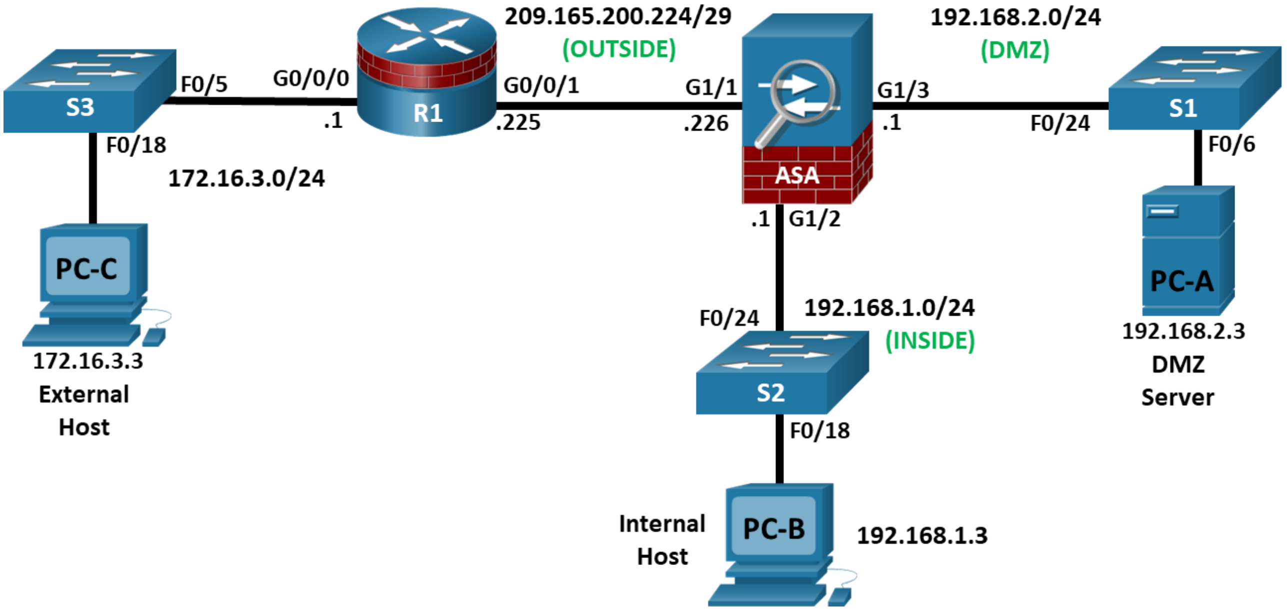
Lab - Configure ASA Basic Settings and Firewall Using ASDM

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	172.16.3.1	255.255.255.0	N/A	S3 F0/5
	G0/0/1	209.165.200.225	255.255.255.248		ASA G1/1
ASA	G1/1 (OUTSIDE)	209.165.200.226	255.255.255.248	N/A	R1 G0/0/1
	G1/2 (INSIDE)	192.168.1.1	255.255.255.0		S2 F0/24
	G1/3 (DMZ)	192.168.2.1	255.255.255.0		S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

Part 2: Access the ASA Console and ASDM

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

Part 4: Configure ASA Settings from the ASDM Configuration Menu

Part 5: Configure DMZ, Static NAT, and ACLs

Background/Scenario

The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall, a VPN, and FirePOWER services. This lab employs an ASA 5506-X 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 to configure 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.

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

Note: The routers used with hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

The ASA used with this lab is a Cisco model 5506-X with an 8-port integrated switch, running OS version 9.15(1), Adaptive Security Device Manager (ASDM) version 7.15(1).

Note: Make sure that the devices have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 3 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 3 PCs (Windows OS with a terminal emulation application and Java version compatible with installed ASDM version)
- 1 ASA 5506-X (OS version 9.15(1) and ASDM version 7.15(1) and Base license or comparable)
- Console cables to configure the Cisco IOS devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings

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

Note: Do not configure ASA settings at this time.

Step 1: Cable the network and clear previous device settings.

Attach the devices that are shown in the topology diagram and cable as necessary. Make sure the router and ASA have been erased and have no startup configuration.

Note: To avoid using the switches, use a cross-over cable to connect the end devices

Step 2: Configure R1 and the end devices.

a. Use the following script to configure R1. No additional configuration for R1 will be required for this lab.

Note: R1 does not need any routing as all inbound packets from the ASA will have 209.165.200.226 as the source IP address.

R1 Script

```
enable
configure terminal
hostname R1
security passwords min-length 10
enable algorithm-type scrypt secret cisco12345
ip domain name netsec.com
username admin01 algorithm-type scrypt secret admin01pass
interface GigabitEthernet0/0/0
 ip address 172.16.3.1 255.255.255.0
 no shutdown
interface GigabitEthernet0/0/1
 ip address 209.165.200.225 255.255.255.248
 no shutdown
crypto key generate rsa general-keys modulus 2048
ip http server
ip http authentication local
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
end
copy running start
```

b. 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 3: Verify connectivity.

Because the ASA is the focal point for the network zones, and it has not yet been configured, there will be no connectivity between devices that are connected to it. However, PC-C should be able to ping the R1 interface. From PC-C, ping the R1 G0/0/1 IP address (209.165.200.225). If these pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Access the ASA Console and ASDM

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

Step 1: Access the ASA console.

a. Accessing the ASA via the console port is the same as accessing it with a Cisco router or switch. Connect to the ASA console port with a rollover cable and use a terminal emulation program, such as TeraTerm or PuTTy to open a serial connection and access the CLI.

b. The ASA initially prompts you to pre-configure the firewall using an interactive prompt. We will not be configuring the ASA this way, therefore enter **no** and press **Enter**. If you have inadvertently started the setup wizard, press **CTRL-Z** to exit it. The terminal screen should display the default ASA user EXEC hostname and prompt ciscoasa>.

c. You will get a prompt requesting that you configure an enable password to enter privileged EXEC mode. Enter **cisco12345** to configure the password and then again to confirm it. You will now be in privileged EXEC mode.

```
enable password cannot be removed
Enter Password: class
Repeat Password: class
Note: Save your configuration so that the password persists across reboots
("write memory" or "copy running-config startup-config").
ciscoasa#
```

Step 2: Clear previous ASA configuration settings.

If the ASA has been previously configured, use **write erase** and then **reload** commands to reset to the default configurations.

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 and set the enable password to **cisco12345**.

```
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
```

```
ciscoasa> enable
The enable password is not set.  Please set it now.
Enter  Password: cisco12345
Repeat Password: cisco12345
Note: Save your configuration so that the password persists across reboots
("write memory" or "copy running-config startup-config").
ciscoasa#
```

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**.

```
ciscoasa# conf t
ciscoasa(config)#

***************************** NOTICE *****************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: no

In the future, if you would like to enable this feature,
issue the command "call-home reporting anonymous".

Please remember to save your configuration.

ciscoasa(config)#
```

d. Configure the INSIDE interface G1/2 to prepare for ASDM access. The Security Level should be automatically set to the highest level of **100**. The interface G1/2 will be used by PC-B to access ASDM on ASA.

```
ciscoasa(config)# interface g1/2
ciscoasa(config-if)# nameif INSIDE
INFO: Security level for "INSIDE" set to 100 by default.
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Virtual0                   127.1.0.1       YES unset  up                    up
GigabitEthernet1/1         unassigned      YES unset  administratively down down
GigabitEthernet1/2         192.168.1.1     YES manual up                    up
GigabitEthernet1/3         unassigned      YES unset  administratively down down
GigabitEthernet1/4         unassigned      YES unset  administratively down down
<output omitted>
```

e. Configure OUTSIDE interface G1/1 and enable the G1/1 interface. You will assign the IP address using ASDM.

```
ciscoasa(config)# interface g1/1
ciscoasa(config-if)# nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
```

f. Test connectivity to the ASA by pinging from PC-B to ASA interface G1/2 **192.168.1.1**. The pings should be successful.

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

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
```

Step 5: Access ASDM and explore the GUI.

a. If you or your instructor have already installed the **Cisco ASDM-ID Launcher**, open the application and proceed to Step 5e. If the **Cisco ASDM-ID Launcher** is not installed, proceed to Step5b.

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

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

c. After entering the URL above, you will be prompted that the connection is not secure.

Note: These steps are for reference only. Your steps maybe different depending on your chosen browser when you attempt to connect to the ASA via a web browser.

Microsoft Explorer or Edge: Click **Continue to this webpage (not recommended)**.

Mozilla Firefox: Click **Advanced** > **Add Exception** > **Confirm Security Exemption**.

Google Chrome: Click **Advanced** > **Proceed to 192.168.1.1 (unsafe)**.

d. You should then see Cisco ASDM Welcome screen that allows you to either **Install ASDM Launcher** or **Install Java Web Start** to run ASDM as a Java Web start application.

e. You should then be required to authenticate to the ASA. Because no username was specified, simply enter the enable password **cisco12345** in the password field and click **OK**.

f. The GUI opens. Click **OK** to the Enable Password dialog.

g. The initial GUI screen is displayed with various areas and options. The menu at the top left of the screen contains three main sections: **Home**, **Configuration**, and **Monitoring**. The **Home** section is the default and has two dashboards: **Device Dashboard** and **Firewall Dashboard**.

h. There are five areas on the **Device Dashboard**:

- Device Information (default ASDM screen)
- Interface Status
- VPN Sessions
- System Resources Status
- Traffic Status

These areas display various information about the ASA. For instance, the Device Information displays device information, such as hostname, ASA version, ASDM version, firewall mode, device type (ASA 5506), and more.

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

i. 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

In this part, you will use ASDM Startup Wizard to modify the configurations.

Note: The following steps are based on ASA version 9.15(1)1 and ASDM version 7.15(1) These steps are for reference only. Your steps maybe different.

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

a. On the menu bar, click **Configuration.** The Configuration screen provides the following five areas of device configuration:

- Device Setup (default display)
- Firewall
- Remote Access VPN
- Site-to-Site VPN
- Device Management

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

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

a. The first Startup Wizard screen enables us to 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.

b. On the Startup Wizard Step 2 screen, configure the ASA hostname **NETSEC-ASA** and domain name **netsec.com**. Click the check box for changing the enable mode password and change it to **cisco12345** and enter it again to confirm. When the entries are completed, click **Next** to continue.

Step 3: Configure the outside interface.

a. On the Startup Wizard Step 3 screen for the outside interface, do not change the current settings because these were previously defined using the CLI. The outside G1/1 is named **OUTSIDE**, and the security level is set to 0 (lowest). Enter the IP address of **209.165.200.226** with a subnet mask of **255.255.255.248**. Click **Next** to continue.

b. On the Startup Wizard Step 4 screen, verify that the inside and outside interfaces are configured correctly according to the Addressing Table. Click **Next** to continue.

Note: The DMZ interface will be configured later in this lab.

Step 4: View the Static Routes screen.

The Startup Wizard Step 5 screen enables us to configure a static route(s). We will be completing this step later in this lab; therefore, click **Next** to continue.

Step 5: Configure DHCP, address translation, and administrative access.

a. On the Startup Wizard Step 6 screen – DHCP Server, click the **Enable DHCP server on the INSIDE interface** check box. Enter a Starting IP Address of **192.168.1.31** and an Ending IP Address of **192.168.1.39**. Enter the DNS Server 1 address of **10.20.30.40** and the Domain Name **netsec.com**. Click **Next** to continue.

   Note: Do **NOT** check the box to Enable auto-configuration from interface.

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. Click **Next** to continue.

   Note: You can also specify a particular IP address for PAT or a range of addresses with NAT.

c. On the Startup Wizard Step 8 screen – Administrative Access, notice that **HTTPS/ASDM** access is already configured for hosts on the inside network 192.168.1.0/24. That is how you are currently accessing the ASA. Click **Add** to add another type of access. Fill in the **Add Administrative Access Entry** dialog with the following settings:

   Access Type: **SSH**

   Interface Name: **INSIDE**

   IP Address: **192.168.1.0**

   Subnet Mask: **255.255.255.0**

   Click **OK** to add this SSH access type to the list.

d. Click **Add** to add another type of access. Fill in the **Add Administrative Access Entry** dialog with the following settings:

   Access Type: **SSH**

   Interface Name: **OUTSIDE**

   IP Address: **172.16.3.3**

   Subnet Mask: **255.255.255.255**

   Click **OK** to add this SSH access type to the list.

e. Click **Next** to continue.

Step 6: Review the summary and deliver the commands to the ASA.

a. On the Startup Wizard Step 9 screen – Auto Update Server, leave everything to the default and click **Next** to continue.

b. On the Startup Wizard Step 10 – Do not enable Smart Call Home, leave everything to the default and click **Next** to continue.

c. 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 **Cisco ASDM-ID Launcher**. 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. Provide the new enable password **cisco12345** with no username when prompted. 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 7: Test access to an external website from PC-B.

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

   Note: You may need to disable some or all of your firewall features on PC-B.

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 **cisco12345**. Exit the browser.

Step 8: Test access to an external website using the ASDM Packet Tracer utility.

a. Click **Tools > Packet Tracer…** from the menu. This tool allows you test a variety of packet types between a specified source and destination.

b. If necessary, 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 G0/0/1) with a Destination Port of **http**.

c. Click **Start** to begin the trace of the packet. You should the output **RESULT - The packet is allowed**.

d. 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 G0/0/1) 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**.

e. Click **Start** to begin the trace of the packet. You should the output **RESULT - The packet is dropped**.

f. Click **Close** to continue.

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. Click **Configuration** > **Device Setup** > **System Time** > **Clock**.

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

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

Note: When using ASDM, it is important that changes be configured using the **Apply** button. Failure to do this will not enable the configuration.

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

a. From the menu, select **Tools** > **Ping…** and enter the IP address of router R1 G0/0/0 (**172.16.3.1**).

b. Click **Ping**. The ASA does not have a default route to unknown external networks. Therefore, the pings should fail because the ASA does not have a route to 172.16.3.1.

c. Click **Close** to continue.

d. From **Device Setup** in the **Configuration** screen, click **Routing** > **Static Routes**.

e. Click **IPv4 only** and click **Add** to add a new static route.

f. On the **Add Static Route** dialog box, select the **OUTSIDE** interface from the drop-down list. Click the ellipsis button to the right of **Network**, select **any4** from the list of network objects, and click **OK**. The selection of **any4** translates to a "quad zero" route.

   For the Gateway IP, enter **209.165.200.225** (R1 G0/0/1).

g. Click **OK**, and then click **Apply** to send the commands to the ASA.

h. From the menu, select **Tools** > **Ping…** again and enter the IP address of router R1 G0/0/0 (**172.16.3.1**).

i. Click **Ping**. The ping should succeed this time. Click **Close** to continue.

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

In a previous step, inside hosts and PC-C were configured SSH access to the ASA. We will now enable AAA user authentication to access the ASA using SSH. To allow the administrator to have SSH access to the ASA, you will add a user in the local database.

a. On the **Configuration** screen and select **Device Management** > **Users/AAA** > **User Accounts**.

b. Click **Add** to open the **Add User Account** dialog.

c. 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**.

d. Click **OK** to add the user and return to the **User Accounts** window. Verify that the new entry is correct.

e. Click **Apply** to send the command to the ASA.

f. Next, we will enable AAA access to the ASA. From the **Users/AAA** submenu, select **AAA Access**.

g. On the **Authentication** tab, click the check boxes to require authentication for **HTTP/ASDM** and **SSH** connections using the **LOCAL** server group to authenticate against.

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

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

Step 4: Test SSH access to the ASA.

a. Open a SSH client on PC-B, such as PuTTY, and connect to the ASA inside interface at IP address **192.168.1.1**.

b. When prompted to log in, enter the user name **admin01** and the password **admin01pass**. (**Note**: If prompted, accept the security warning.)

c. From **PC-C**, open an SSH client, such as PuTTY, and attempt to access the ASA outside interface at **209.165.200.226**.

d. When prompted to log in, enter the user name **admin01** and the password **admin01pass**.

e. After logging in to the ASA using SSH, enter the **enable** command and provide the password **cisco12345**.

f. Issue the **show run** command to display the current configuration that you have created using ASDM.

   Note: The idle timeout for SSH could also 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. Verify if PC-B can ping a destination host. From PC-B, **ping** the external interface of R1 G0/0/0 (**172.16.3.1**). The pings should fail because the ASA default global inspection policy does not inspect ICMP and consequently, does not inside hosts ping outside hosts. To enable hosts on the internal network to ping external hosts and receive replies, ICMP traffic must be inspected.

b. On the **Configuration** screen, click **Firewall**. If prompted, authenticate using the username **admin01** with the password **admin01pass**.

c. Click **Service Policy Rules** to display the current policies enabled on the ASA.

d. To enable ICMP, select the **inspection_default** policy, and then click **Edit**. The **Edit Service Policy Rule** dialog opens.

e. Click the **Rule Actions** tab and select the **ICMP** check box. Do not change the other default protocols that are checked.

f. Click **OK** and then **Apply** to send the commands to the ASA. If prompted, log in as **admin01** with the password **admin01pass**.

g. From PC-B, **ping** the external interface of R1 G0/0/0 (**172.16.3.1**). 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 on interface G1/3.

In this step, you will configure the G1/3 interface, name it **DMZ**, set the security level to **70**, and limit communication from this interface to the INSIDE interface G1/2.

a. From the **Configuration** screen, select **Device Setup** > **Interface Settings** > **Interfaces**. Currently, only the INSIDE (G1/2) and OUTSIDE (G1/1) interfaces are configured.

b. Select the **GigabitEthernet1/3** interface and click **Edit**.

c. In the **Edit Interface** dialog box, enter **DMZ** as the **Interface Name**. Enter **70** in the **Security Level** field. Select the **Enable Interface** checkbox. 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 continue.

d. If a **Security Level Change** window is displayed, read the warning and click **OK** to continue. In the list of interfaces, verify that G1/3 is enabled and configured with the correct name, security level, and IP address.

e. Select the checkbox **Enable traffic between two or more interfaces which are configured with the same security levels**. Click **Apply** to send the configuration to the ASA.

Step 2: Configure the DMZ server and static NAT.

To accommodate the addition of a DMZ and a web server, you will use another address from the ISP range assigned, 209.165.200.224/29 (.224-.231). R1 G0/0/1 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. From the **Configuration** screen, select **Firewall** > **Public Servers**.

b. Click **Add** to define the DMZ server and services offered.

c. In the **Add Public Server** dialog box, the **Private Interface** should already be set as **DMZ**. Set the **Public Interface** as **OUTSIDE**, and the **Public IP Address** as **209.165.200.227**.

d. Click the ellipsis button to the right of **Private IP Address** to open the **Browse Private IP Address** window.

e. Click **Add** to open the **Add Network Object** dialog box.

f. Enter the name **DMZ-SERVER**, select **Host** from the **Type** menu**,** enter the IP Address **192.168.2.3**, and a **Description** of **PC-A**. Click **OK** to continue.

g. From the **Browse Private IP Address** window, click the plus sign next to **Network Objects** to expand it. Double-click the **DMZ-SERVER** to add it as the **Selected Private IP Address**.

h. Click **OK**. You will return to the **Add Public Server** dialog box. Click the ellipsis button to the right of **Private Service**.

i. In the **Browse Private Service** window, you will double-click various services to select them and add them to the Public Service field. Double-click the following services: **tcp/ftp**, **tcp/http**, **icmp/echo,** and **icmp/echo-reply** (**Note**: scroll down to see all services).

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

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

k. Click **OK**, and then click **Apply** to send the configuration to the ASA. Re-authenticate if necessary.

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

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

To view this ACL, in the **Firewall** menu, select **Access Rules**. It appears as an OUTSIDE incoming rule. You can select the rule and use the horizontal scroll bar to see all of the components.

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

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

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. Ping the DMZ server (PC-A) internal IP address **192.168.2.3** from inside network host PC-B. The pings should be successful. This is because the ASA inside interface G1/2 is set to security level 100 (the highest) and the DMZ interface G1/3 is set to 70.

c. Try to ping from the DMZ server PC-A to PC-B at the IP address **192.168.1.3**. The pings should not be successful. The reason the DMZ server cannot ping PC-B on the inside network is because the DMZ interface G1/3 has a lower security level than the inside interface.

Reflection

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

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

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.