10.1.4.8 Lab – Configure ASA 5506-X Basic Settings and Firewall Using ASDM Answers

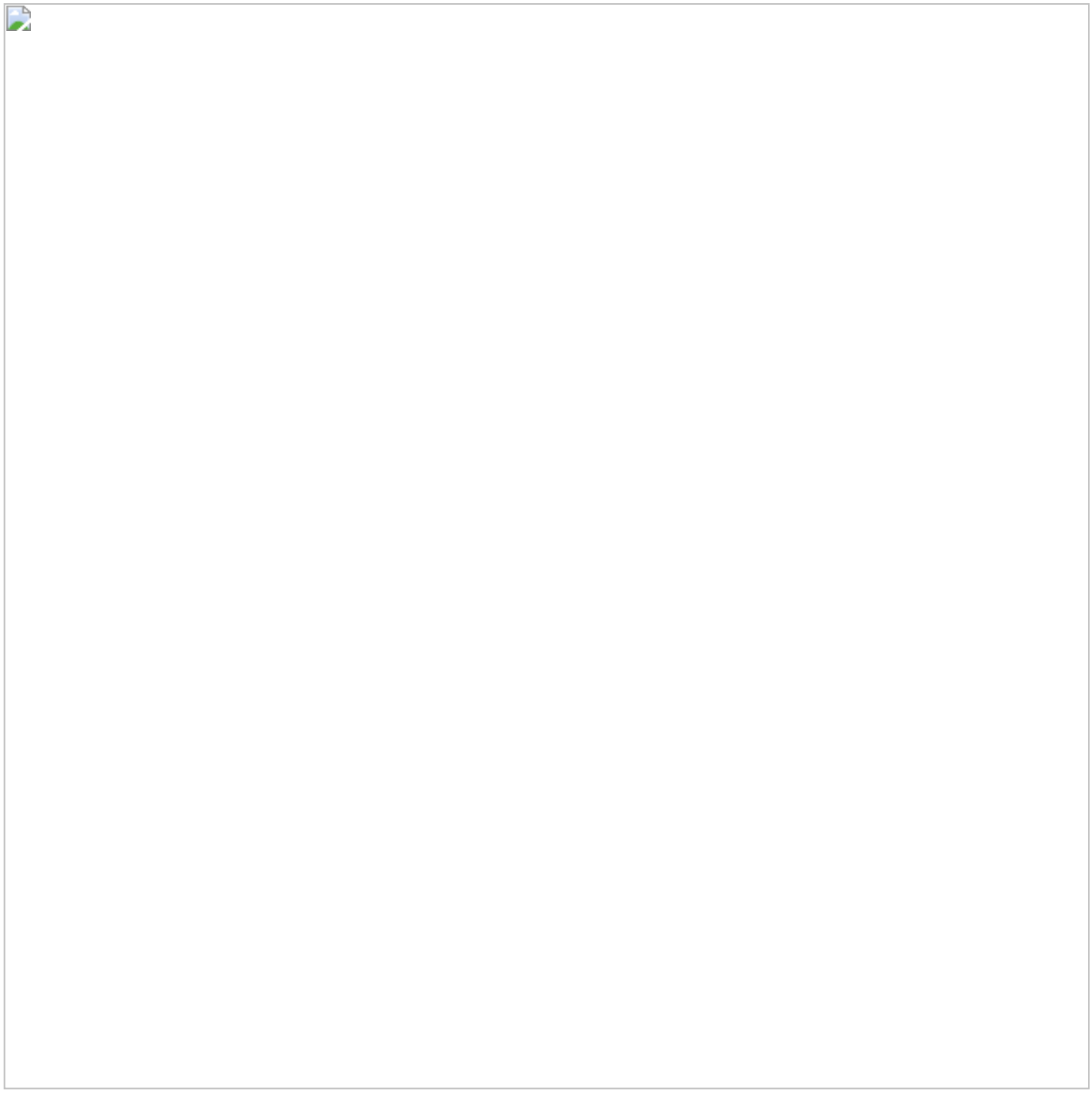
itexamanswers.net/10-1-4-8-lab-configure-asa-5506-x-basic-settings-and-firewall-using-asdm-answers.html

June 6, 2022

10.1.4.8 Lab – Configure ASA 5506-X Basic Settings and Firewall Using ASDM (Instructor Version)

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

Topology



Note: ISR G1 devices use FastEthernet interfaces instead of GigabitEthernet interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	209.165.200.225	255.255.255.248	N/A	ASA G1/1
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R2	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	S3 F0/5
R3	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	G1/1 (outside)	209.165.200.226	255.255.255.248	NA	R1 G0/0
ASA	G1/2 (inside)	192.168.1.1	255.255.255.0	NA	S2 F0/24
ASA	G1/3 (dmz)	192.168.2.1	255.255.255.0	NA	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Objectives

Part 1: Configure Basic Device Settings

- Cable the network and clear previous device settings.
- Configure basic settings for routers and switches.
- Configure static routes on R2 and default routes on R1 and R3.
- Enable the HTTP server on R1 and set the enable and VTY passwords.
- Configure PC host IP settings.
- Verify connectivity.

Part 2: Access the ASA Console and ASDM

- Access the ASA console and view hardware, software, and configuration settings.
- Clear previous ASA configuration settings.
- Bypass Setup mode and configure the ASDM VLAN interfaces.
- Configure ASDM and verify access to the ASA.
- Access ASDM and explore the GUI.

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

- Access the Configuration menu and launch the Startup wizard.
- Configure the hostname, domain name, and enable the password.
- Configure the inside and outside VLAN interfaces.
- Configure DHCP, address translation, and administrative access.
- Review the summary and deliver the commands to the ASA.
- Test access to an external website from PC-B.
- Test access to an external website using the ASDM Packet Tracer utility.

Part 4: Configure ASA Settings from the ASDM Configuration Menu

- Set the ASA date and time.
- Configure a static default route for the ASA.
- Configure AAA user authentication using the local ASA database.
- Test SSH access to the ASA.
- Test connectivity using ASDM Ping and Traceroute.
- Modify the MPF application inspection policy.

Part 5: Configure DMZ, Static NAT, and ACLs

- Configure the ASA DMZ VLAN 3 interface.
- Configure the DMZ server and static NAT.
- View the DMZ Access Rule generated by ASDM.
- Test access to the DMZ server from the outside network.

Background/Scenario

The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall, a VPN, and 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 router commands and output in this lab are from a Cisco 1941 router with Cisco IOS Release 15.4(3)M2 (with a Security Technology Package license). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and the output produced might vary from what is shown in this lab.

The ASA used with this lab is a Cisco model 5506-X with an 8-port integrated switch, running OS version 9.10(1), Adaptive Security Device Manager (ASDM) version 7.10(1), and comes with a Base license that allows a maximum of five VLANs.

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

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

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology Package license)
- 3 Switches (Cisco 2960 with cryptography IOS image for SSH support – Release 15.0(2)SE7 or comparable) (not required)
- 1 ASA 5506-X (OS version 9.10(1) and ASDM version 7.10(1) and Base license or comparable)
- 3 PCs (Windows, SSH Client and Java version compatible with installed ASDM version)
- Serial and Ethernet cables, as shown in the topology
- Console cables to configure Cisco networking devices

Instructor Notes:

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

Part 1: Configure Basic Device Settings

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

Note: Do not configure ASA settings at this time.

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

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

Step 2: Configure basic settings for routers and switches.

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

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

c. Configure the hostname for the switches. With the exception of the hostname, the switches can be left in their default configuration state.

Step 3: Configure static routing on the routers.

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

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

b. Configure a static route from R2 to the R1 G0/0 subnet (connected to ASA interface G1/1) and a static route from R2 to the R3 LAN.

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

Step 4: Configure and encrypt passwords on R1.

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

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

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

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

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

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

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

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

to support SSH.

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

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

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

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

Step 5: Configure PC host IP settings.

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

Step 6: Verify connectivity.

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

Note: If you can ping from PC-C to R1 G0/0 and S0/0/0, you have demonstrated that addressing has been configured properly, and static routing is configured and functioning correctly.

Step 7: Save the basic running configuration for each router and switch.

Part 2: Access the ASA Console and ASDM

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

Step 1: Access the ASA console.

a. Accessing the ASA via the console port is the same as accessing it with a Cisco router or switch. Connect to the ASA console port with a rollover cable 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. Enter privileged mode with the **enable** command. The password is blank by default therefore press **Enter**. If the password has been changed to what is specified in this lab, enter the word **cisco12345**.

```
ciscoasa> enable
Password: cisco12345 (or press Enter if no password is set)
```

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. 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 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)# exit
```

ASA 5506-X interface notes:

The ASA 5506-X comes with an integrated eight-port Ethernet switch. Ports G1/1 to G1/8 are normal GigabitEthernet ports.

By default, all ASA physical interfaces are administratively down unless the Setup utility has been run, or the factory defaults have been reset. Use the **show interface ip brief** command to verify this.

```
ciscoasa(config-if)# 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 administratively down down
GigabitEthernet1/3         unassigned      YES unset  administratively down down
GigabitEthernet1/4         unassigned      YES unset  administratively down down
<output omitted>
```

e. Enable the G1/2 interface using the **no shutdown** command and verify the G1/2 interface status. The status and protocol for interface G1/2 should be up/up.

```
ciscoasa(config)# interface G1/2
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>
```

f. 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
```

g. 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. 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.

b. 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)**.

c. You should then see Cisco ASDM Welcome screen that allows you to: Install ASDM Launcher, Run ASDM or Install Java Web Start.

d. Click **Install ASDM Launcher** to install the Launcher or **Run ASDM** to start the Launcher. Follow the directions on the screen and accept the security warning.

If one of the choices is **Install Java Web Start**, you will need to input https://192.168.1.1/admin/public/startup.jnlp in a browser if you do not want to install the Launcher. Open the downloaded file **startup.jnlp** using Java ™ Web Start Launcher.

e. After the ASDM Launcher starts, you will be prompted for a username and password. Leave the fields empty and click **OK**.

f. 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.

Note: If the Startup wizard displays, click **Cancel** to continue.

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**.

g. 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 9.10(1), ASDM version 7.10(1) and Java version 1.8(201). 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 **CCNAS-ASA** and domain name **ccnasecurity.com**. Click the check box for changing the enable mode password and change it from blank (no password) 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 IP Addressing Table. Click Next to continue.

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

Step 4: Configure the static route.

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 ccnasecurity.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, 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.

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.

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

b. 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.

Note: The process to restart ASDM would be different if ASDM was installed on your PC or ran from the web browser. If it was installed, launch ASDM from the program menu. Otherwise, ASDM can be started from the web browser.

c. 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 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 8: 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 G0/0) with a Destination Port of http.

c. Click Start to begin the trace of the packet. The packet should be permitted.
d. Click Clear to reset the entries. Try another trace and select outside from the Interface drop-down list and leave TCP as the packet type. From the Sources drop-down list, select IP Address, and enter 209.165.200.225 (R1 G0/0) and a Source Port of 1500. From the Destination drop-down list, select IP Address and enter the address 209.165.200.226 (ASA outside interface) with a Destination Port of telnet.

e. Click Start to begin the trace of the packet. The packet should be 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. 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.)

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. On the ASDM Tools menu, select Ping and enter the IP address of router R1 S0/0/0 (10.1.1.1).

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 10.1.1.1.

c. Click Close to continue.

d. From the Configuration screen > Device Setup menu, 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).

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

h. On the ASDM Tools menu, select Ping and enter the IP address of router R1 S0/0/0 (10.1.1.1).

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

j. We will now verify the routing hops to PC-C. From the ASDM Tools menu, select Traceroute.

k. Enter the IP address of external host PC-C (172.16.3.3).

l. Click Trace Route. The traceroute should succeed and show the hops from the ASA through R1, R2, and R3 to host PC-C. Click Close to continue.

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

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.

b. Click Users/AAA > User Accounts.

c. To add a new user, click Add to open the Add User Account window

d. 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.

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

f. Click Apply to send the command to the ASA.

g. Next we will enable AAA access to the ASA. In the Device Management > Users/AAA > and select AAA Access.

h. 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.

i. 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 S0/0/0 (10.1.1.1). 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 > Firewall area menu. 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. We need to enable ICMP; therefore, select the inspection_default policy and click Edit to modify the default inspection rules in the Edit Service Policy Rules window.

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 S0/0/0 (10.1.1.1). The pings should be successful.

Part 5: Configure DMZ, Static NAT, and ACLs

In Part 3, you configured address translation using PAT for the inside network. In this part, you will create a DMZ on the ASA, configure static NAT to a DMZ server, and apply an ACL to control access to the server.

Step 1: Configure the ASA DMZ 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 and click Interface Settings.

b. Click Interfaces to open the Interface window. Currently, only the inside (G1/2) and outside (G1/1) interfaces are configured.

c. Select the GigabitEthernet1/3 interface and click Edit. (Note: You could also double-click the interface.)

d. 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.

e. If a Security Level Change window is displayed, click OK to continue. Verify that G1/3 is enabled and configured with the correct name, security level, and IP address.

f. Select the checkbox Enable traffic between two or more interfaces which are configured with the same security levels. Click Apply to continue.

Step 2: Configure the DMZ server and static NAT.

To accommodate the addition of a DMZ and a web server, you will use another address from the ISP range assigned, 209.165.200.224/29 (.224-.231). R1 G0/0 and the ASA outside interface are already using 209.165.200.225 and .226. You will use public address 209.165.200.227 and static NAT to provide address translation access to the server.

a. On the Firewall menu, click the Public Servers option

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

c. 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.

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

e. Click Add to define the server as a Network Object.

f. 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. Click OK to continue.

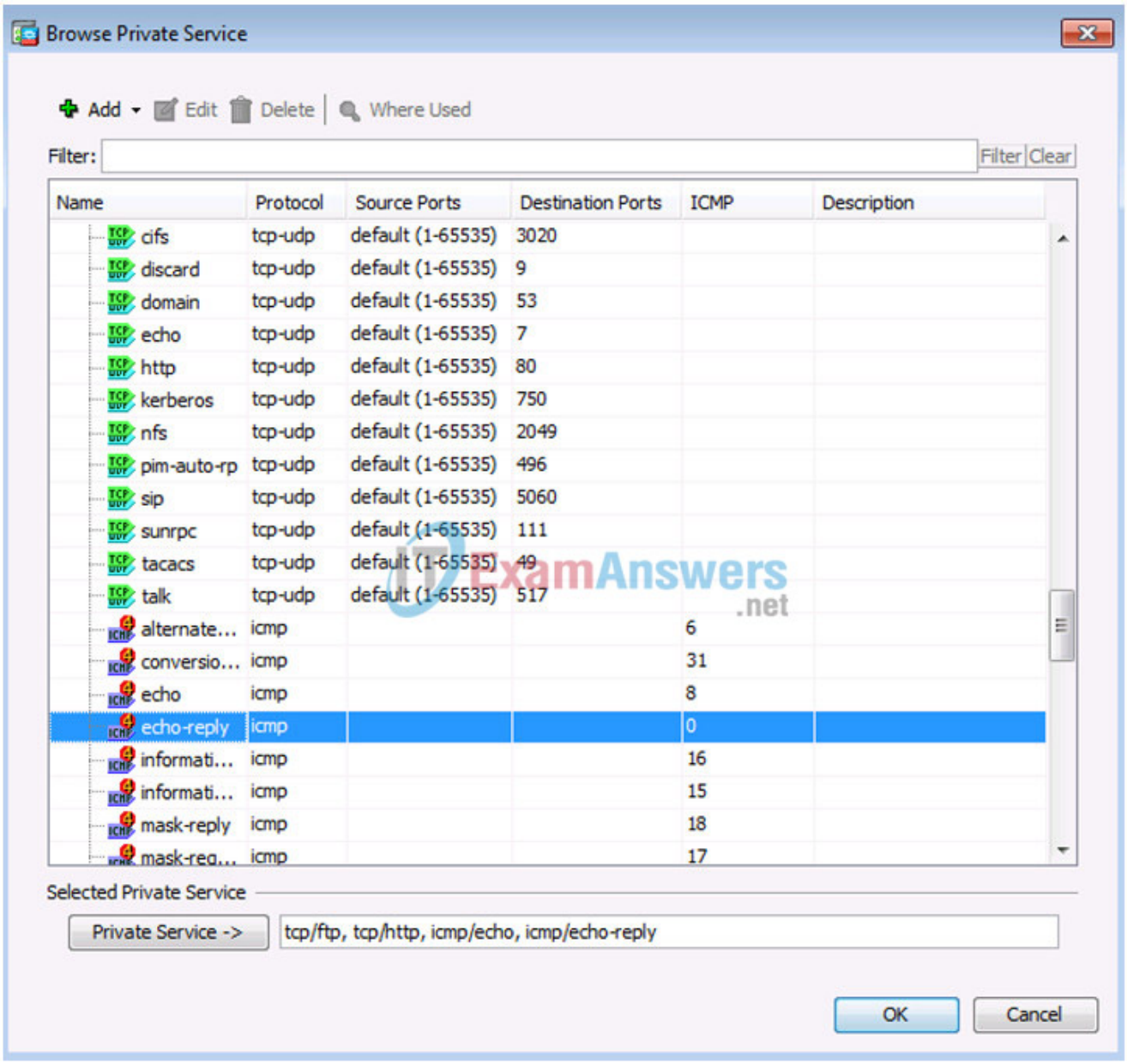
g. From the Browse Private IP Address window, click Network Objects to expand it. Verify that the DMZ-Server appears in the Selected Private IP Address field.

h. Double-click the DMZ-Server to add it to the DMZ-Server field.

i. Click OK. You will return to the Add Public Server dialog box.

j. In the Add Public Server dialog, click the ellipsis button to the right of Private Service.

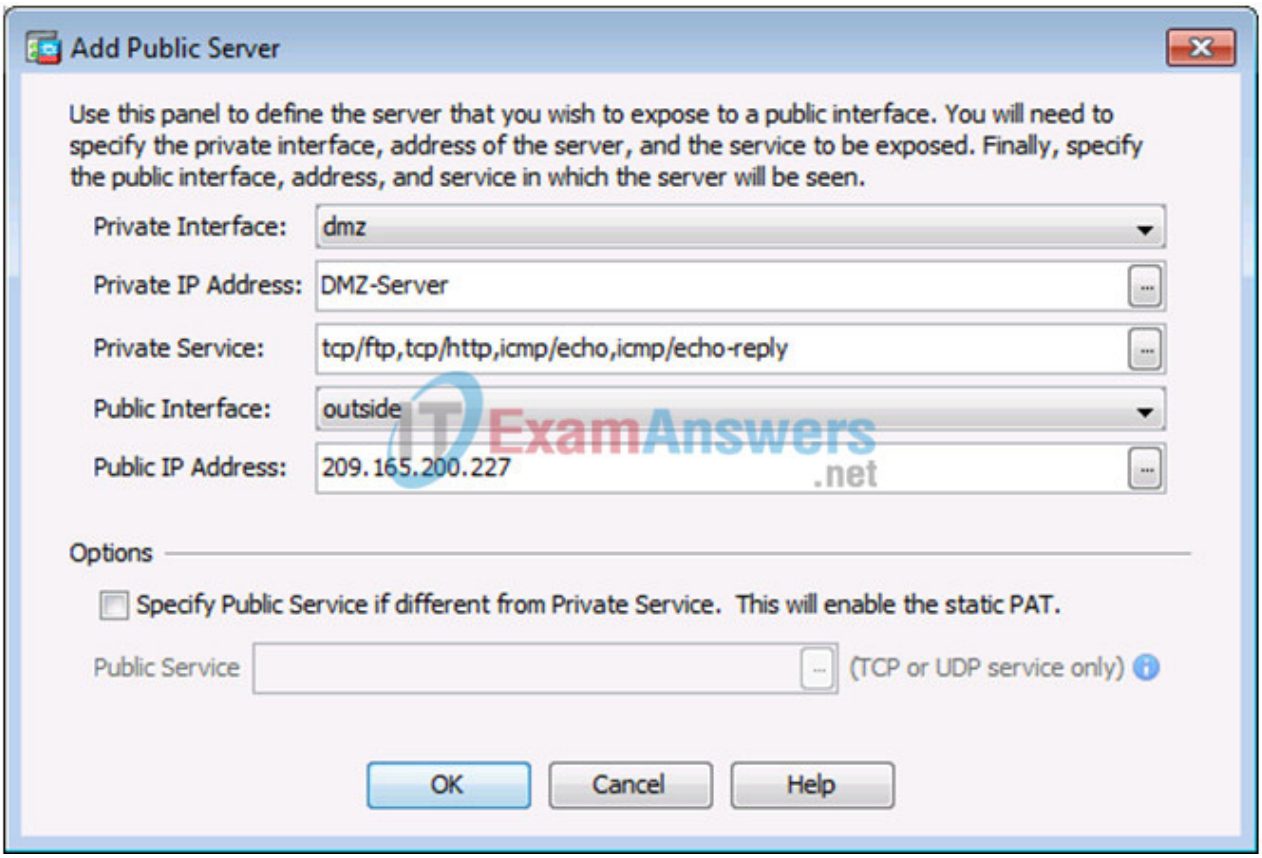
k. In the Browse Private Service window, you will double-click various services to select them and add them to the Public Service field. Double-click the following services: tcp/ftp, tcp/http, icmp/echo, and icmp/echo-reply (Note: scroll down to see all services).



l. 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.

m. When you have completed all the information in the Add Public Server dialog box, it should look like the one shown below.



n. Click OK to continue and then Apply to commit the changes.

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

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

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

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

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

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.

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.

b. Select Packet Counts and click Add to add the graph. The exhibit below shows Packet Counts added.

c. Click Show Graphs to display the graph. Initially, there is no traffic displayed.

d. 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
```

e. 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.

f. Ping from PC-B to R1 S0/0/0 at 10.1.1.1 using the –n option (number of packets) to specify 100 packets.

```
C:>\ ping 10.1.1.1 –n 100
```

Note: The response from the PC is relatively slow, and it may take a while to show up on the graph as Output Packet Count.

Reflection

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

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

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

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

Router Interface Summary Table

Router Interface Summary

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Device Configs

ASA 5506-X

```
CCNA-ASA# show run
: Saved

:
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
:
ASA Version 9.10(1)
!
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password ***** pbkdf2
names
no mac-address auto

!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet1/3
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet1/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/8
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management1/1
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
clock timezone MST -7
dns server-group DefaultDNS
 domain-name ccnasecurity.com
same-security-traffic permit inter-interface
object network DMZ-Server
 host 192.168.2.3
 description PC-A
object-group service DM_INLINE_SERVICE_0
 service-object icmp echo
 service-object icmp echo-reply
 service-object tcp destination eq ftp
 service-object tcp destination eq www
access-list outside_access extended permit object-group DM_INLINE_SERVICE_0 any4 object
DMZ-Server
pager lines 24
mtu inside 1500
mtu outside 1500
mtu dmz 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
object network DMZ-Server
 nat (dmz,outside) static 209.165.200.227
!
nat (inside,outside) after-auto source dynamic any interface
access-group outside_access in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication http console LOCAL
```

```
aaa authentication ssh console LOCAL
aaa authentication login-history
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3 255.255.255.255 outside
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd address 192.168.1.31-192.168.1.39 inside
dhcpd dns 10.20.30.40 interface inside
dhcpd domain ccnasecurity.com interface inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
username admin01 password ***** pbkdf2 privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect dns preset_dns_map
```

```
  inspect icmp
policy-map type inspect dns migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:73c5debae28a29f558cb43240eaebe6e
: end
```

Router R1

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

Current configuration : 1673 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 9 $9$P1rs5T9Im9YQKE$lCFKlTDFO3etXYLUZKWSOqz/QGzxjkhzZiJUENyJ4bI
!
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
username admin01 secret 9 $9$D96eQuJ01ZvWE.$m/ePFFlbfwd72xBHxVhrmlxsTy9IMxUa58HsDFOfA5w
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
```

```
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login local
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 exec-timeout 5 0
 logging synchronous
 login local
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Router R2

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

Current configuration : 1373 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 64000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
```

```
ip route 172.16.3.0 255.255.255.0 10.2.2.1
ip route 209.165.200.224 255.255.255.248 10.1.1.1
!
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

Router R3

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

Current configuration : 1314 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
```

```
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
control-plane
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

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