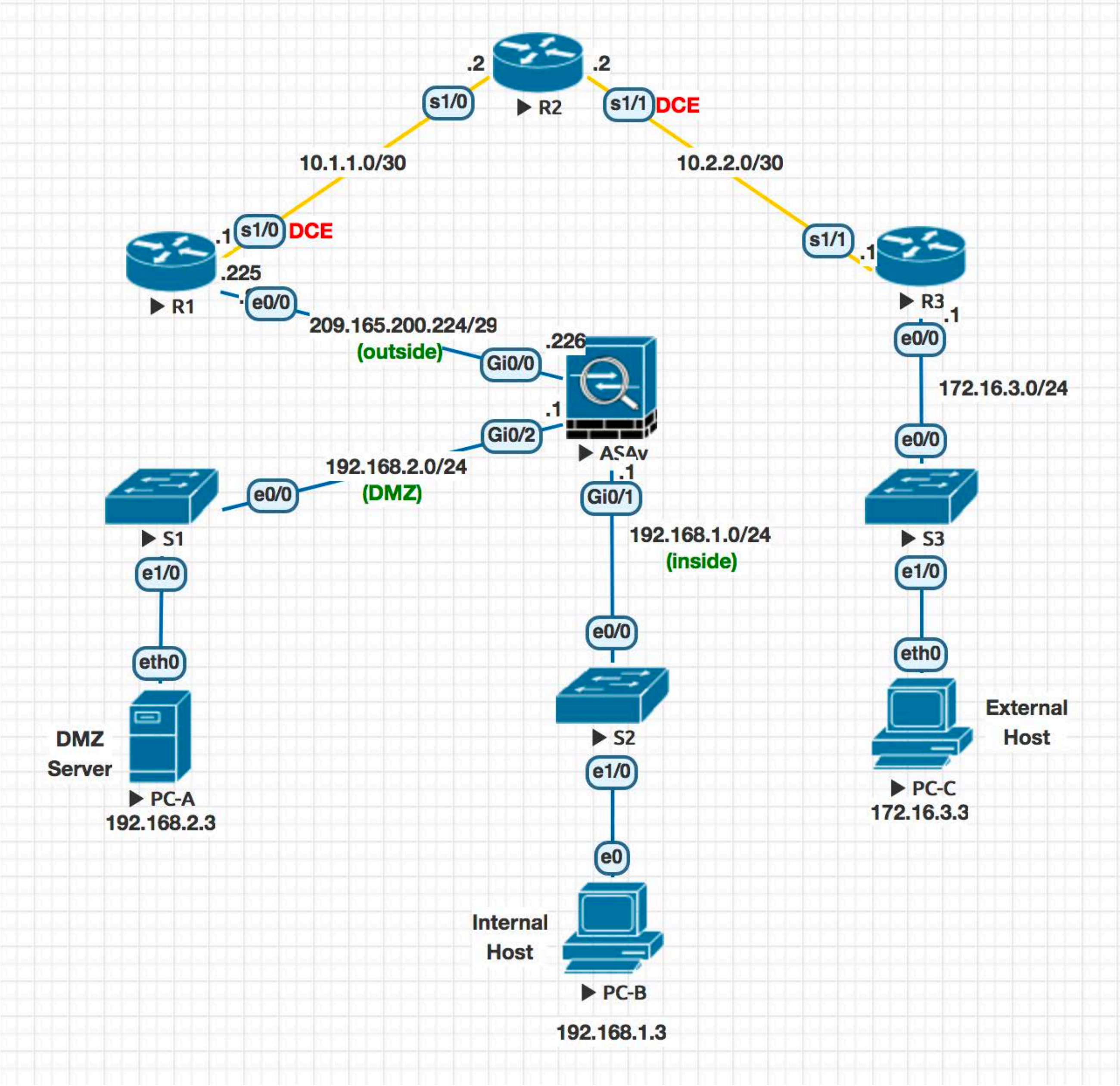
Lab2: Configure ASA Basic Settings and Firewall using ASDM

Topology



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	e0/0	209.165.200.225	255.255.255.248	N/A	ASA Gi0/0
	s1/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	s1/0	10.1.1.2	255.255.255.252	N/A	N/A
	s1/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	e0/0	172.16.3.1	255.255.255.0	N/A	S3 e0/0
	s1/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	Gi0/1 (inside)	192.168.1.1	255.255.255.0	NA	S2 e0/0
ASA	Gi0/0 (ouside)	209.165.200.226	255.255.255.248	NA	R1 e0/0
ASA	Gi0/2 (DMZ)	192.168.2.1	255.255.255.0	NA	S1 e0/0
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 e1/0
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 e1/0
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 e1/0

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 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 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 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 device 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. Routed 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.

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the routers, such as interface IP addresses and static routing.

Note: Do not configure ASA settings at this time.

Step 1: Configure basic settings for routers and switches.

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

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

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

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 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 2: Configure static routing on the routers.

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

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

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

b. Configure a static route from R2 to the R1 e0/0 subnet (connected to ASA interface Gi0/0) and a static route from R2 to the R3 LAN.

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

Step 3: Configure and encrypt passwords on R1.

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

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

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

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

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

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

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

Step 4: Configure PC host IP settings.

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

Step 5: Verify connectivity.

There will be no connectivity between devices that are connected to the ASA because the ASA is the focal point for the network zones and it has not been configured. However, PC-C should be able to ping the R1 interface e0/0. From PC-C, ping the R1 e0/0 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 e0/0 and S1/0, you have demonstrated that addressing has been configured properly, and static routing is configured and functioning correctly.

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

Part 2: Access the ASA Console and ASDM

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

Step 1: Access the ASA console.

a. Double click on the ASA appliance to open a terminal console connected to it

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

c. 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 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 Gi0/1 to prepare for ASDM access. The Security Level should be automatically set to the highest level of **100**. The inside interface will be used by PC-B to access ASDM on ASA physical interface Gi0/1.

```
ciscoasa (config)# interface g0/1
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)# no shutdown
ciscoasa(config-if)# exit
```

e. verify the Gi0/1 interface status. The status and protocol for interface Gi0/1 should be up/up

```
CCNAS-ASA(config)# show interface ip brief
Interface            IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0   unassigned      YES  unset  administratively down  up
GigabitEthernet0/1   192.168.1.1     YES  manual  up                    up
GigabitEthernet0/2   unassigned      YES  unset    administratively down  up
GigabitEthernet0/3   unassigned      YES  unset    administratively down  up
GigabitEthernet0/4   unassigned      YES  unset    administratively down  up
GigabitEthernet0/5   unassigned      YES  unset    administratively down  up
GigabitEthernet0/6   unassigned      YES  unset    administratively down  up
Management0/0        unassigned      YES  unset    administratively down  up
```

f. Pre-configure Gi0/0 as the outside interface, and bring it up. You will assign the IP address using ASDM.

```
ciscoasa(config)# int g0/0
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
```

g. Test connectivity to the ASA by pinging from PC-B to ASA interface Gi0/1 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**

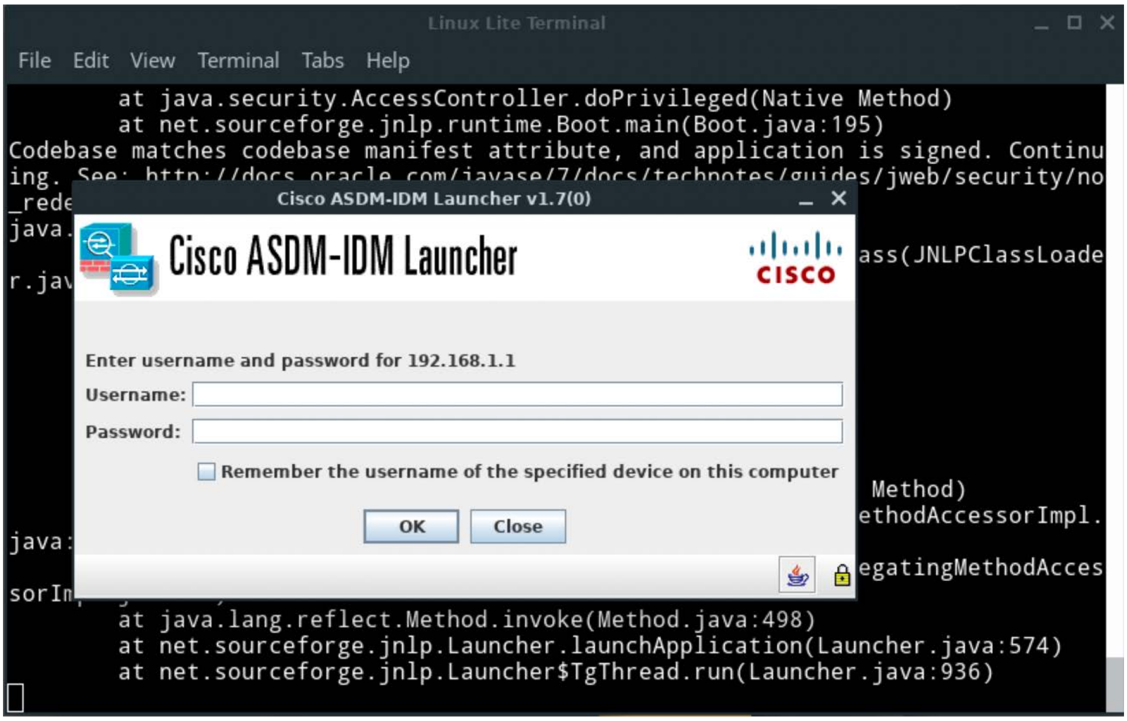
b. Open PC-B using a VNC application. On the linux console issue the command **./asdm 192.168.1.1**

Note: this command will prompt a script that start the **javaws** plugin. To investigate the script type **cat asdm** on console

You will be prompted with a security certificate warning. Select **Always trust..”** and click **Yes** for the other security warnings. You should see the Cisco ASDM-IDM Launcher

Step 5: Access ASDM and explore the GUI.

a. 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.



```
        at java.security.AccessController.doPrivileged(Native Method)
        at net.sourceforge.jnlp.runtime.Boot.main(Boot.java:195)
Codebase matches codebase manifest attribute, and application is signed. Continu
ing. See: http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/security/no
_rede
java.                                                          ass(JNLPClassLoade
r.jav

                                                                Method)
                                                               ethodAccessorImpl.
java:
                                                               egatingMethodAcces
sorIn
        at java.lang.reflect.Method.invoke(Method.java:498)
        at net.sourceforge.jnlp.Launcher.launchApplication(Launcher.java:574)
        at net.sourceforge.jnlp.Launcher$TgThread.run(Launcher.java:936)
```

Enter username and password for 192.168.1.1

Username:

Password:

□ Remember the username of the specified device on this computer

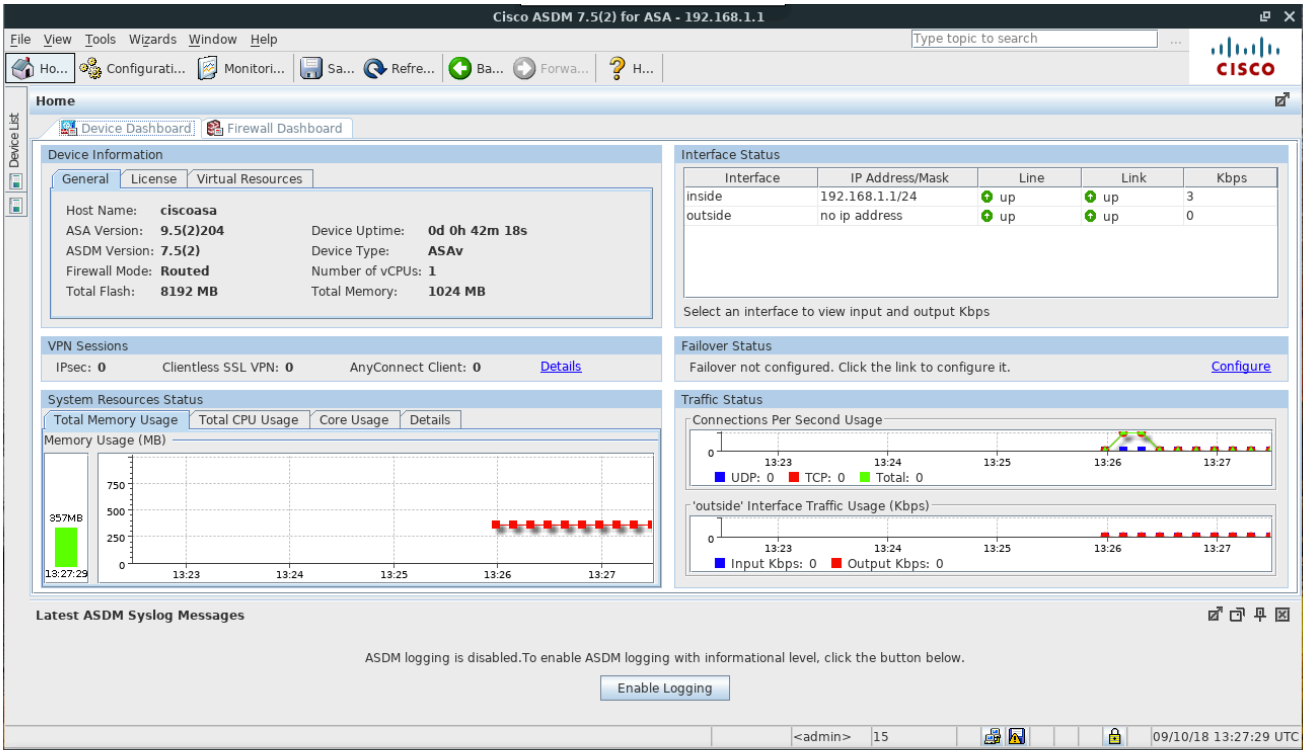
OK Close

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

c. 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 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**.


Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Ho... Configurati... Monitori... Sa... Refre... Ba... Forwa... H...
Device List
Home
Device Dashboard
Firewall Dashboard
General License Virtual Resources
Total Memory Usage Total CPU Usage Core Usage Details
Memory Usage (MB)
357MB
13:27:29
750
500
250
0
13:23 13:24 13:25 13:26 13:27
Connections Per Second Usage
'outside' Interface Traffic Usage (Kbps)
Latest ASDM Syslog Messages
Enable Logging
<admin> 15
09/10/18 13:27:29 UTC

Device Information

Host Name: ciscoasa
ASA Version: 9.5(2)204
ASDM Version: 7.5(2)
Firewall Mode: Routed
Total Flash: 8192 MB
Device Uptime: 0d 0h 42m 18s
Device Type: ASAv
Number of vCPUs: 1
Total Memory: 1024 MB

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

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

Failover Status

Failover not configured. Click the link to configure it. Configure

System Resources Status

Traffic Status

UDP: 0 TCP: 0 Total: 0

Input Kbps: 0 Output Kbps: 0

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

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

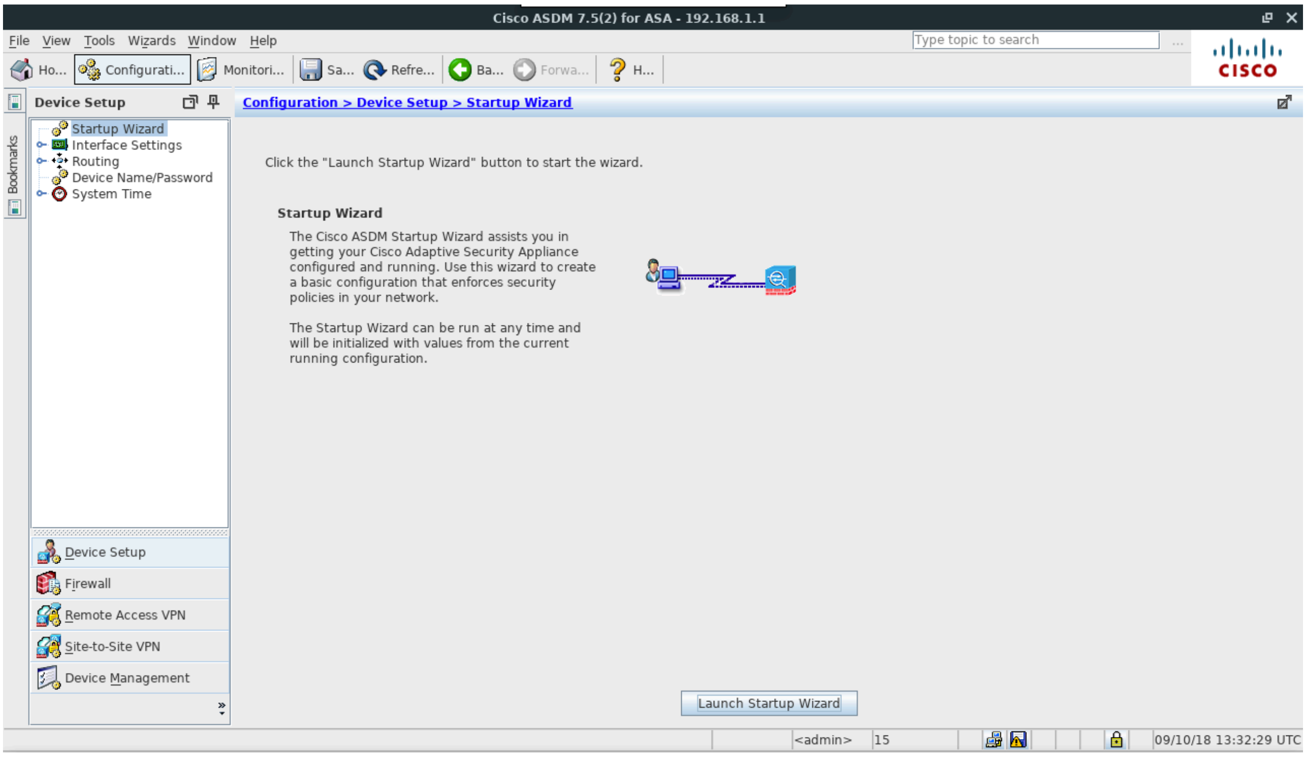
Part 3: Configure Basic ASA Settings and Firewall Using the ASDM Startup Wizard

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**.



Cisco ASDM 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Ho... Configurati... Monitori... Sa... Refre... Ba... Forwa... H...
Device Setup
Startup Wizard
Interface Settings
Routing
Device Name/Password
System Time
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Setup > Startup Wizard
Launch Startup Wizard
<admin> 15 09/10/18 13:32:29 UTC

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

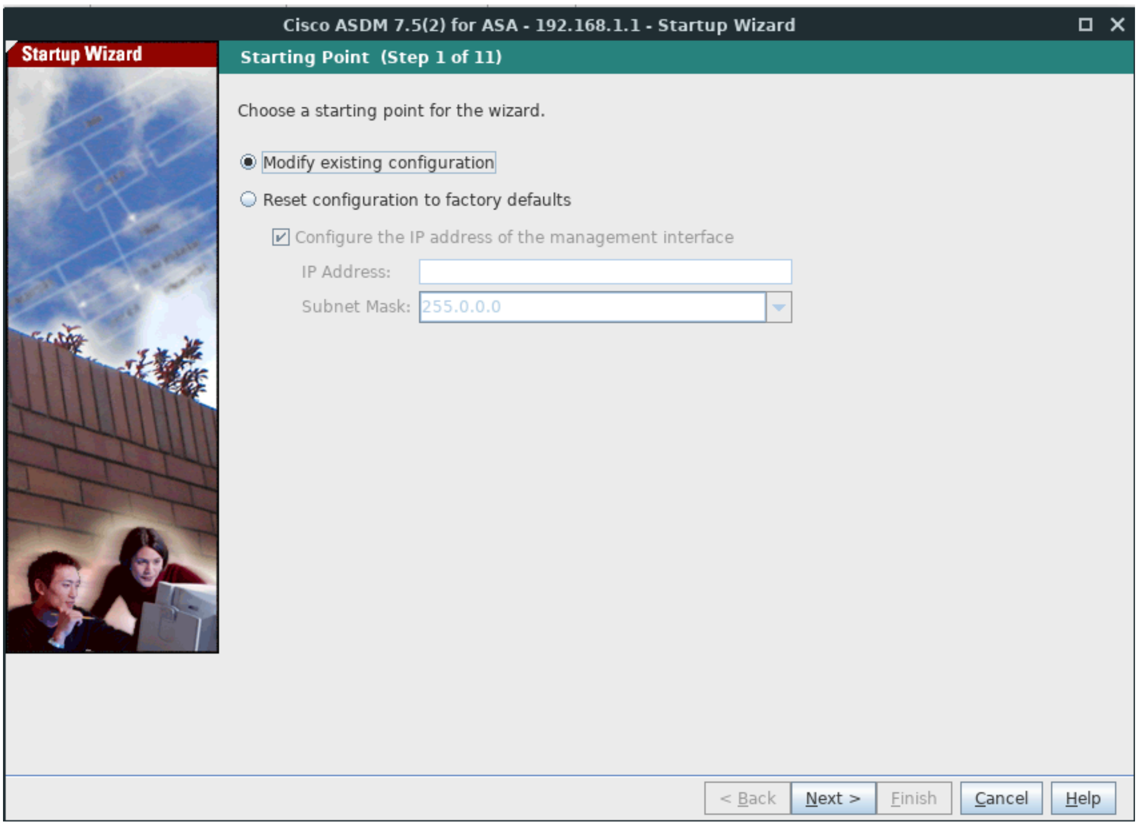
Startup Wizard

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

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

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

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



Cisco ASDM 7.5(2) for ASA - 192.168.1.1 - Startup Wizard
Startup Wizard
Starting Point (Step 1 of 11)
< Back
Next >
Finish
Cancel
Help

Choose a starting point for the wizard.

● Modify existing configuration

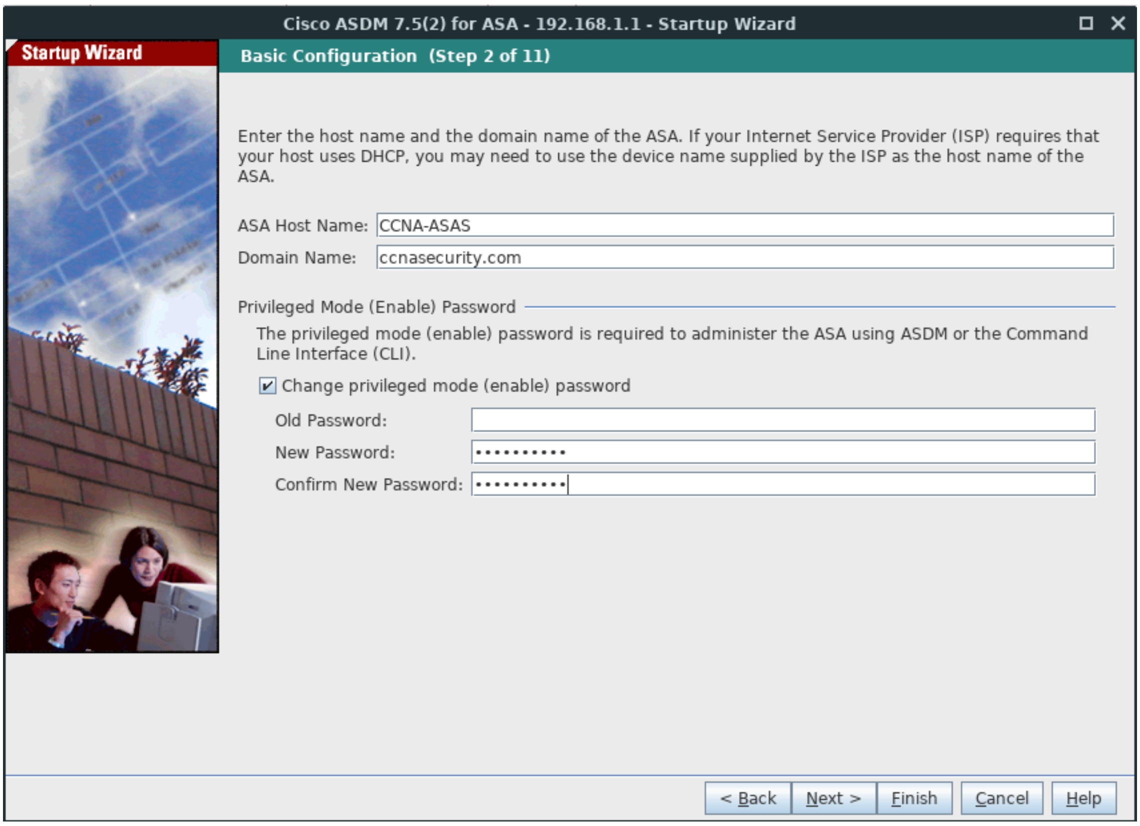
○ Reset configuration to factory defaults

☑ Configure the IP address of the management interface

IP Address:

Subnet Mask: 255.0.0.0

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



Cisco ASDM 7.5(2) for ASA - 192.168.1.1 - Startup Wizard

Basic Configuration (Step 2 of 11)

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: CCNA-ASAS

Domain Name: ccnasecurity.com

Privileged Mode (Enable) Password

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

☑ Change privileged mode (enable) password

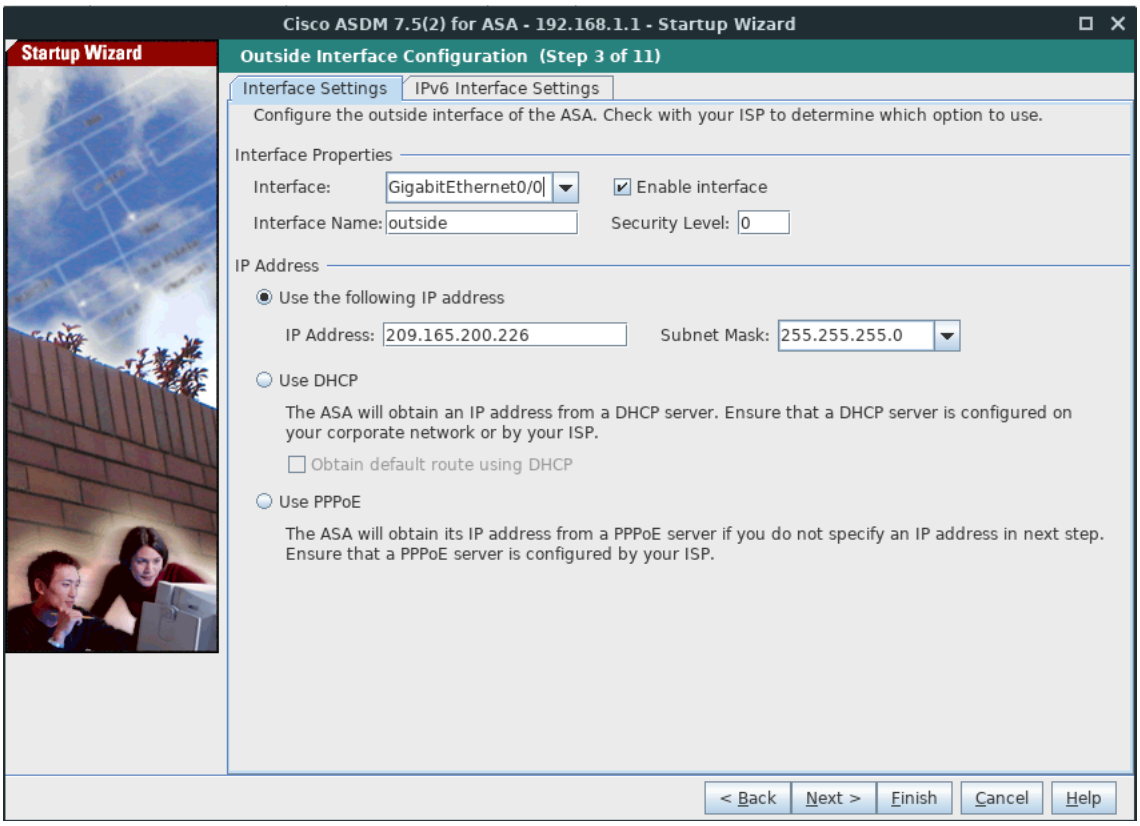
Old Password:

New Password: ••••••••••

Confirm New Password: ••••••••••

Step 3: Configure the inside and outside interfaces security level and IP addresses.

a. On the Startup Wizard Step 3 screen select the interface **GigabitEthernet0/0,** enable it, set the **outside** interface name**,** set the address **209.165.200.226** and **255.255.255.0** mask.



Outside Interface Configuration (Step 3 of 11)

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

Interface Properties

Interface: GigabitEthernet0/0 ☑ Enable interface

Interface Name: outside Security Level: 0

IP Address

● Use the following IP address

IP Address: 209.165.200.226 Subnet Mask: 255.255.255.0

○ Use DHCP

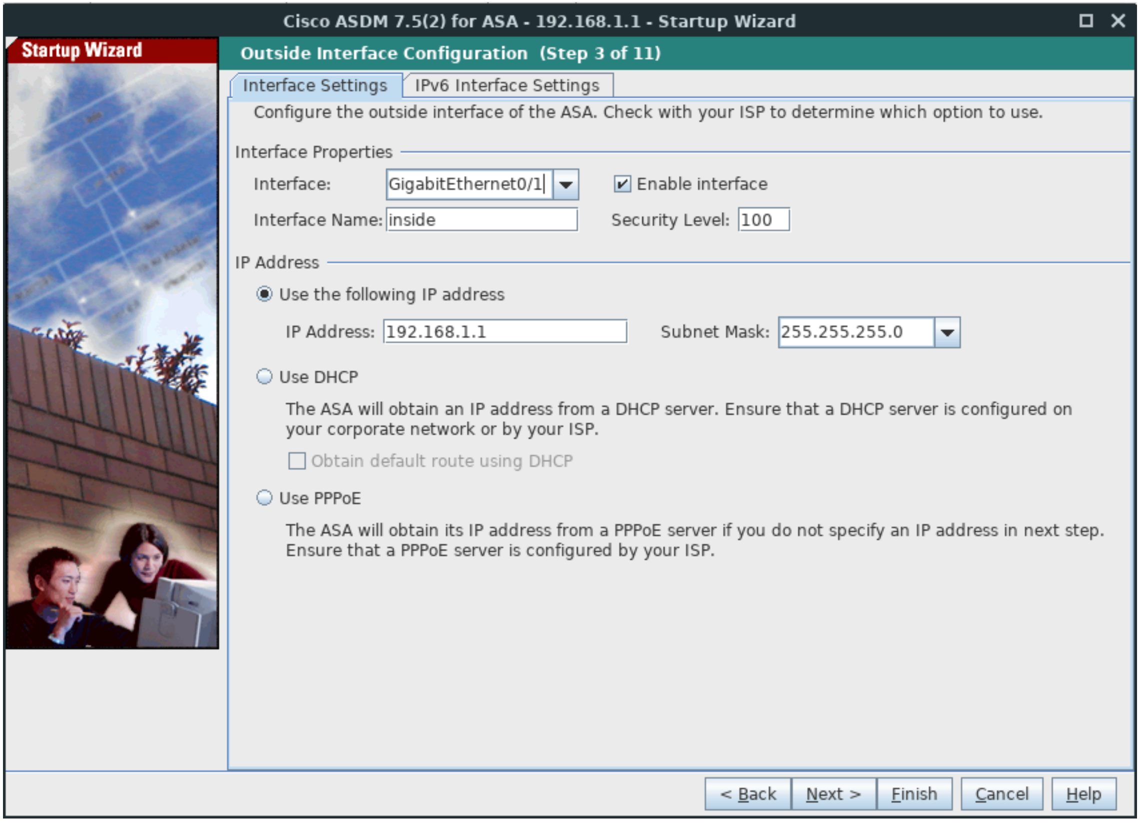
The ASA will obtain an IP address from a DHCP server. Ensure that a DHCP server is configured on your corporate network or by your ISP.

□ Obtain default route using DHCP

○ Use PPPoE

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

b. Select the interface **GigabitEthernet0/1** and check that the settings previously configured from CLI are correct.



Outside Interface Configuration (Step 3 of 11)

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

Interface Properties

Interface: GigabitEthernet0/1 ☑ Enable interface

Interface Name: inside Security Level: 100

IP Address

● Use the following IP address

IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

○ Use DHCP

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

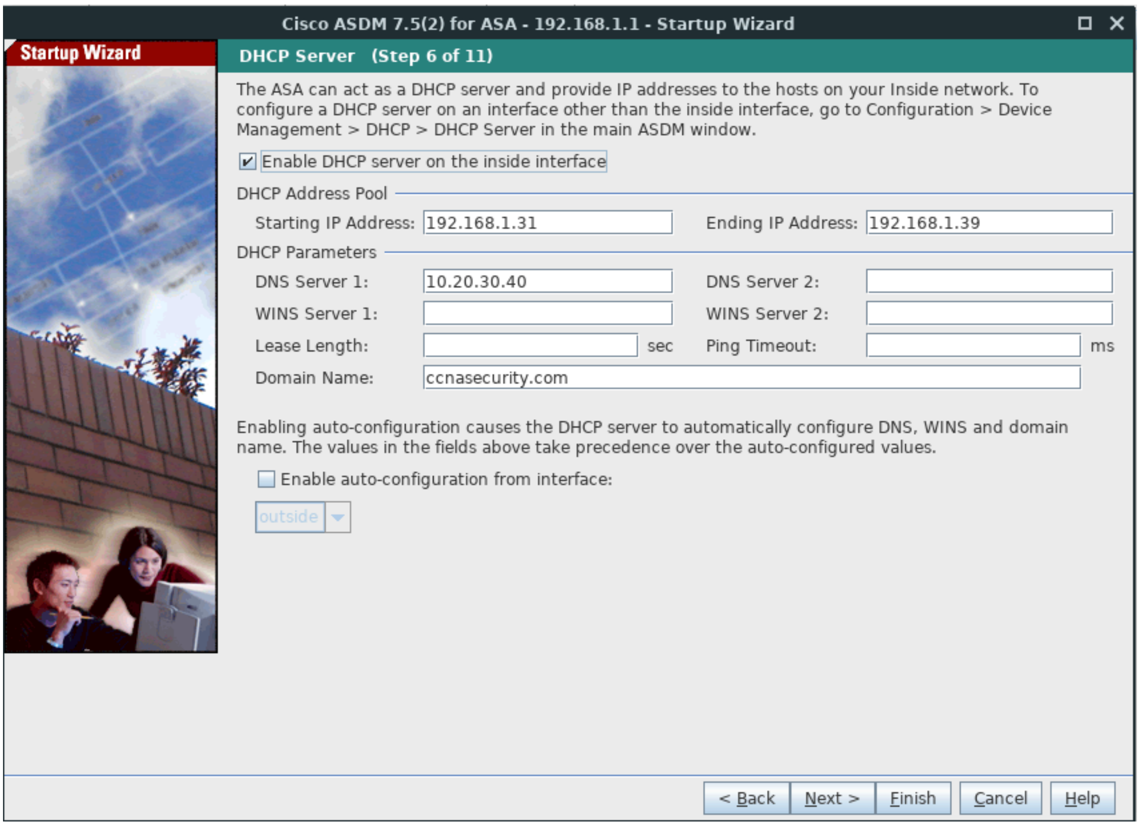
□ Obtain default route using DHCP

○ Use PPPoE

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

Step 4: Configure DHCP, address translation, and administrative access.

a. Review the address configuration on Wizards step 4 and click next. Ignore step 5. 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.



Cisco ASDM 7.5(2) for ASA - 192.168.1.1 - Startup Wizard

DHCP Server (Step 6 of 11)

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

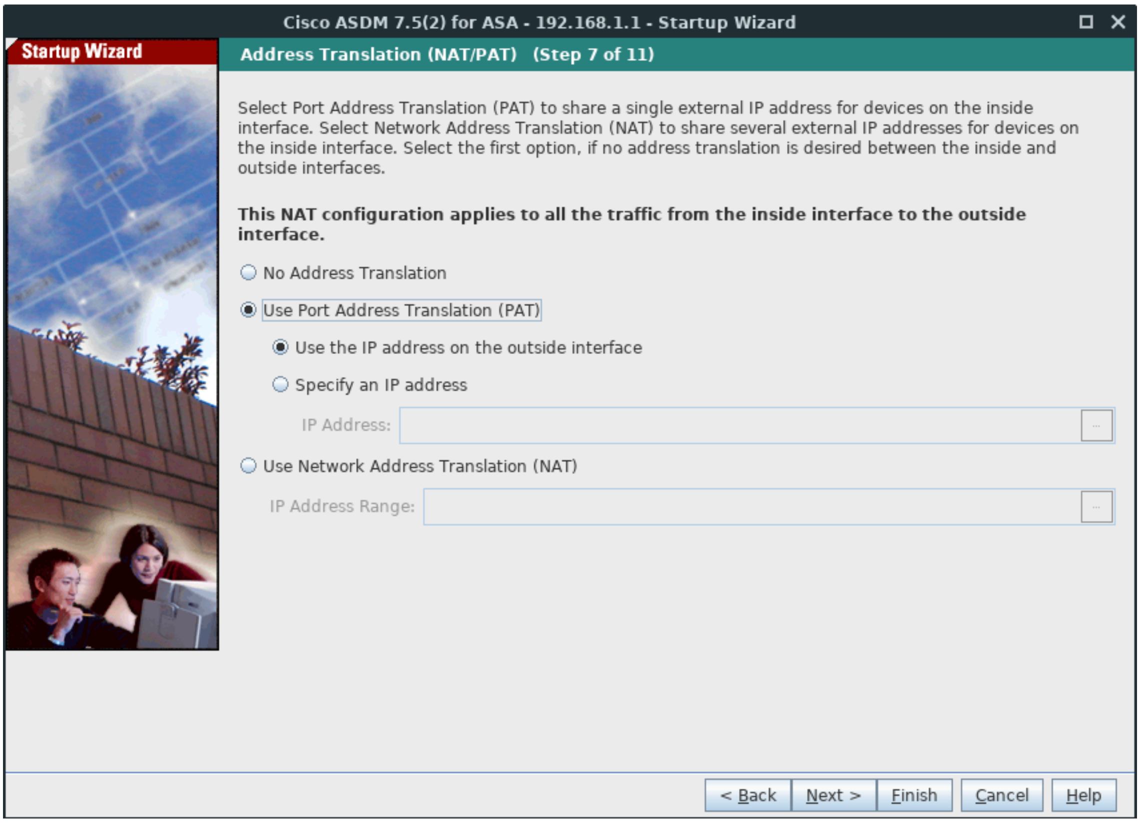
Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

☐ 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.



Cisco ASDM 7.5(2) for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Address Translation (NAT/PAT) (Step 7 of 11)

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

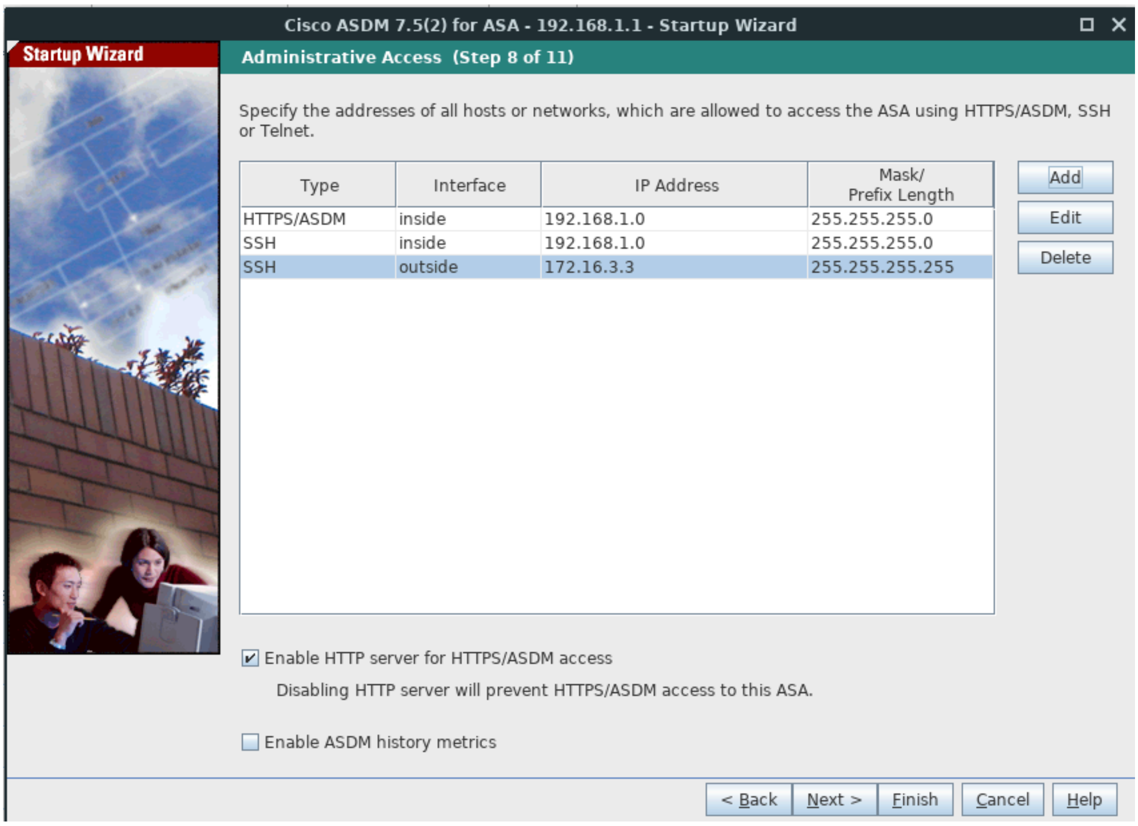
○ Specify an IP address

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.



Cisco ASDM 7.5(2) for ASA - 192.168.1.1 - Startup Wizard

Administrative Access (Step 8 of 11)

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

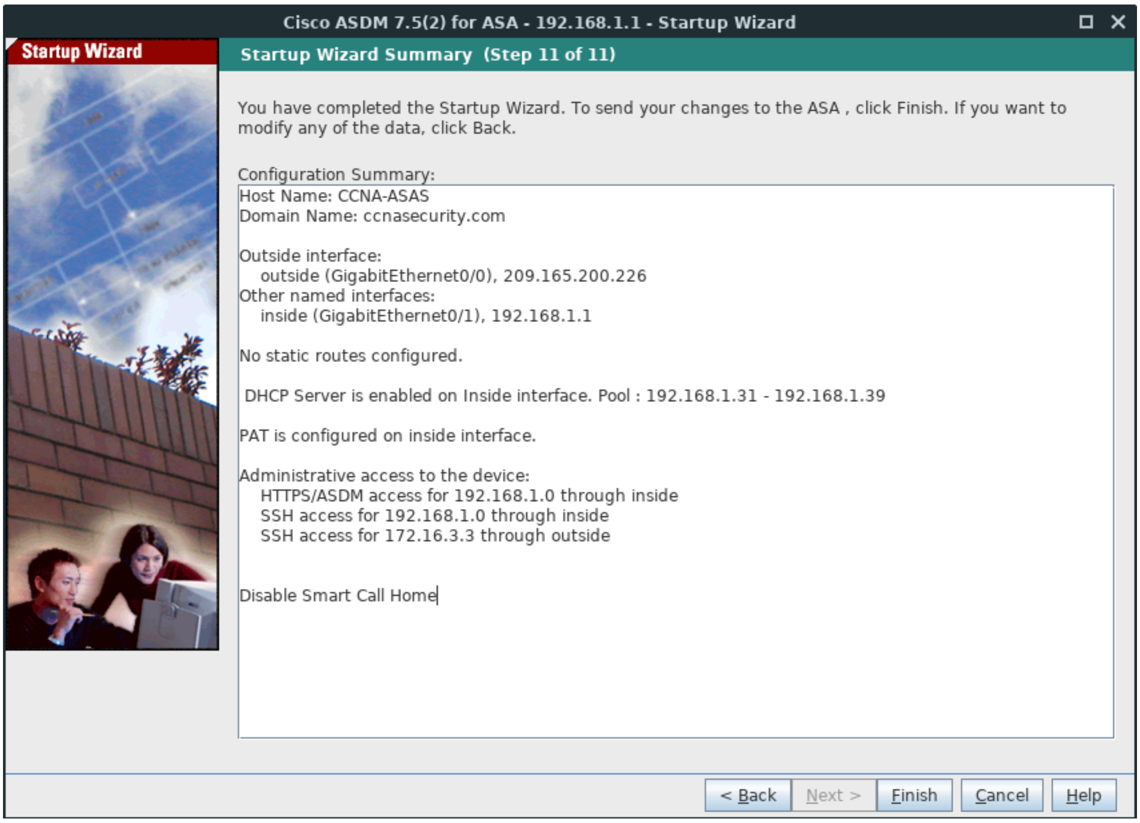
Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

☐ Enable ASDM history metrics

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

a. Skip Step 9 (uncheck the box “Enable Auto Update for ASA) and Step 10. On the Startup Wizard Step 11 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.



Startup Wizard Summary (Step 11 of 11)

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: CCNA-ASAS
Domain Name: ccnasecurity.com

Outside interface:
   outside (GigabitEthernet0/0), 209.165.200.226
Other named interfaces:
   inside (GigabitEthernet0/1), 192.168.1.1

No static routes configured.

 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 192.168.1.0 through inside
   SSH access for 172.16.3.3 through outside


Disable Smart Call Home
```

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.

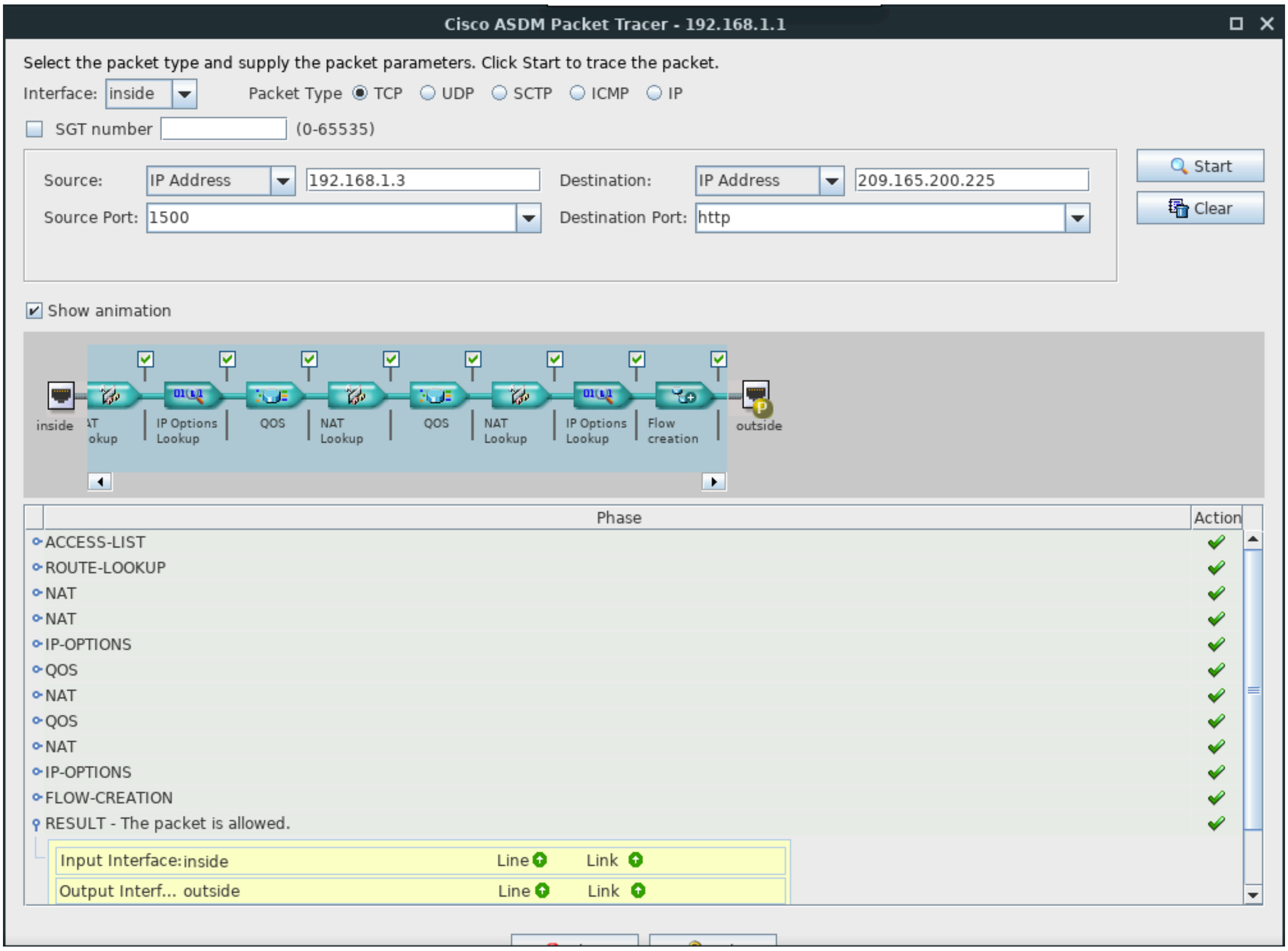
a. Open a browser on PC-B and enter the IP address of the R1 e0/0 interface (**209.165.200.225**) to simulate access to an external website.

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 e0/0) 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 ○ SCTP ○ ICMP ○ IP

□ SGT number (0-65535)

Source: IP Address 192.168.1.3   Destination: IP Address 209.165.200.225

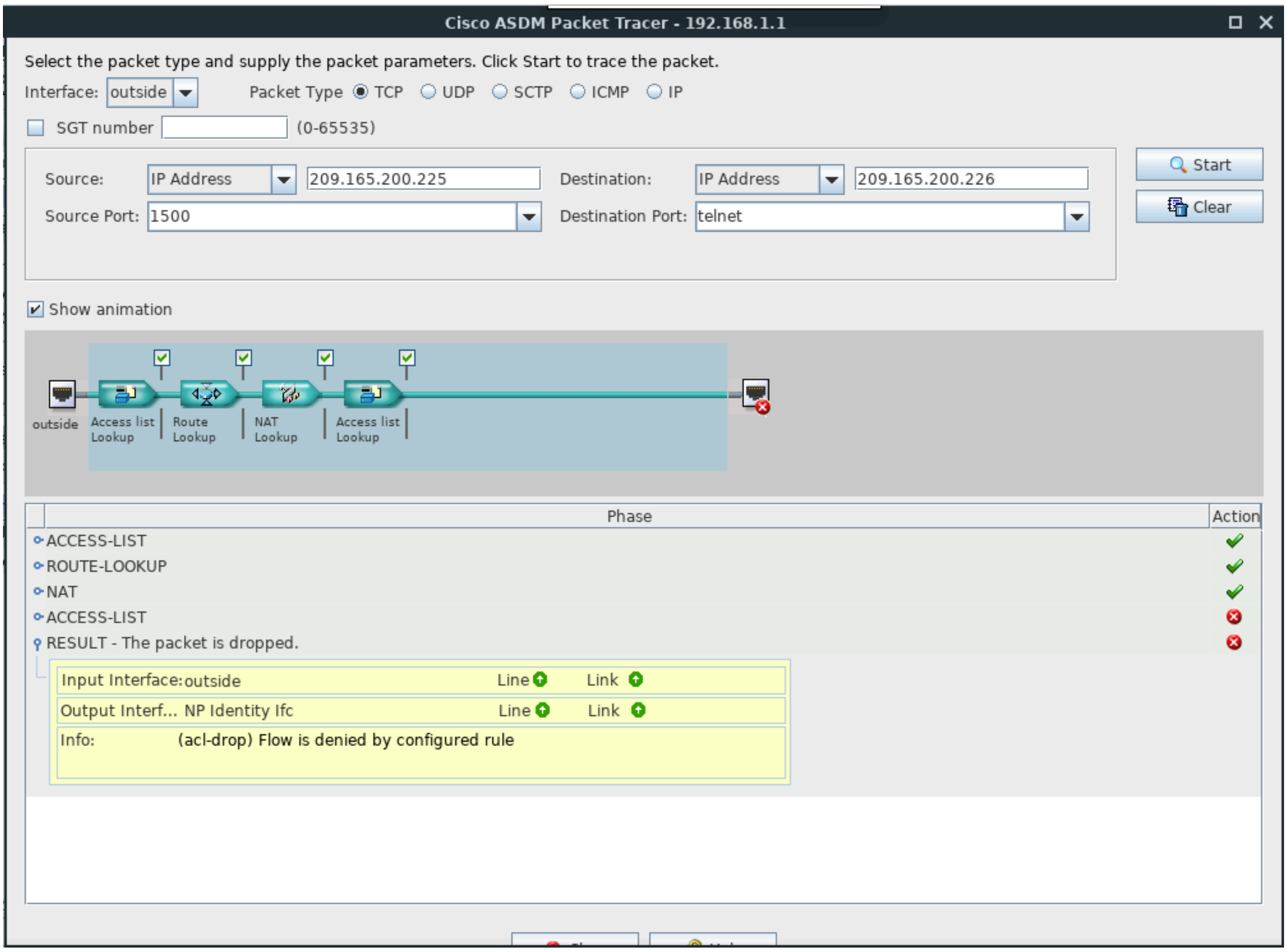
Source Port: 1500   Destination Port: http

☑ Show animation

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

Input Interface: inside	Line ●	Link ●
Output Interf... outside	Line ●	Link ●

c. Click **Clea**r 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 e0/0) 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 ○ SCTP ○ ICMP ○ IP

□ SGT number (0-65535)

Source: IP Address 209.165.200.225   Destination: IP Address 209.165.200.226

Source Port: 1500   Destination Port: telnet

☑ Show animation

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

Input Interface: outside   Line   Link

Output Interf... NP Identity Ifc   Line   Link

Info: (acl-drop) Flow is denied by configured rule

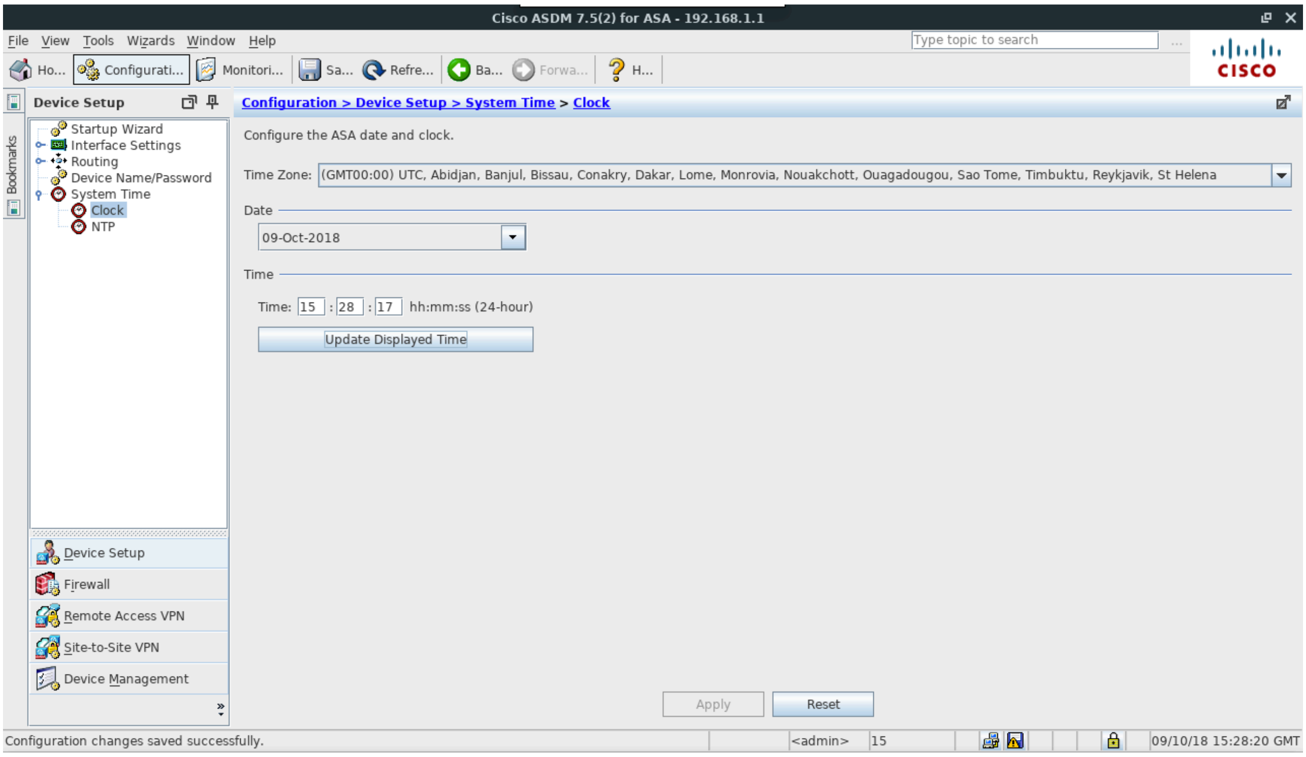
Part 4: Configure ASA Settings from the ASDM Configuration Menu

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.



Cisco ASDM 7.5(2) for ASA - 192.168.1.1

Configuration > Device Setup > System Time > Clock

Configure the ASA date and clock.

Time Zone: (GMT00:00) UTC, Abidjan, Banjul, Bissau, Conakry, Dakar, Lome, Monrovia, Nouakchott, Ouagadougou, Sao Tome, Timbuktu, Reykjavik, St Helena

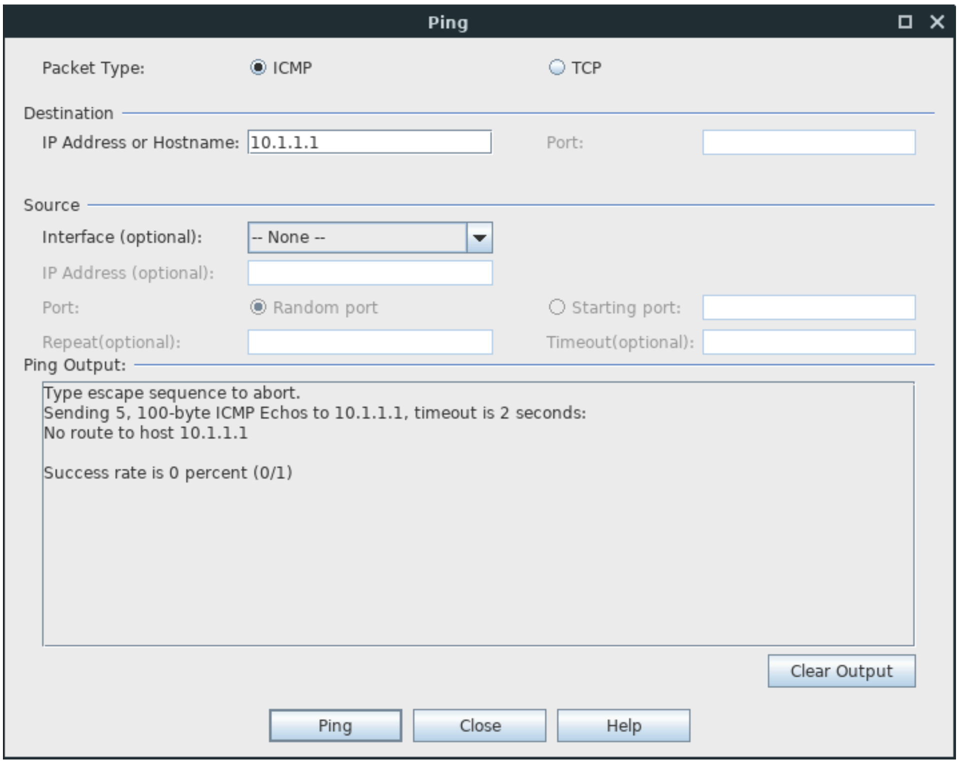
Date: 09-Oct-2018

Time: 15 : 28 : 17 hh:mm:ss (24-hour)

Configuration changes saved successfully. <admin> 15 09/10/18 15:28:20 GMT

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 S1/0 (**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.



Packet Type: ● ICMP ○ TCP

IP Address or Hostname: 10.1.1.1

Port:

Interface (optional): -- None --

IP Address (optional):

Port: ● Random port ○ Starting port:

Repeat(optional):

Timeout(optional):

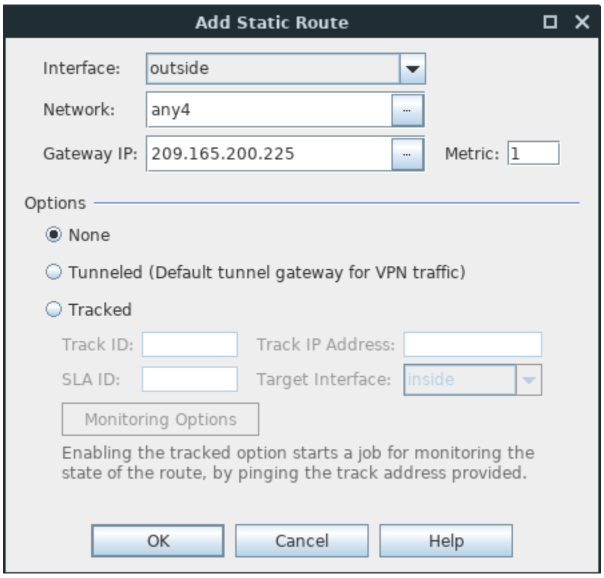
Ping Output:

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

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

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 e0/0).



Interface: outside

Network: any4

Gateway IP: 209.165.200.225

Metric: 1

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

Track ID:

Track IP Address:

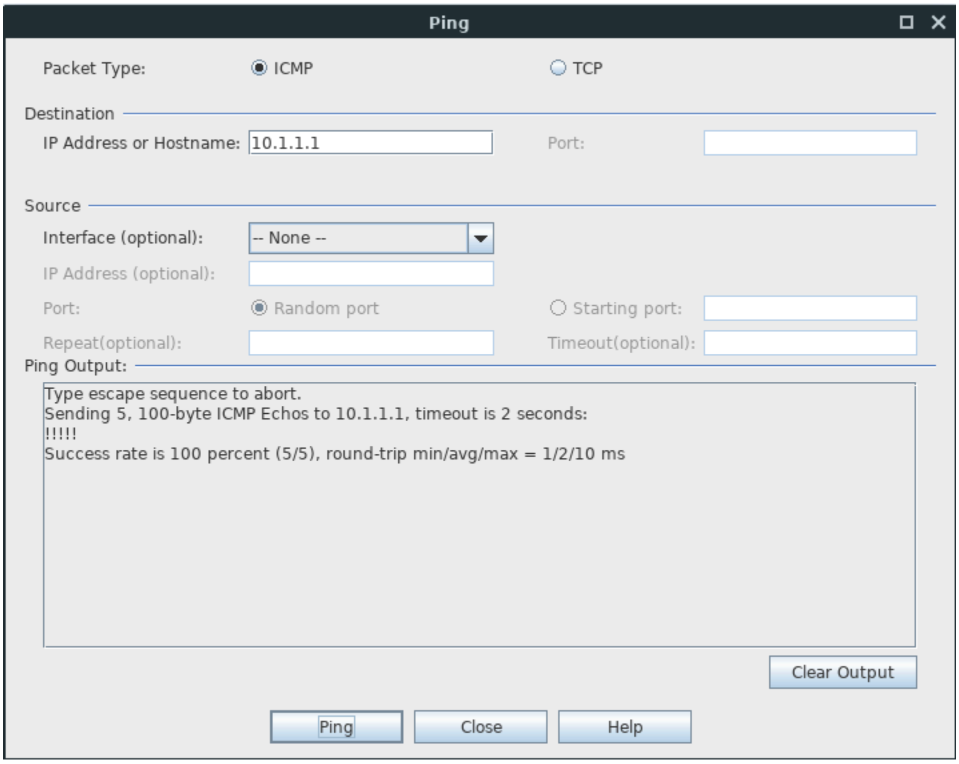
SLA ID:

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.

e. On the ASDM **Tools** menu, select **Ping** and enter the IP address of router R1 S1/0 (**10.1.1.1**). The ping should succeed this time. Click **Close** to continue.



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:

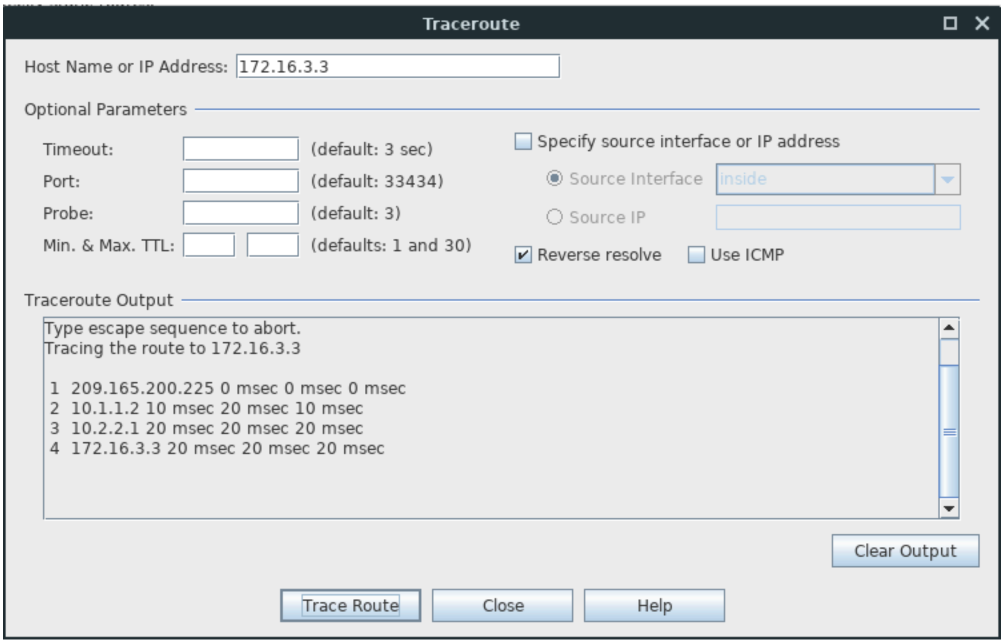
Repeat(optional):

Timeout(optional):

Ping Output:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 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

Optional Parameters

Timeout: (default: 3 sec)

Port: (default: 33434)

Probe: (default: 3)

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

□ Specify source interface or IP address

● Source Interface: inside

○ Source IP

☑ Reverse resolve □ Use ICMP

Traceroute Output

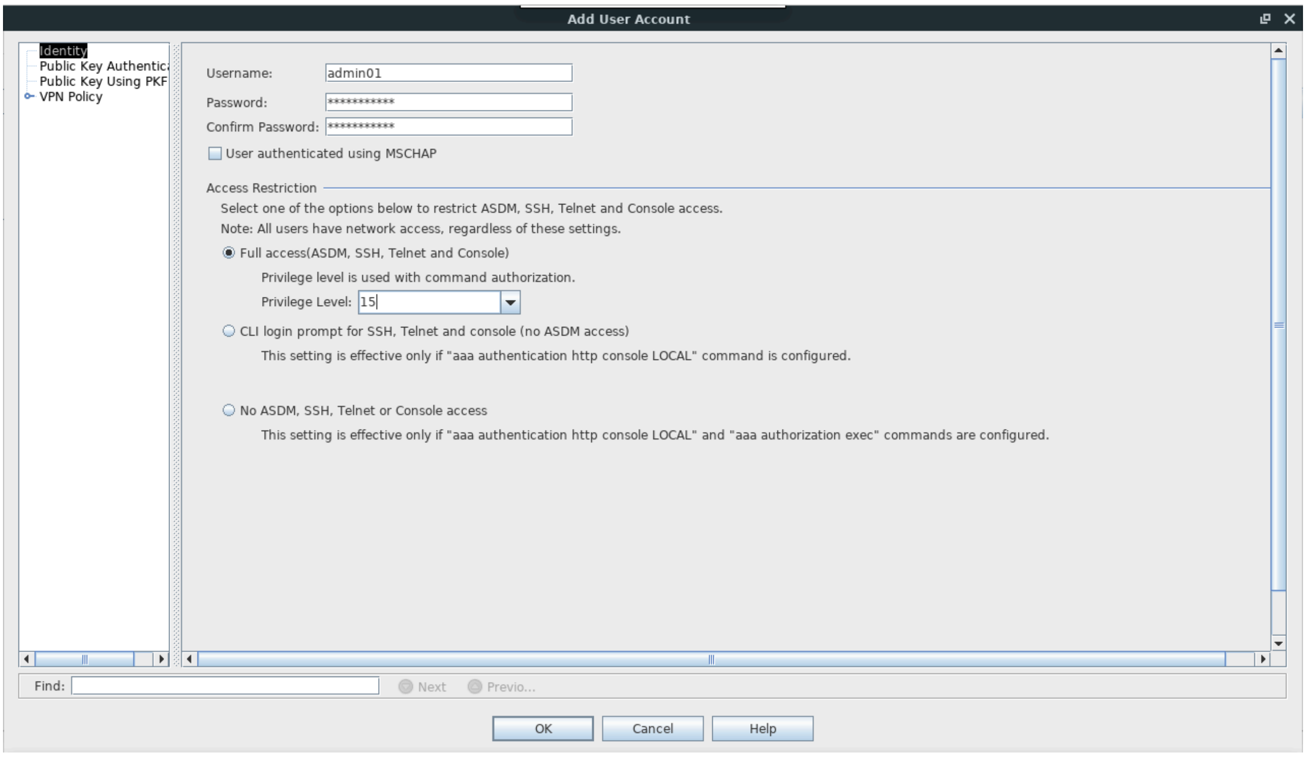
```
Type escape sequence to abort.
Tracing the route to 172.16.3.3

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

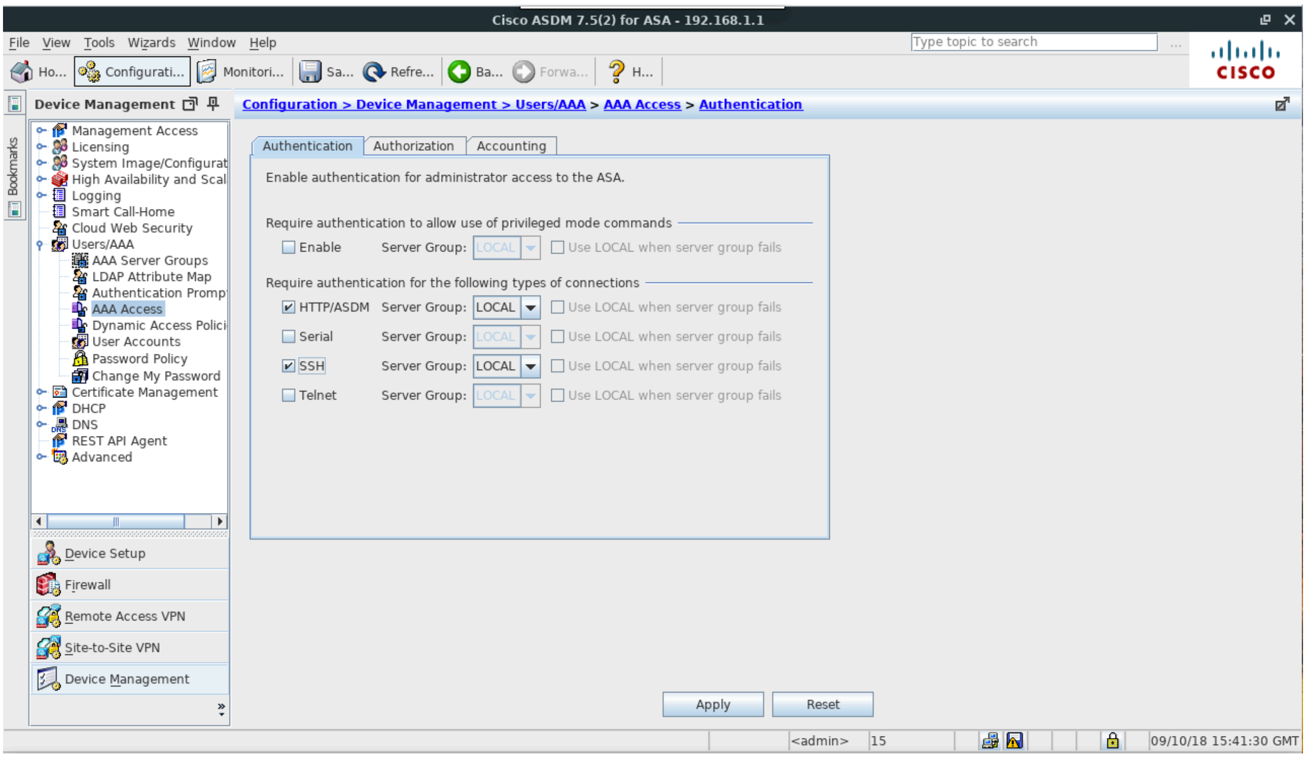
○ CLI login prompt for SSH, Telnet and console (no ASDM access)

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.



Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

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

Require authentication for the following types of connections

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

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

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

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

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

Step 4: Test SSH access to the ASA.

a. Open another terminal window on PC-B and type the command

ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 admin01@192.168.1.1

Note: this command instead of the **ssh admin01@192.168.1.1** is needed because of some legacy issues. To have more information have a look on the **OpenSSH** web page here

And use the password **admin01pass** when prompted.

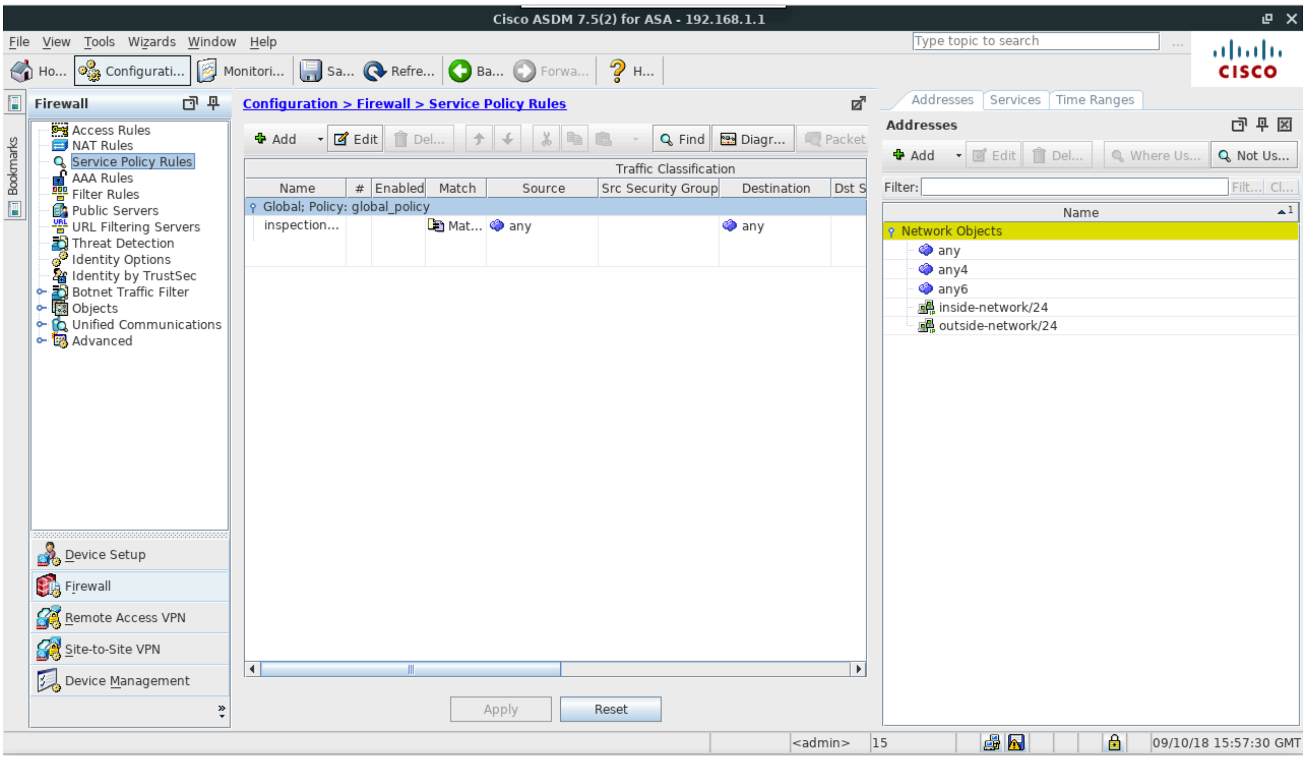
b. After logging in to the ASA using SSH, enter the **enable** command and provide the password **cisco12345**. Issue the **show run** command to display the current configuration that you have created using ASDM.

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**.

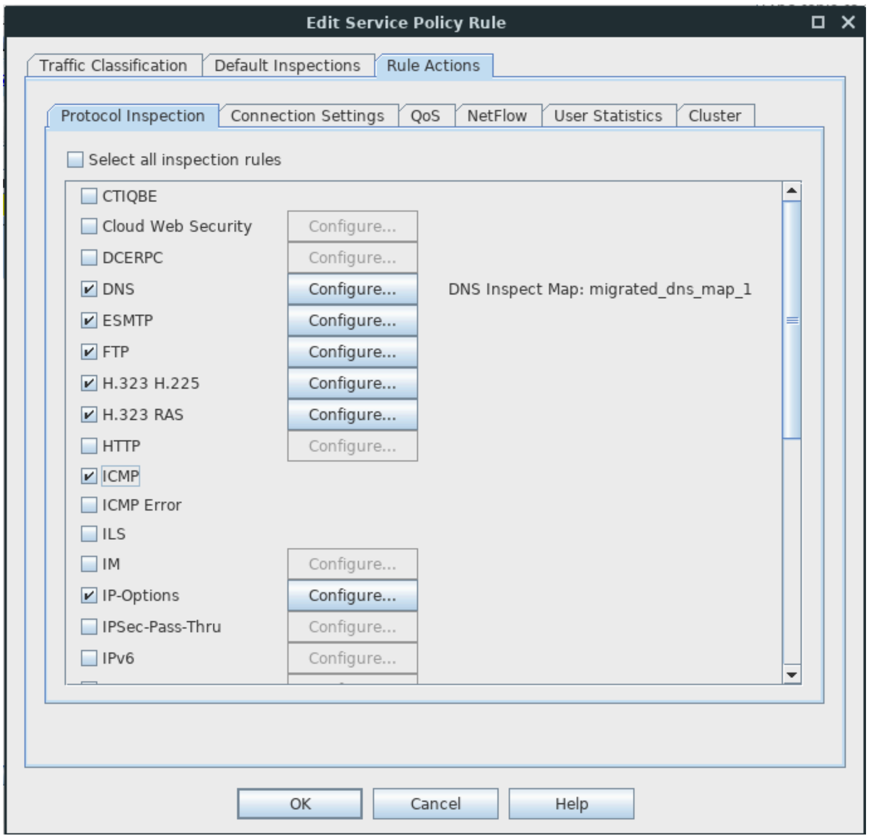
Step 5: Modify the MPF application inspection policy.

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 7.5(2) for ASA - 192.168.1.1
File View Tools Wizards Window Help
Ho... Configurati... Monitori... Sa... Refre... Ba... Forwa... H...
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Firewall > Service Policy Rules
Add Edit Del... Find Diagr... Packet
Traffic Classification
Name # Enabled Match Source Src Security Group Destination Dst S
Global; Policy: global_policy
inspection... Mat... any any
Apply Reset
Addresses Services Time Ranges
Addresses
Add Edit Del... Where Us... Not Us...
Filter:
Name
Network Objects
any
any4
any6
inside-network/24
outside-network/24
<admin> 15 09/10/18 15:57:30 GMT

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
□ Cloud Web Security
□ DCERPC
☑ DNS — DNS Inspect Map: migrated_dns_map_1
☑ ESMTP
☑ FTP
☑ H.323 H.225
☑ H.323 RAS
□ HTTP
☑ ICMP
□ ICMP Error
□ ILS
□ IM
☑ IP-Options
□ IPSec-Pass-Thru
□ IPv6

c. From PC-B, **ping** the external interface of R1 S1/0 (**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.

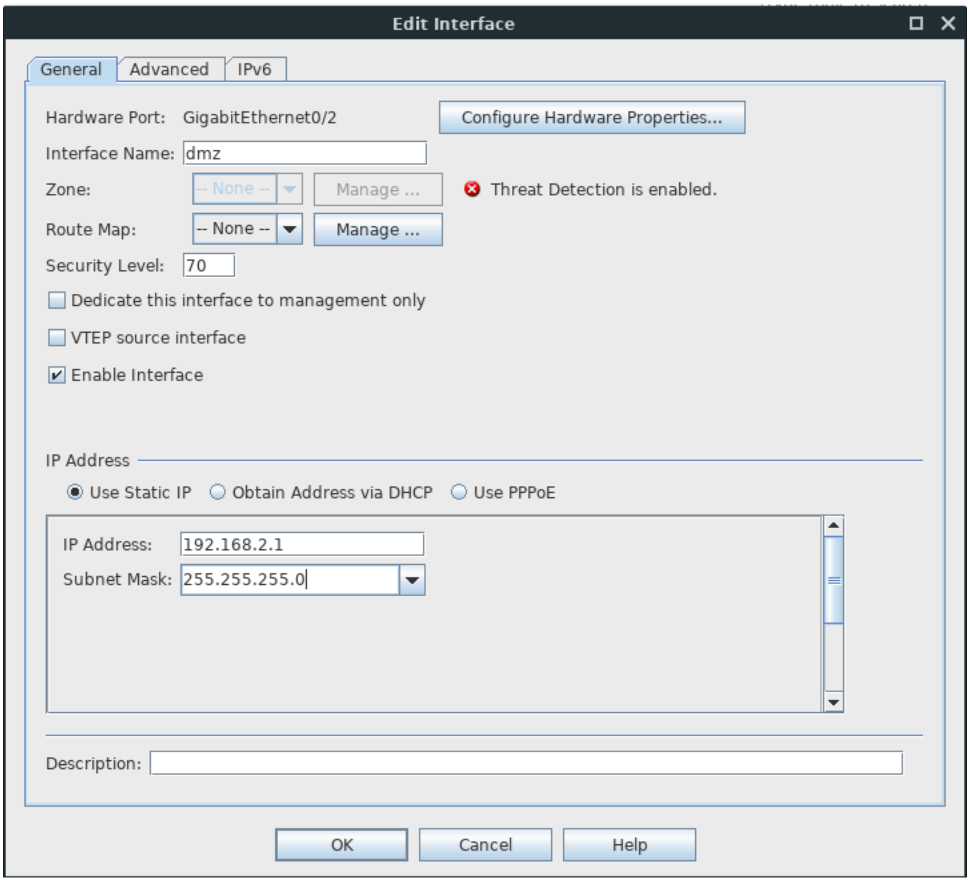
Step 1: Configure the ASA DMZ interface on Gi0/2.

In this step, you will create assign the DMZ interface name to the physical interface Gi0/2, set the security level to **70**, and limit communication from this interface to the inside (Gi0/1) interface.

a. On the **Configuration** screen > **Device Setup** menu, click **Interfaces**. The Interface tab is displayed by default and the currently defined inside (Gi0/1) and outside (Gi0/0) interfaces are listed. Notice that all the other port are listed as well. Select **GigabitEthernet0/2** and click **Edit** to edit the interface.

b. 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**. Click **OK** to confirm.



Edit Interface

General | Advanced | IPv6

Hardware Port: GigabitEthernet0/2

Interface Name: dmz

Zone: -- None --

Route Map: -- None --

Security Level: 70

☐ Dedicate this interface to management only

☐ VTEP source interface

☑ Enable Interface

IP Address

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

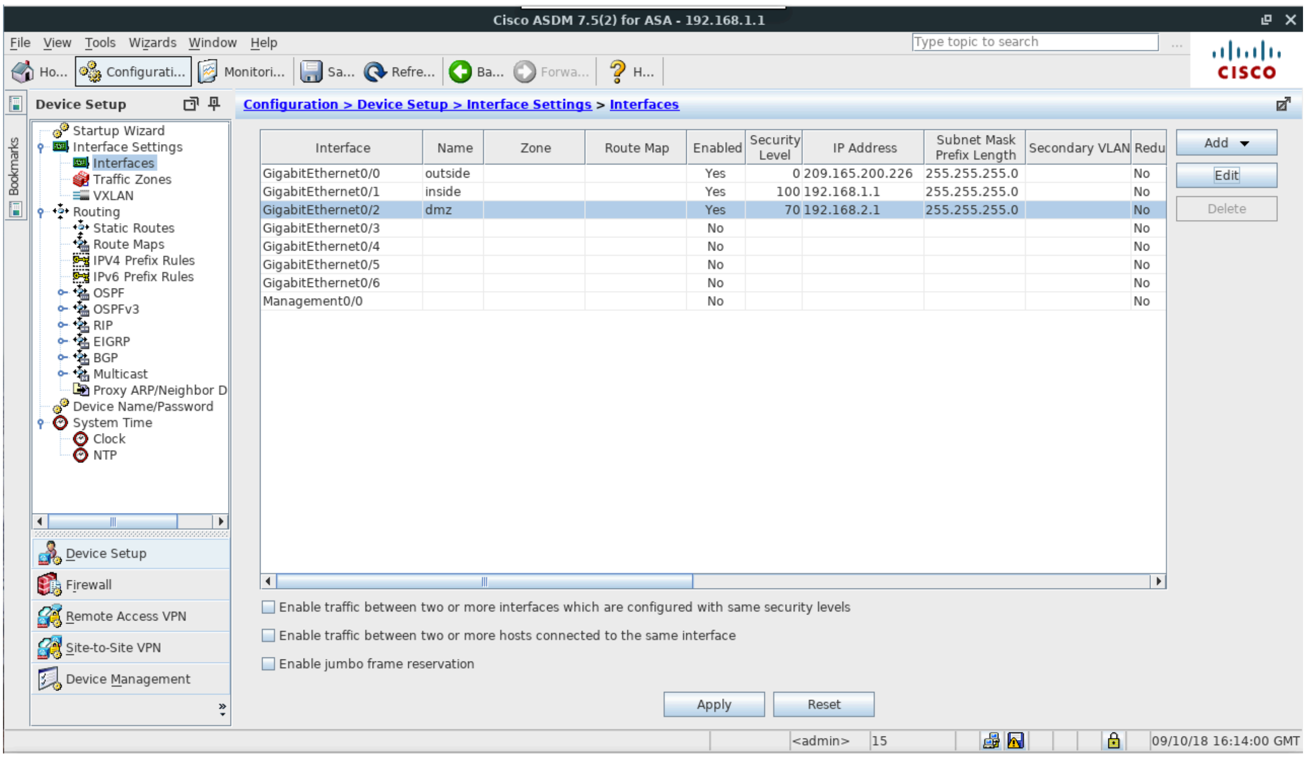
IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Description:

Configure Hardware Properties...
Manage ...
Manage ...
Threat Detection is enabled.
OK
Cancel
Help

d. 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 > Interface Settings > Interfaces

Interface	Name	Zone	Route Map	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Redu
GigabitEthernet0/0	outside			Yes	0	209.165.200.226	255.255.255.0		No
GigabitEthernet0/1	inside			Yes	100	192.168.1.1	255.255.255.0		No
GigabitEthernet0/2	dmz			Yes	70	192.168.2.1	255.255.255.0		No
GigabitEthernet0/3				No					No
GigabitEthernet0/4				No					No
GigabitEthernet0/5				No					No
GigabitEthernet0/6				No					No
Management0/0				No					No

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

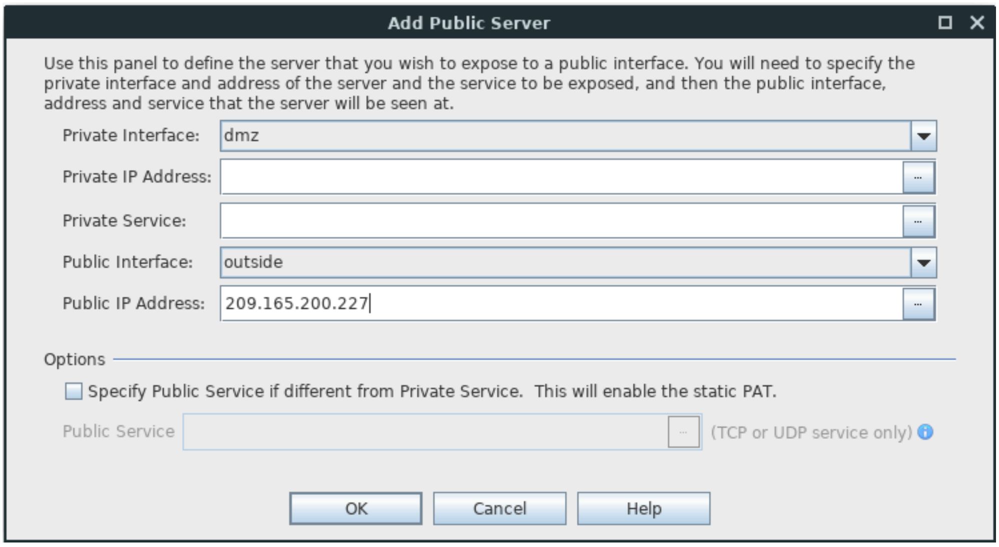
□ Enable traffic between two or more hosts connected to the same interface

□ Enable jumbo frame reservation

Step 2: Configure the DMZ server and static NAT.

To accommodate the addition of a DMZ and a web server, you will use another address from the ISP range assigned, 209.165.200.224/29 (.224-.231). R1 e0/0 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**.



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.

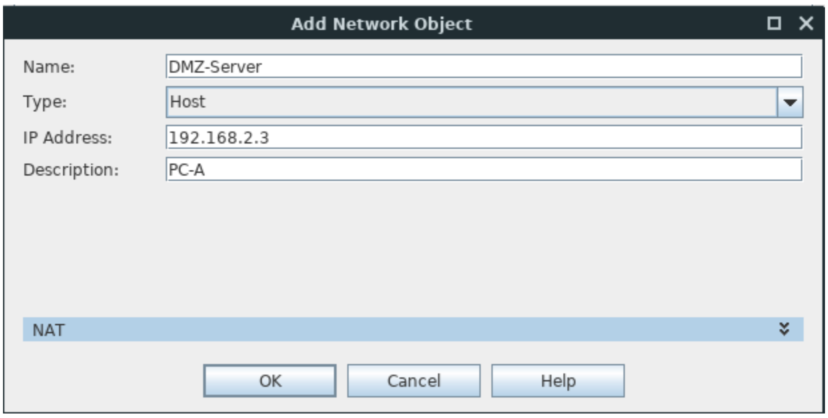
Private Interface:	dmz
Private IP Address:	
Private Service:	
Public Interface:	outside
Public IP Address:	209.165.200.227

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

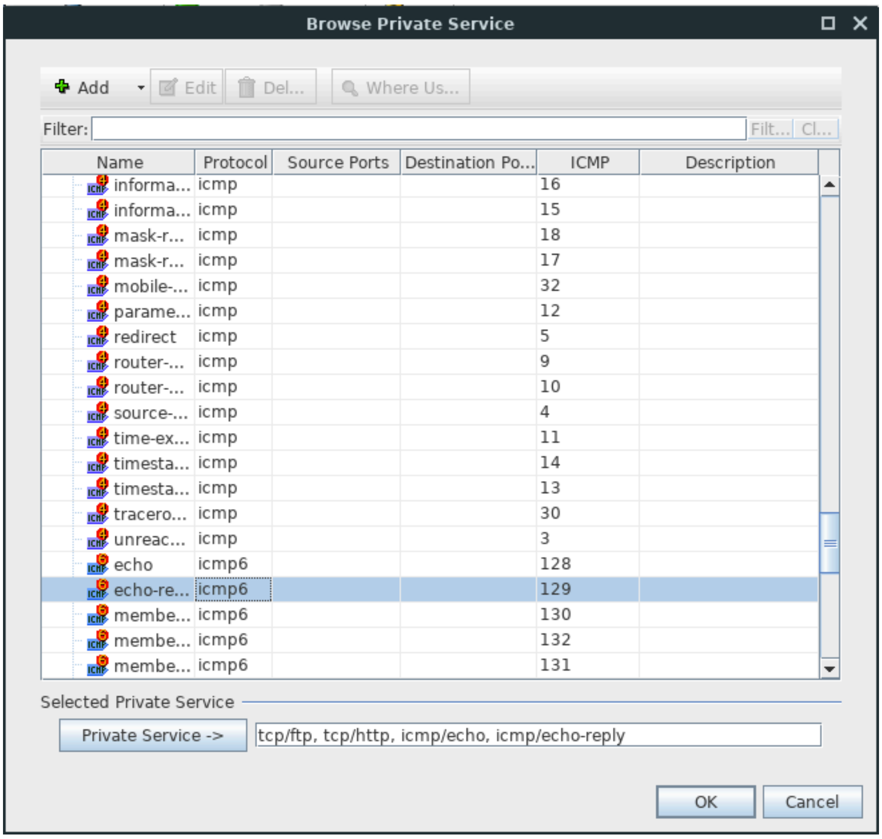
IP Address: 192.168.2.3

Description: PC-A

c. From the Browse Private IP Address window, verify that the DMZ-Server appears in the Selected Private IP Address by clicking on 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.



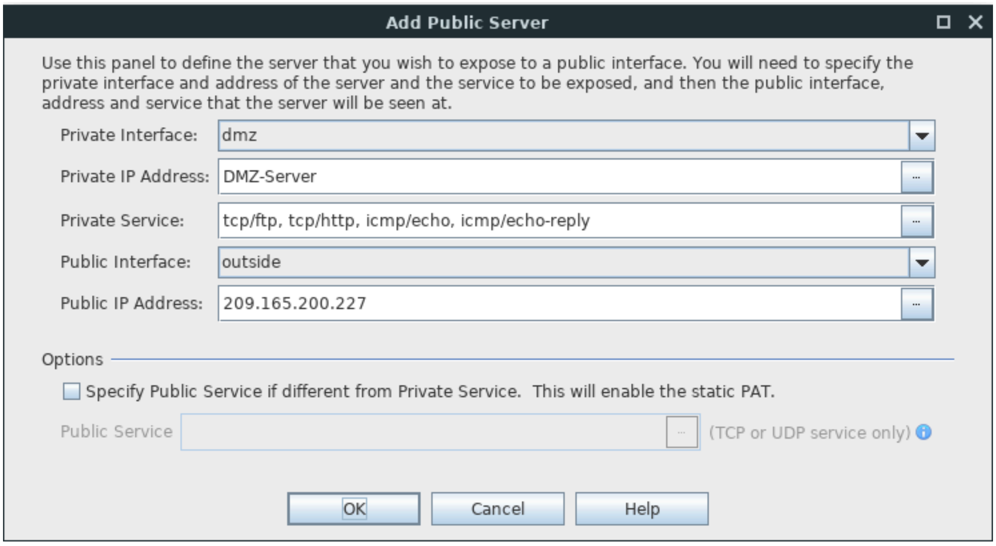
Browse Private Service

Name	Protocol	Source Ports	Destination Po...	ICMP	Description
informa...	icmp			16	
informa...	icmp			15	
mask-r...	icmp			18	
mask-r...	icmp			17	
mobile-...	icmp			32	
parame...	icmp			12	
redirect	icmp			5	
router-...	icmp			9	
router-...	icmp			10	
source-...	icmp			4	
time-ex...	icmp			11	
timesta...	icmp			14	
timesta...	icmp			13	
tracero...	icmp			30	
unreac...	icmp			3	
echo	icmp6			128	
echo-re...	icmp6			129	
membe...	icmp6			130	
membe...	icmp6			132	
membe...	icmp6			131	

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.



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/ftp, tcp/http, icmp/echo, icmp/echo-reply

Public Interface: outside

Public IP Address: 209.165.200.227

Options

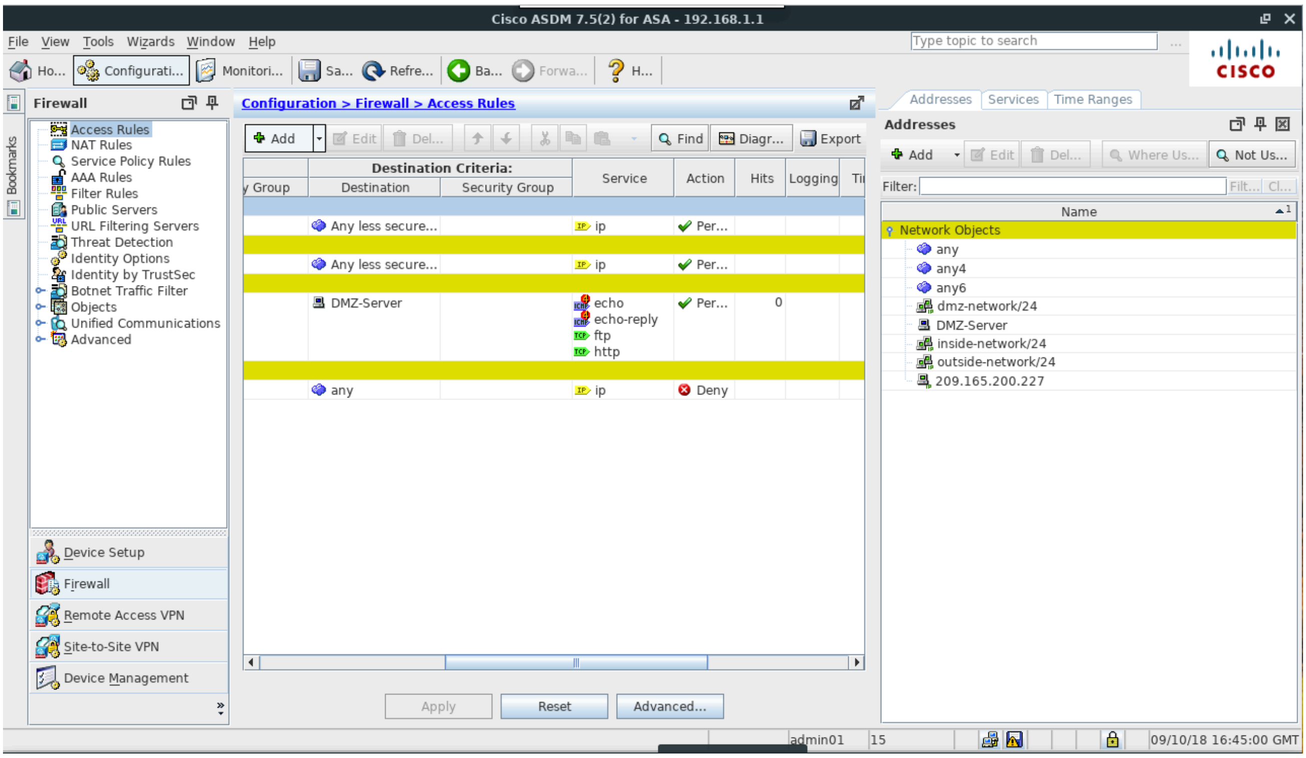
□ Specify Public Service if different from Private Service. This will enable the static PAT.

Public Service (TCP or UDP service only)

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.



Configuration > Firewall > Access Rules

y Group	Destination Criteria: Destination	 Security Group	Service	Action	Hits	Logging	Ti
	Any less secure...		ip	Per...			
	Any less secure...		ip	Per...			
	DMZ-Server		echo echo-reply ftp http	Per...	0		
	any		ip	Deny			

Addresses | Services | Time Ranges

Addresses

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

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

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

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

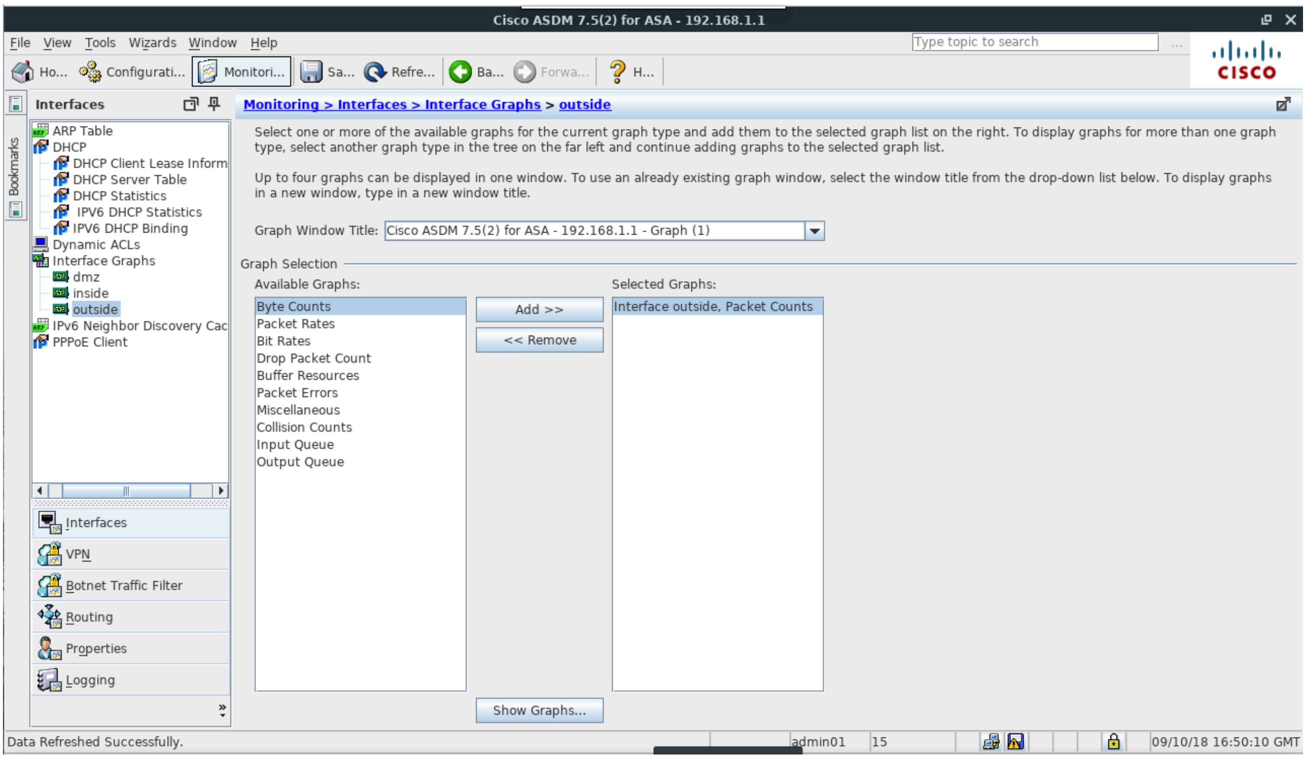
b. Because the ASA inside interface (Gi0/1) is set to security level 100 (the highest) and the DMZ interface (Gi0/2) is set to 70, you can also access the DMZ server from a host on the inside network. The ASA acts like a router between the two networks. Ping the DMZ server (PC-A) internal address (**192.168.2.3**) 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 Gi0/2 has a lower security level. 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.



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 7.5(2) for ASA - 192.168.1.1 - Graph (1)

Selected Graphs: Interface outside, Packet Counts

Data Refreshed Successfully. admin01 15 09/10/18 16:50:10 GMT

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.

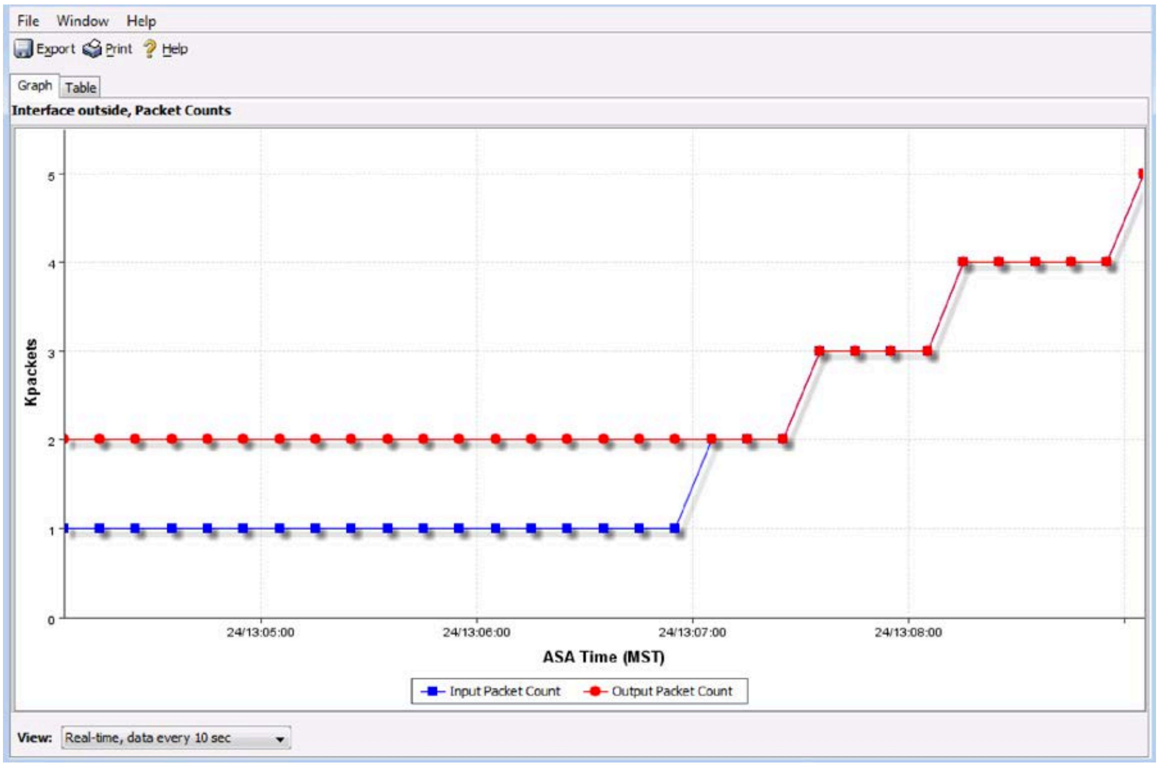
```
R2# ping 209.165.200.227 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 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 s1/0 at **10.1.1.1** using the **–c** option (count) to specify **100** packets.

ping -c 100 10.1.1.1

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