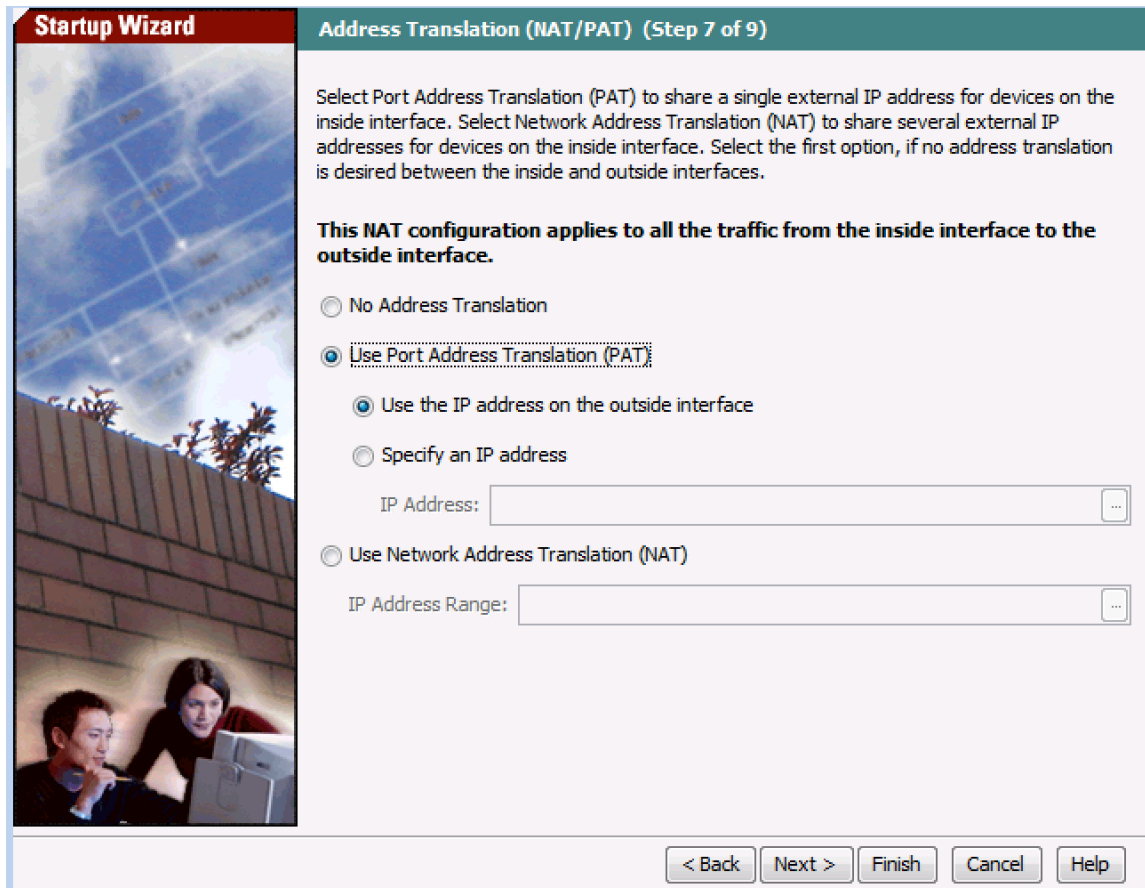
Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

☐ Enable auto-configuration from interface:

< Back Next > Finish Cancel Help

- b. On the Startup Wizard Step 7 screen – 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.



The image shows the 'Startup Wizard' interface for Step 7 of 9, titled 'Address Translation (NAT/PAT)'. On the left is a vertical sidebar with a graphic of a brick wall and a person looking at a computer. The main area contains instructions: '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.' Below this, a bold statement reads: 'This NAT configuration applies to all the traffic from the inside interface to the outside interface.' There are two main radio button options: 'No Address Translation' and 'Use Port Address Translation (PAT)'. The 'Use Port Address Translation (PAT)' option is selected and has a sub-option 'Use the IP address on the outside interface' also selected. There is also a 'Specify an IP address' option with an 'IP Address:' text box and a selection button. The 'Use Network Address Translation (NAT)' option is unselected and has an 'IP Address Range:' text box and a selection button. At the bottom are buttons for '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

**Startup Wizard**

**Address Translation (NAT/PAT) (Step 7 of 9)**

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:

< Back   Next >   Finish   Cancel   Help

- c. On the Startup Wizard Step 8 screen – 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.

**Startup Wizard**

**Administrative Access (Step 8 of 9)**

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/<br>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.

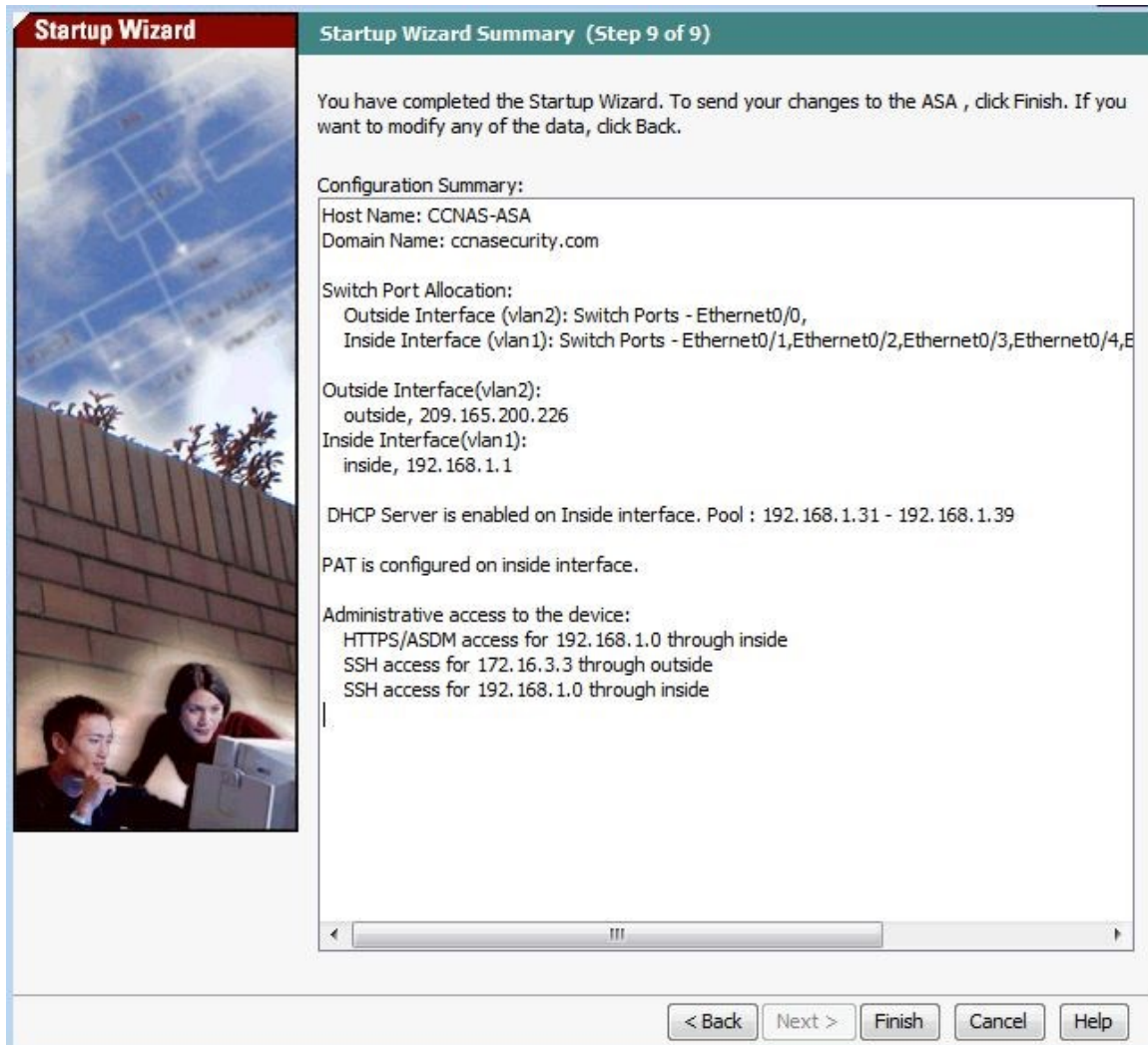
☐ Enable ASDM history metrics

< Back   Next >   Finish   Cancel   Help

**Step 5: Review the summary and deliver the commands to the ASA.**

- a. On the Startup Wizard Step 9 screen – 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 the GUI dialogue box stops responding during the reload process, close it, exit ASDM, and restart the browser and ASDM. If prompted to save the configuration to flash memory, respond with **Yes**. Even though ASDM may not appear to have reloaded the configuration, the commands were delivered. If there are errors encountered as ASDM delivers the commands, you will be notified with a list of commands that succeeded and the commands that failed.



- b. Restart ASDM and provide the new enable password **cisco12345** with no username. 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. The Traffic Status window may show the ASDM access as TCP traffic spike.

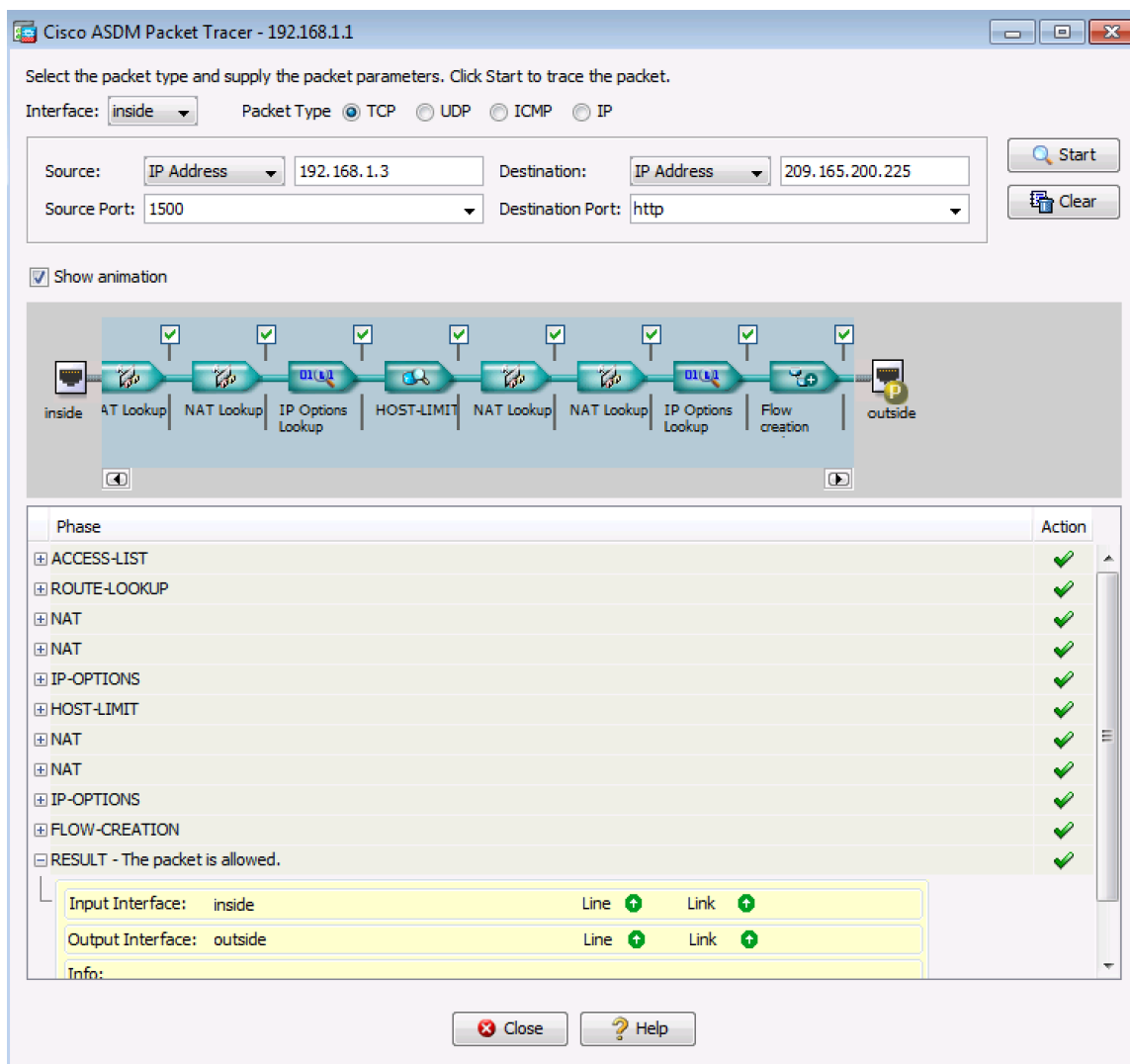
**Step 6: Test access to an external website from PC-B.**

- 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.

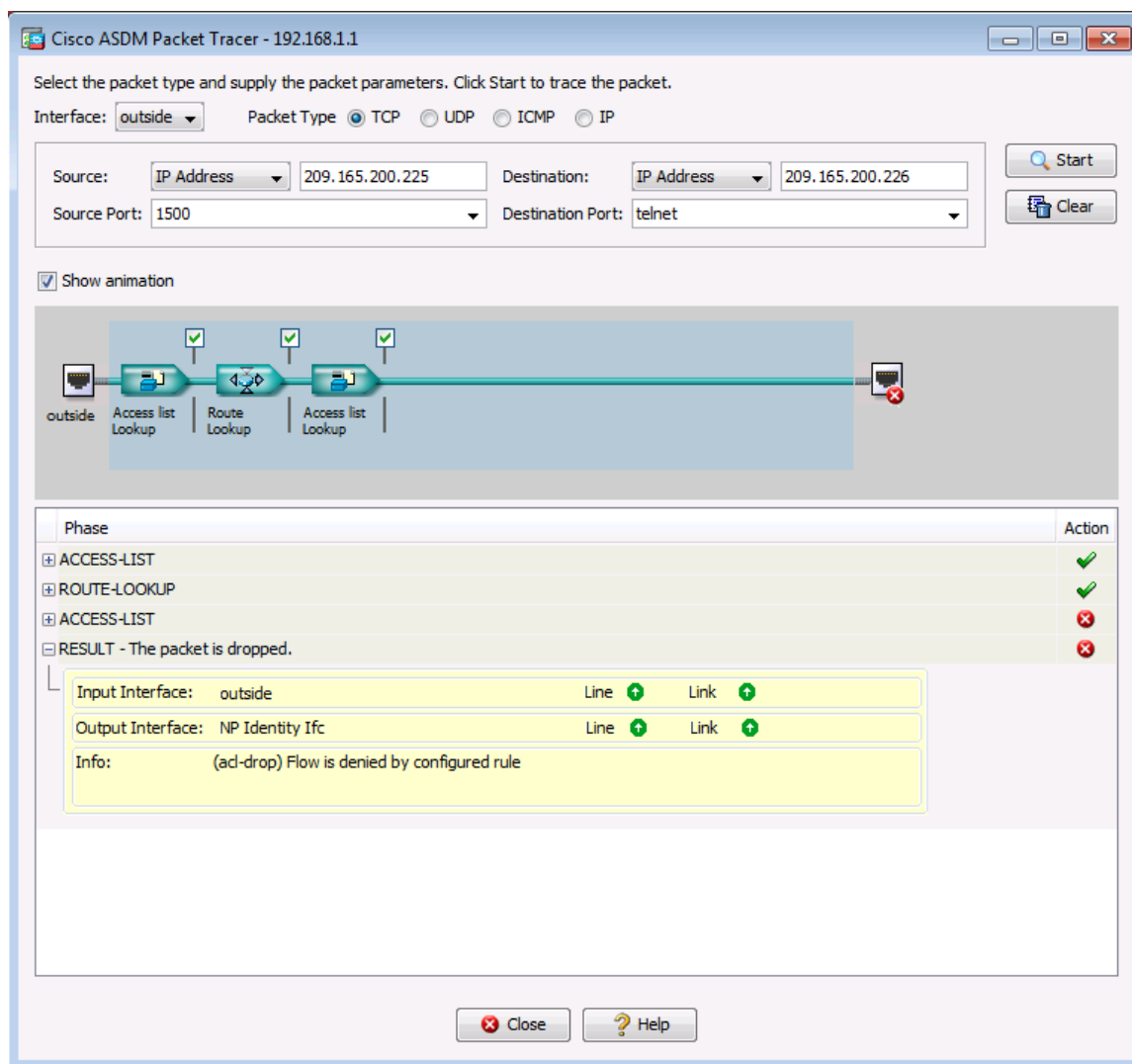
- b. The R1 HTTP server was enabled in Part 1. You should be prompted with a user authentication login dialog box from the R1 GUI device manger. Enter the username **admin01** and the password **admin01pass**. Exit the browser. You should see TCP activity in the ASDM Device dashboard Traffic Status window on the Home page.

### Step 7: Test access to an external website using the ASDM Packet Tracer utility.

- a. Click **Tools > Packet Tracer**.
- b. Select the **inside** interface from the Interface drop-down list and click **TCP** from the Packet Type radio buttons. 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 Fa0/0) with a Destination Port of **HTTP**. Click **Start** to begin the trace of the packet. The packet should be permitted.



- c. Click **Clear** to reset the entries. Try another trace and select **outside** from the **Interface** drop-down list and leave **TCP** as the packet type. 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**. Click **Start** to begin the trace of the packet. The packet should be dropped. Click **Close** to continue.



The screenshot shows the Cisco ASDM Packet Tracer interface. The title bar reads "Cisco ASDM Packet Tracer - 192.168.1.1". The main window has a header that says "Select the packet type and supply the packet parameters. Click Start to trace the packet." Below this, the "Interface" is set to "outside", "Packet Type" is "TCP", "Source" is "IP Address" with value "209.165.200.225", "Destination" is "IP Address" with value "209.165.200.226", "Source Port" is "1500", and "Destination Port" is "telnet". There are "Start" and "Clear" buttons. A checkbox "Show animation" is checked. Below this is a visual representation of the packet's path: "outside" (with a green checkmark) -> "Access list Lookup" (with a green checkmark) -> "Route Lookup" (with a green checkmark) -> "Access list Lookup" (with a green checkmark) -> "NP Identity Ifc" (with a red X). Below the path is a table showing the phases of the packet trace.

| Phase                           | Action |
|---------------------------------|--------|
| + ACCESS-LIST                   | ✓      |
| + ROUTE-LOOKUP                  | ✓      |
| + ACCESS-LIST                   | ✗      |
| RESULT - The packet is dropped. | ✗      |

Below the table, there is a yellow box containing the following information:

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

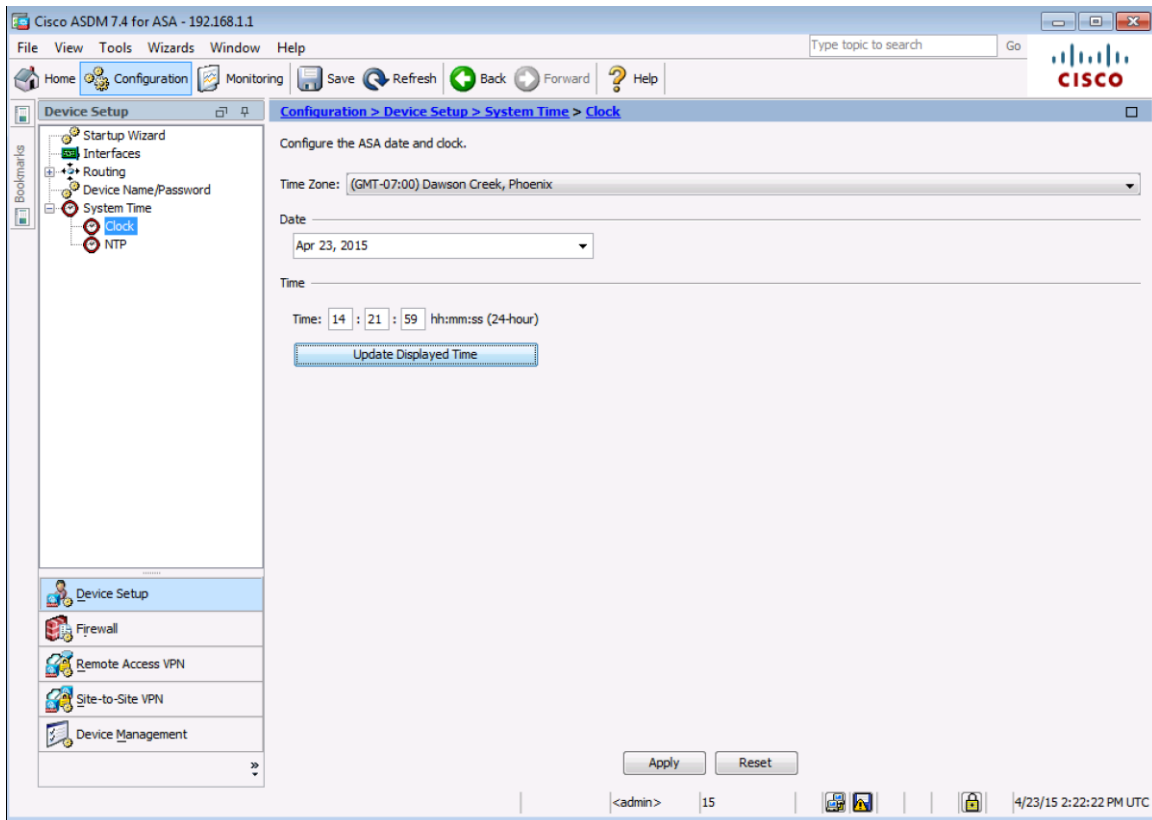
At the bottom of the window are "Close" and "Help" buttons.

## 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.

- On the **Configuration** screen > **Device Setup** menu, click **System Time** > **Clock**.
- 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.) Click **Apply** to send the commands to the ASA.





**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**). 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. Click **Close** to continue.

**Ping**

Packet Type: ☒ ICMP ☐ TCP

Destination

IP Address or Hostname: 10.1.1.1 Port:

Source

Interface (optional): -- None --

IP Address (optional):

Port: ☒ Random port ☐ Starting port:

Repeat(optional): Timeout(optional):

Ping Output:

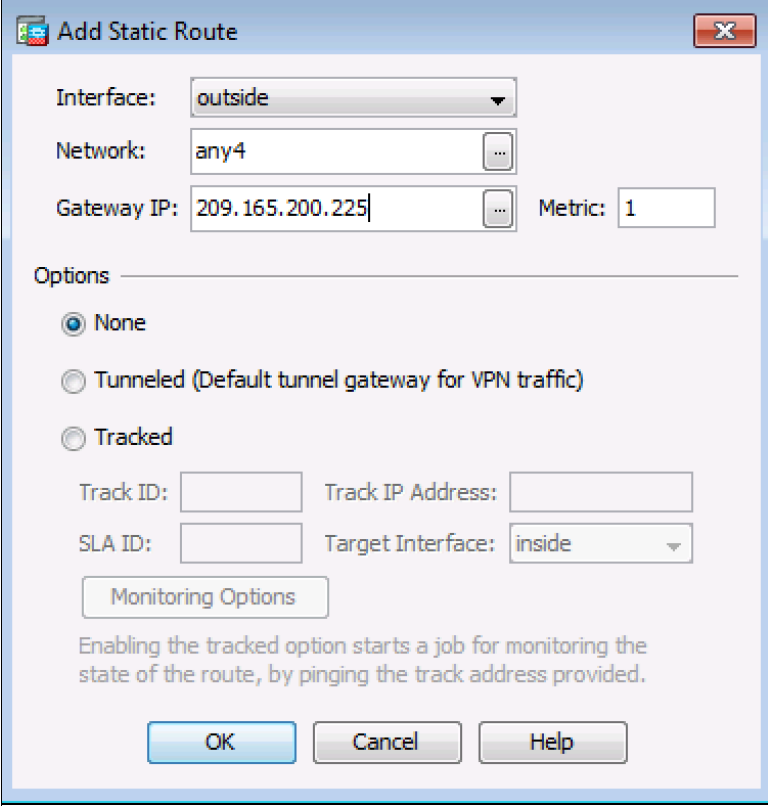
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:  
No route to host 10.1.1.1  
Success rate is 0 percent (0/1)

Clear Output

Ping Close Help

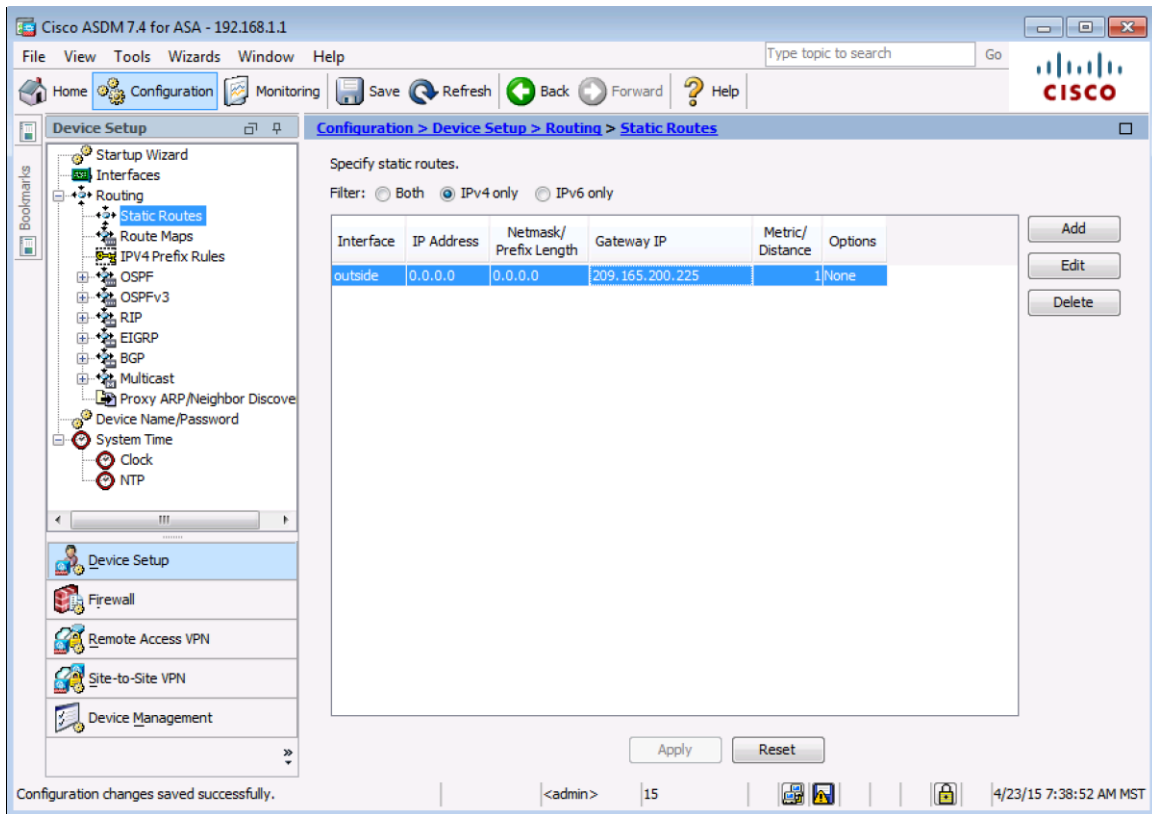
- b. From the **Configuration** screen > **Device Setup** menu, click **Routing** > **Static Routes**. Click **IPv4 Only** and click **Add** to add a new static route.

- c. On the Add Static Route dialog box, select the **outside** interface from the drop-down list. Click the ellipsis button to the right of **Network**, select **any4** from the list of network objects, and click **OK**. The selection of **any4** translates to a “quad zero” route. For the Gateway IP, enter **209.165.200.225** (R1 G0/0).

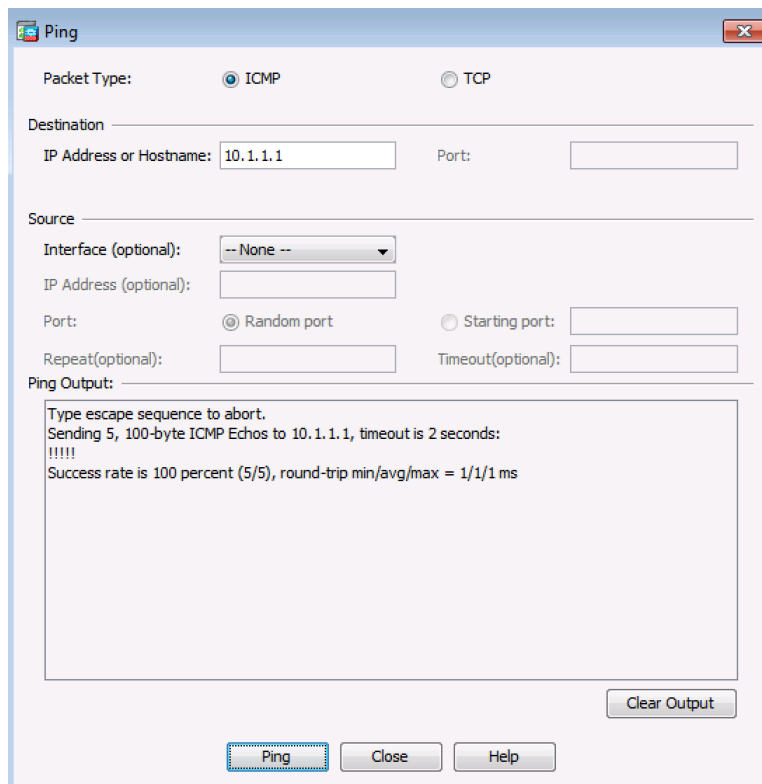


The image shows the "Add Static Route" dialog box in a network configuration tool. The "Interface" dropdown is set to "outside". The "Network" field is set to "any4", with an ellipsis button to its right. The "Gateway IP" field is set to "209.165.200.225", also with an ellipsis button. The "Metric" field is set to "1". Under the "Options" section, the "None" radio button is selected. Below this, there are fields for "Track ID", "Track IP Address", "SLA ID", and "Target Interface" (set to "inside"). A "Monitoring Options" button is located below these fields. A note at the bottom states: "Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided." At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

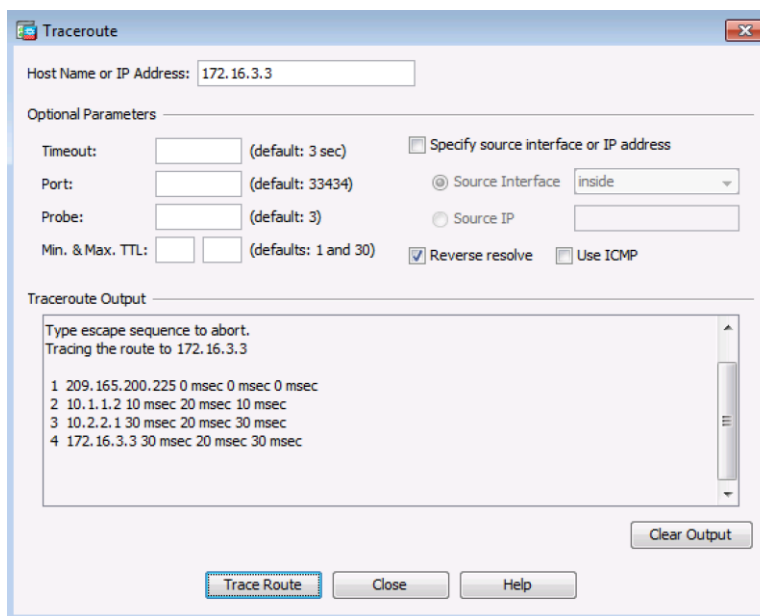
- d. Click **OK** > **Apply** to send the commands to the ASA.



- e. 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.



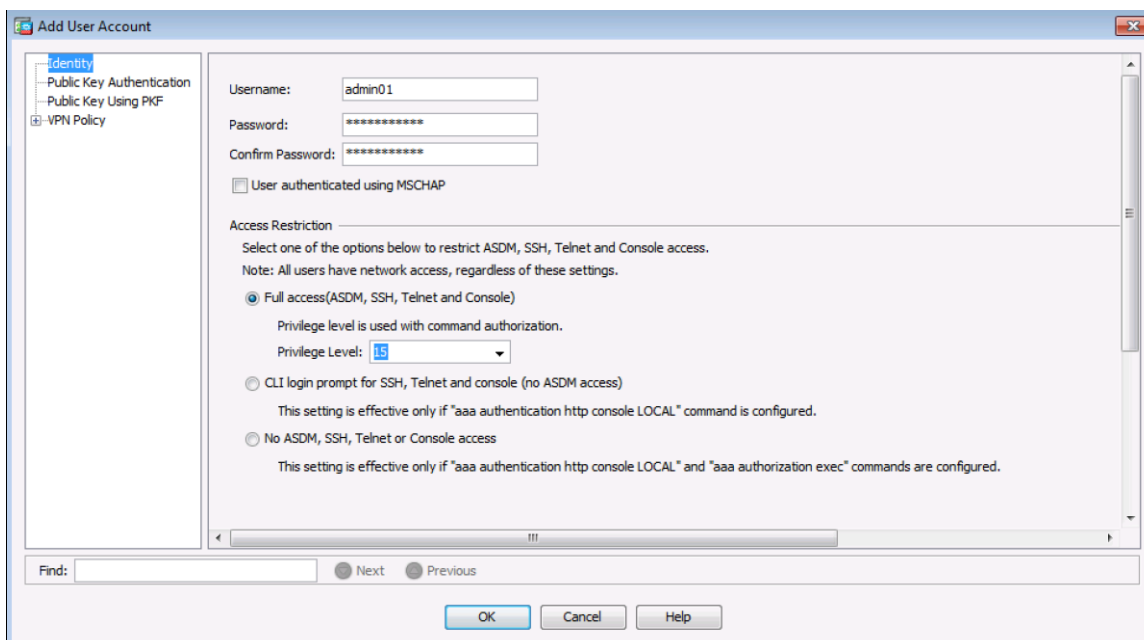
- f. On the ASDM **Tools** menu, select **Traceroute** and enter the IP address of external host PC-C (**172.16.3.3**). Click **Trace Route**. The traceroute should succeed and show the hops from the ASA through R1, R2, and R3 to host PC-C. Click **Close** to continue.



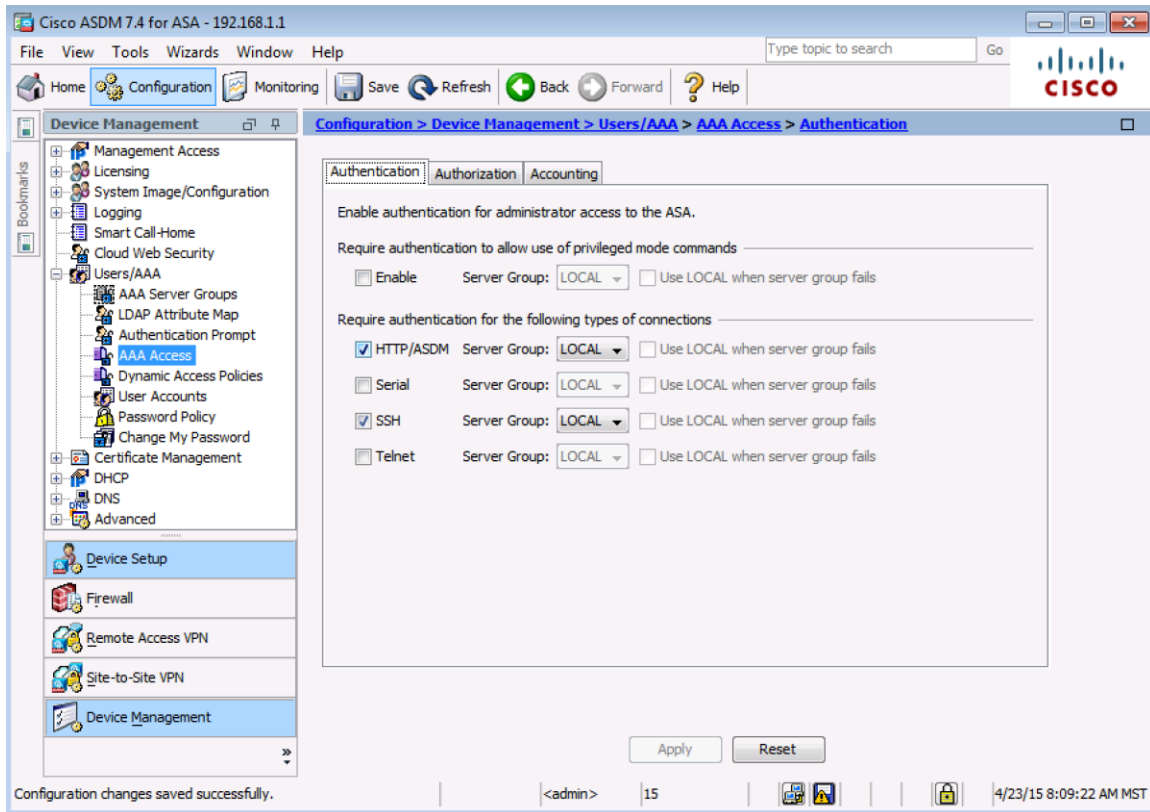
### Step 3: Configure AAA user authentication using the ASA local database.

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**. Click **User Accounts** > **Add**. Create a new user named **admin01** with a password of **admin01pass** 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**. Click **OK** to add the user and click **Apply** to send the command to the ASA.



- b. On the **Configuration** screen > **Device Management** area, click **Users/AAA**. Click **AAA Access**. 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. Click **Apply** to send the commands to the ASA.



**Note:** The next action you attempt within ASDM will require that you log in as **admin01** with the password **admin01pass**.

#### Step 4: Test SSH access to the ASA.

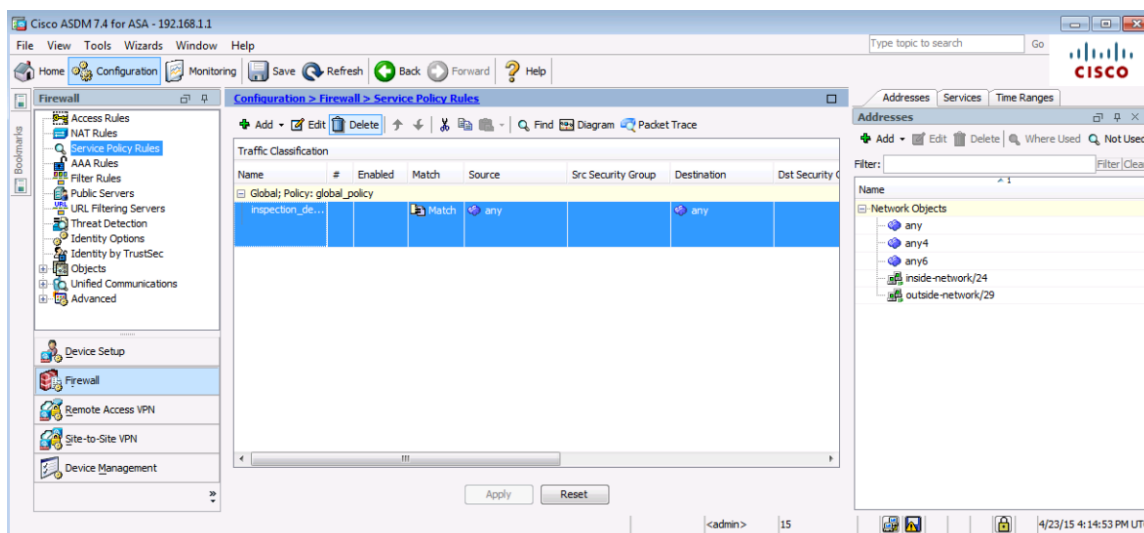
- Open a SSH client on PC-B, such as PuTTY, and connect to the ASA inside interface at IP address **192.168.1.1**. When prompted to log in, enter the user name **admin01** and the password **admin01pass**.
- From **PC-C**, open an SSH client, such as PuTTY, and attempt to access the ASA outside interface at **209.165.200.226**. When prompted to log in, enter the user name **admin01** and the password **admin01pass**.
- 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.

**Note:** The idle timeout for SSH can be modified. You can change this setting by using the CLI **logging synchronous** command or go to ASDM **Device Management > Management Access > ASDM/HTTP/Telnet/SSH**.

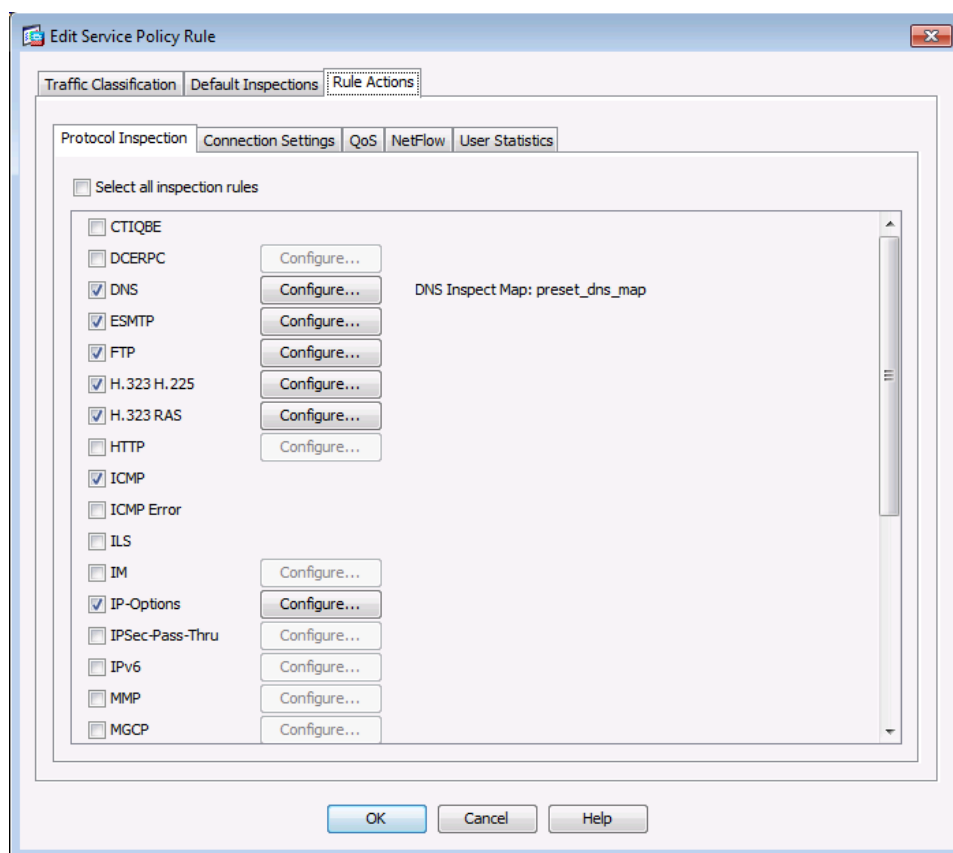
#### Step 5: Modify the MPF application inspection policy.

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. On the **Configuration** screen > **Firewall** area menu, click **Service Policy Rules**.



- b. Select the **inspection\_default** policy and click **Edit** to modify the default inspection rules. 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. Click **OK > Apply** to send the commands to the ASA. If prompted, log in as **admin01** with the password **admin01pass**.



- c. 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 Part 3, you configured address translation using PAT for the inside network. 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 create a new interface VLAN 3 named **dmz**, assign physical interface E0/2 to the VLAN, set the security level to **70**, and limit communication from this interface to the inside (VLAN1) interface.

- On the **Configuration** screen > **Device Setup** menu, click **Interfaces**. The Interface tab is displayed by default and the currently defined inside (VLAN 1, E0/1) and outside (VLAN 2, E0/0) interfaces are listed. Click **Add** to create a new interface.
- In the Add Interface dialog box, select port **Ethernet0/2** and click **Add**. You will be prompted to change the interface from the inside network. Click **OK** on the message to remove the port from the inside interface and add it to this new interface. 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.
- 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**. Do NOT click **OK** at this time.

**Add Interface**

General Advanced IPv6

Switch Ports

Available Switch Ports

- Ethernet0/0
- Ethernet0/1
- Ethernet0/2**
- Ethernet0/4
- Ethernet0/5
- Ethernet0/6

Add >>

Remove <<

Selected Switch Ports

- Ethernet0/2**

Interface Name: **dmz**

Security Level: **70**

☐ Dedicate this interface to management only

☒ 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**

Description:

OK Cancel Help

- d. ASDM will configure this interface as VLAN ID 12 by default. Before clicking **OK** to add the interface, click the **Advanced** tab and specify this interface as VLAN ID **3**.

**Note:** If you are working with the ASA 5505 Base license, you are allowed to create up to three named interfaces. However, you must disable communication between the third interface and one of the other interfaces. Because the DMZ server does not need to initiate communication with the inside users, you can disable forwarding to interfaces VLAN 1.

- e. On the Advanced tab, you need to block traffic from this interface VLAN 3 (dmz) to the VLAN 1 (inside) interface. In the Block Traffic area, select **vlan1 (inside)** from the drop-down list. Click **OK** to return to the Interfaces window.

- f. You should see the new interface named **dmz**, in addition to the inside and outside interfaces. Check the box **Enable traffic between two or more interfaces which are configured with the same security levels**. Click **Apply** to send the commands to the ASA.

| Name    | Switch Ports                    | Enabled | Security Level | IP Address      | Subnet Mask Prefix Length | Restrict Traffic flow |
|---------|---------------------------------|---------|----------------|-----------------|---------------------------|-----------------------|
| inside  | Ethernet0/1, Ethernet0/3, Et... | Yes     | 100            | 192.168.1.1     | 255.255.255.0             |                       |
| outside | Ethernet0/0                     | Yes     | 0              | 209.165.200.226 | 255.255.255.248           |                       |
| dmz     | Ethernet0/2                     | Yes     | 70             | 192.168.2.1     | 255.255.255.248           | vlan1 (inside)        |

☒ 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



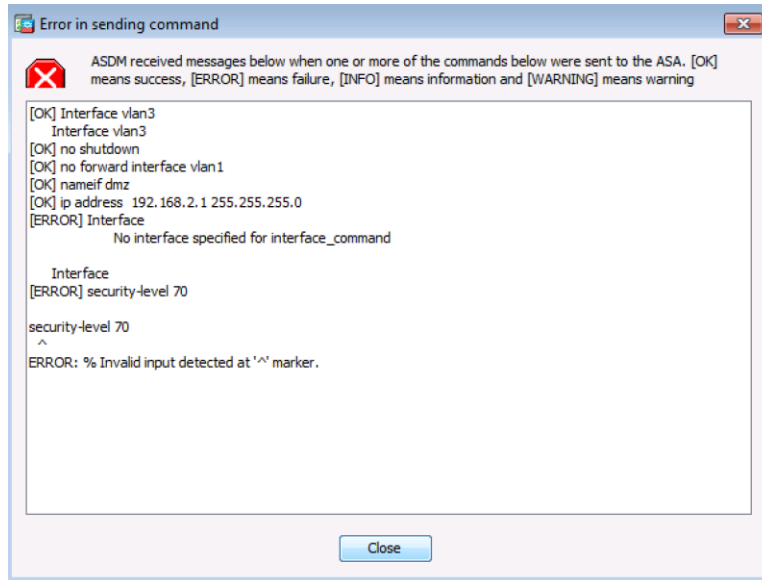
**Note:** If an **Error in sending command** window appears when you apply the dmz interface configuration to the ASA, you will need to manually configure the **security-level 70** command to VLAN 3 on the ASA. Close the **Error in sending command** window. Using the ASA CLI, add the **security-level 70** command to VLAN 3.

```
CCNA-ASA(config)# interface vlan 3
```

```
CCNA-ASA(config-if)# security-level 70
```

```
CCNA-ASA(config-if)# exit
```

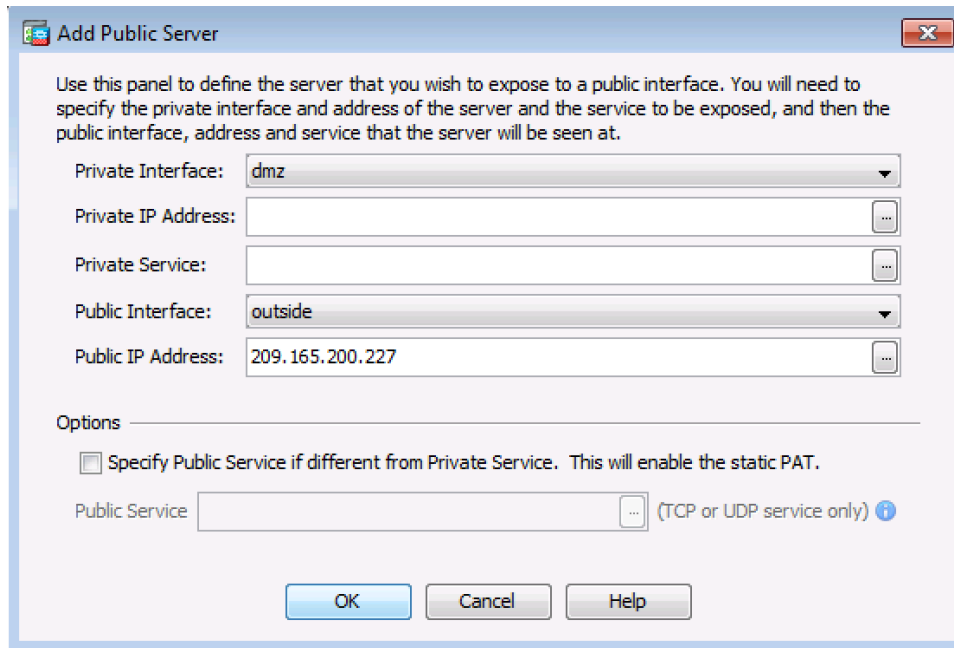
After entering the CLI commands, ASDM will prompt you to refresh the screen. After you refresh, **70** should appear in the Security Level column for the dmz interface.



## 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.

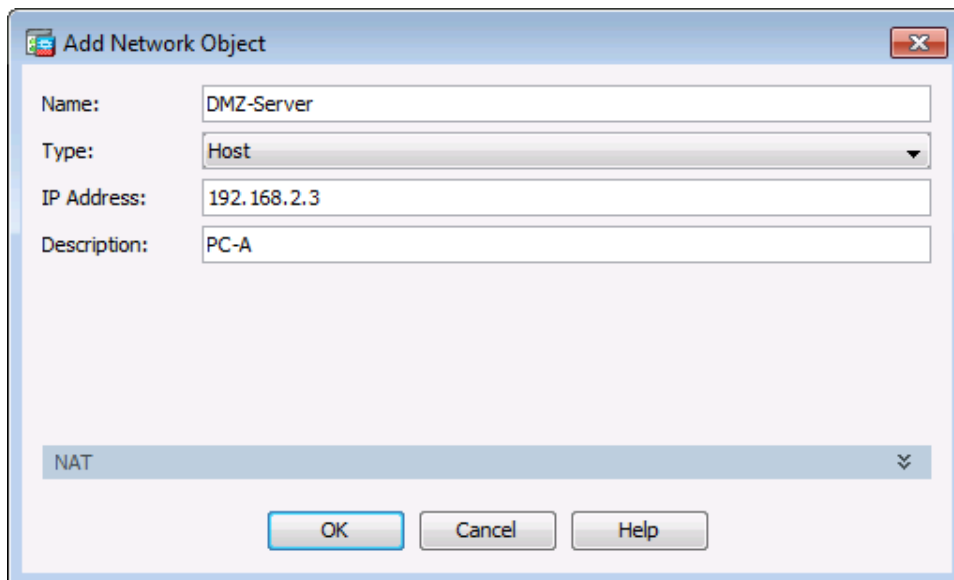
- a. On the **Firewall** menu, click the **Public Servers** option and click **Add** to define the DMZ server and services offered. In the Add Public Server dialog box, specify the Private Interface as **dmz**, the Public Interface as **outside**, and the Public IP address as **209.165.200.227**.



The "Add Public Server" dialog box is shown. It contains the following fields and options:

- Private Interface: **dmz** (dropdown menu)
- Private IP Address: (empty text box with ellipsis button)
- Private Service: (empty text box with ellipsis button)
- Public Interface: **outside** (dropdown menu)
- Public IP Address: **209.165.200.227** (text box with ellipsis button)
- Options section:
  - ☐ Specify Public Service if different from Private Service. This will enable the static PAT.
  - Public Service: (empty text box with ellipsis button) (TCP or UDP service only) ⓘ
- Buttons: OK, Cancel, Help

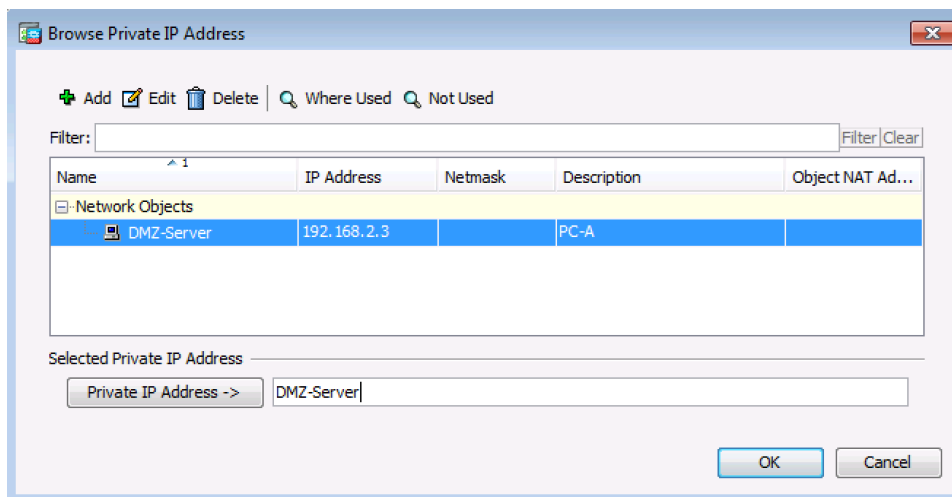
- b. Click the ellipsis button to the right of Private IP Address. In the Browse Private IP Address window, click **Add** to define the server as a **Network Object**. Enter the name **DMZ-Server**, select **Host** from the Type pull-down menu, enter the IP Address **192.168.2.3**, and a Description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



The "Add Network Object" dialog box is shown. It contains the following fields and options:

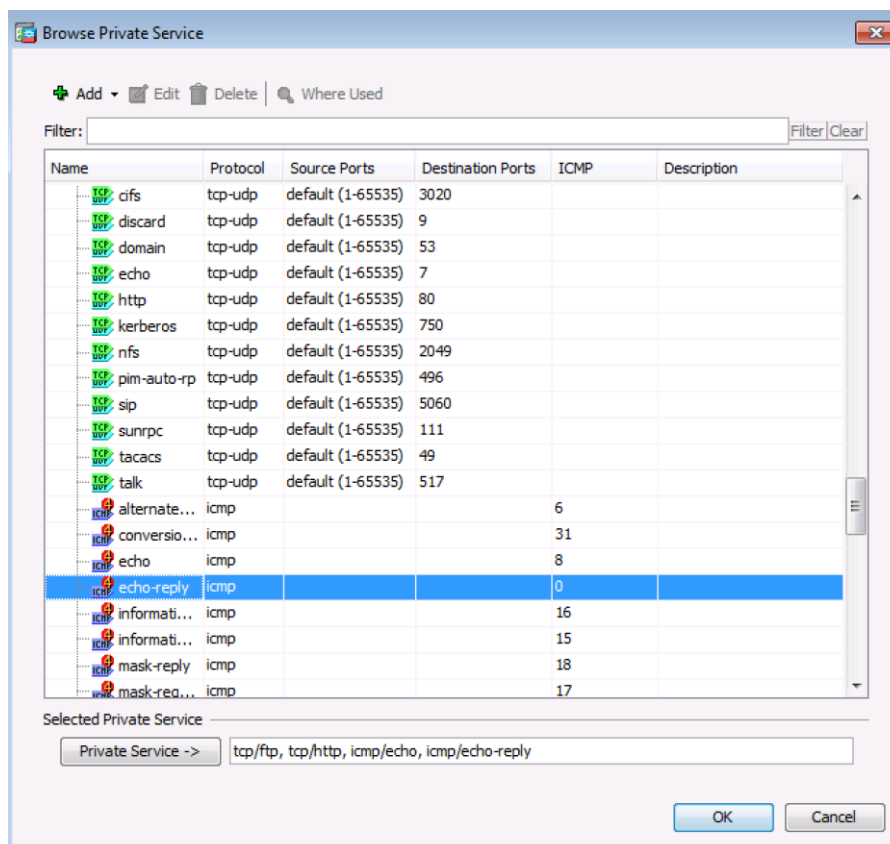
- Name: **DMZ-Server** (text box)
- Type: **Host** (dropdown menu)
- IP Address: **192.168.2.3** (text box)
- Description: **PC-A** (text box)
- NAT: (dropdown menu showing "NAT")
- Buttons: OK, Cancel, Help

- c. 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.



- d. In the Add Public Server dialog, click the ellipsis button to the right of Private Service. In the Browse Private Service window, double-click to select the following services: **tcp/ftp**, **tcp/http**, **icmp/echo**, and **icmp/echo-reply** (scroll down to see all services). 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.



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

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:

Private IP Address:

Private Service:

Public Interface:

Public IP Address:

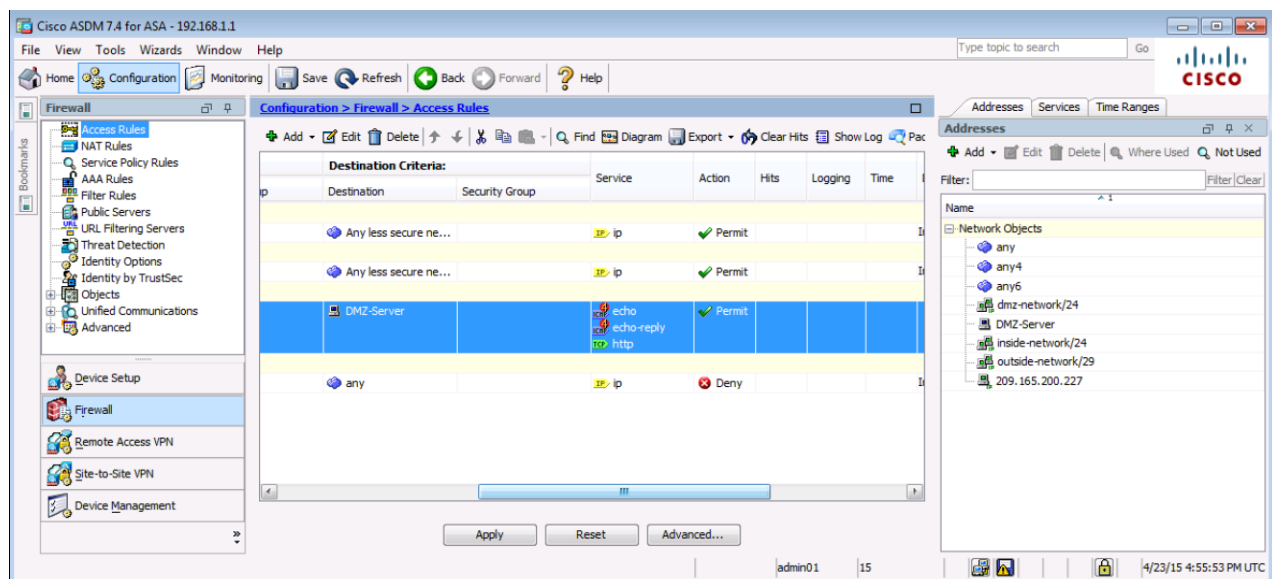
Options

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

Public Service  (TCP or UDP service only)

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

- 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.
- 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.



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

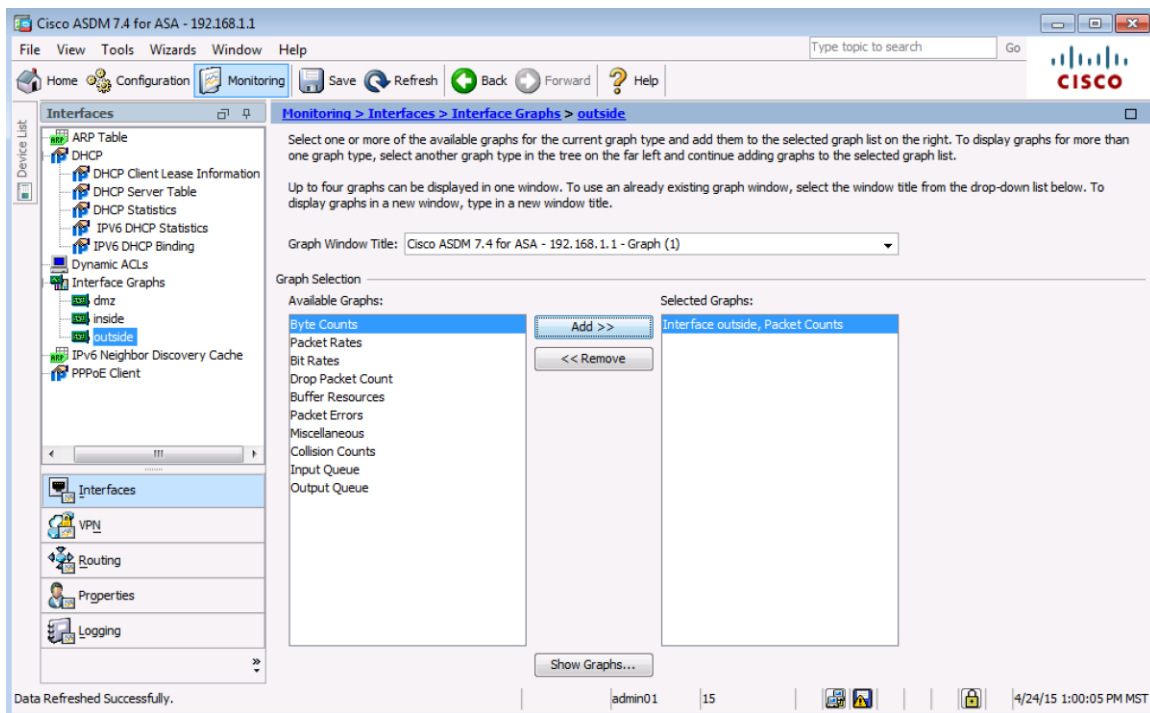
**Step 4: Test access to the DMZ server from the outside network.**

- From PC-C, ping the IP address of the static NAT public server address (**209.165.200.227**). The pings should be successful.
- Because the ASA inside interface (VLAN 1) is set to security level 100 (the highest) and the DMZ interface (VLAN 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.
- The DMZ server cannot ping PC-B on the inside network. This is because the DMZ interface VLAN 3 has a lower security level and the fact that, when the VLAN 3 interface was created, it was necessary to specify the **no forward** command. Try to ping from the DMZ server PC-A to PC-B at the IP address 192.168.1.X. 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.

- 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.



- 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:

[illegible]

.....

```
<output omitted>
```

[illegible][illegible]

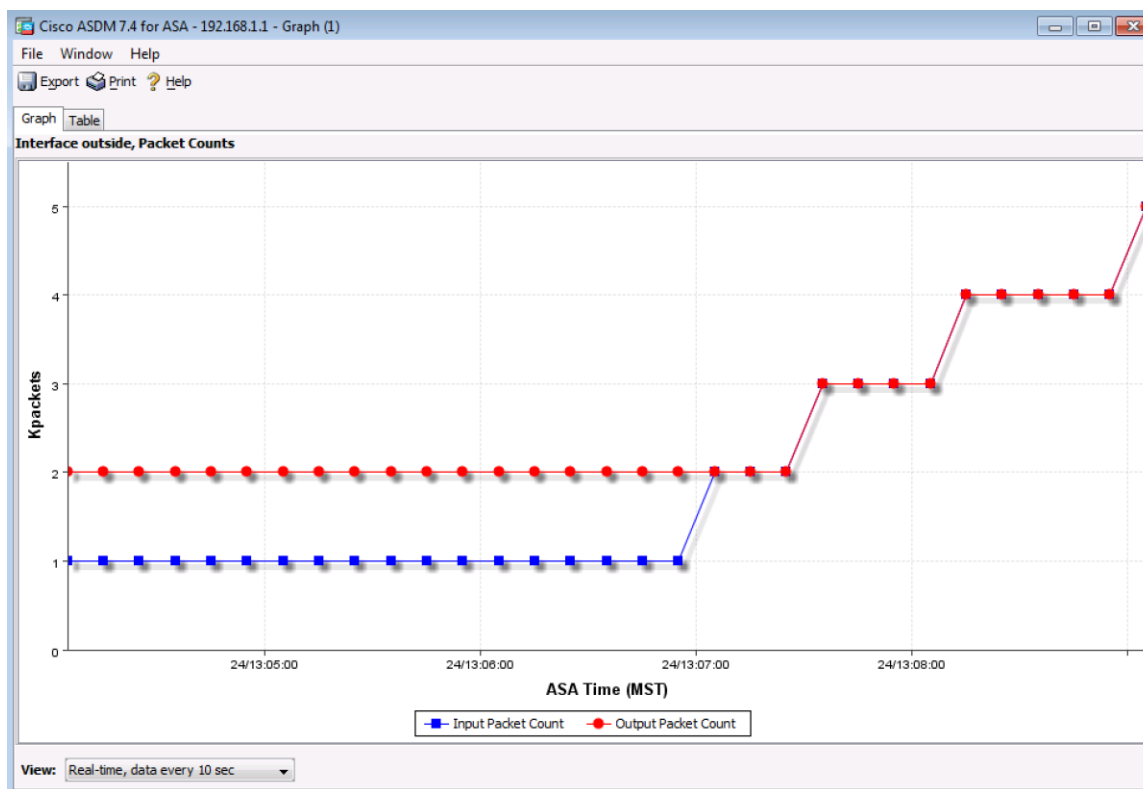
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/12 ms

- d. You should see the results of the pings from R2 on the graph as an Input Packet Count. 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.



## 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) |
| <b>Note:</b> 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. |                             |                             |                       |                       |