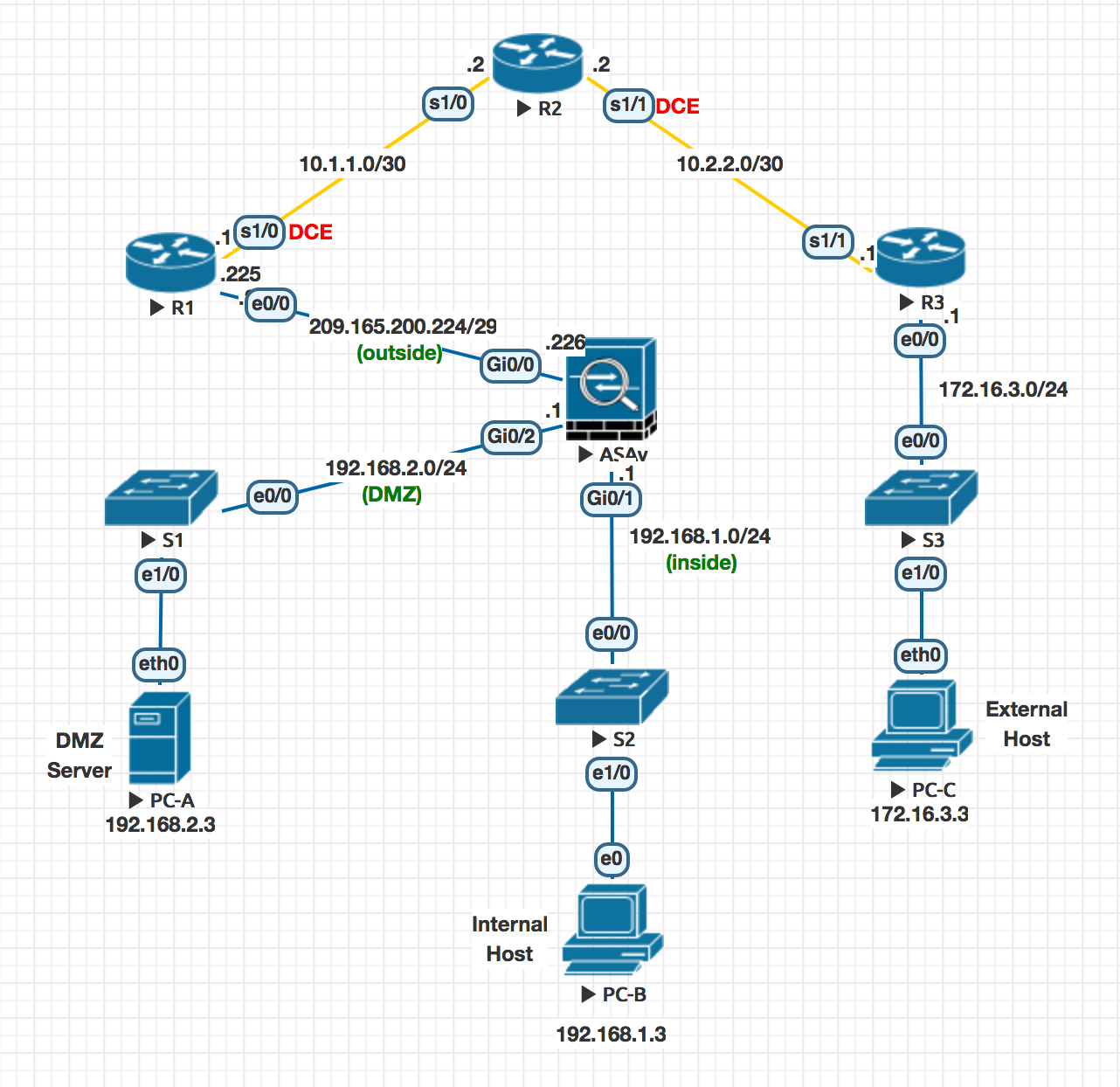
Lab2: Configure ASA Basic Settings and Firewall using ASDM

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.

1. 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.

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.

* + 1. Configure basic settings for routers and switches.
       1. Configure hostnames, as shown in the topology, for each router.
       2. Configure router interface IP addresses, as shown in the IP Addressing table.
       3. 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**

* + - 1. 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.
    1. Configure static routing on the routers.
       1. 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**

* + - 1. 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**

* + 1. 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.

* + - 1. Configure a minimum password length. Use the **security passwords** command to set a minimum password length of 10 characters.
      2. Configure the enable secret password on both routers with a password of **cisco12345**. Use the type 9 (SCRYPT) hashing algorithm.
      3. Create a local **admin01** account using **admin01pass** for the password. Use the type 9 (SCRYPT) hashing algorithm and set privilege level to 15
      4. 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.
      5. 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.

* + 1. 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.

* + 1. 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.

* + 1. Save the basic running configuration for each router and switch.

1. 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.

* + 1. Access the ASA console.
       1. Double click on the ASA appliance to open a terminal console connected to it
       2. If prompted to enter Interactive Firewall configuration (Setup mode), answer **no**.
       3. 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)

* + 1. Clear previous ASA configuration settings.
       1. 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.

* + - 1. 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>

* + 1. 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.

* + - 1. When prompted to pre-configure the firewall through interactive prompts (Setup mode), respond with **no**.

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

* + - 1. Enter privileged EXEC mode with the **enable** command. The password should be blank (no password) at this point.
      2. 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**.
      3. 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**

* + - 1. 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

* + - 1. 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**

* + - 1. 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.
    1. Configure ASDM and verify access to the ASA.
       1. 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**

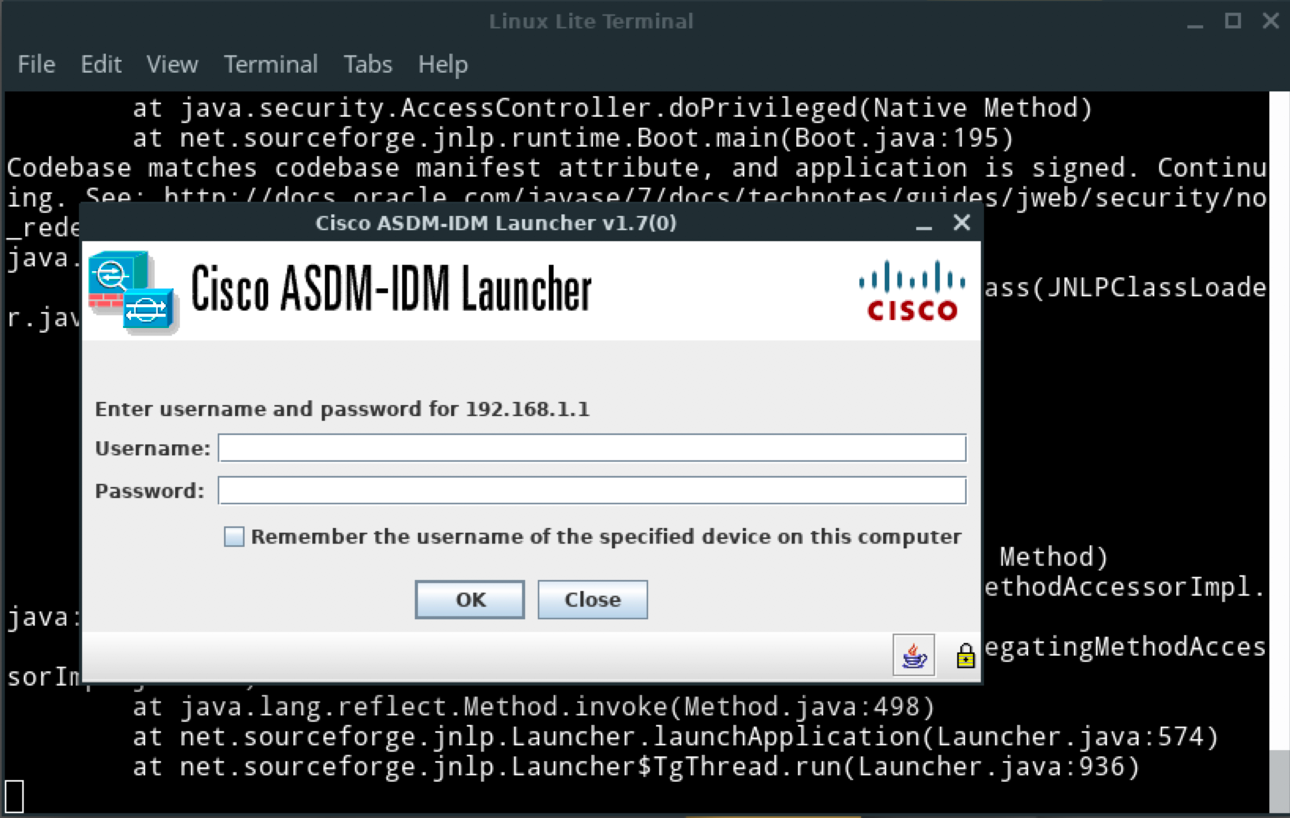
ciscoasa(config)# **http 192.168.1.0 255.255.255.0 inside**

* + - 1. 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

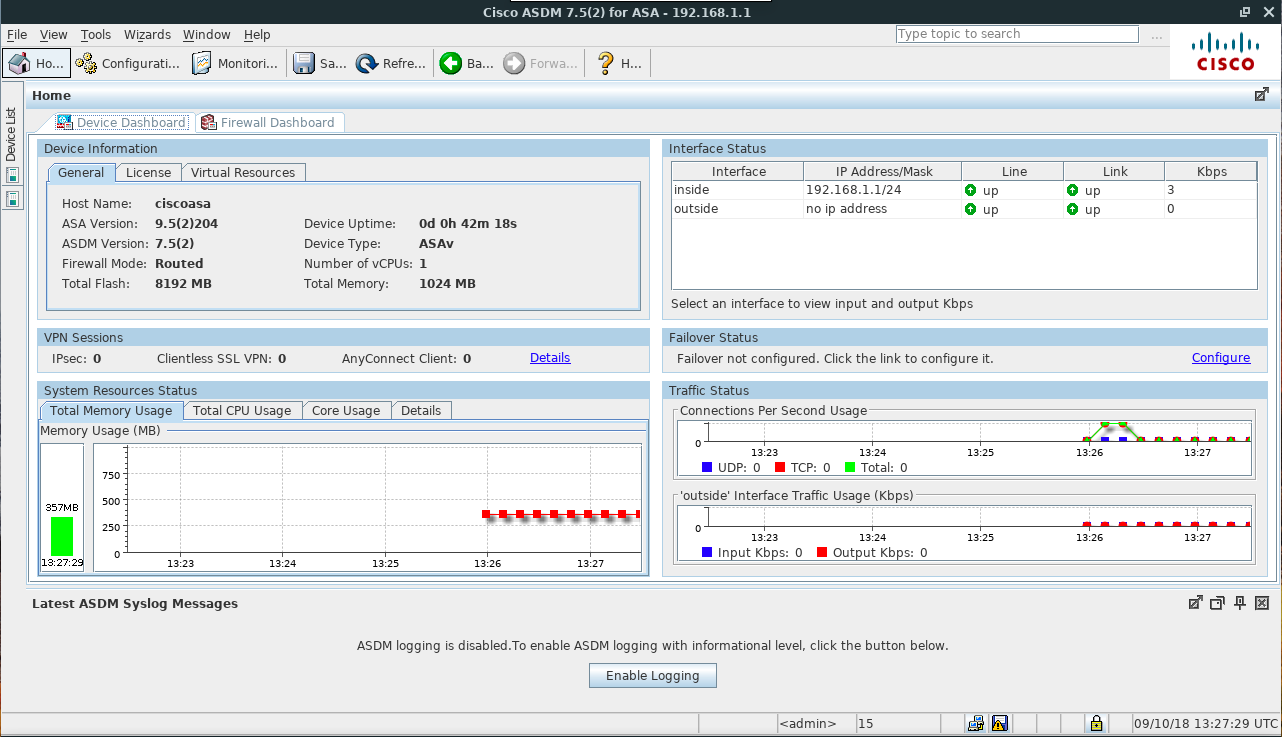
You will be prompted with a security certificate warning. Select **Always trust..”** and click **Yes** for the other security warnings. You should see the Cisco ASDM-IDM Launcher

* + 1. Access ASDM and explore the GUI.
       1. 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.



* + - 1. Click **OK** to continue. ASDM will load the current configuration into the GUI.
      2. 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

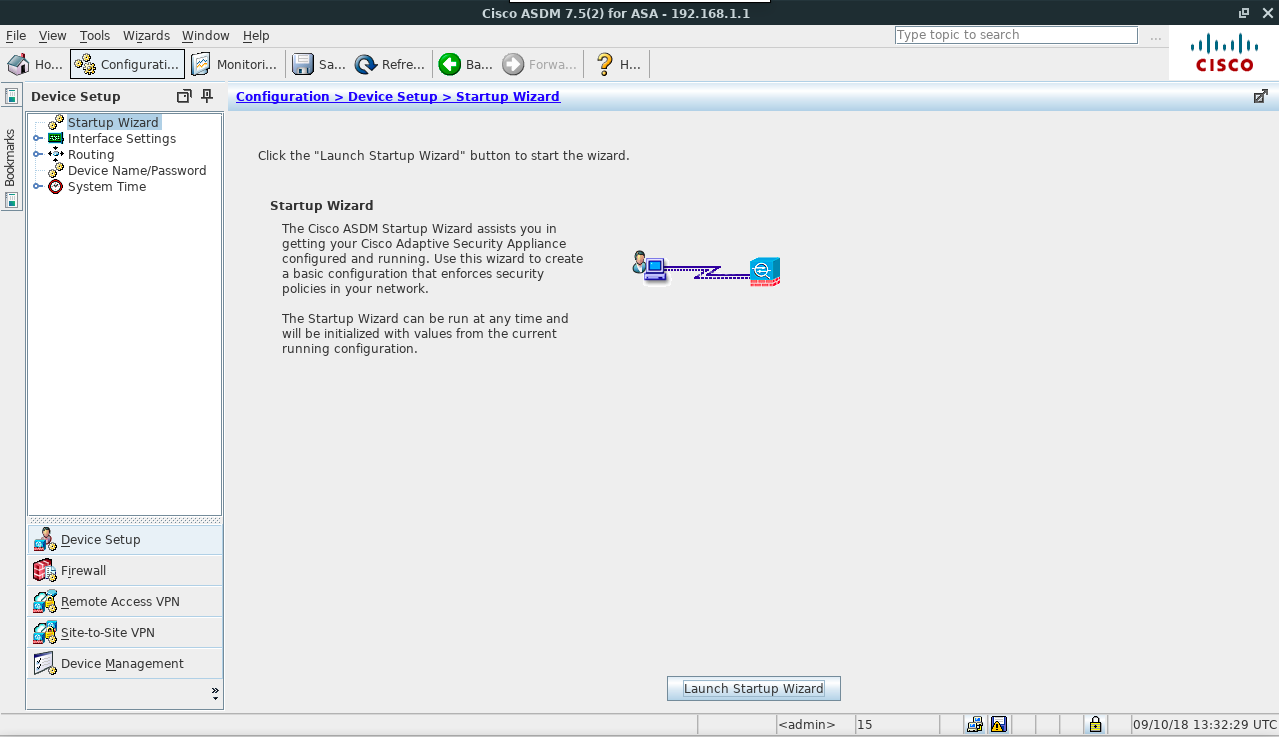
**Note**: If the Cisco Smart Call Home window appears, click **Do not enable Smart Call Home** and click **OK**.



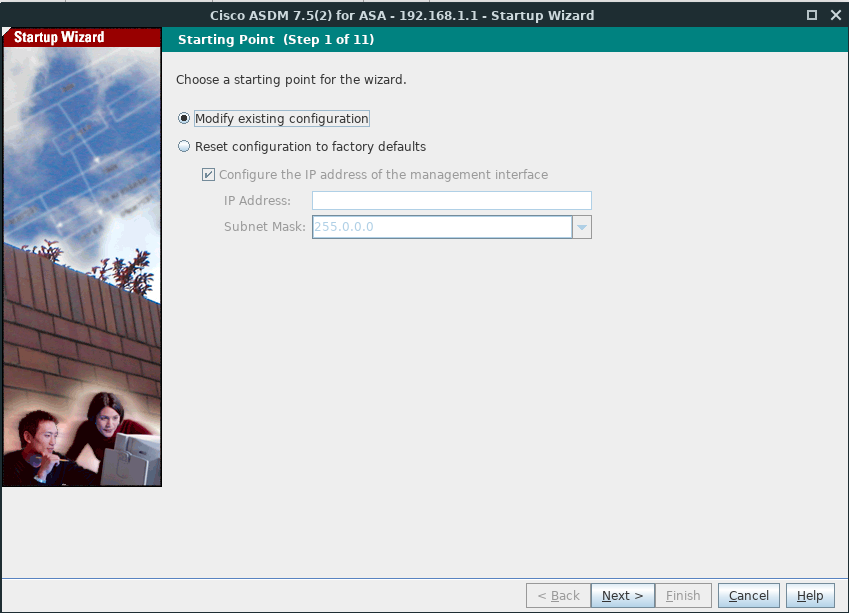
* + - 1. Click the **Configuration** and **Monitoring** buttons to become familiar with their layout and to see what options are available.

1. Configure Basic ASA Settings and Firewall Using the ASDM Startup Wizard
   * 1. Access the Configuration menu and launch the Startup wizard.
        1. On the menu bar, click **Configuration**. There are five main configuration areas:

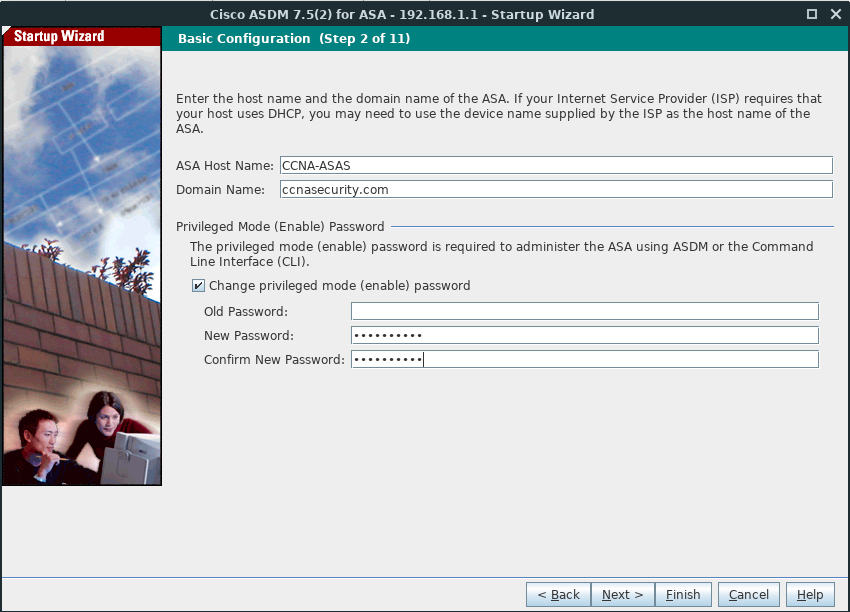
* Device Setup
* Firewall
* Remote Access VPN
* Site-to-Site VPN
* Device Management
  + - 1. The Device Setup Startup wizard is the first option available and displays by default. Read through the on-screen text describing the Startup wizard, and then click **Launch Startup Wizard**.



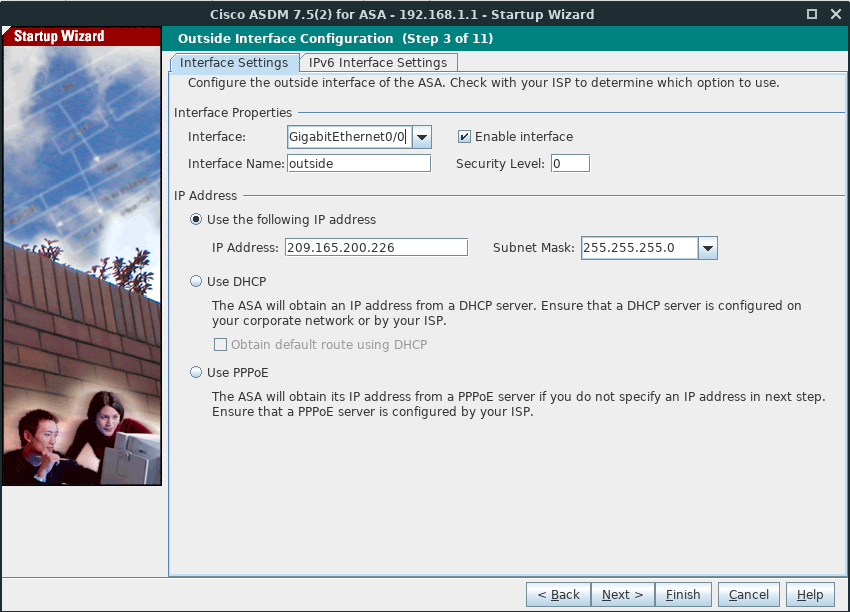
* + 1. Configure hostname, domain name, and the enable password.
       1. On the first Startup Wizard screen, modify the existing configuration or reset the ASA to the factory defaults. Ensure that the **Modify Existing Configuration** option is selected, and click **Next** to continue.

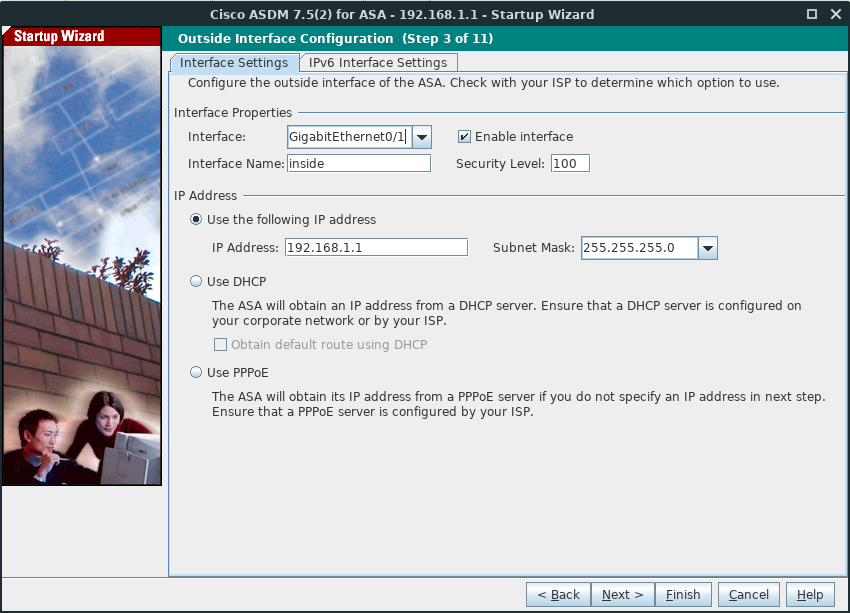


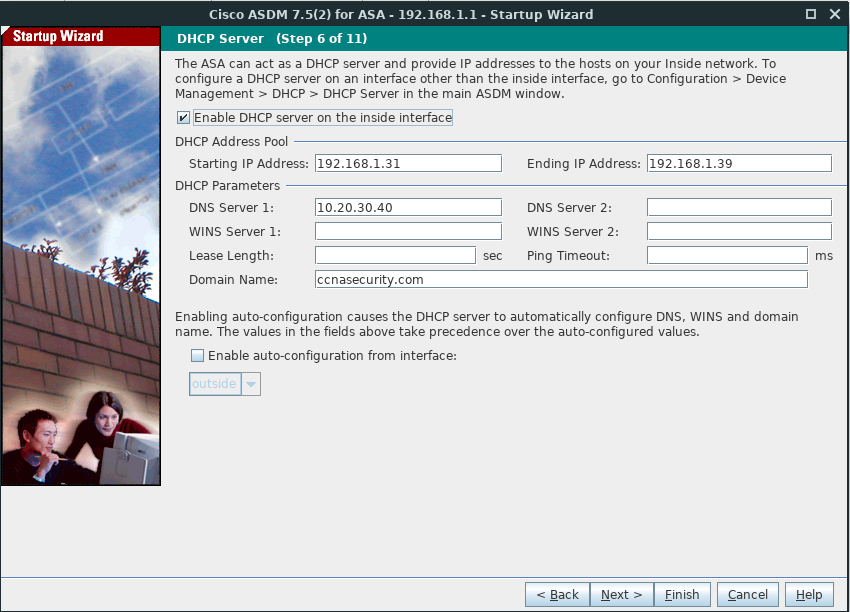
* + - 1. On the Startup Wizard Step 2 screen, configure the ASA hostname **CCNAS-ASA** and domain name **ccnasecurity.com**. Click the check box for changing the enable mode password, change it from blank (no password) to **cisco12345**, and enter it again to confirm. When the entries are completed, click **Next** to continue.



* + 1. Configure the inside and outside interfaces security level and IP addresses.
       1. 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.

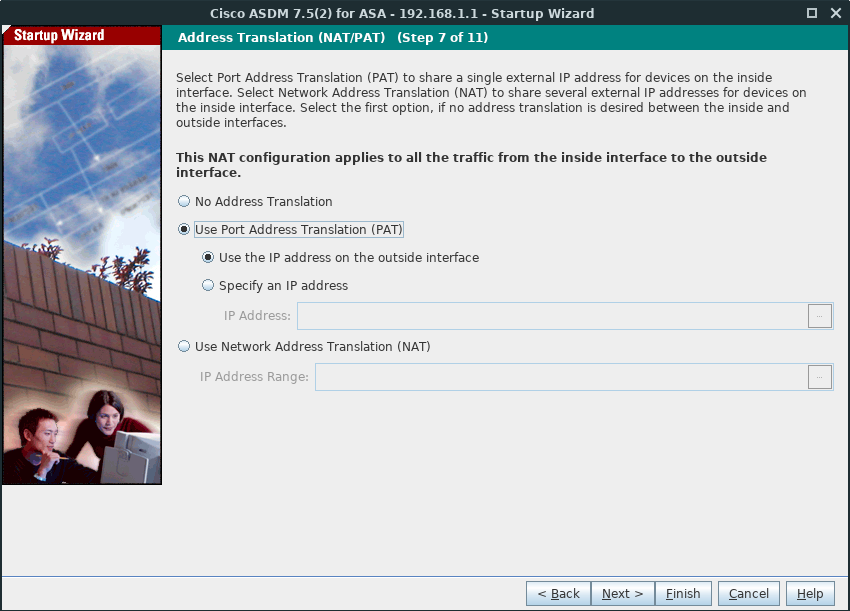


* + - 1. Select the interface **GigabitEthernet0/1** and check that the settings previously configured from CLI are correct.
    1. Configure DHCP, address translation, and administrative access.
       1. Review the address configuration on Wizards step 4 and click next. Ignore step 5. On the Startup 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.

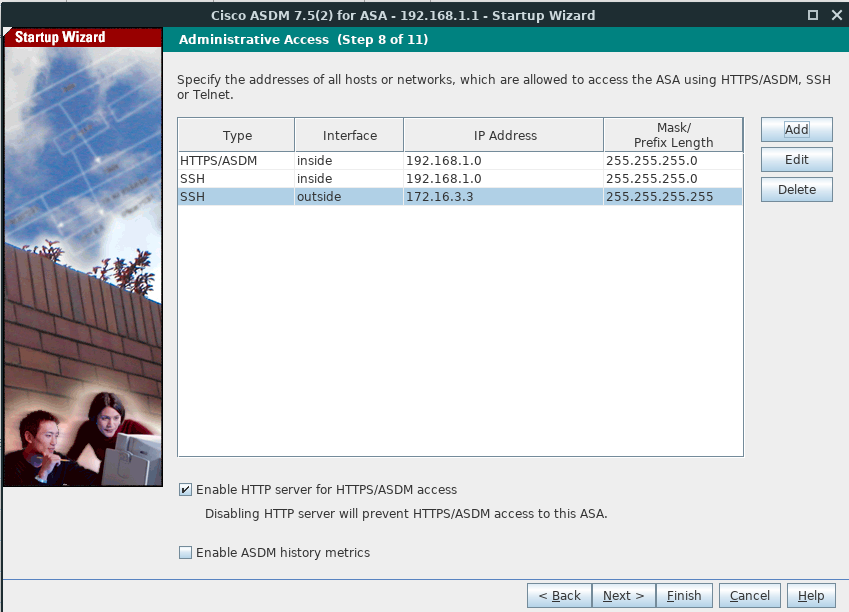


* + - 1. On the Startup Wizard Step 7 screen – Address Translation (NAT/PAT), click **Use Port Address Translation (PAT)**. The default is to use the IP address of the outside interface.

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

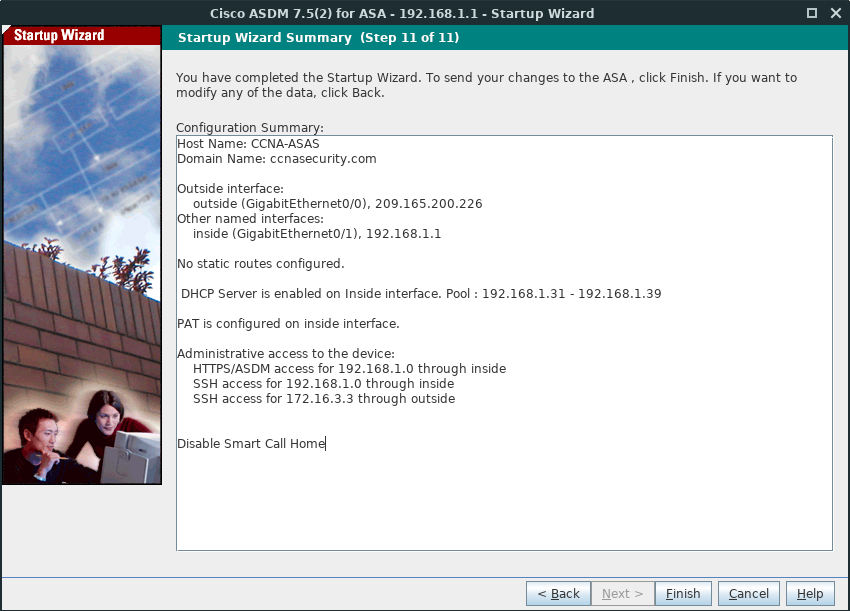


* + - 1. On the Startup Wizard Step 8 screen – Administrative Access, HTTPS/ASDM access is currently configured for hosts on the inside network 192.168.1.0/24. Add **SSH** access to the ASA for the inside network **192.168.1.0** with a subnet mask of **255.255.255.0**. Add **SSH** access to the ASA from 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.

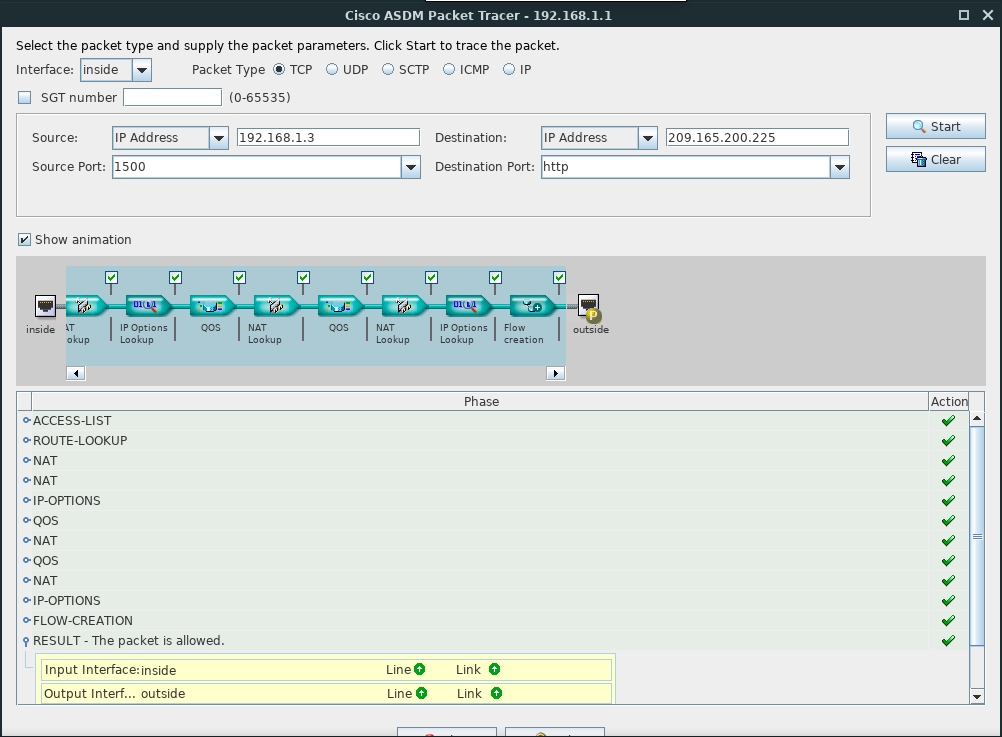


* + 1. Review the summary and deliver the commands to the ASA.
       1. Skip Step 9 (uncheck the box “Enable Auto Update for ASA) and Step 10. On the Startup Wizard Step 11 screen – Startup Wizard Summary, review the **Configuration Summary** and click **Finish**. ASDM will deliver the commands to the ASA device and then reload the modified configuration.

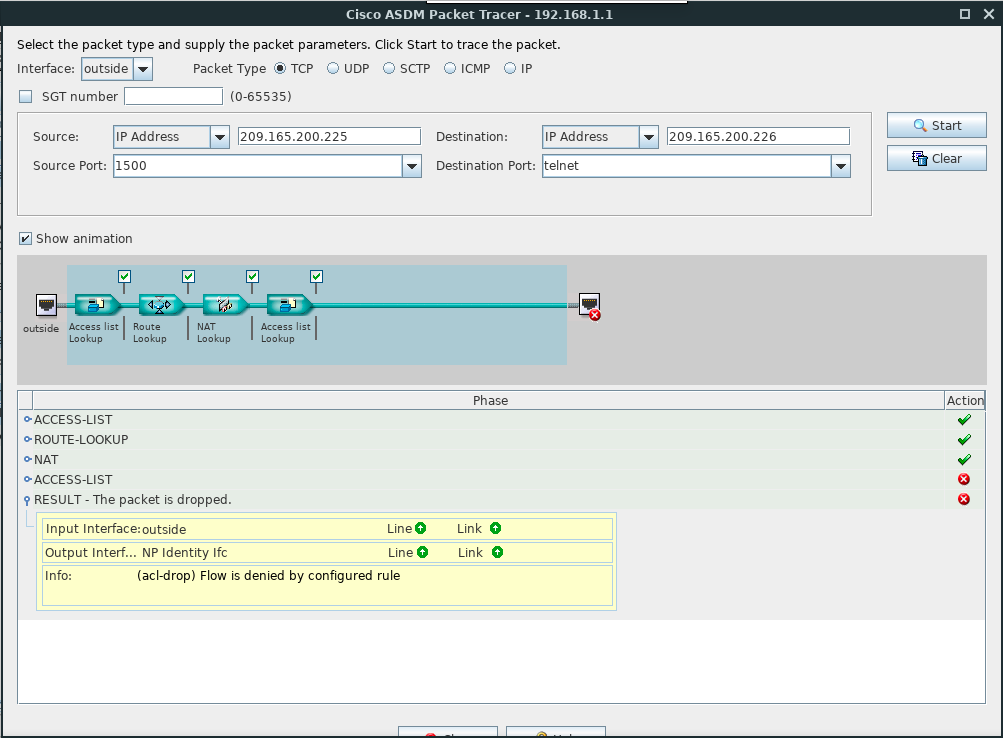
**Note**: If the GUI dialogue box stops responding during the reload process, close it, exit ASDM, and restart the browser and ASDM. If prompted to save the configuration to flash memory, respond with **Yes**. Even though ASDM may not appear to have reloaded the configuration, the commands were delivered. 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.



* + - 1. 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.
    1. Test access to an external website from PC-B.
       1. 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.
       2. 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.
    2. Test access to an external website using the ASDM Packet Tracer utility.
       1. Click **Tools** > **Packet Tracer**.
       2. 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.



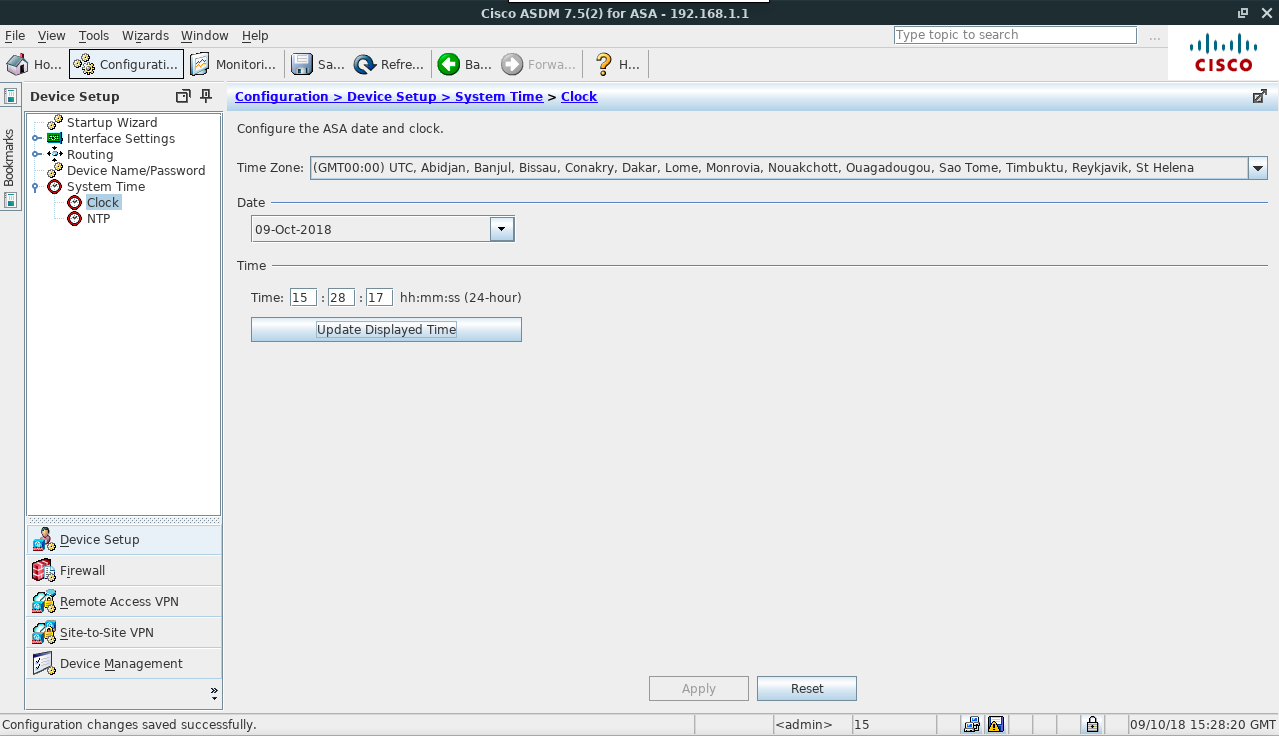
* + - 1. Click **Clea**r to reset the entries. Try another trace and select **outside** from the **Interface** drop-down list and leave **TCP** as the packet type. From the **Sources** drop-down list, select **IP Address**, and enter **209.165.200.225** (R1 e0/0) and a Source Port of 1500. From the **Destination** 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.



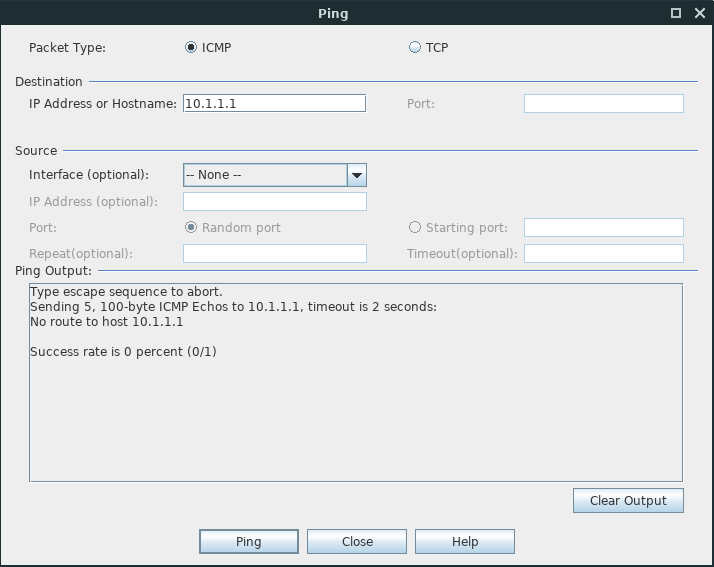
1. Configure ASA Settings from the ASDM Configuration Menu

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.

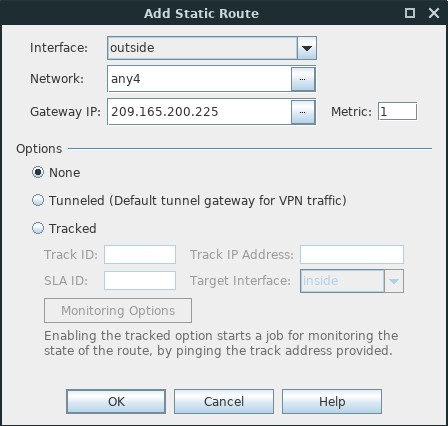
* + 1. Set the ASA date and time.
       1. On the **Configuration** screen > **Device Setup** menu, click **System Time** > **Clock**.
       2. Select your **Time Zone** from the drop-down list and enter the current date and time in the fields provided. (The clock is a 24-hour clock.) Click **Apply** to send the commands to the ASA.



* + 1. Configure a static default route for the ASA.
       1. 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.



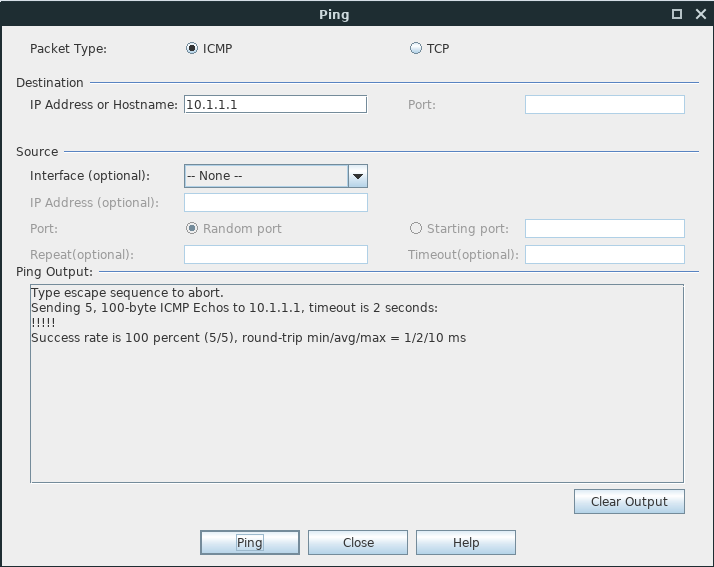
* + - 1. From the **Configuration** screen> **Device Setup** menu, click **Routing** > **Static Routes**. Click **IPv4 Only** and click **Add** to add a new static route.
      2. On the Add Static Route dialog box, select the **outside** interface from the drop-down list. Click the ellipsis button to 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).



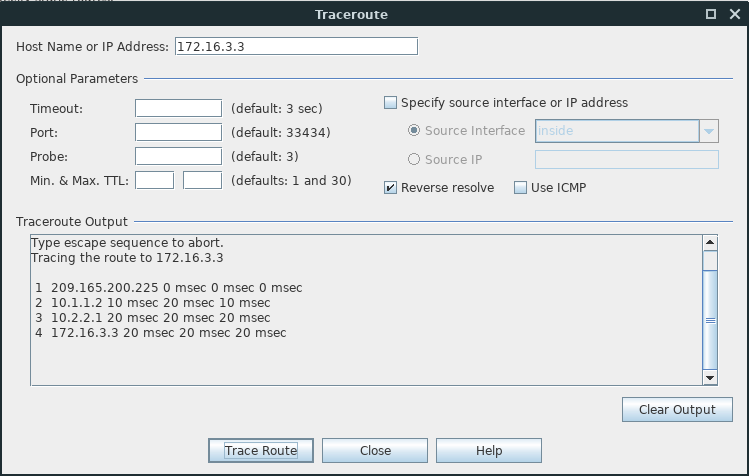
* + - 1. Click **OK** > **Apply** to send the commands to the ASA.

z

* + - 1. 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.



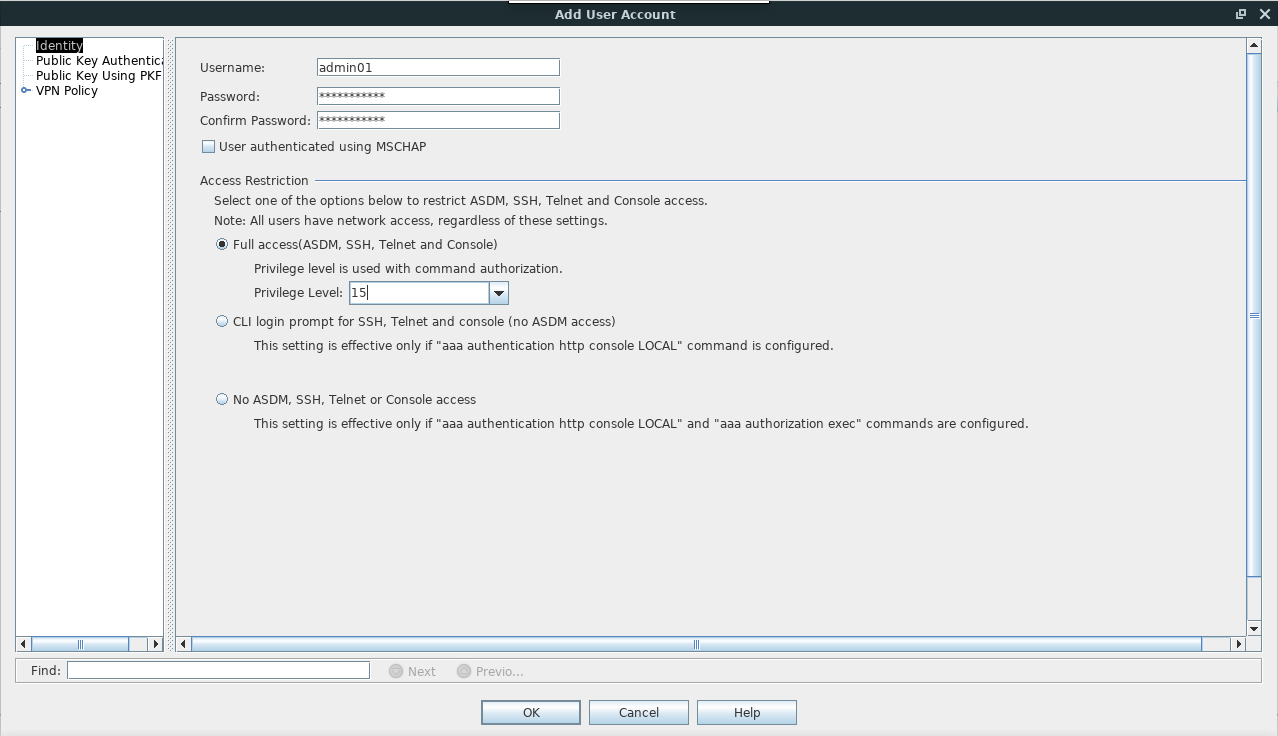
* + - 1. On the ASDM **Tools** menu, select **Traceroute** and enter the IP address of external host PC-C (**172.16.3.3**). Click **Trace Route**. The traceroute should succeed and show the hops from the ASA through R1, R2, and R3 to host PC-C. Click **Close** to continue.



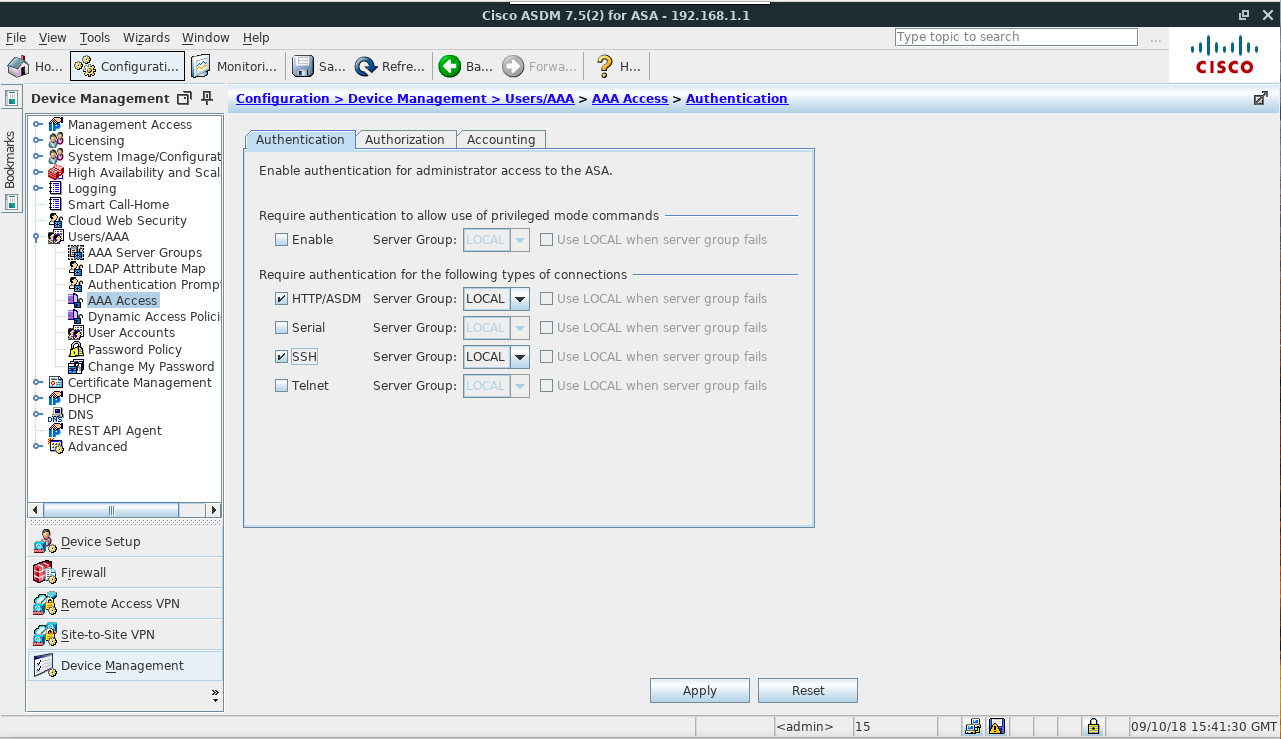
* + 1. Configure AAA user authentication using the ASA local database.

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.

* + - 1. 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 toconfirm 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.



* + - 1. On the **Configuration** screen > **Device Management** area, click **Users/AAA**. Click **AAA Access**. On the **Authentication** tab, click the check box to require authentication for **HTTP/ASDM** and **SSH** connections and specify the **LOCAL** server group for each connection type. Click **Apply** to send the commands to the ASA.



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

* + 1. Test SSH access to the ASA.
       1. 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](http://www.openssh.com/legacy.html)

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

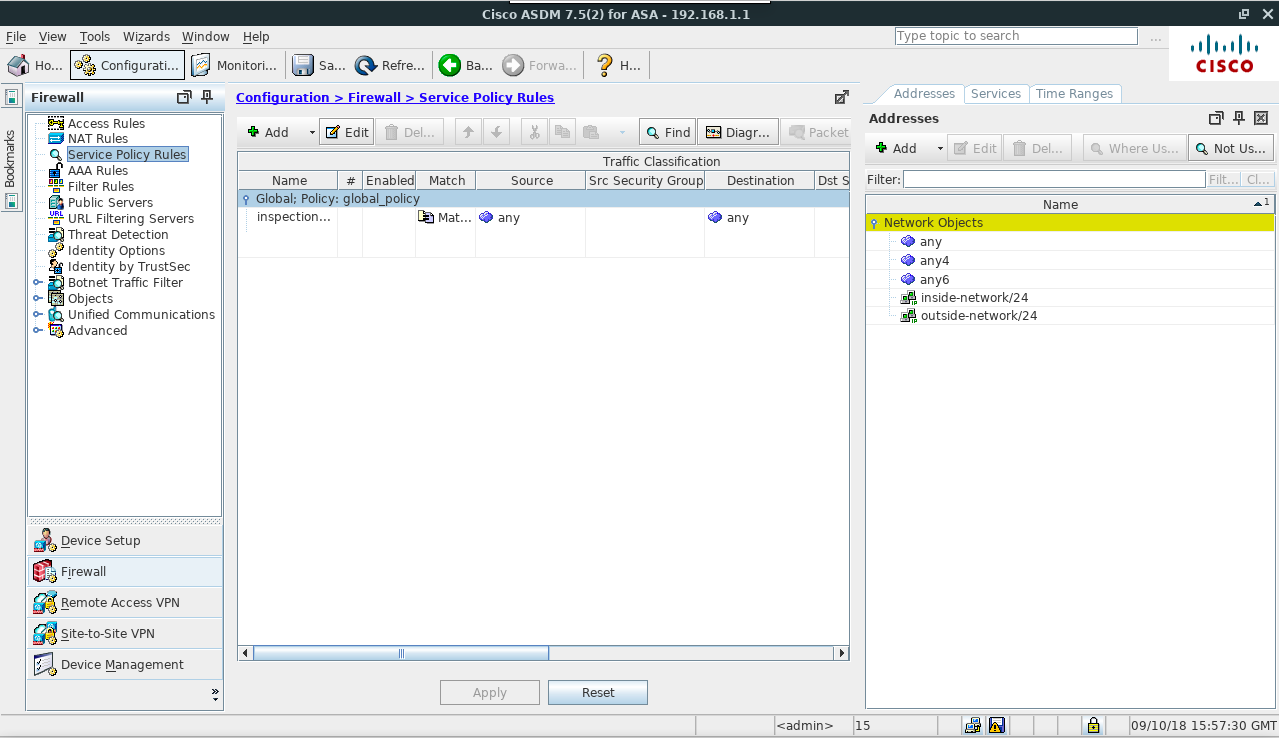
* + - 1. After logging in to the ASA using SSH, enter the **enable** command and provide the password **cisco12345**. Issue the **show run** command to display the current configuration that you have created using ASDM.

**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**.

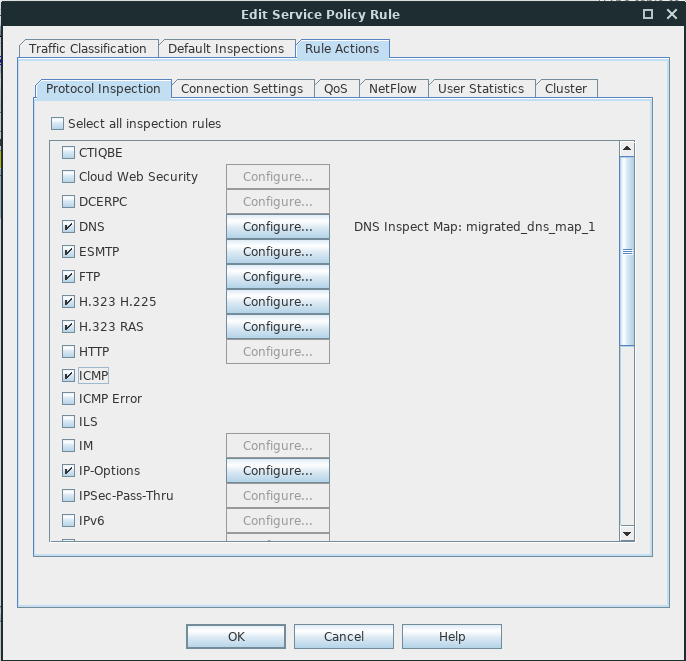
* + 1. Modify the MPF application inspection policy.

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

* + - 1. 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**.



* + - 1. 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**.



* + - 1. From PC-B, **ping** the external interface of R1 S1/0 (**10.1.1.1**). The pings should be successful.

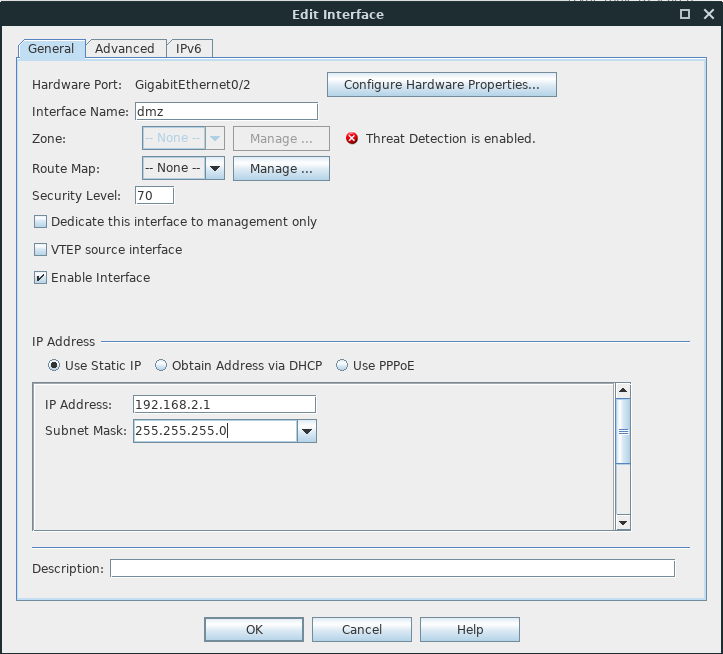
1. Configure DMZ, Static NAT, and ACLs

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.

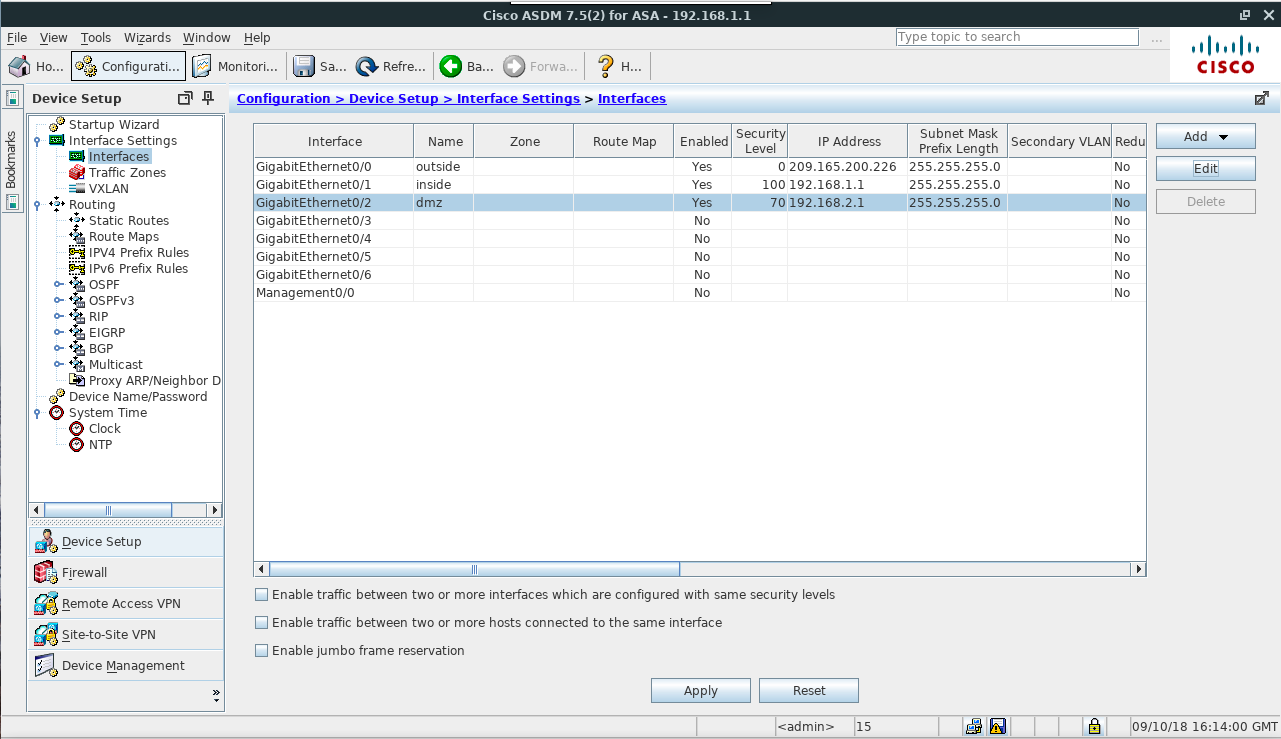
* + 1. Configure the ASA DMZ interface on Gi0/2.

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.

* + - 1. 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.
      2. In the Interface Namebox, name the interface **dmz**, assign it a security level of **70**, and make sure the **Enable Interface** checkbox is checked.
      3. 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.



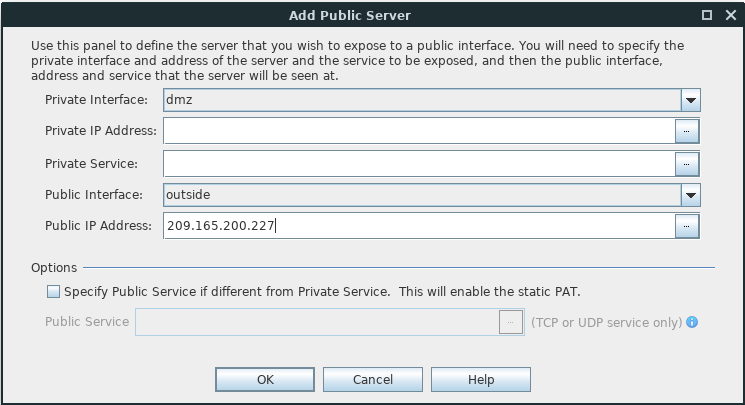
* + - 1. You should see the new interface named **dmz**, in addition to the inside and outside interfaces. Check the box **Enable traffic between two or more interfaces which are configured with the same security levels**. Click **Apply** to send the commands to the ASA.



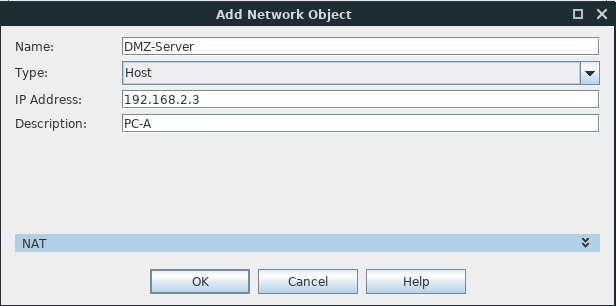
* + 1. Configure the DMZ server and static NAT.

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.

* + - 1. 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 addressas **209.165.200.227**.

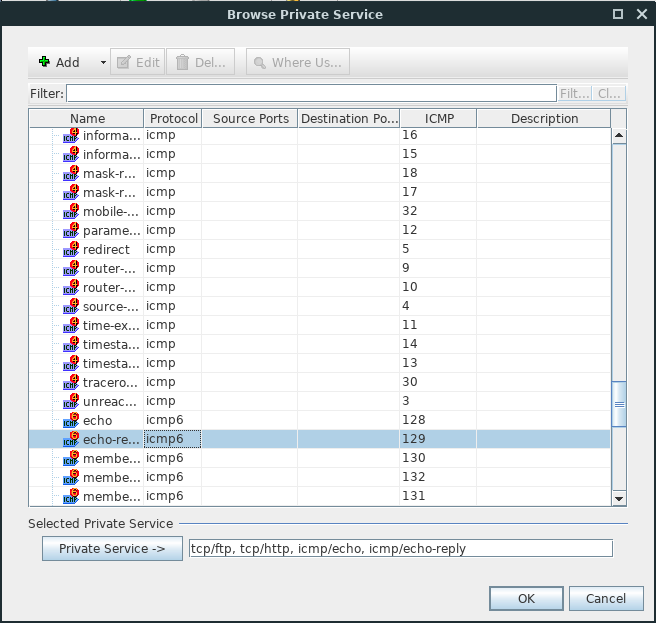


* + - 1. Click the ellipsis button to the right of Private IP Address.In the Browse Private IP Address window, click **Add** to define the server as a **Network Object**. Enter the name **DMZ-Server**, select **Host** from the Type pull-down menu**,** enter the IP Address **192.168.2.3**, and a Description of **PC-A**.

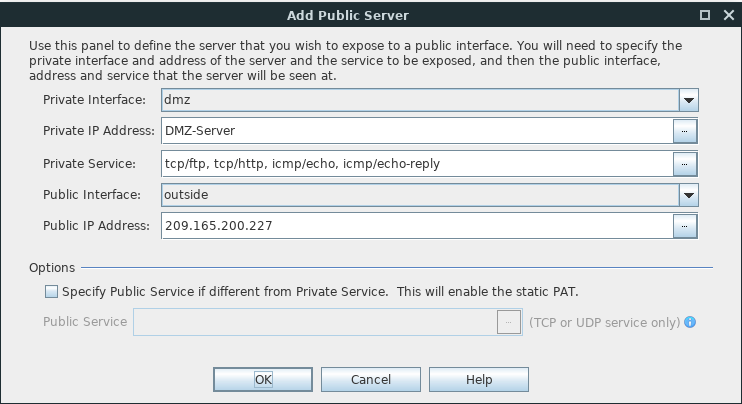


* + - 1. From the Browse Private IP Address window, verify that the DMZ-Server appears in the Selected Private IP Address by clicking on Private IP Address field and click **OK**. You will return to the Add Public Server dialog box.
      2. In the Add Public Server dialog, click the ellipsis button 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.

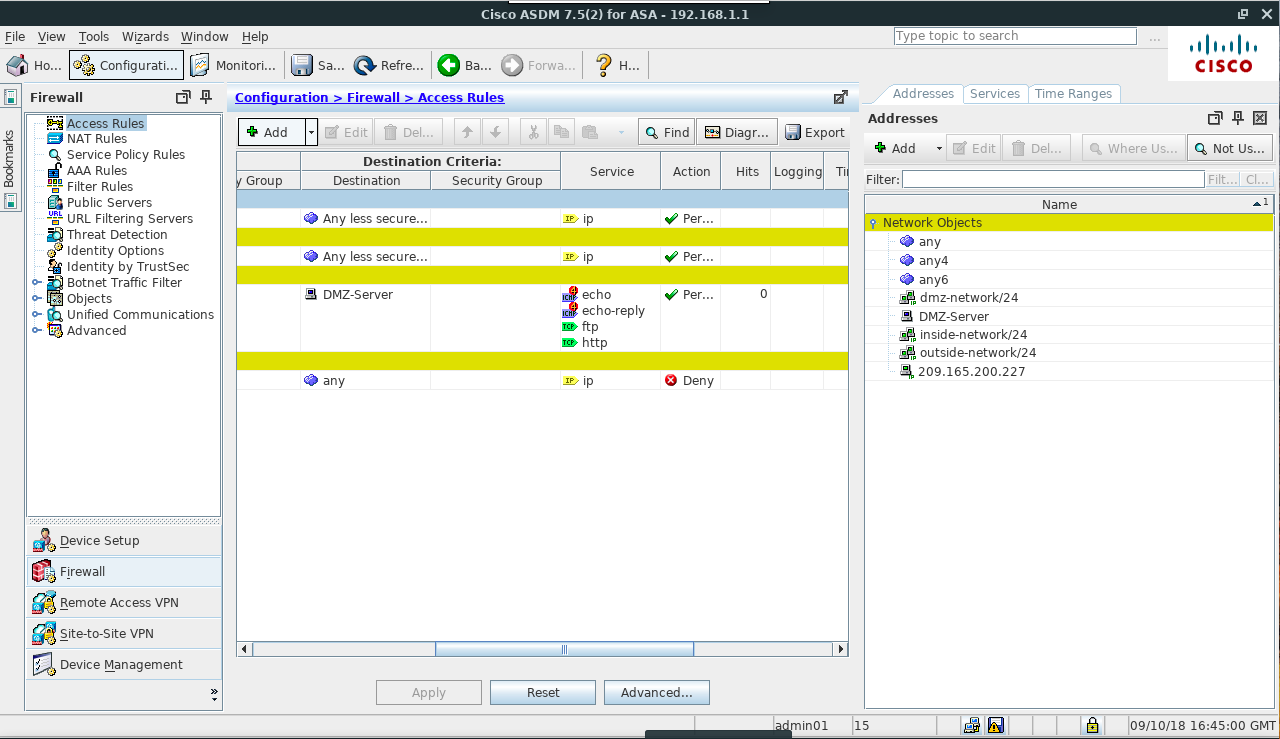
**Note**: You can specify Public services if they are different from the Private services, using the option on this screen.



* + - 1. 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.



* + 1. View the DMZ Access Rule generated by ASDM.
       1. 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.
       2. View this ACL in ASDM by clicking **Configuration** > **Firewall** > **Access Rules**. It appears as an outside incoming rule. You can select the rule and use the horizontal scroll bar to see all of the components.

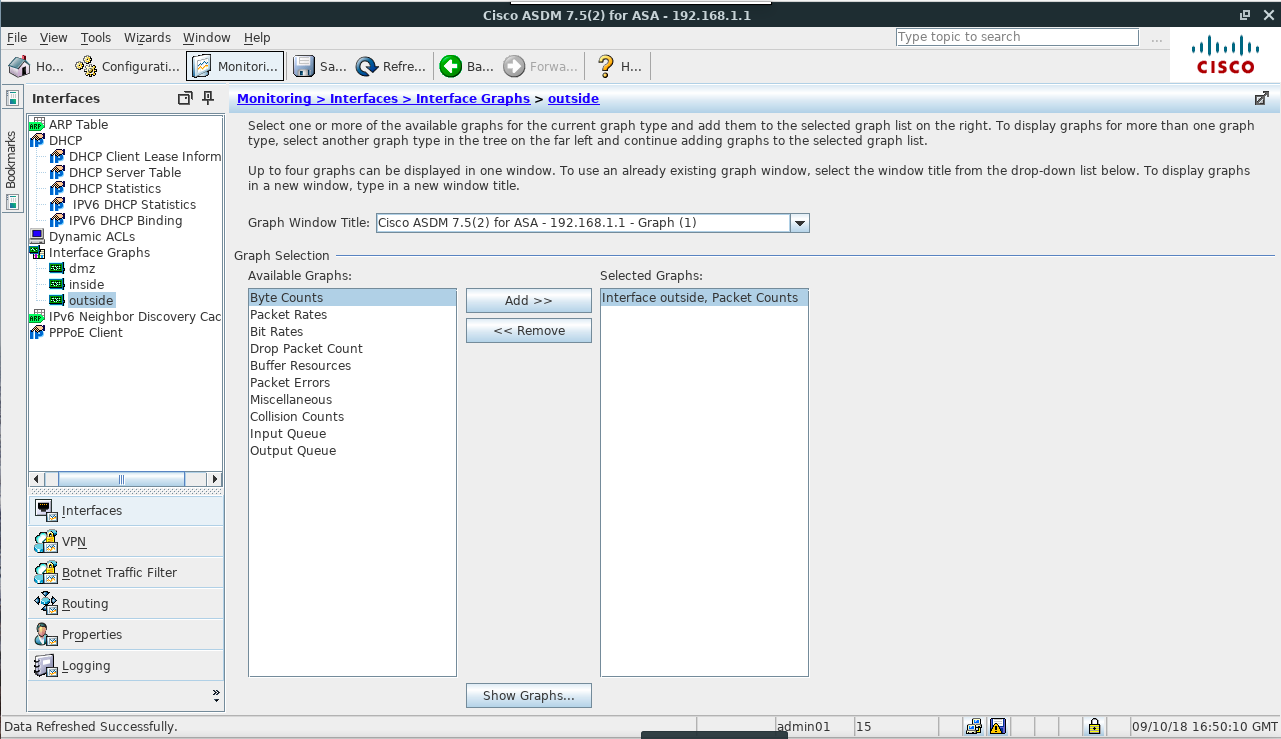


**Note**: You can also see the commands generated by using the **Tools** > **Command Line Interface** and entering the **show run** command.

* + 1. Test access to the DMZ server from the outside network.
       1. From PC-C, ping the IP address of the static NAT public server address (**209.165.200.227**). The pings should be successful.
       2. 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.
       3. 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.
    2. 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.

* + - 1. 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.



* + - 1. Click **Show Graphs** to display the graph. Initially, there is no traffic displayed.
      2. 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

* + - 1. 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.
      2. 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.

