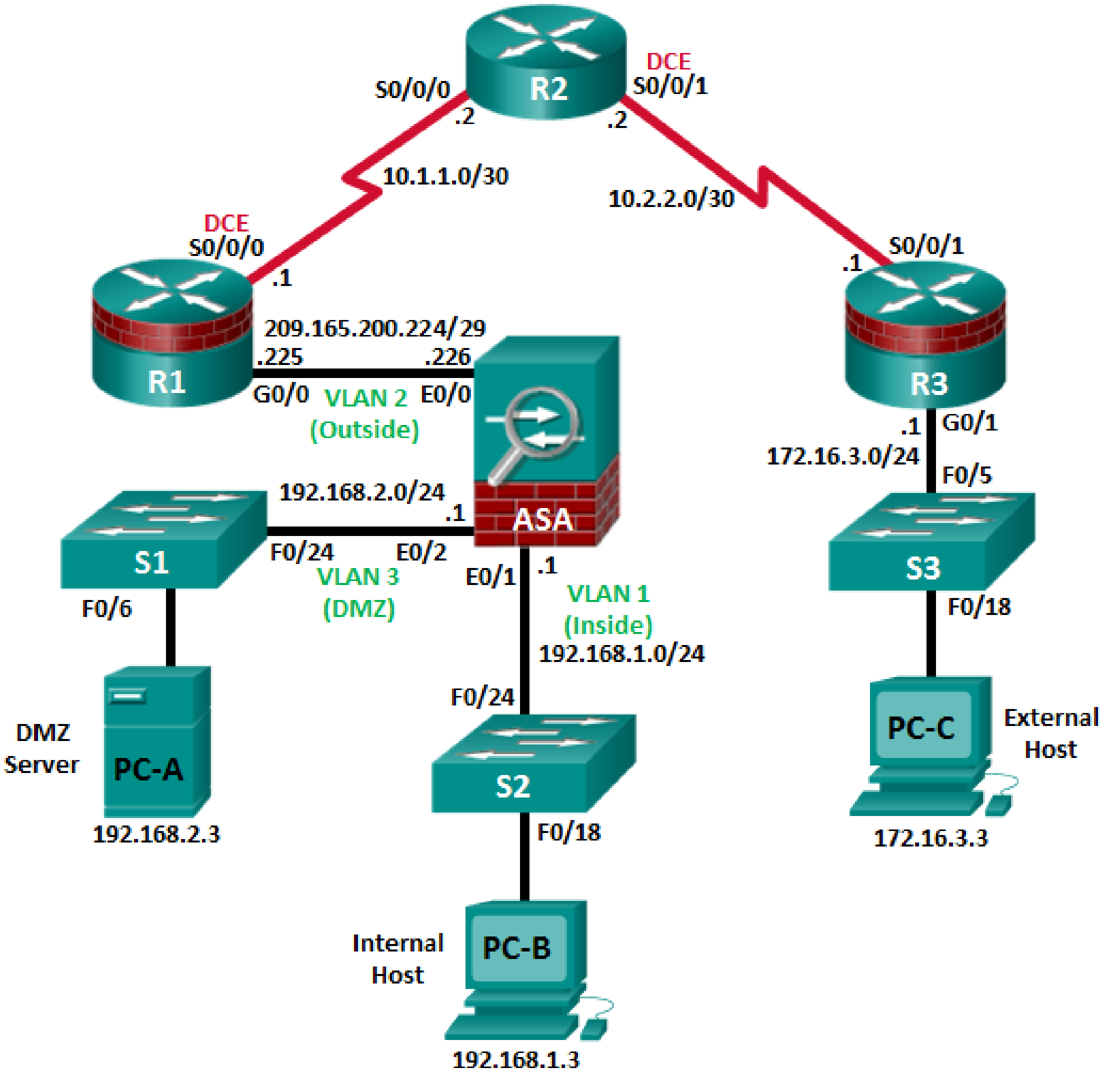
CCNA Security

Lab - Configure ASA 5505 Basic Settings and Firewall using ASDM (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

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.

Instructor Note: Instructions for erasing switches and routers are provided in Chapter 0.0.0.0.

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

Instructor Notes:

- This lab is divided into five parts. Part 1 and 2 can be performed separately but must be performed before Parts 3 through 5. Part 2 uses the ASA CLI to prepare the ASA for ASDM Access. Parts 3 through 5 can be performed individually, or in combination with others as time permits, but they should be performed sequentially. In some cases, a task assumes the configuration of certain features in a prior task.
- The main goal is to use an ASA to implement firewall and other services that might previously have been configured on an ISR. In the Chapter 9 Lab, the student configured the most common basic ASA settings and services, such as NAT, ACL, DHCP, AAA, and SSH from the CLI. In this lab, the student uses ASDM to configure these features.
- The final running configs for all devices are found at the end of the lab.

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.

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 64000
```

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 3: 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 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.

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

```
R1(config)# security passwords min-length 10
```

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

```
R1(config)# enable algorithm-type scrypt secret cisco12345
```

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

```
R1(config)# username admin01 privilege 15 algorithm-type scrypt secret
admin01pass
```

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.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config-line)# transport input ssh
```

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

```
R1(config)# ip http server
R1(config)# ip http authentication local
```

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.

a. 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.

b. 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.

c. If prompted to enter Interactive Firewall configuration (Setup mode), answer **no**.

d. 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?

All ASA ports (other than E0/0, in some cases) are in VLAN 1 by default.

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.

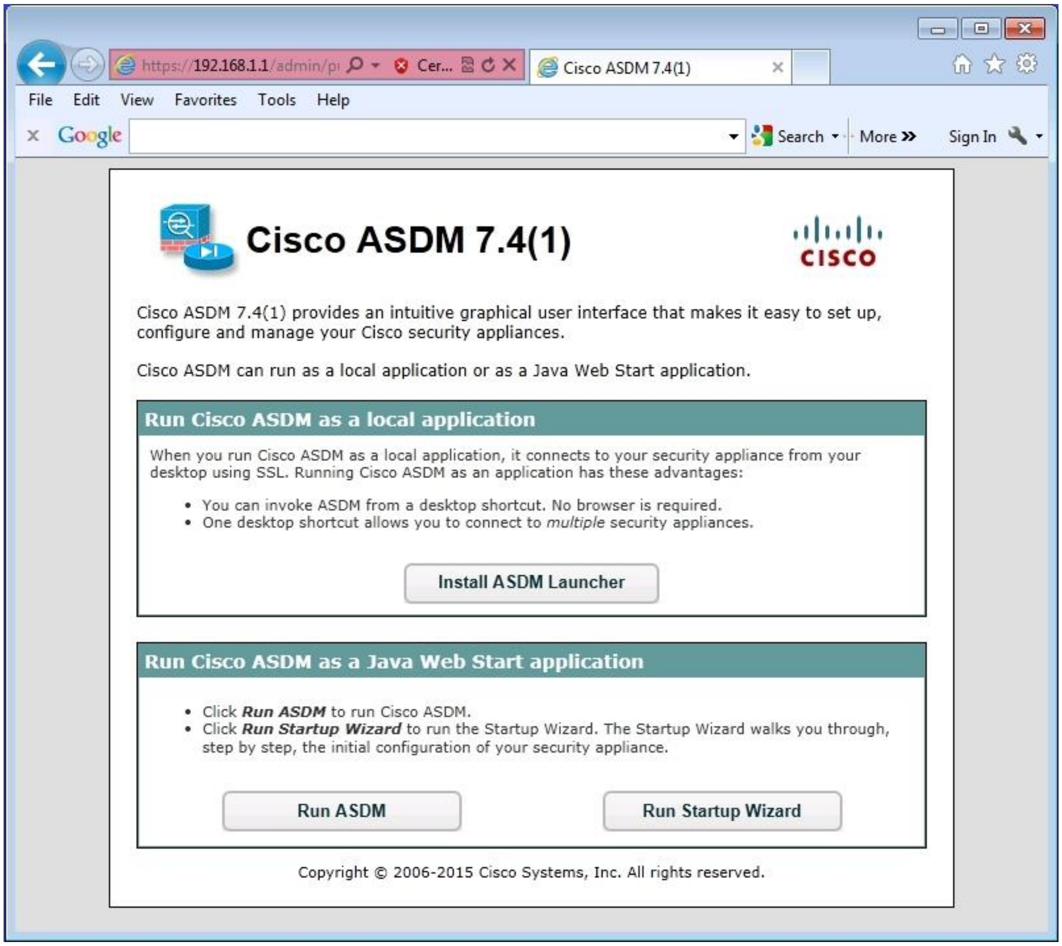
```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

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.



Cisco ASDM 7.4(1)

Cisco ASDM 7.4(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.

Install ASDM Launcher

Run Cisco ASDM as a Java Web Start application

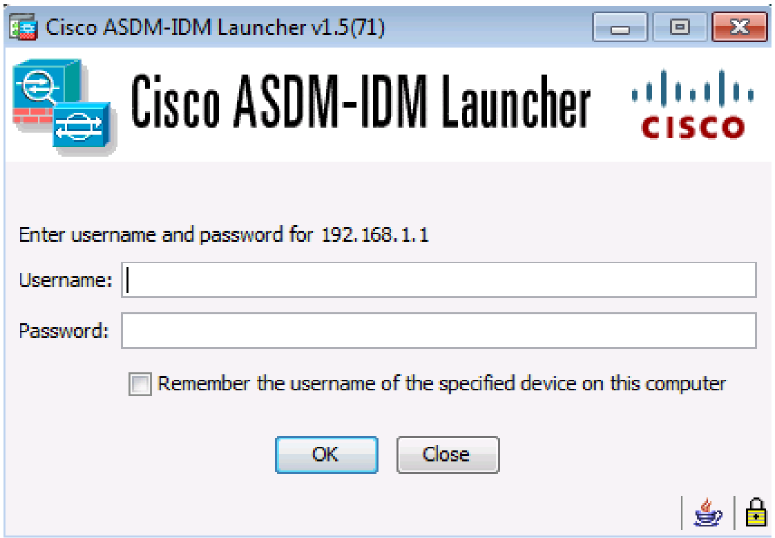
- Click ***Run ASDM*** to run Cisco ASDM.
- Click ***Run Startup Wizard*** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

Run ASDM   Run Startup Wizard

Copyright © 2006-2015 Cisco Systems, Inc. All rights reserved.

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.



Enter username and password for 192.168.1.1

Username:

Password:

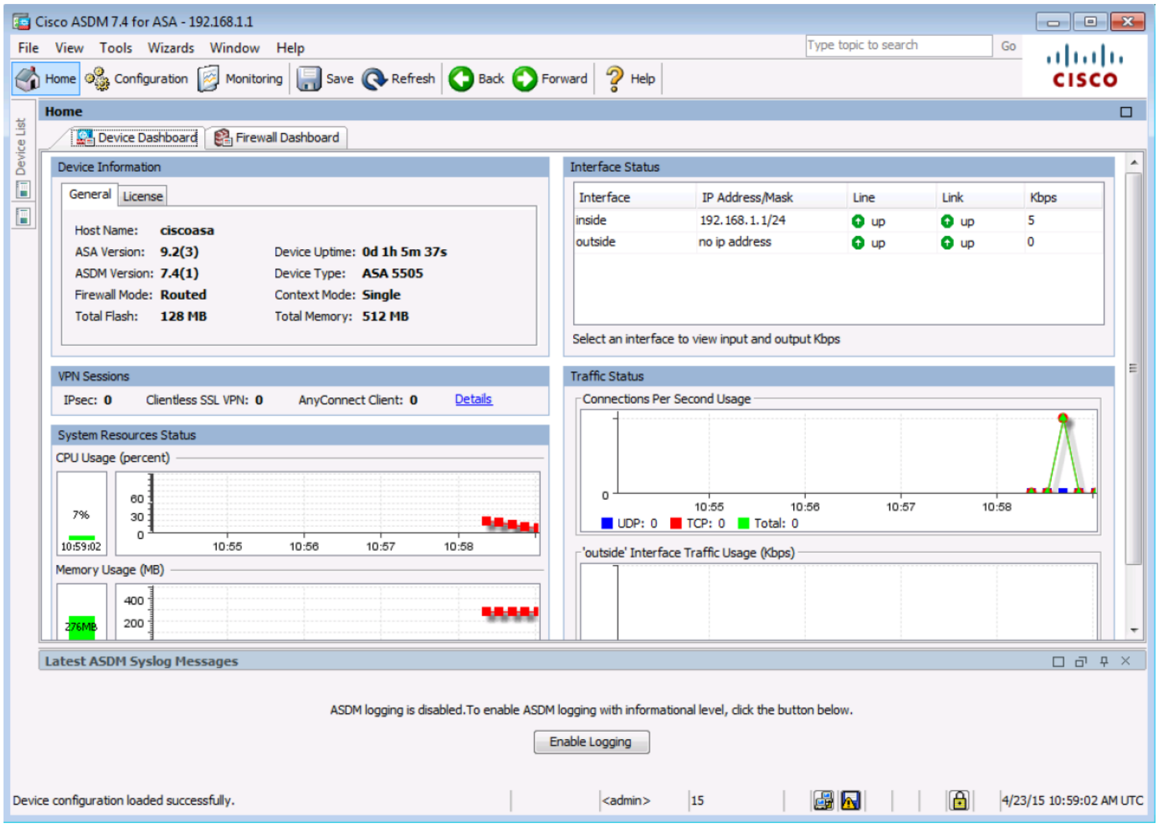
□ Remember the username of the specified device on this computer

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**.



Host Name: **ciscoasa**

ASA Version: **9.2(3)** Device Uptime: **0d 1h 5m 37s**

ASDM Version: **7.4(1)** Device Type: **ASA 5505**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **128 MB** Total Memory: **512 MB**

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	up	up	5
outside	no ip address	up	up	0

Select an interface to view input and output Kbps

IPsec: **0** Clientless SSL VPN: **0** AnyConnect Client: **0** Details

UDP: 0 TCP: 0 Total: 0

ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.

Device configuration loaded successfully. <admin> 15 4/23/15 10:59:02 AM UTC

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

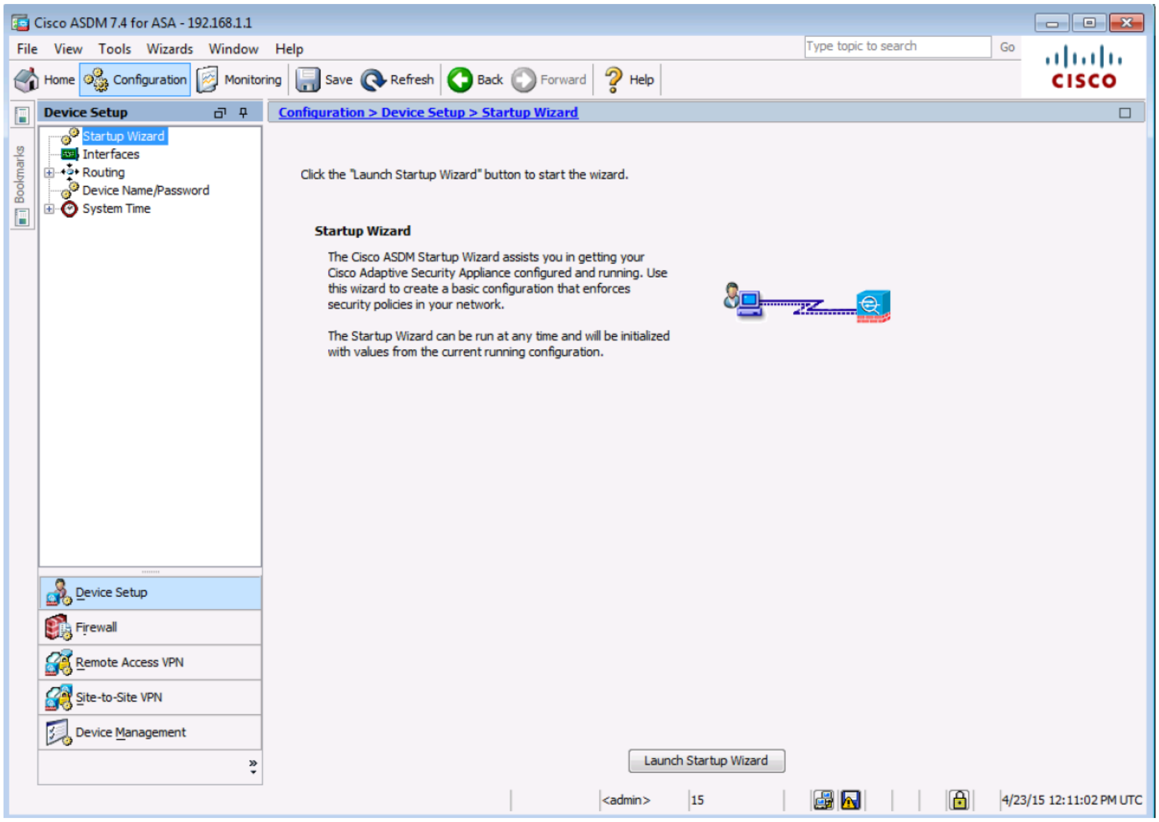
Part 3: Configure Basic ASA Settings and Firewall Using the ASDM Startup Wizard

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**.



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

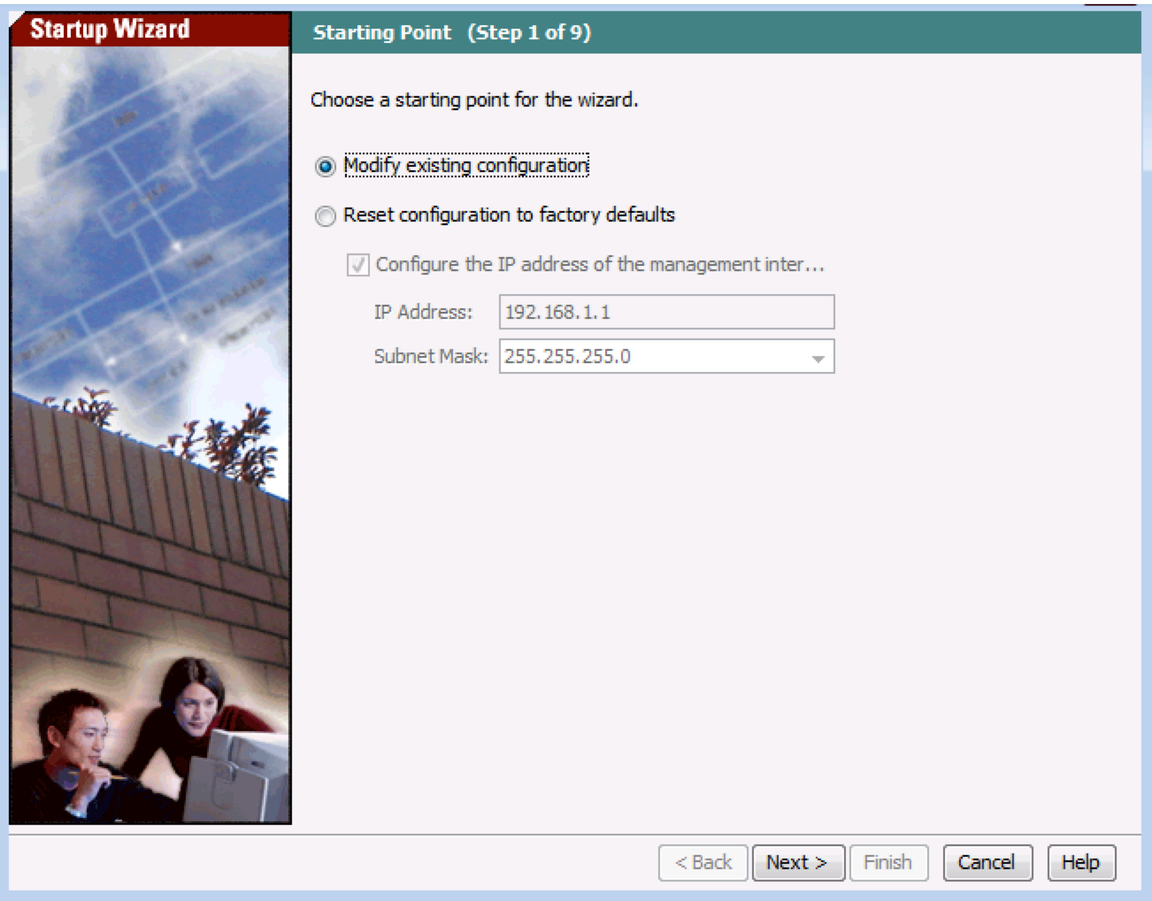
Startup Wizard

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.



Choose a starting point for the wizard.

● Modify existing configuration

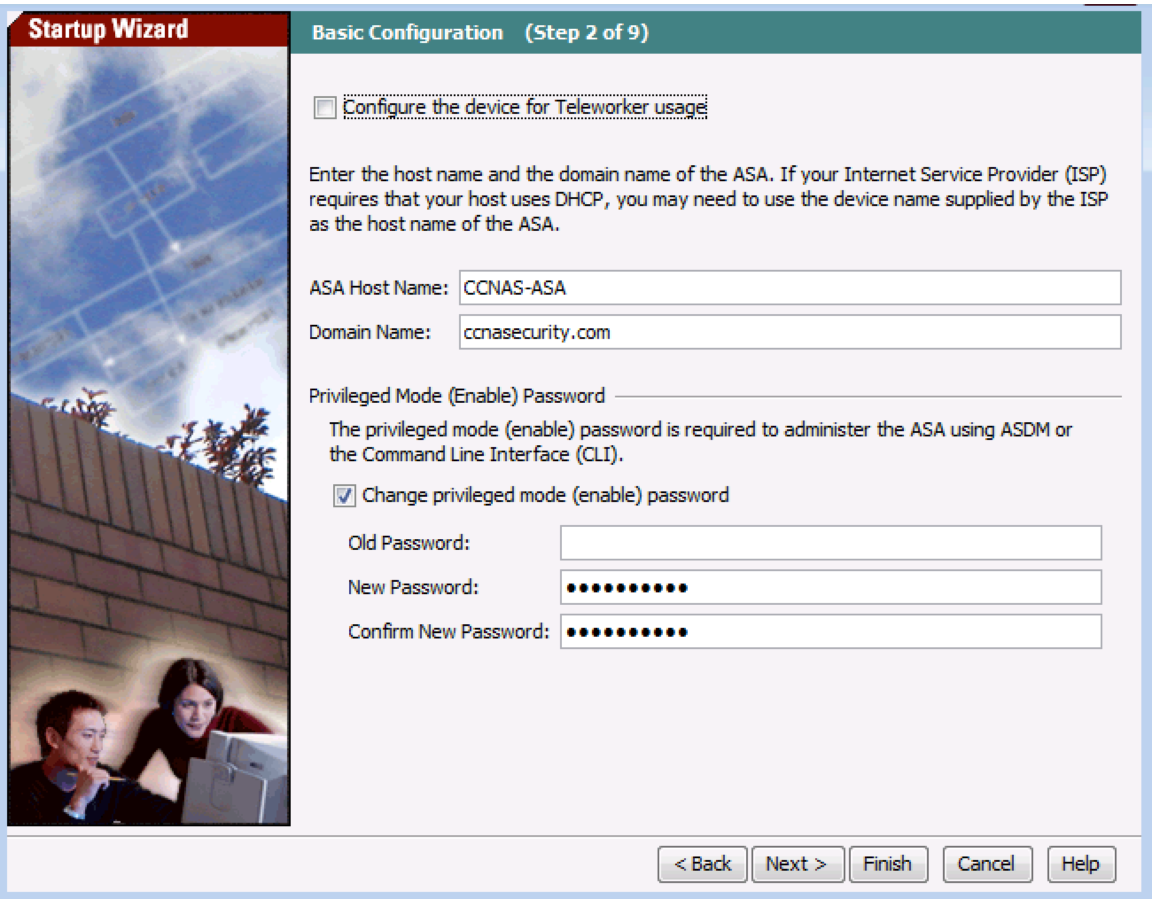
○ Reset configuration to factory defaults

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

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.



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: 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

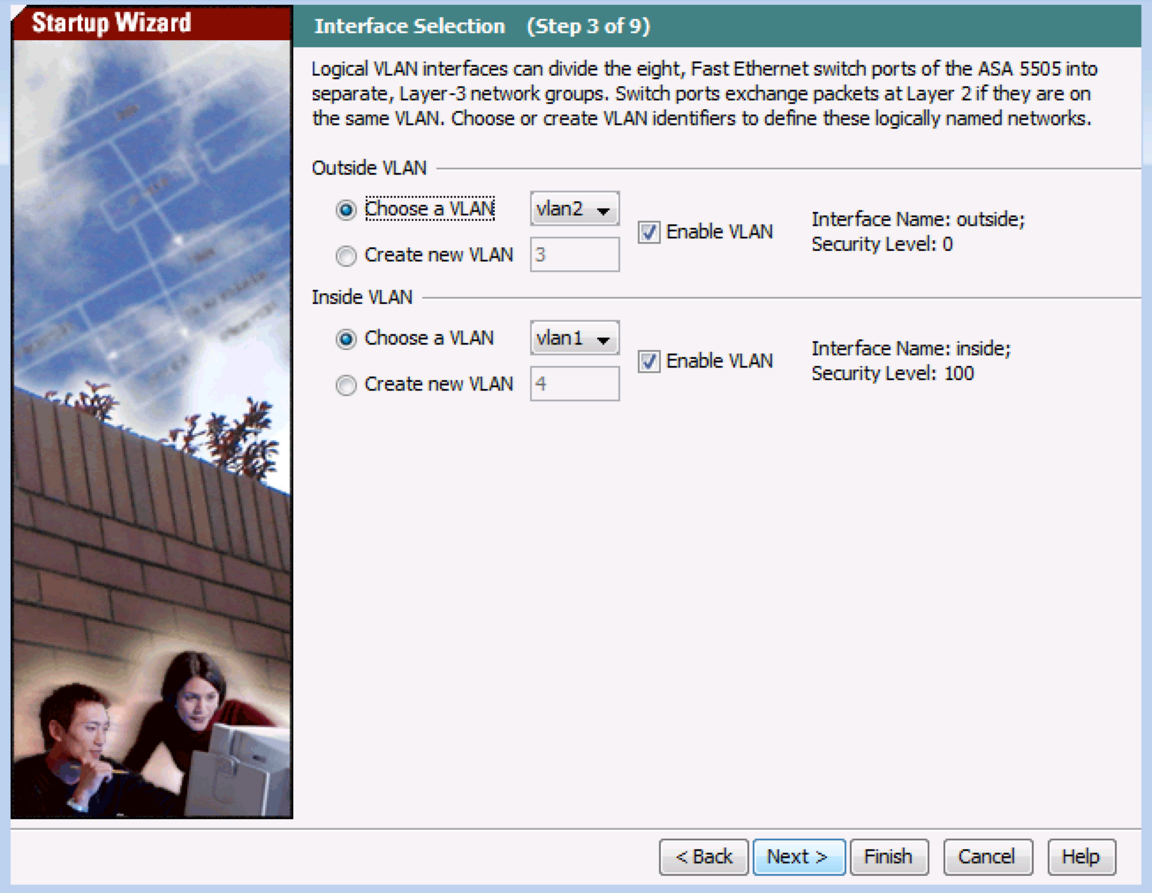
Old Password:

New Password: ●●●●●●●●●●

Confirm New Password: ●●●●●●●●●●

Step 3: Configure the inside and outside 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.



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

○ Create new VLAN: 3

☑ Enable VLAN

Interface Name: outside;
Security Level: 0

Inside VLAN

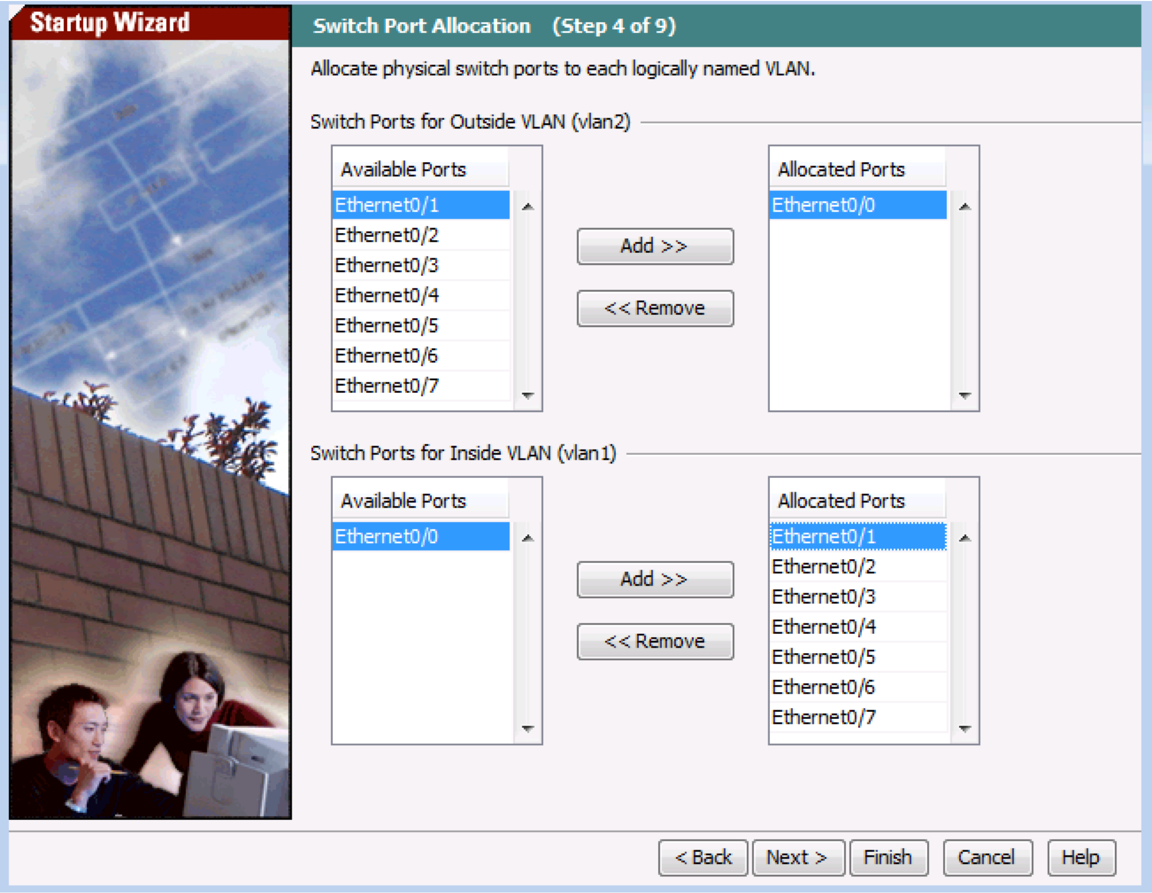
● Choose a VLAN: vlan1

○ Create new VLAN: 4

☑ Enable VLAN

Interface Name: inside;
Security Level: 100

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.



Allocate physical switch ports to each logically named VLAN.

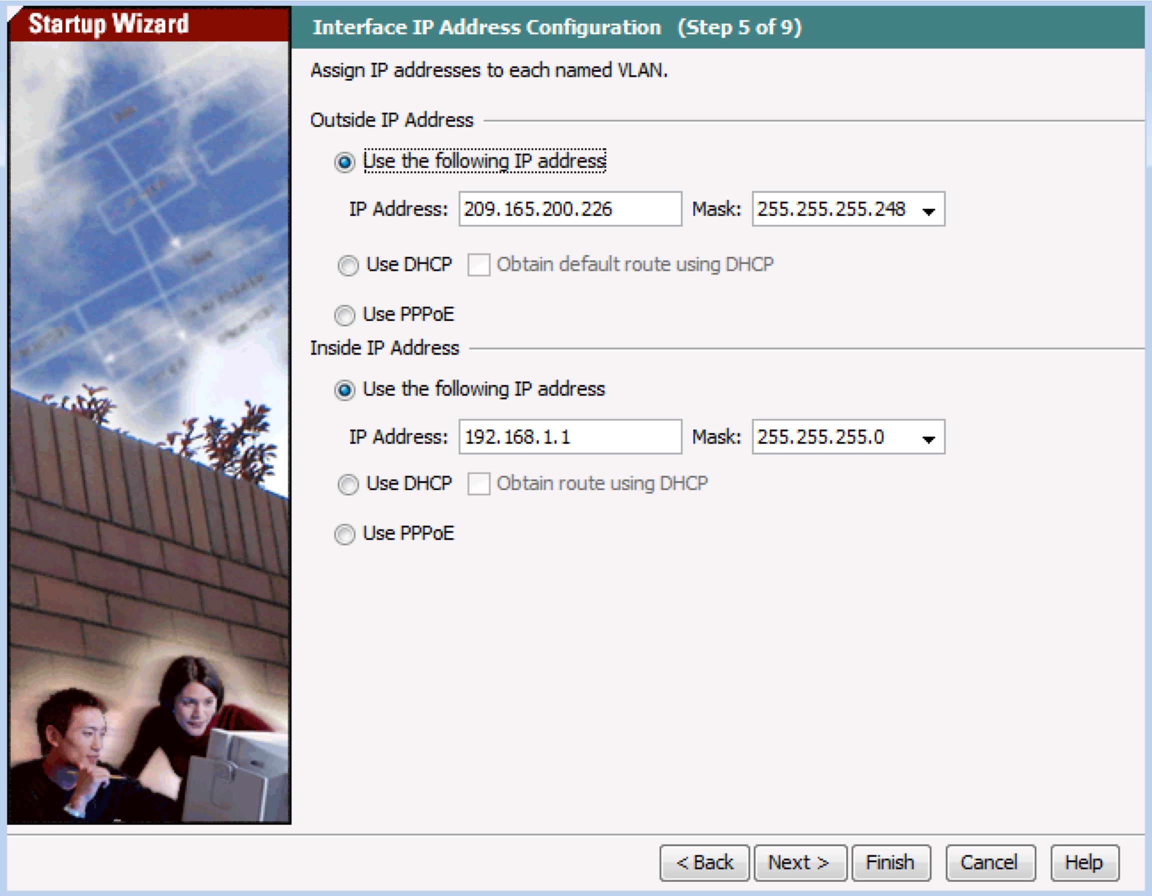
Switch Ports for Outside VLAN (vlan2)

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

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

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.



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

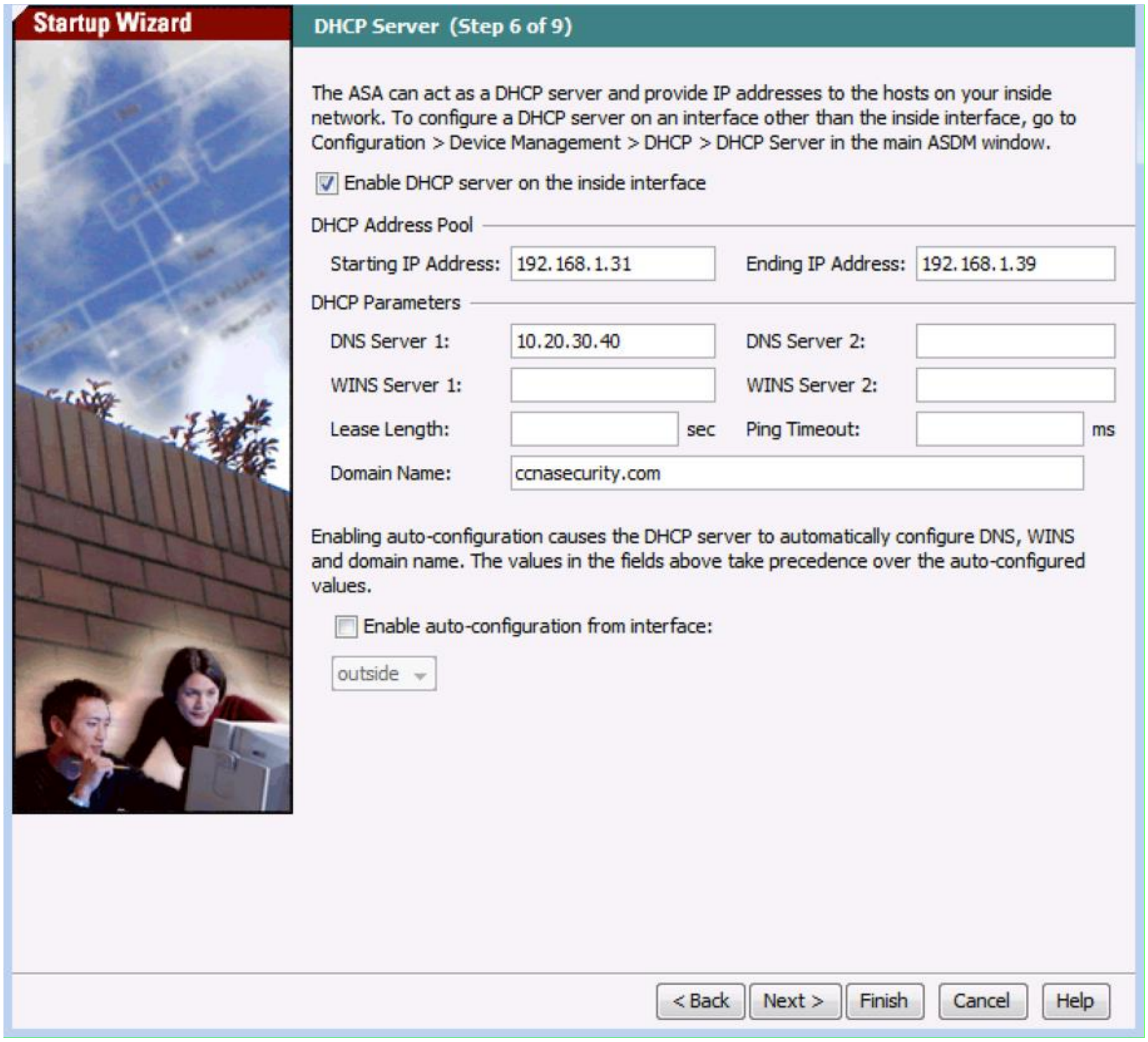
IP Address: 192.168.1.1 Mask: 255.255.255.0

○ Use DHCP □ Obtain route using DHCP

○ Use PPPoE

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.



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: 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

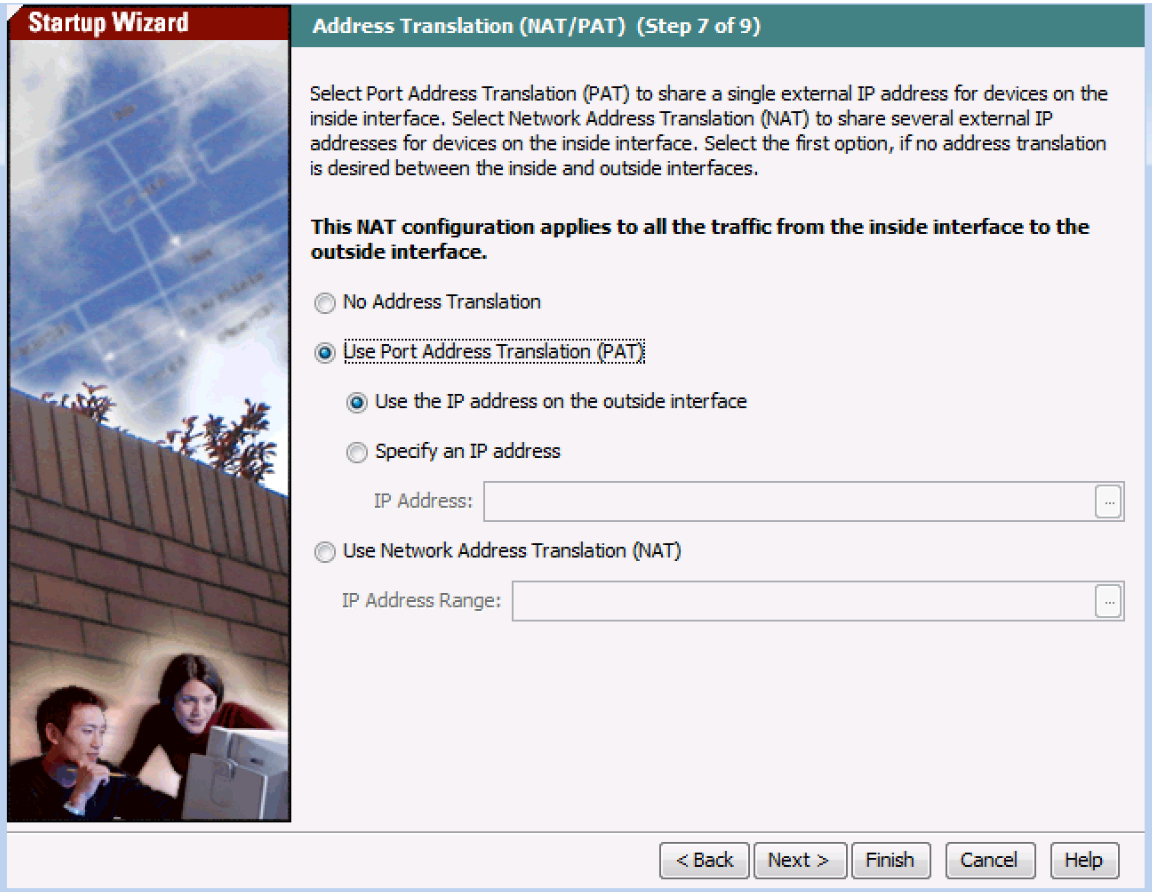
Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

☐ Enable auto-configuration from interface:

outside

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.



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

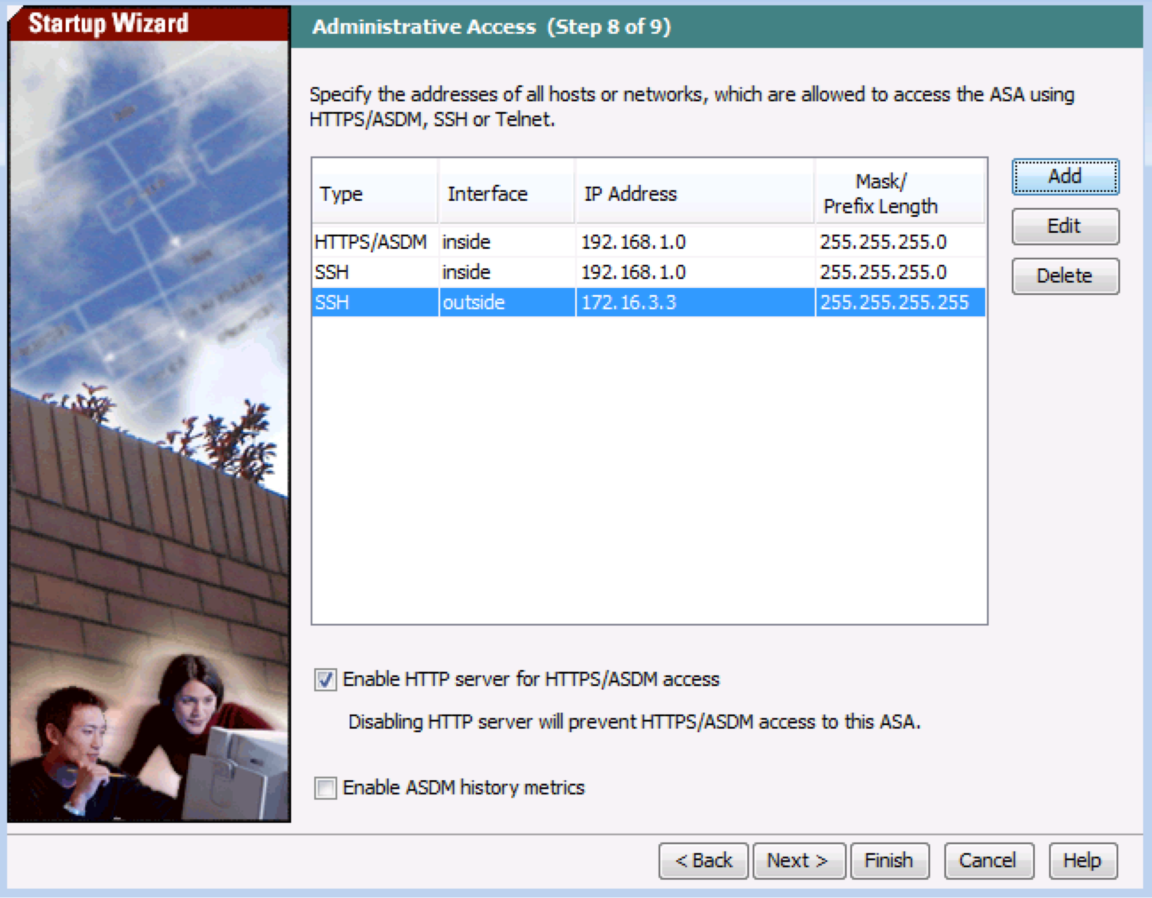
○ Specify an IP address

IP Address:

○ Use Network Address Translation (NAT)

IP Address Range:

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.



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/ 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

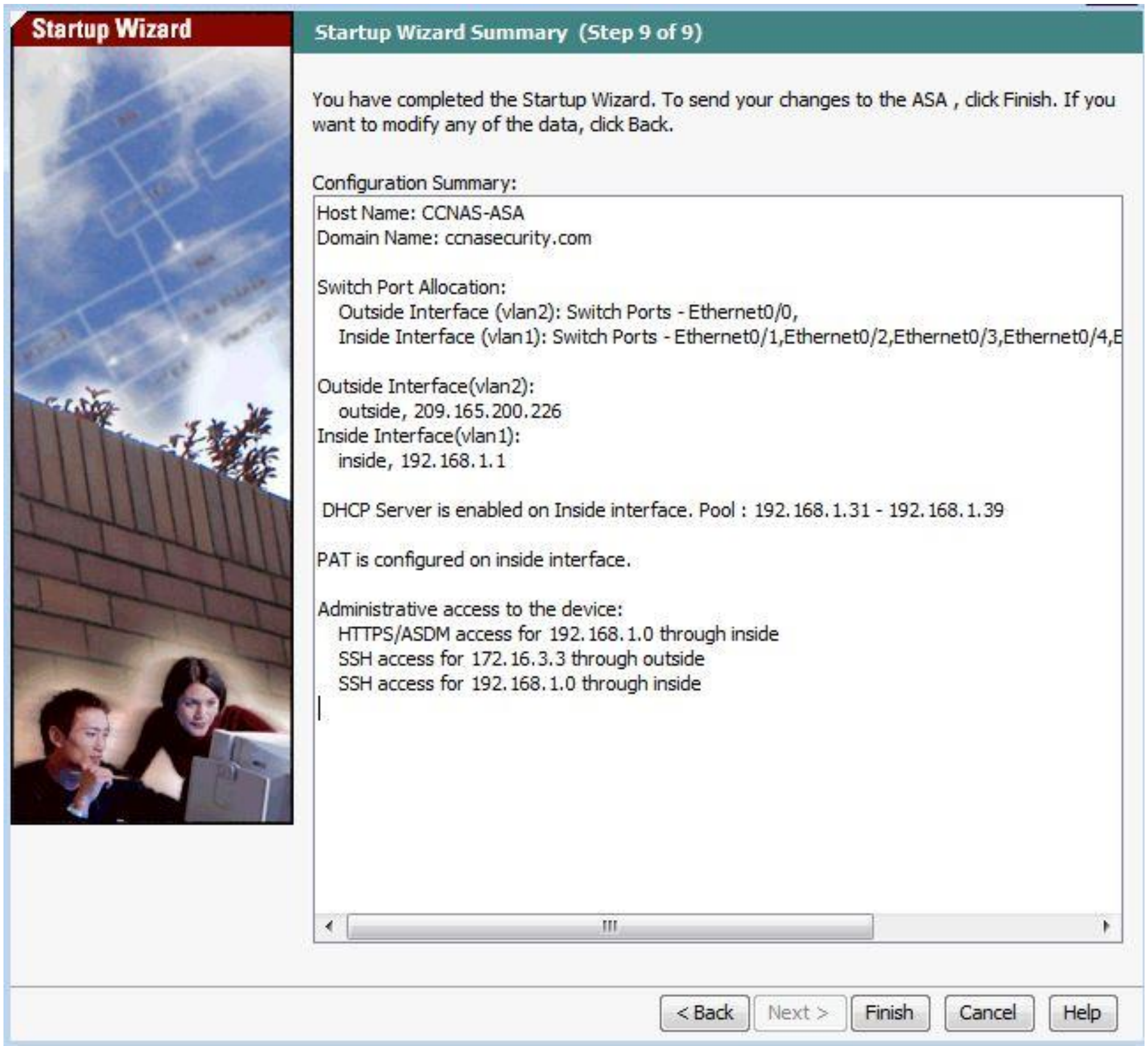
Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

□ Enable ASDM history metrics

Step 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.



You have completed the Startup Wizard. To send your changes to the ASA , click Finish. If you want to modify any of the data, click Back.

Configuration Summary:

```
Host Name: CCNAS-ASA
Domain Name: ccnasecurity.com

Switch Port Allocation:
   Outside Interface (vlan2): Switch Ports - Ethernet0/0,
   Inside Interface (vlan1): Switch Ports - Ethernet0/1,Ethernet0/2,Ethernet0/3,Ethernet0/4,E

Outside Interface(vlan2):
   outside, 209.165.200.226
Inside Interface(vlan1):
   inside, 192.168.1.1

 DHCP Server is enabled on Inside interface. Pool : 192.168.1.31 - 192.168.1.39

PAT is configured on inside interface.

Administrative access to the device:
   HTTPS/ASDM access for 192.168.1.0 through inside
   SSH access for 172.16.3.3 through outside
   SSH access for 192.168.1.0 through inside
```

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.

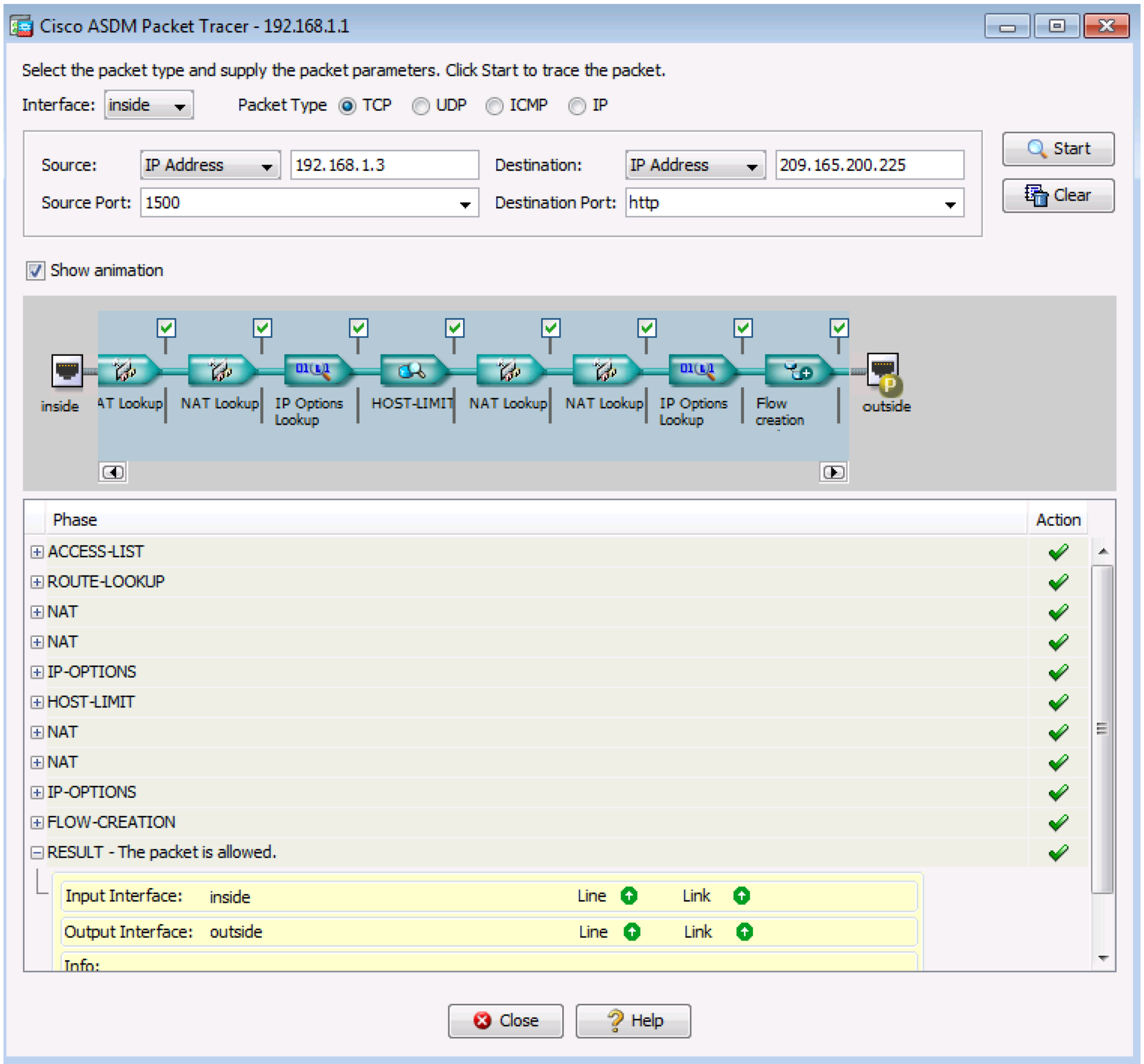
a. Open a browser on PC-B and enter the IP address of the R1 G0/0 interface (**209.165.200.225**) to simulate access to an external website.

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.



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 ○ ICMP ○ IP

Source: IP Address 192.168.1.3   Destination: IP Address 209.165.200.225

Source Port: 1500   Destination Port: http

☑ Show animation

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

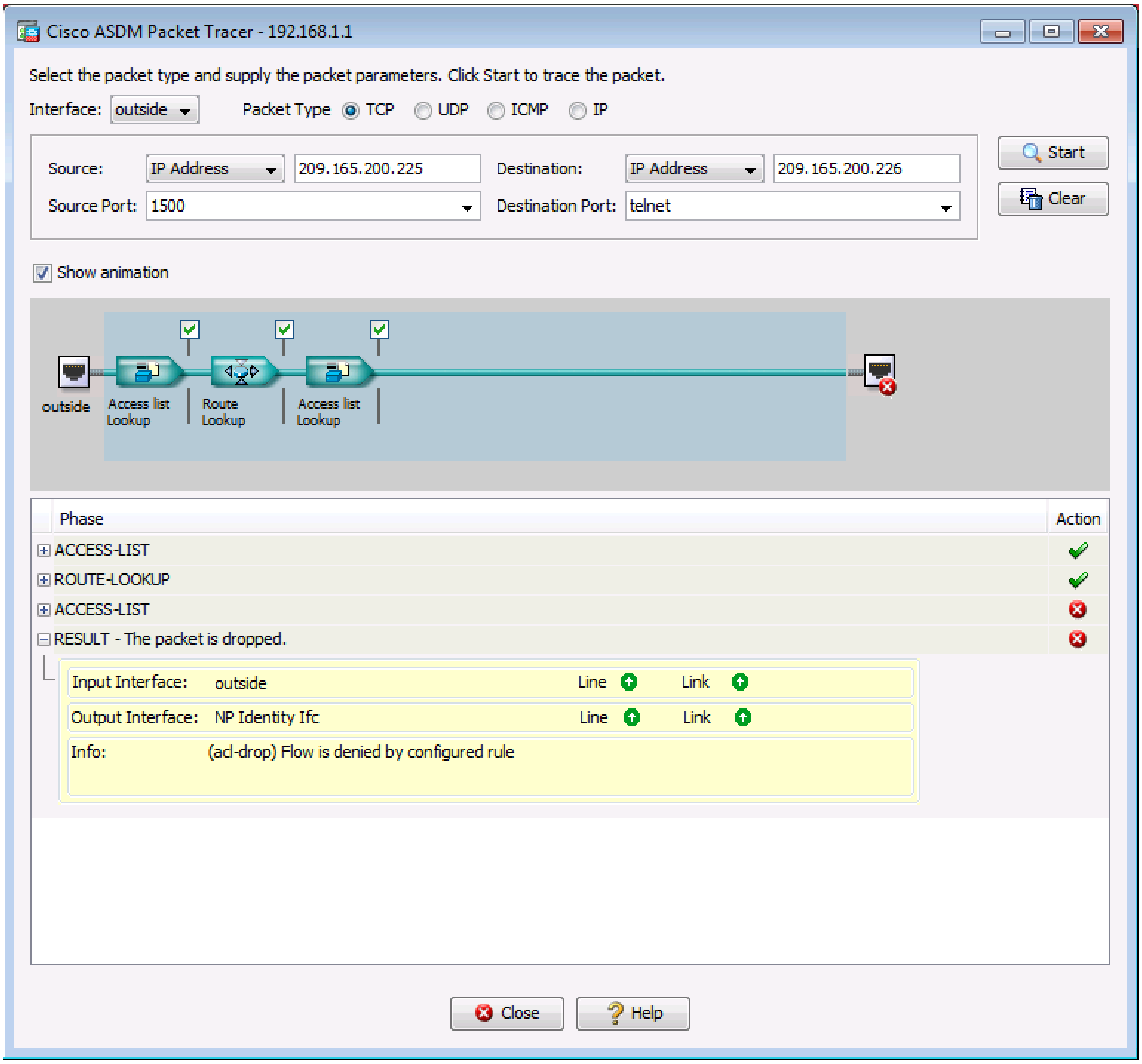
Input Interface: inside   Line ●   Link ●

Output Interface: outside   Line ●   Link ●

Info:

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.



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 ○ ICMP ○ IP

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	✓
⊞ 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

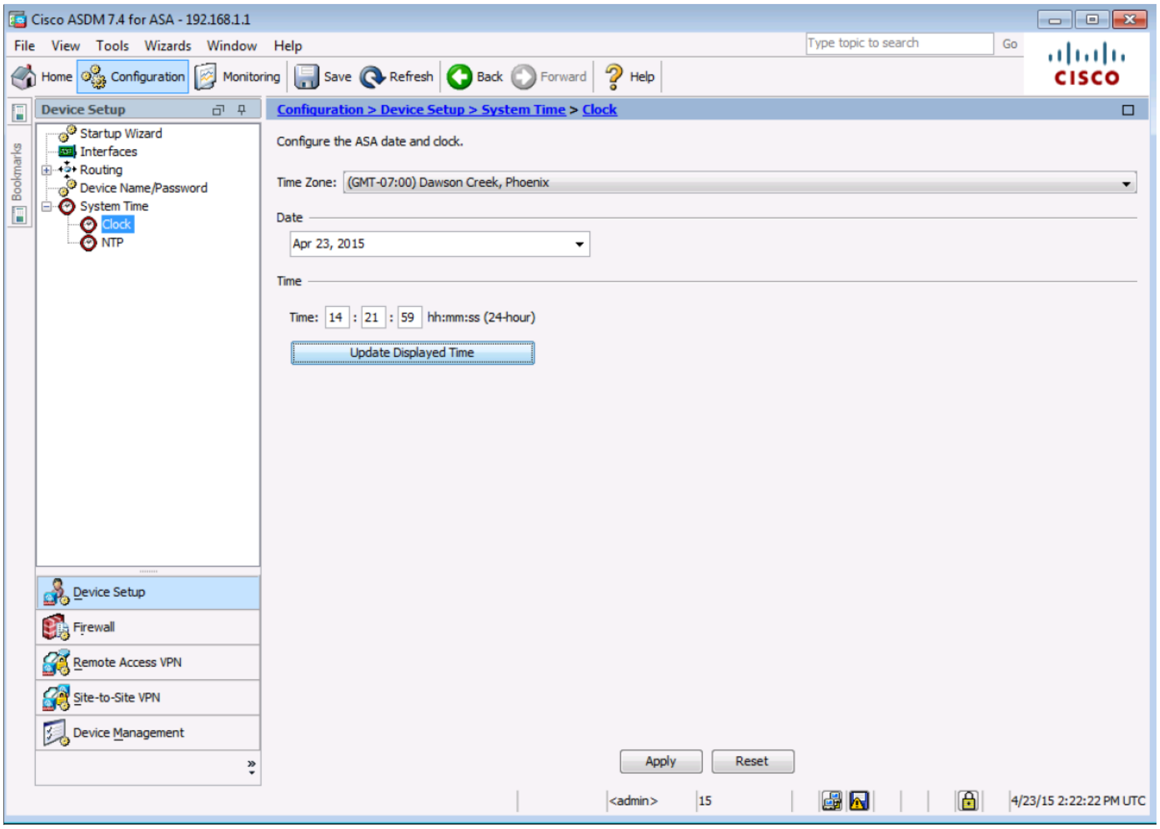
Part 4: Configure ASA Settings from the ASDM Configuration Menu

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



Configure the ASA date and clock.

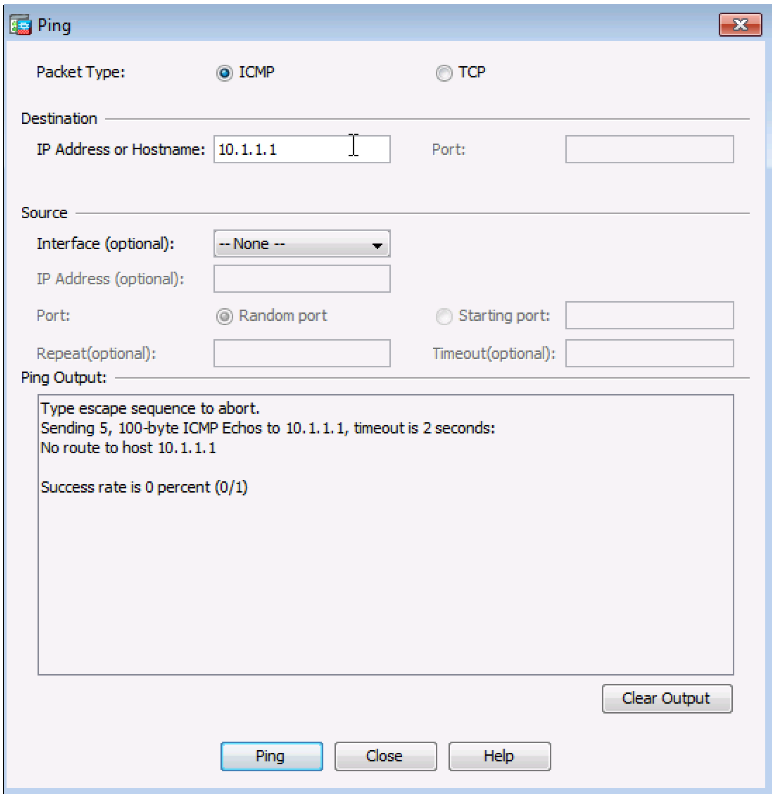
Time Zone: (GMT-07:00) Dawson Creek, Phoenix

Date: Apr 23, 2015

Time: 14 : 21 : 59 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**). 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.



IP Address or Hostname: 10.1.1.1

Interface (optional): -- None --

IP Address (optional):

Port: ● Random port ○ Starting port:

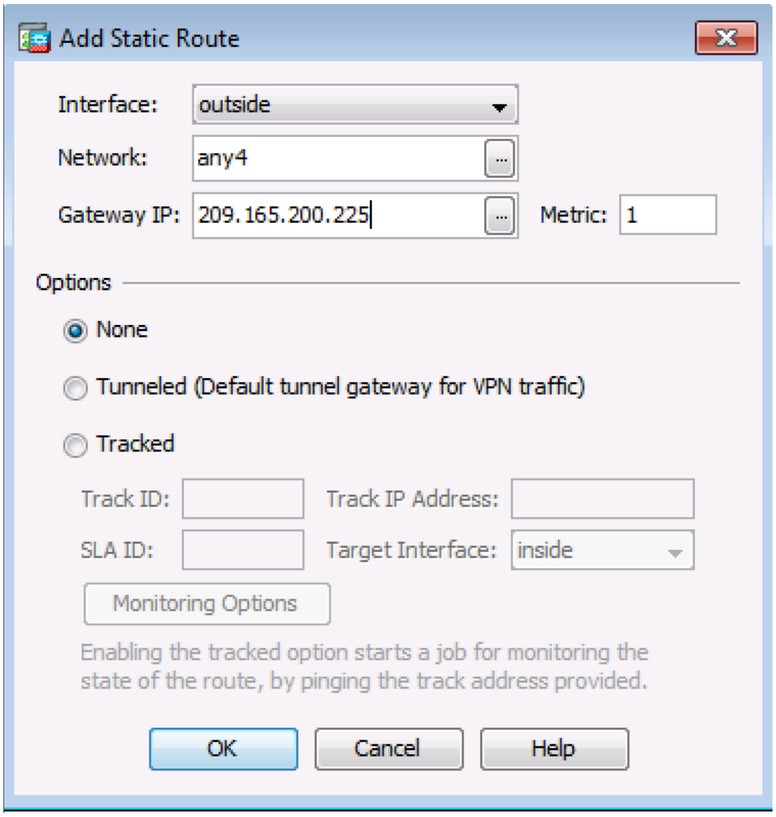
Repeat(optional):

Timeout(optional):

```
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)
```

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).



Add Static Route

Interface: outside

Network: any4

Gateway IP: 209.165.200.225 Metric: 1

Options

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

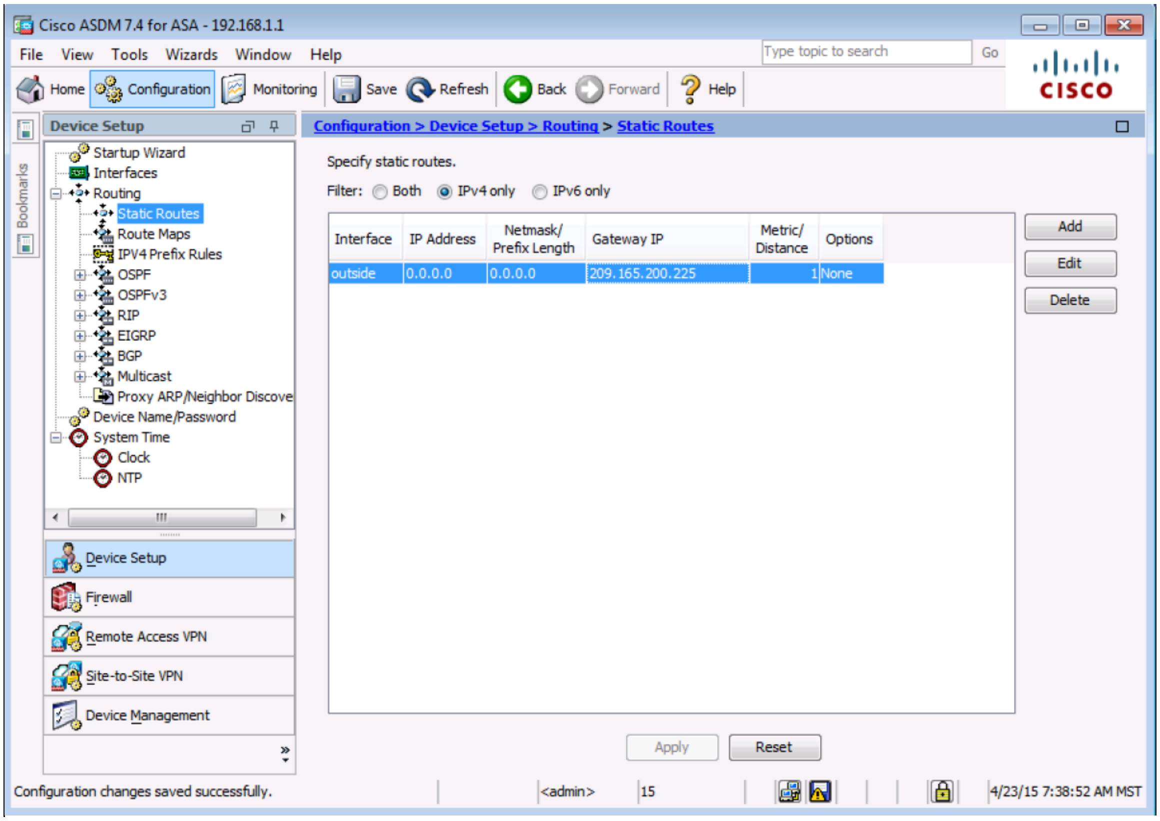
○ Tracked

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.

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



Configuration > Device Setup > Routing > Static Routes

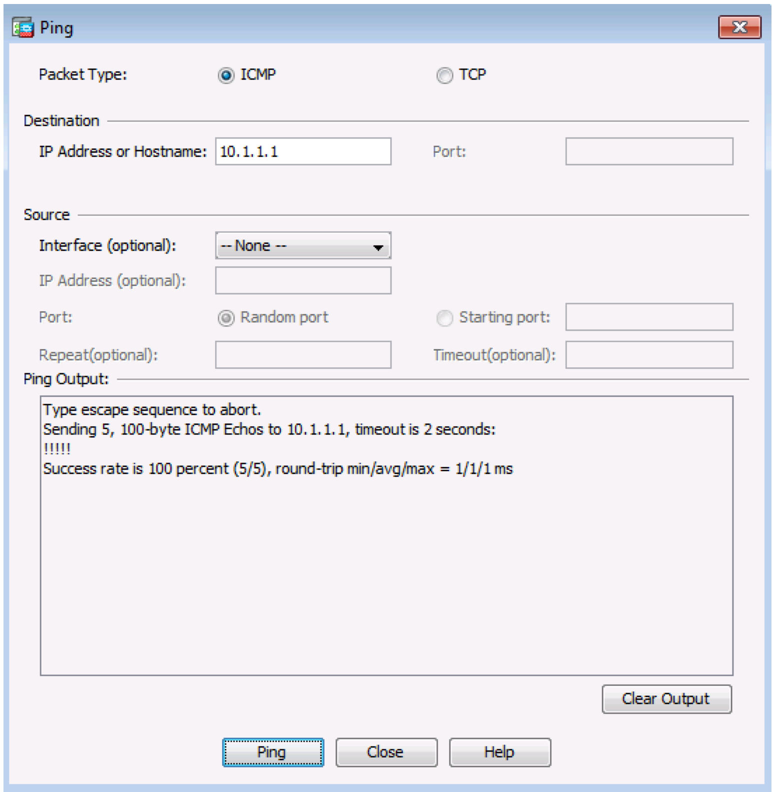
Specify static routes.

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	209.165.200.225	1	None

Configuration changes saved successfully. <admin> 15 4/23/15 7:38:52 AM MST

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.



Packet Type: ● ICMP ○ TCP

IP Address or Hostname: 10.1.1.1 Port:

Interface (optional): -- None --

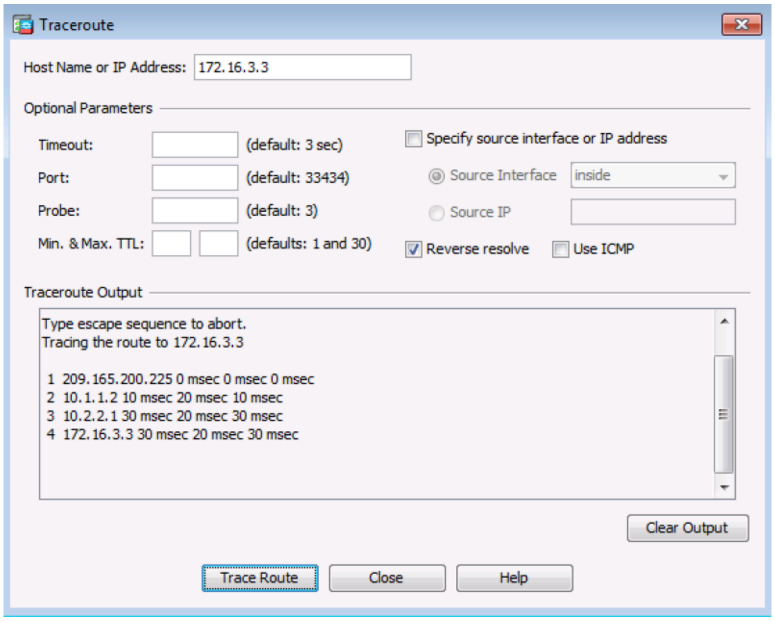
IP Address (optional):

Port: ● Random port ○ Starting port:

Repeat(optional): Timeout(optional):

```
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
```

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.



Host Name or IP Address: 172.16.3.3

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

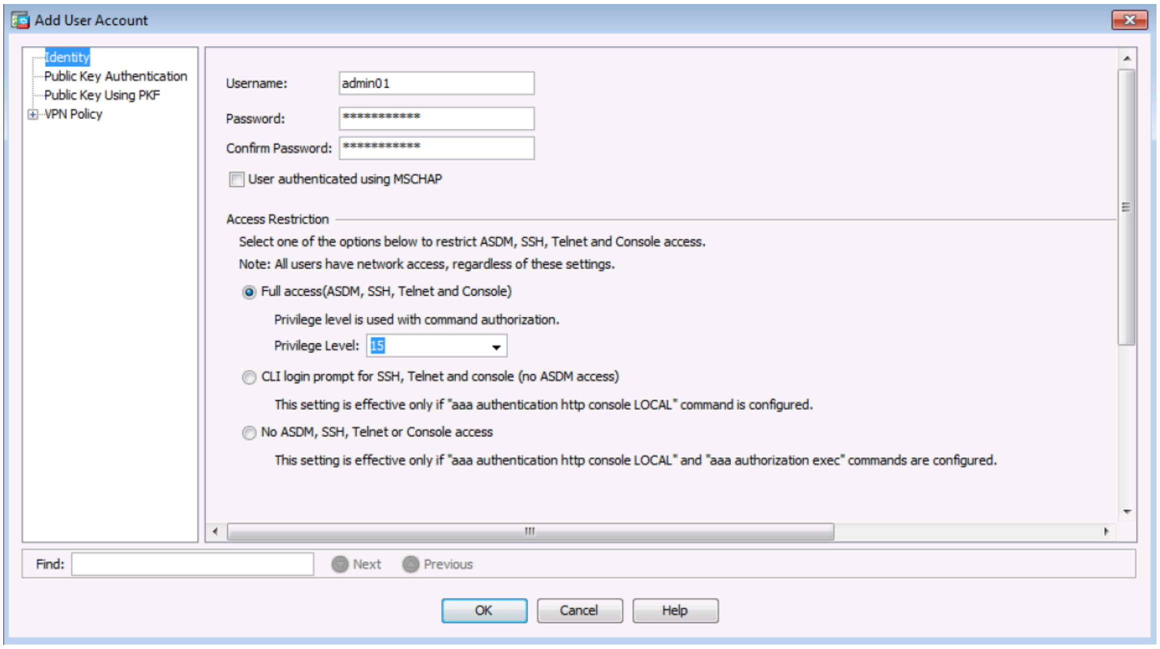
☑ Reverse resolve □ Use ICMP

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

 1  209.165.200.225 0 msec 0 msec 0 msec
 2  10.1.1.2 10 msec 20 msec 10 msec
 3  10.2.2.1 30 msec 20 msec 30 msec
 4  172.16.3.3 30 msec 20 msec 30 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**. 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.



Username: admin01

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

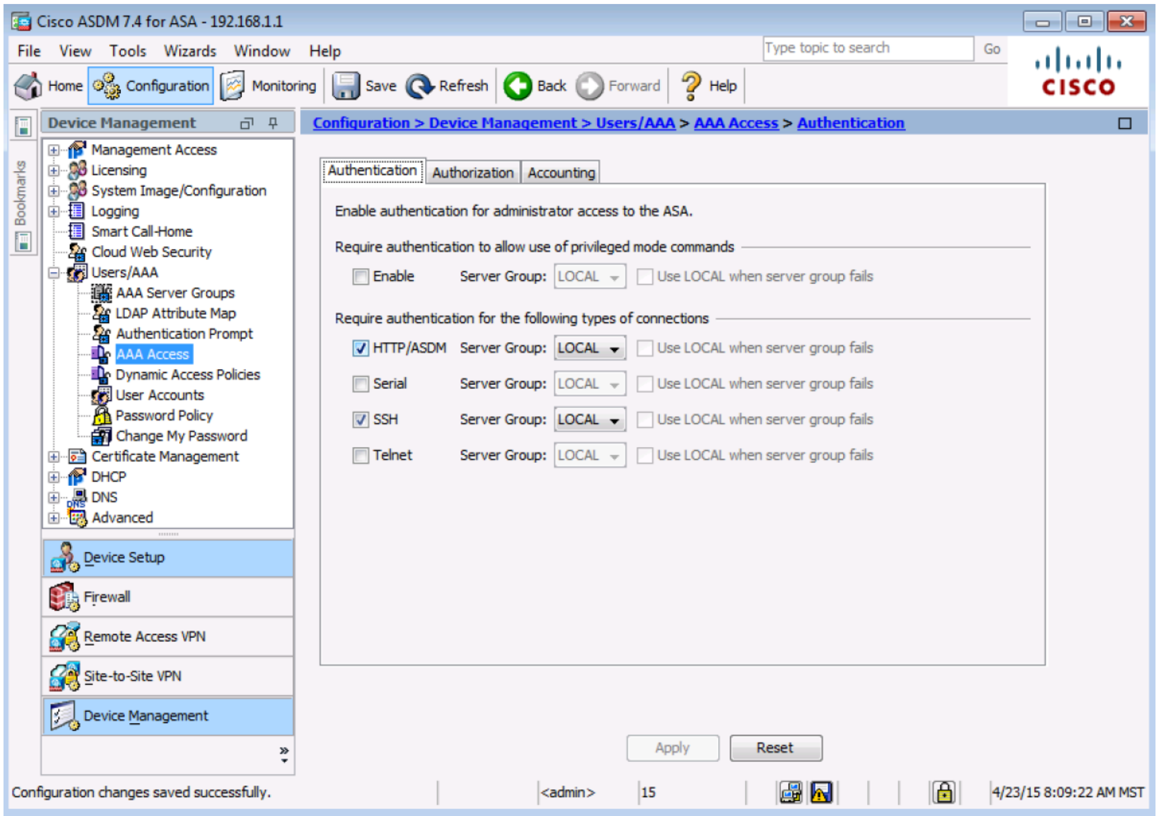
○ CLI login prompt for SSH, Telnet and console (no ASDM access)

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.

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.



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

Configuration changes saved successfully. <admin> 15 4/23/15 8:09:22 AM MST

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.

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 **admin01** and the password **admin01pass**.

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 **admin01** and the password **admin01pass**.

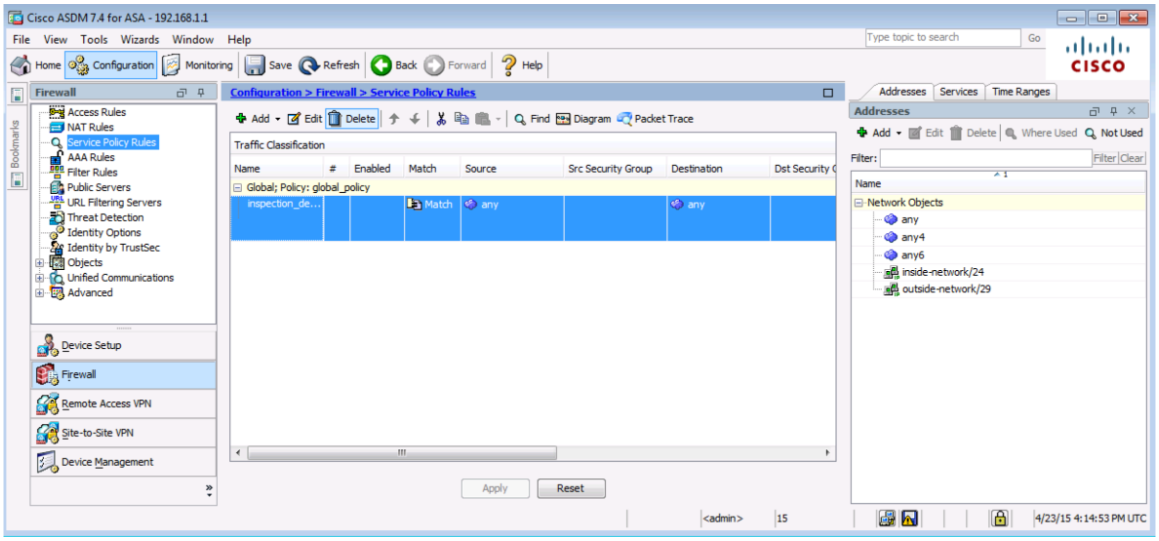
c. After logging in to the ASA using SSH, enter the **enable** command and provide the password **cisco12345**. Issue the **show run** command to display the current configuration that you have created using ASDM.

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**.

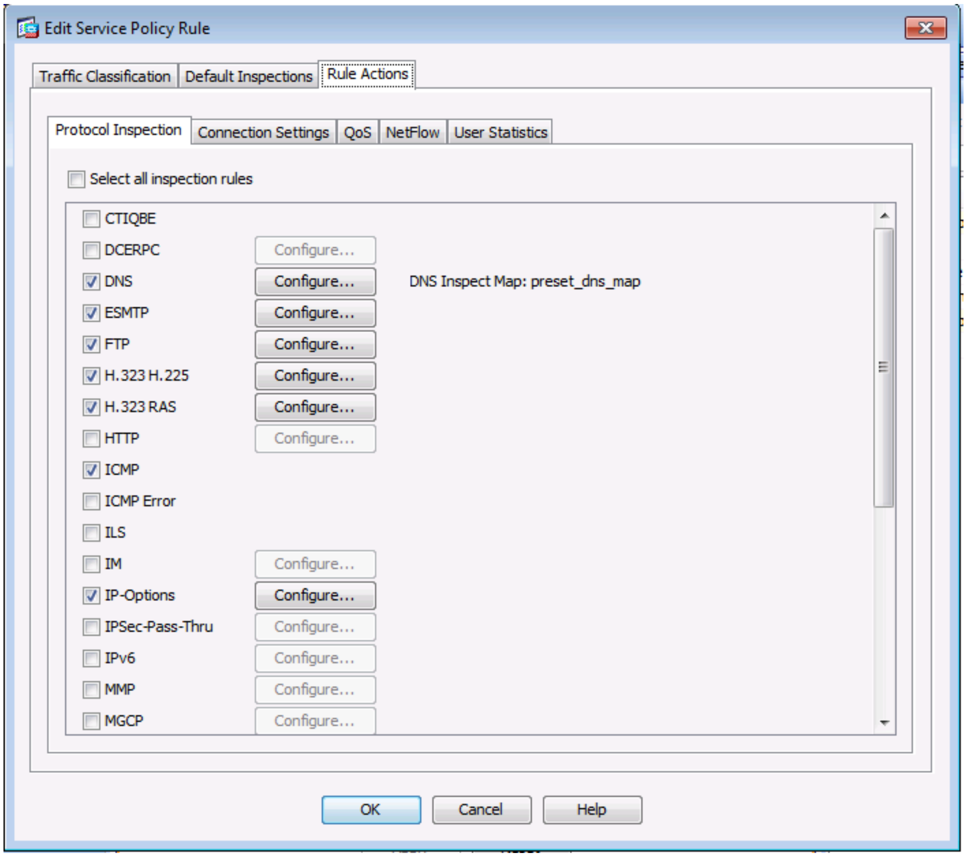
Step 5: Modify the MPF application inspection policy.

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**.


Cisco ASDM 7.4 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
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Bookmarks
Configuration > Firewall > Service Policy Rules
Add Edit Delete Find Diagram Packet Trace
Traffic Classification
Name # Enabled Match Source Src Security Group Destination Dst Security
Global; Policy: global_policy
inspection_de... Match any any
Apply Reset
Addresses Services Time Ranges
Addresses
Add Edit Delete Where Used Not Used
Filter: Filter Clear
Name
Network Objects
any
any4
any6
inside-network/24
outside-network/29
<admin> 15 4/23/15 4:14:53 PM UTC

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**.



□ Select all inspection rules

□ CTIQBE
□ DCERPC
☑ DNS — DNS Inspect Map: preset_dns_map
☑ ESMTP
☑ FTP
☑ H.323 H.225
☑ H.323 RAS
□ HTTP
☑ ICMP
□ ICMP Error
□ ILS
□ IM
☑ IP-Options
□ IPSec-Pass-Thru
□ IPv6
□ MMP
□ MGCP

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.

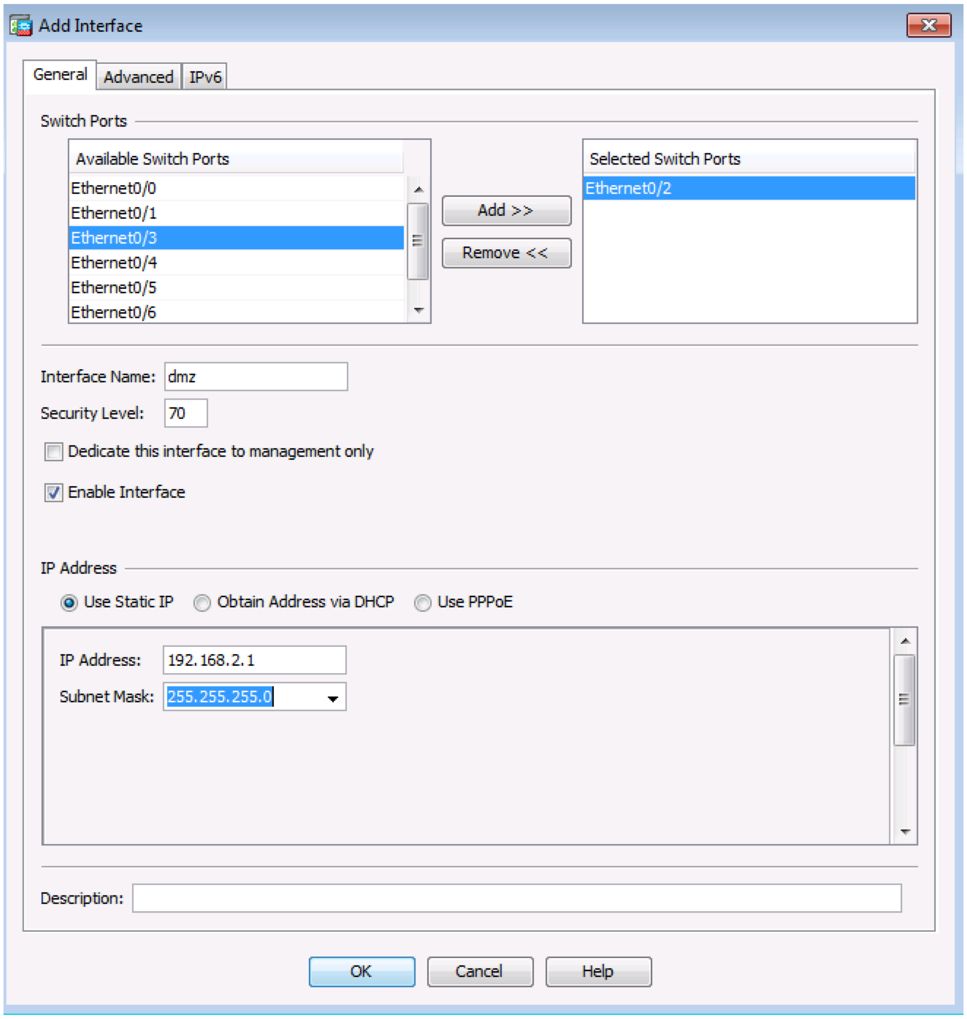
Step 1: Configure the ASA DMZ VLAN 3 interface.

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.

a. 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.

b. 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.

c. 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.



Available Switch Ports:
- Ethernet0/0
- Ethernet0/1
- Ethernet0/3
- Ethernet0/4
- Ethernet0/5
- Ethernet0/6

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

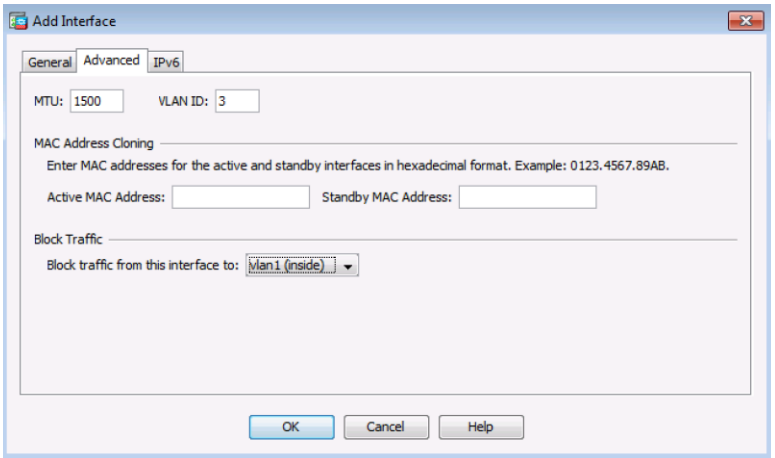
Subnet Mask: 255.255.255.0

Description:

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.



MTU: 1500 VLAN ID: 3

MAC Address Cloning

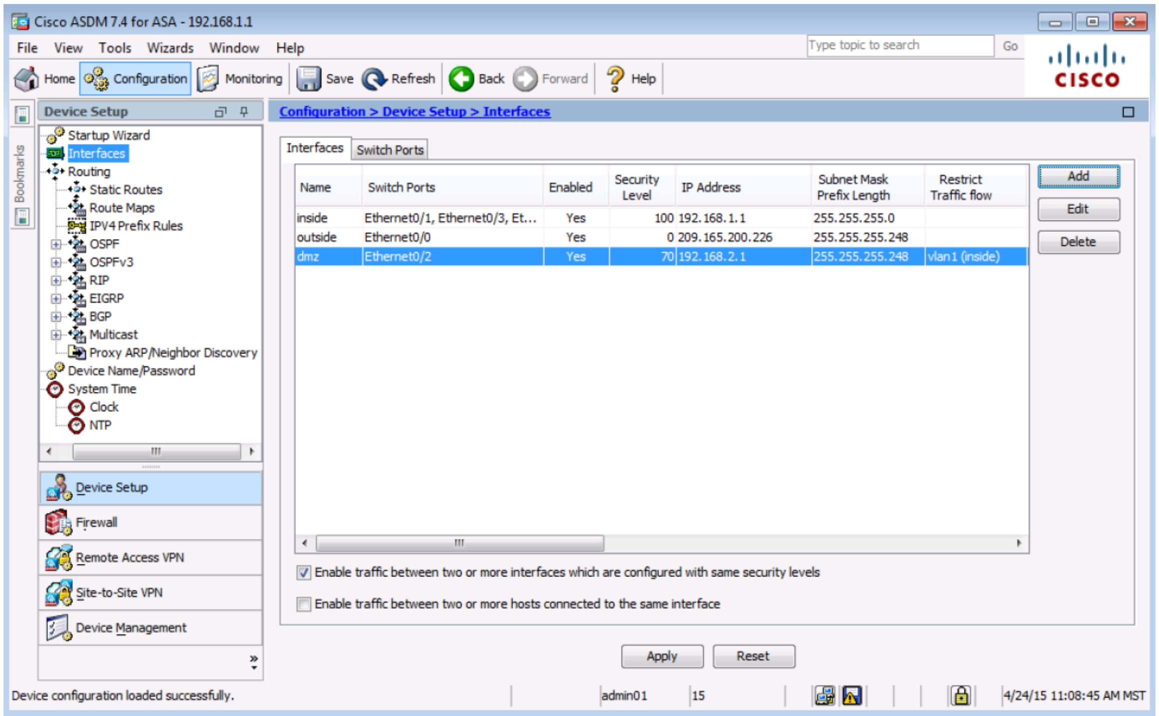
Enter MAC addresses for the active and standby interfaces in hexadecimal format. Example: 0123.4567.89AB.

Active MAC Address: Standby MAC Address:

Block Traffic

Block traffic from this interface to: vlan1 (inside)

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.



Configuration > Device Setup > Interfaces

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

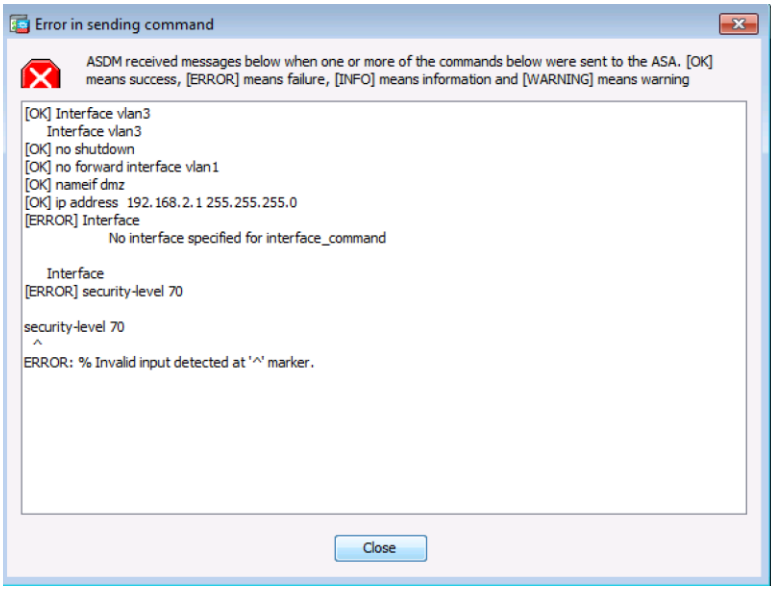
☐ Enable traffic between two or more hosts connected to the same interface

Device configuration loaded successfully.

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.



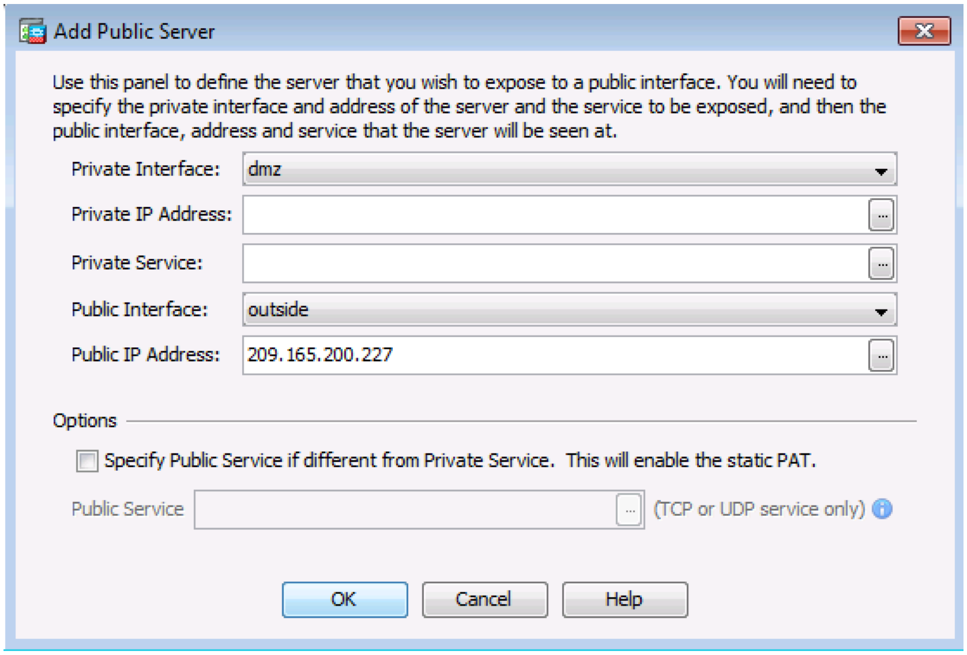
ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning

```
[OK] Interface vlan3
    Interface vlan3
[OK] no shutdown
[OK] no forward interface vlan1
[OK] nameif dmz
[OK] ip address  192.168.2.1 255.255.255.0
[ERROR] Interface
              No interface specified for interface_command

    Interface
[ERROR] security-level 70

security-level 70
 ^
ERROR: % Invalid input detected at '^' marker.
```

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**.



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

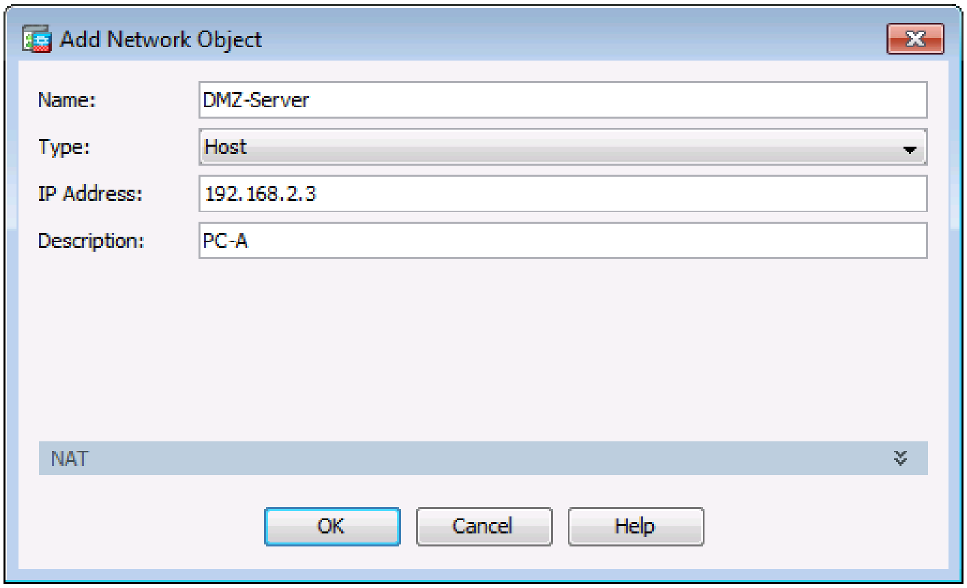
Public IP Address: 209.165.200.227

Options

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

Public Service (TCP or UDP service only)

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**.



Add Network Object

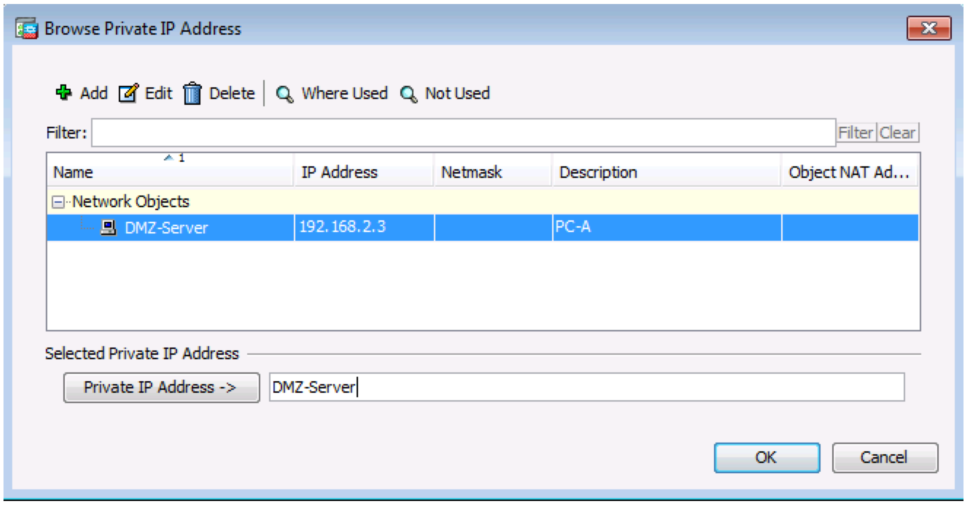
Name: DMZ-Server

Type: Host

IP Address: 192.168.2.3

Description: PC-A

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.



Filter:

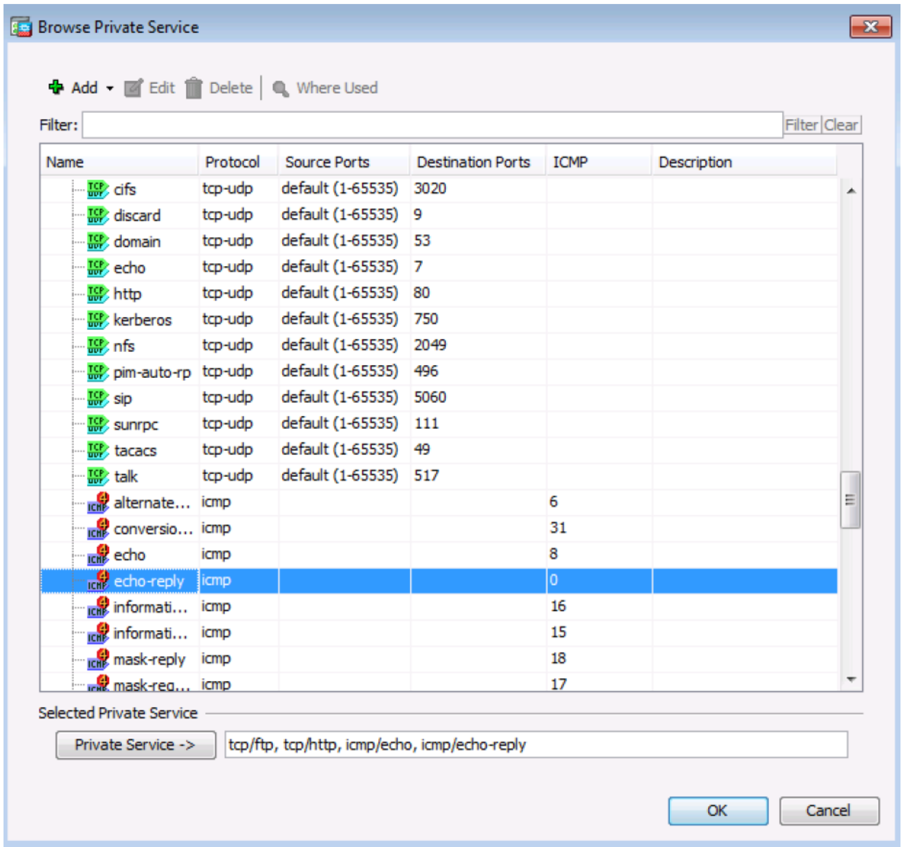
Name	IP Address	Netmask	Description	Object NAT Ad...
Network Objects				
DMZ-Server	192.168.2.3		PC-A	

Selected Private IP Address

Private IP Address -> DMZ-Server

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.



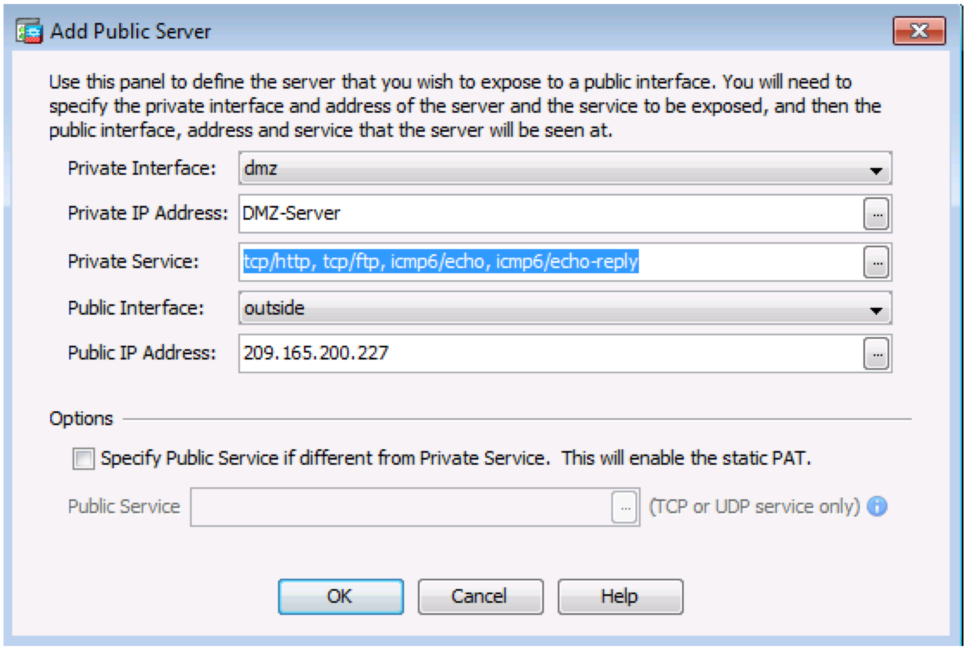
Filter:

Name	Protocol	Source Ports	Destination Ports	ICMP	Description
cifs	tcp-udp	default (1-65535)	3020		
discard	tcp-udp	default (1-65535)	9		
domain	tcp-udp	default (1-65535)	53		
echo	tcp-udp	default (1-65535)	7		
http	tcp-udp	default (1-65535)	80		
kerberos	tcp-udp	default (1-65535)	750		
nfs	tcp-udp	default (1-65535)	2049		
pim-auto-rp	tcp-udp	default (1-65535)	496		
sip	tcp-udp	default (1-65535)	5060		
sunrpc	tcp-udp	default (1-65535)	111		
tacacs	tcp-udp	default (1-65535)	49		
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	

Selected Private Service

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

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.



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: DMZ-Server

Private Service: tcp/http, tcp/ftp, icmp6/echo, icmp6/echo-reply

Public Interface: outside

Public IP Address: 209.165.200.227

Options

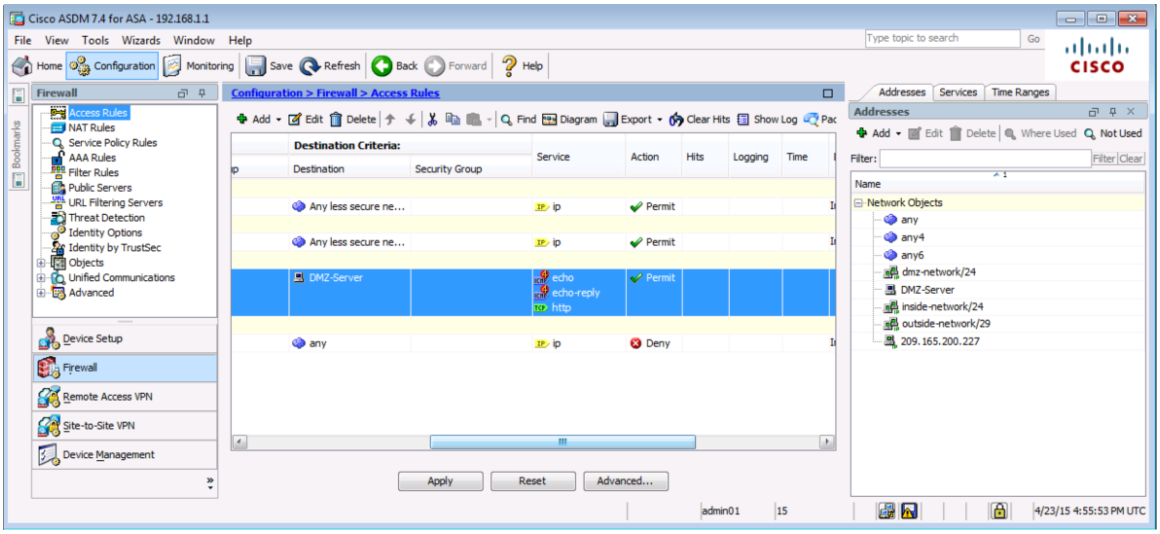
□ Specify Public Service if different from Private Service. This will enable the static PAT.

Public Service (TCP or UDP service only)

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 7.4 for ASA - 192.168.1.1

Configuration > Firewall > Access Rules

Destination	Security Group	Service	Action	Hits	Logging	Time
Any less secure ne...		ip	Permit			
Any less secure ne...		ip	Permit			
DMZ-Server		echo echo-reply http	Permit			
any		ip	Deny			

Addresses

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

admin01 15 4/23/15 4:55:53 PM UTC

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.

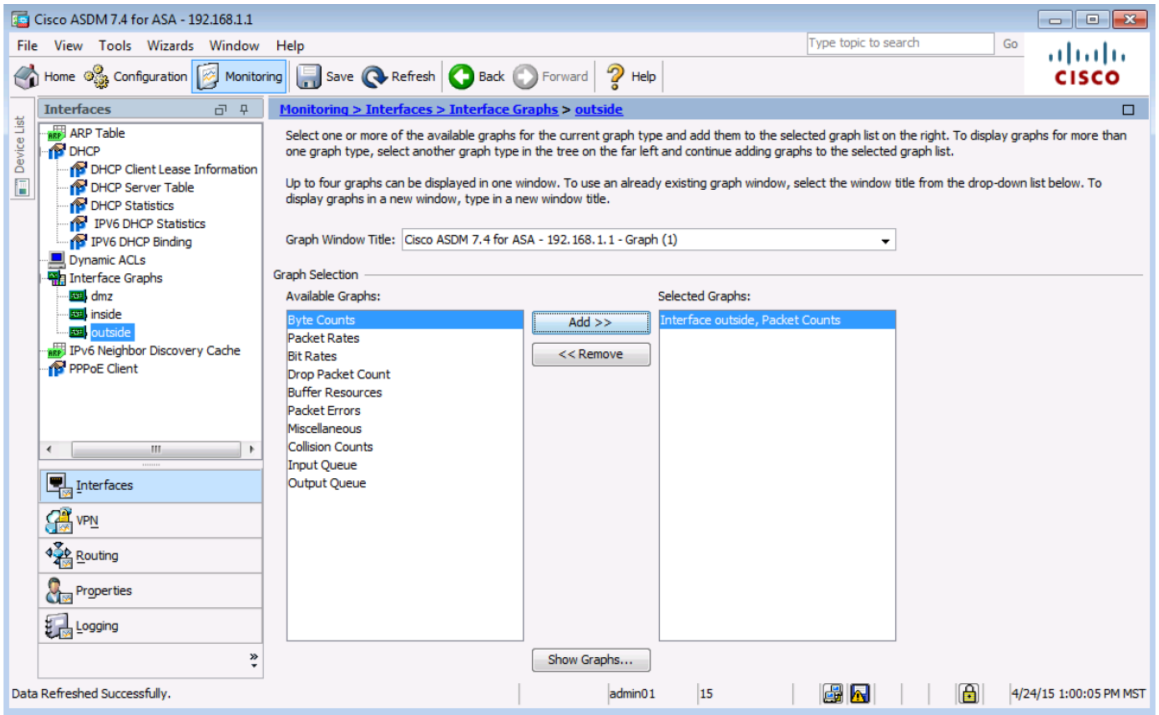
b. Because the ASA inside interface (VLAN 1) is set to security level 100 (the highest) and the DMZ interface (VLAN 3) is set to 70, you can also access the DMZ server from a host on the inside network. The ASA acts like a router between the two networks. Ping the DMZ server (PC-A) internal address (**192.168.2.3**) 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.

c. 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.

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 7.4 for ASA - 192.168.1.1

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 7.4 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

Data Refreshed Successfully. admin01 15 4/24/15 1:00:05 PM MST

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.
```

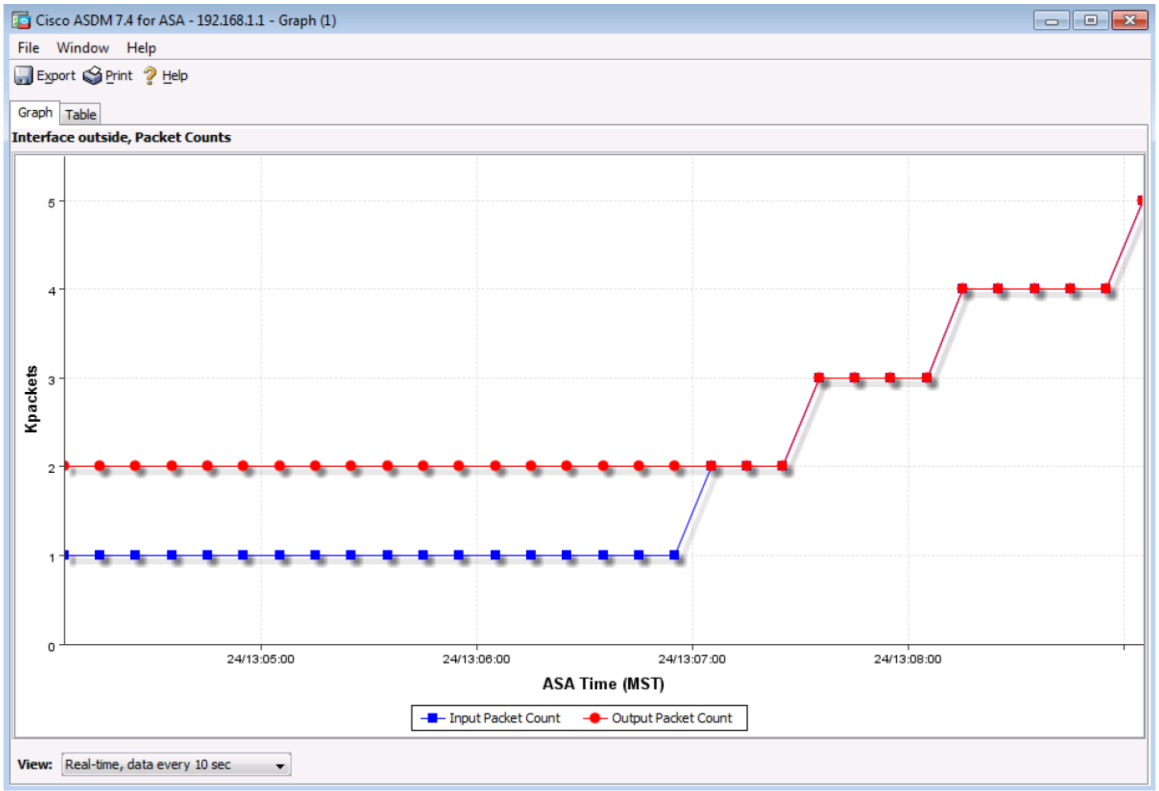
```
Sending 1000, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
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 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.



View: Real-time, data every 10 sec

Reflection

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

____

____

____

____

____

____

   The ASDM GUI is easier to use, especially for less technical staff, and can generate very complex configurations through the use of mouse selections, fill-in fields, and wizards.

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

____

____

____

____

____

____

   In some cases, the CLI can provide more precise control over the desired configuration. Also, some CLI commands are necessary to prepare the ASA for GUI access. CLI requires only a serial console connection, whereas ASDM requires Layer 3 (IP) connectivity to an ASA interface.

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.				

Device Configs

ASA 5505

```
CCNA-ASA# show run
: Saved
:
: Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
:
ASA Version 9.2(3)
!
hostname CCNA-ASA
domain-name ccnasecurity.com
enable password 9D8jmmmgkfNZLETh encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
!
ftp mode passive
clock timezone MST -7
dns server-group DefaultDNS
 domain-name ccnasecurity.com
same-security-traffic permit inter-interface
object network DMZ-Server
 host 192.168.2.3
 description PC-A
object-group service DM_INLINE_SERVICE_0
 service-object tcp destination eq ftp
 service-object tcp destination eq www
 service-object icmp echo
 service-object icmp echo-reply
access-list outside_access extended permit object-group DM_INLINE_SERVICE_0 any4
object DMZ-Server
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network DMZ-Server
 nat (dmz,outside) static 209.165.200.227
!
nat (inside,outside) after-auto source dynamic any interface
access-group outside_access in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
```

```
user-identity default-domain LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3 255.255.255.255 outside
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd address 192.168.1.31-192.168.1.39 inside
dhcpd dns 10.20.30.40 interface inside
dhcpd domain ccnassecurity.com interface inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin01 password UsMZmktANM6Z2Y9I encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:ae125013af19c6ec37b50b075f2e8561
: end
```

Router R1

```
R1# show run
Building configuration...

Current configuration : 1673 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 9 $9$P1rs5T9Im9YQKE$lCFKlTDFO3etXYLUZKWSOqz/QGzxjkhzZiJUENyJ4bI
!
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
```

```
!
cts logging verbose
!
username admin01 secret 9
$9$D96eQuJ01ZvWE.$m/ePFFlbfwd72xBHxVhrmlxsTy9IMxUa58HsDFOfA5w
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 logging synchronous
 login local
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R2

```
R2# show run
Building configuration...

Current configuration : 1373 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 64000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 172.16.3.0 255.255.255.0 10.2.2.1
ip route 209.165.200.224 255.255.255.248 10.1.1.1
!
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R3

```
R3# show run
Building configuration...

Current configuration : 1314 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
```

```
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Switches S1, S2, and S3 – Use default configs, except for host name