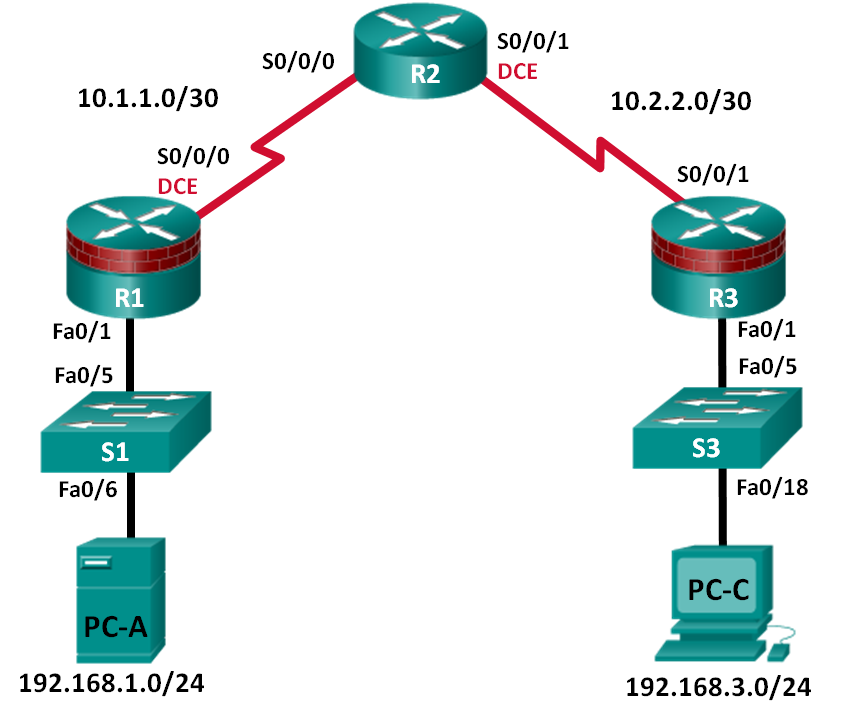
1. CCNA Security

Lab - Configuring Zone-Based Policy Firewalls

1. Topology



**Note**: ISR G2 devices have Gigabit Ethernet interfaces instead of Fast Ethernet Interfaces.

1. IP Addressing Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway | Switch Port |
| R1 | Fa0/1 | 192.168.1.1 | 255.255.255.0 | N/A | S1 Fa0/5 |
|  | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
|  | S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| R3 | Fa0/1 | 192.168.3.1 | 255.255.255.0 | N/A | S3 Fa0/5 |
|  | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S1 Fa0/6 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | S3 Fa0/18 |

1. Objectives

Part 1: Basic Router Configuration

* Configure host names, interface IP addresses, and access passwords.
* Configure the OSPF dynamic routing protocol.
* Use the Nmap port scanner to test for router vulnerabilities.

Part 2: Configuring a Zone-Based Policy Firewall (ZBF)

* Use CCP to configure a Zone-Based Policy Firewall.
* Use CCP Monitor to verify configuration.

1. Background

The most basic form of a Cisco IOS firewall uses access control lists (ACLs) to filter IP traffic and monitor established traffic patterns. This is referred to as a traditional Cisco IOS firewall.

The newer Cisco IOS Firewall implementation uses a zone-based approach that operates as a function of interfaces instead of access control list. A Zone-Based Policy Firewall (ZBF) allows different inspection policies to be applied to multiple host groups connected to the same router interface. It also has the ability to prohibit traffic via a default deny-all policy between firewall zones. ZBF is suited for multiple interfaces that have similar or varying security requirements. CCP generates a ZBF firewall by default.

In this lab, you build a multi-router network and configure the routers and hosts. You use CCP to configure a Zone-Based Policy Firewall.

**Note**: The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 15.1(4)M8 (Advanced IP Services image). 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 output produced might vary from what is shown in this lab.

**Note**: Make sure that the routers and switches have been erased and have no startup configurations.

1. Required Resources

* 3 Routers (Cisco 1841 with Cisco IOS Release 15.1(4)M8 Advanced IP Services image or comparable)
* 2 Switches (Cisco 2960 or comparable)
* 2 PCs (Windows Vista or Windows 7 with CCP 2.5, latest version of Java, Internet Explorer, and Flash Player)
* Serial and Ethernet cables, as shown in the topology
* Console cables to configure Cisco networking devices

**CCP Notes**:

* Refer to Lab 0.0.0.0 for instructions on how to install and run CCP.
* If the PC on which CCP is installed is running Windows Vista or Windows 7, it may be necessary to right-click on the CCP icon or menu item, and choose **Run as administrator**.
* In order to run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

1. Basic Router Configuration

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, dynamic routing, device access, and passwords.

**Note**: All tasks should be performed on routers R1, R2, and R3. The procedure for R1 is shown here as an example.

* 1. Configure Basic Router Settings
     1. Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

* + 1. Configure basic settings for each router.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for the serial router interfaces with a DCE serial cable attached.

R1(config)# **interface S0/0/0**

R1(config-if)# **clock rate 64000**

* + 1. Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

R1(config)# **no ip domain-lookup**

* + 1. Configure the OSPF routing protocol on R1, R2, and R3.
       1. On R1, use the following commands.

R1(config)# **router ospf 1**

R1(config-router)# **network 192.168.1.0 0.0.0.255 area 0**

R1(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

* + - 1. On R2, use the following commands.

R2(config)# **router ospf 1**

R2(config-router)# **network 10.1.1.0 0.0.0.3 area 0**

R2(config-router)# **network 10.2.2.0 0.0.0.3 area 0**

* + - 1. On R3, use the following commands.

R3(config)# **router ospf 1**

R3(config-router)# **network 192.168.3.0 0.0.0.255 area 0**

R3(config-router)# **network 10.2.2.0 0.0.0.3 area 0**

* + 1. Configure PC host IP settings.
       1. Configure a static IP address, subnet mask, and default gateway for PC-A, as shown in the IP addressing table.
       2. Configure a static IP address, subnet mask, and default gateway for PC-C, as shown in the IP addressing table.
    2. Verify basic network connectivity.
       1. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

* + - 1. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

**Note**: If you can ping from PC-A to PC-C, you have demonstrated that the OSPF routing protocol is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the **show run** and **show ip route** commands to help identify routing protocol-related problems.

* + 1. Configure a minimum password length.

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

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

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

* + 1. Configure basic console, auxiliary port, and vty lines.
       1. Configure a console password and enable login for router R1. For additional security, the exec-timeout command causes the line to log out after **5** minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

**Note**: To avoid repetitive logins during this lab, the **exec-timeout** can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

R1(config)# **line console 0**

R1(config-line)# **password ciscoconpass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **login**

R1(config-line)# **logging synchronous**

* + - 1. Configure a password for the aux port for router R1.

R1(config)# **line aux 0**

R1(config-line)# **password ciscoauxpass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **login**

* + - 1. Configure the password on the vty lines for router R1.

R1(config)# **line vty 0 4**

R1(config-line)# **password ciscovtypass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **login**

* + - 1. Repeat these configurations on both R2 and R3.
    1. Enable HTTP server.

Enabling these services allows the router to be managed using the GUI and a web browser.

R1(config)# **ip http server**

R1(config)# **ip http secure-server**

* + 1. Encrypt clear text passwords.
       1. Use the **service password-encryption** command to encrypt the console, aux, and vty passwords.

R1(config)# **service password-encryption**

* + - 1. Issue the **show run** command. Can you read the console, aux, and vty passwords? Explain.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

No. The passwords are now encrypted.

* + - 1. Repeat this configuration on both R2 and R3.
    1. Save the basic running configuration for all three routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

R1# **copy running-config startup-config**

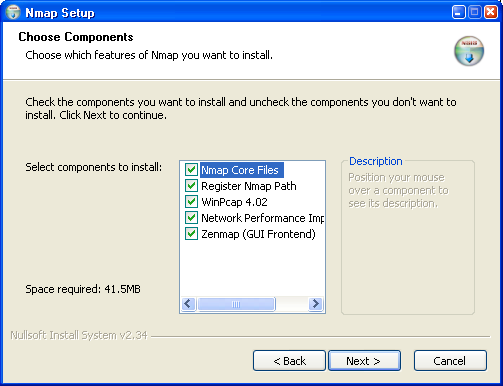
* 1. Use the Nmap Port Scanner to Determine Router Vulnerabilities

In this task, you determine open ports or services running on R1 using Nmap, before configuring a firewall.

* + 1. (Optional) Download and install Nmap and the Zenmap GUI front-end.

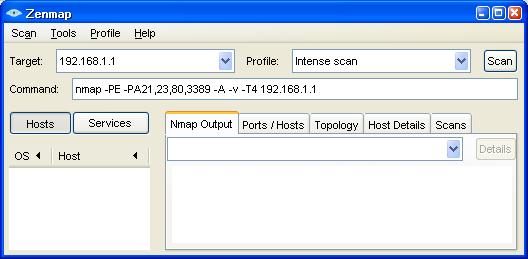
Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing.

* + - 1. If Nmap is already installed on PC-A and PC-C, go to Step 2. Otherwise, download the latest Windows version from <http://nmap.org/download.html>.
      2. On PC-A and PC-C, run the Nmap setup utility and install all components listed, including the Zenmap GUI front-end. Click **Next** to accept the defaults when prompted.

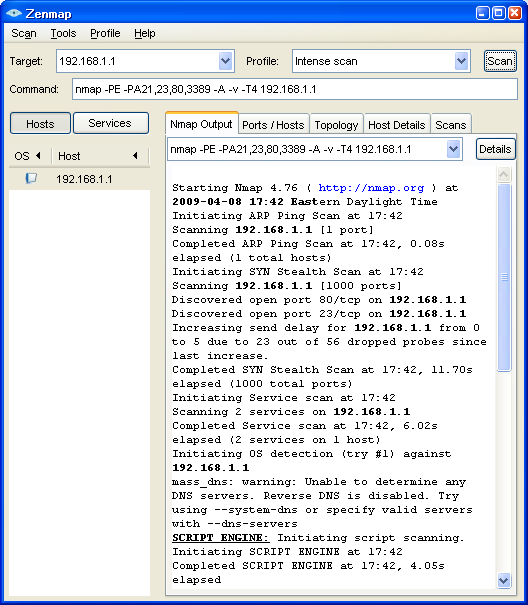


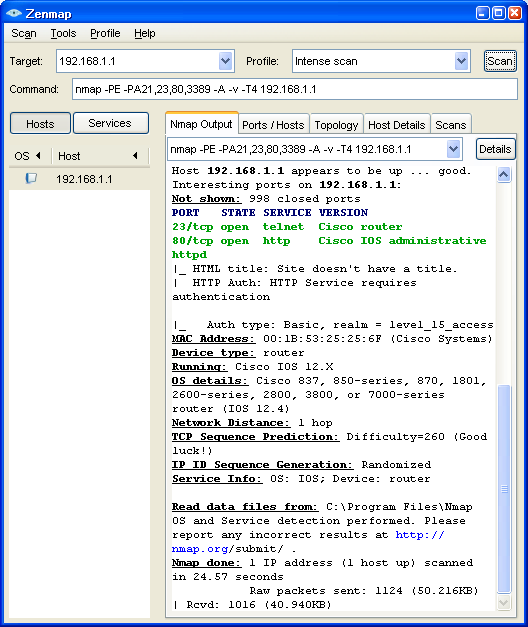
* + 1. Scan for open ports on R1 using Nmap from internal host PC-A.
       1. From internal host PC-A, start the Nmap-Zenmap application and enter the IP address of the default gateway, R1 Fa0/1 (**192.168.1.1**), as the Target. Accept the default Nmap command entered for you in the Command window and use the **Intense scan** profile.

**Note**: If the PC is running a personal firewall, it may be necessary to turn it off temporarily to obtain accurate test results.



* + - 1. Click the **Scan** button to begin the scan of R1 from internal host PC-A. Allow some time for the scan to complete. The next two screens show the entire output of the scan after scrolling.





**IOS 15 Note**: Nmap/Zenmap may not detect the correct IOS image version.

* + - 1. Click the **Service** button in the upper left side of the screen. What ports are open on R1 Fa0/1 from the perspective of internal host PC-A?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

From internal PC-A, Nmap detects open ports 23 (Telnet) and 80 (HTTP).

What is the MAC address of the R1 Fa0/1 interface?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answers will vary. For this router, it is 00:1B:53:25:25:6F.

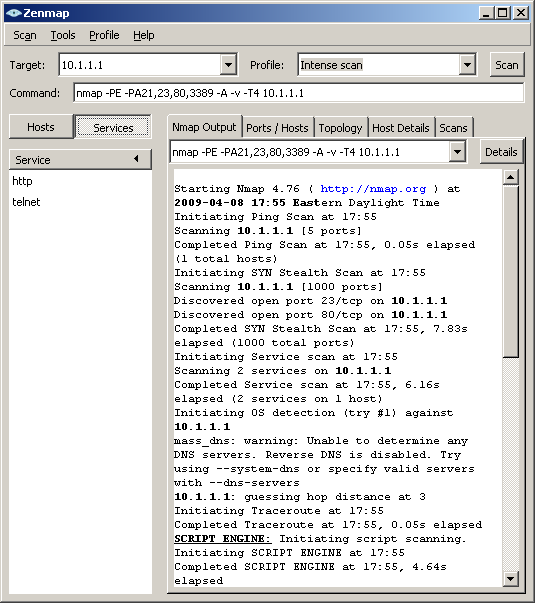
For R1, what type of device and what OS version does Nmap detect?

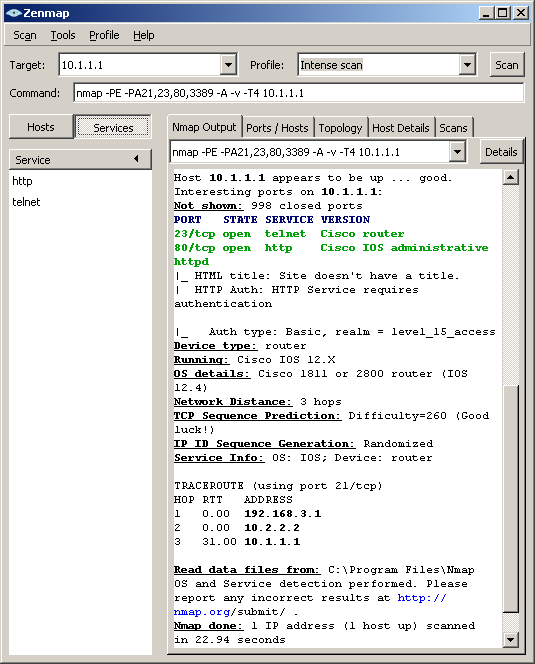
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answers may vary, but Nmap determines that R1 is a router and that it is running Cisco IOS version 12.4.

* + 1. Scan for open ports on R1 using Nmap from external host PC-C.
       1. From external host PC-C, start the Nmap-Zenmap application and enter the IP address of R1 S0/0/0 (**10.1.1.1**) as the Target. Accept the default Nmap command entered for you in the Command window and use the **Intense scan** profile.
       2. Click the **Scan** button. Allow some time for the scan to complete. The next two screens show the entire output of the scan after scrolling.





* + - 1. Click the Services button below the Command entry field. What services are running and available on R1 from the perspective of PC-C?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telnet and HTTP

* + - 1. In the Nmap scan output, refer to the TRACEROUTE information. How many hops are between PC-C and R1 and through what IP addresses did the scan have to go to reach R1?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Three hops. The scan went from PC-C to the R3 Fa0/1 default gateway (192.168.3.1) to R2 S0/0/1 (10.2.2.2) and then to R1 S0/0/0 (10.1.1.1).

1. Configuring a Zone-Based Policy Firewall (ZBF) Using CCP

In Part 2 of this lab, you configure a zone-based firewall (ZBF) on R3 by using CCP.

* 1. Verify Current Router Configurations.

In this task, you will verify end-to-end network connectivity, and R3 is configured correctly before implementing ZBF.

* + 1. Verify end-to-end network connectivity.
       1. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

* + - 1. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

* + 1. Display the R3 running configurations prior to starting CCP.
       1. Issue the **show run** command to review the current basic configuration on R3.
       2. Verify the R3 basic configuration as performed in Part 1 of the lab. Are there any security commands related to access control?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

There should not be. There is a minimum password length of 10. Login passwords and exec-timeout are defined on the console, vty, and aux lines.

* 1. Create a Zone-Based Policy Firewall

In this task, you use CCP to create a zone-based policy firewall on R3.

* + 1. Configure the enable secret password and HTTP router access prior to starting CCP.
       1. From the CLI, configure the enable secret password for use with CCP on R3.

R3(config)# **enable secret cisco12345**

* + - 1. Enable the HTTP server on R3.

R3(config)# **ip http server**

R3(config)# **ip http secure-server**

* + - 1. Add admin user to the local database.

R3(config)# **username admin privilege 15 secret cisco12345**

* + - 1. Have CCP use the local database to authenticate web sessions.

R3(config)# **ip http authentication local**

* + 1. Access CCP and discover R3.
       1. Start CCP on PC-C. In the Manage Devices window, add R3 IP address **192.168.3.1** in the first IP address field. Enter **admin** in the Username field, and **cisco12345** in the Password field.
       2. At the CCP Dashboard, click the **Discover** button to discover and connect to R3. If discovery fails, click the **Discovery Details** button to determine the problem.
    2. Use the CCP Firewall wizard to configure a zone-based firewall.
       1. Click **Monitor** > **Security** > **Firewall Status**. What is the state of the Firewall Policies?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

There is no Zone Based Firewall Policy present in the router for monitoring.

* + - 1. Click **Configure** > **Security** > **Firewall** > **Firewall**, read through the overview descriptions for the Basic and Advanced Firewall options. What are some of the key differences?

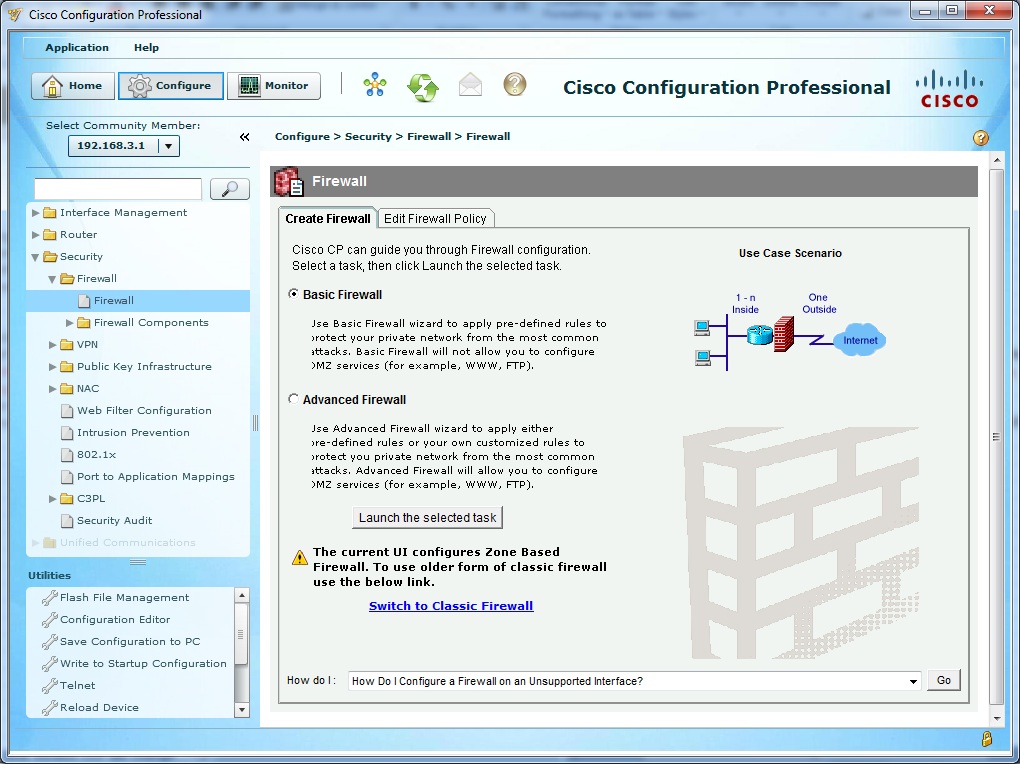
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Basic Firewall applies a predefined set of rules to protect the internal network, but does not allow the creation of a DMZ. Advanced Firewall allows predefined or customized rules to protect the internal network and also allows the configuration of DMZ services such as FTP or WWW.



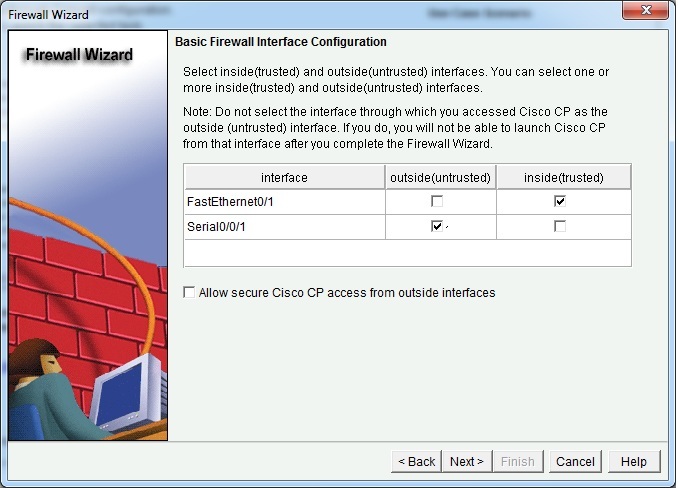
* + - 1. Choose **Basic Firewall** and click the **Launch the selected task** button.

In the Basic Firewall Configuration Wizard window, familiarize yourself with what the Basic Firewall does. What does the Basic Firewall do with traffic from outside zones to inside zones?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Deny it.

* + - 1. Click **Next** to continue.
      2. Check the **inside (trusted)** check box for **Fast Ethernet0/1** and the **outside (untrusted)** check box for **Serial0/0/1**. Click **Next**.



* + - 1. Click **OK** when the warning is displayed informing you that you cannot launch CCP from the S0/0/1 interface after the Firewall wizard completes.
      2. Move the slider between High, Medium, and Low security to familiarize yourself with what each provides. What is the main difference between High security and Medium or Low security?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

High security identifies inbound and outbound IM and peer-to-peer (P2P) traffic and drops it. This prevents these applications from being used on the network. Medium security identifies inbound and outbound IM and P2P for tracking, but does not drop it. Low security does not identify application-specific traffic, but it does inspect it to verify that it was initiated from within the internal network.

* + - 1. Move the slider to **Low Security** and click the **Preview Commands** button to preview the commands that are delivered to the router. When you are finished reviewing the commands, click **Close** and then click **Next**.
      2. Review the Firewall Configuration Summary. What does this display provide?

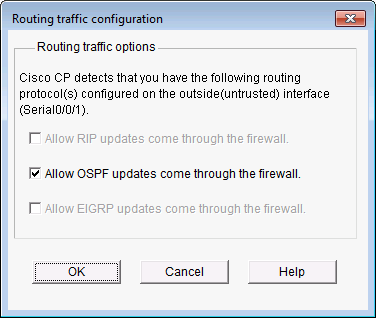
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A textual description (no commands) of what the Firewall wizard does based on the selections that you made.

* + - 1. Click **Finish** to complete the Firewall wizard.
      2. When the Routing traffic configuration window displays, ensure that the check box **Allow OSPF updates come through the firewall** is checked and click **OK**.

**Note**: This screen only displays if a dynamic routing protocol is configured.



What would happen if this box was not checked?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

OSPF routing updates from R2 would be blocked at the firewall, and R3 would not learn about the 10.1.1.0/30 or 192.168.1.0/24 networks.

* + - 1. In addition to OSPF, for what other routing protocols does the firewall allow updates?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

RIP and EIGRP

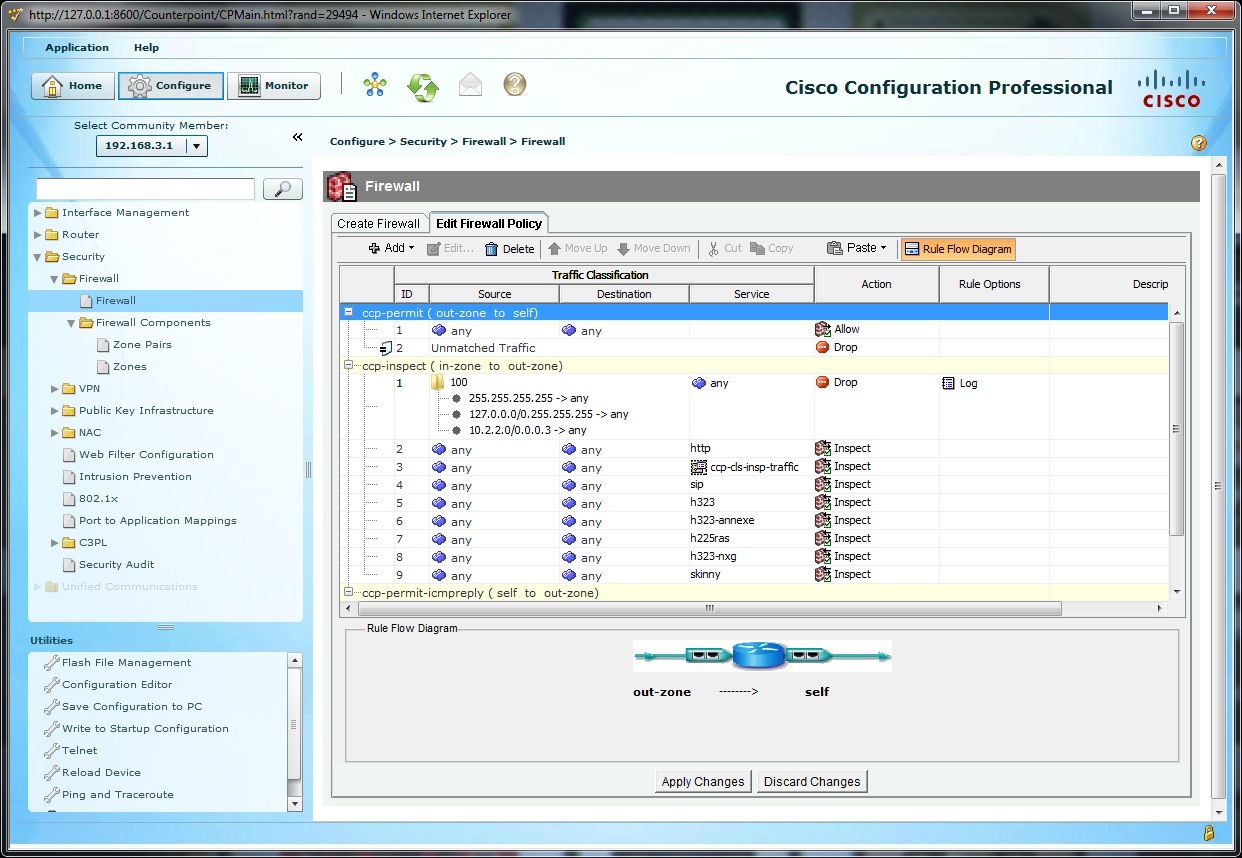
* + - 1. In the Deliver Configuration to Router window, click **Deliver**.
      2. Click **OK** in the Commands Delivery Status window. How many commands were generated by the Firewall wizard?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

145 commands with CCP 2.5.

* + - 1. Click **OK** to display the message that you have successfully configured a firewall on the router. Click **OK** to close the message window.
      2. The Edit Firewall Policy window displays with the Rule Diagram.



In the Rule Diagram, locate access list 100 (folder icon). What action is taken and what rule options are applied for traffic with an invalid source address in the 127.0.0.0/8 address range?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Traffic is dropped and logged.

* 1. Review the Zone-Based Firewall Configuration
     1. Examine the R3 running configuration with the CLI.
        1. From the R3 CLI, display the running configuration to view the changes that the CCP Basic Firewall wizard made to the router.
        2. The following commands are related to ACL 100 and class-map ccp-invalid-source.

class-map type inspect match-all ccp-invalid-src

match access-group 100

<output omitted>

policy-map type inspect ccp-inspect

class type inspect ccp-invalid-src

drop log

<output omitted>

access-list 100 remark CCP\_ACL Category=128

access-list 100 permit ip host 255.255.255.255 any

access-list 100 permit ip 127.0.0.0 0.255.255.255 any

access-list 100 permit ip 10.2.2.0 0.0.0.3 any

<output omitted>

* + - 1. In ACL 100, notice that the source addresses listed are permitted. The ACL uses **permit** statements to identify these addresses as a group so that they can be matched with the **class-map type inspect match-all ccp-invalid-src** command and then dropped and logged by the **class type inspect ccp-invalid-src** command, which is one of the class types specified for the **ccp-inspect** policy-map.
      2. Issue the command **show run | beg OSPF** to display the running configuration beginning with the line that contains the first occurrence of OSPF. Continue to press **Enter** until you see all the commands in the firewall configuration that are related to OSPF routing protocol updates on R3. You should see the following commands:

R3# **show run | beg OSPF**

class-map type inspect match-any SDM\_OSPF

match access-group name SDM\_OSPF

class-map type inspect match-any ccp-cls-insp-traffic

match protocol cuseeme

match protocol dns

match protocol ftp

match protocol https

<output omitted>

class-map type inspect match-all SDM\_OSPF\_PT

match class-map SDM\_OSPF\_TRAFFIC

class-map type inspect match-any ccp-h323-inspect

match protocol h323

class-map type inspect match-all ccp-invalid-src

match access-group 100

class-map type inspect match-all ccp-icmp-access

match class-map ccp-cls-icmp-access

class-map type inspect match-any ccp-sip-inspect

match protocol sip

class-map type inspect match-all ccp-protocol-http

match protocol http

<output omitted>

policy-map type inspect ccp-permit

class type inspect SDM\_OSPF\_PT

pass

class class-default

drop

<output omitted>

* + 1. Use CCP to examine the R3 firewall configuration.
       1. Click the **Configure** button and choose **Router** > **ACL** > **Firewall Rules**. There should be an ACL that lists fake source addresses, such as the broadcast address of 255.255.255.255 and the 127.0.0.0/8 network. These were identified in the running configuration output in Task 3, Step 1b.
       2. Click the **Configure** button and choose **Security** > **Firewall** > **Firewall Components** > **Zones** to verify the zones configuration. What interfaces are listed and with which zones are they associated?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Interface Serial0/0/1 is in zone **out-zone**, and interface FastEthernet0/1 is in zone **in-zone**.

* + - 1. Click **Configure** and choose **Security** > **Firewall** > **Firewall Components** > **Zones Pairs** to verify the zone pairs configuration. Fill in the following information.

|  |  |  |  |
| --- | --- | --- | --- |
| Zone Pair | Source | Destination | Policy |
| ccp-zp-out-self | out-zone | self | ccp-permit |
| ccp-zp-in-out | in-zone | out-zone | ccp-inspect |
| ccp-zp-self-out | Self | out-zone | ccp-permit-icmpreply |

* + - 1. What is C3PL short for?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cisco Common Classification Policy Language

* + - 1. Click **Configure** and choose **Security** > **C3PL** > **Class Map** > **Inspection**. How many class maps were created by the CCP Firewall wizard?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

15

* + - 1. Choose **Security** > **C3PL** > **Policy Map** > **Protocol Inspection**. How many policy maps were created by the CCP Firewall wizard?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3

* + - 1. Examine the details for the policy map ccp-permit that is applied to the ccp-zp-out-self zone pair. Fill in the information below. List the action for the traffic matching each of the class maps referenced within the ccp-permit policy map.

**Match Class Name**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ SDM\_OSPF\_PT **Action**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Pass

**Match Class Name**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ class-default **Action**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Drop

* 1. Verify OSPF Routing Functionality on R3
     1. Display the R3 routing table using the CLI.

In Task 2, Step 3, the Firewall wizard configured the router to allow OSPF updates. Verify that OSPF messages are still being exchanged using the **show ip route** command and verify that there are still OSPF learned routes in the routing table.

R3# **show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/30 is subnetted, 2 subnets

C 10.2.2.0 is directly connected, Serial0/0/1

O 10.1.1.0 [110/128] via 10.2.2.2, 01:55:30, Serial0/0/1

O 192.168.1.0/24 [110/129] via 10.2.2.2, 01:54:53, Serial0/0/1

C 192.168.3.0/24 is directly connected, FastEthernet0/1

What are the networks on R3 that were learned via the OSPF routing protocol?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10.1.1.0/30 and 192.168.1.0/24

* 1. Verify Zone-Based Firewall Functionality
     1. From PC-C, ping the R3 internal LAN interface.

From PC-C, ping the R3 interface Fa0/1 at IP address 192.168.3.1.

C:\> **ping 192.168.3.1**

Were the pings successful? Explain.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Yes. The PC-C IP address and the R3 Fa0/1 IP address are on the same internal network, and the firewall does not come into play. The R3 Fa0/1 IP address is the default gateway of PC-C.

* + 1. From PC-C, ping the R2 external WAN interface.

From PC-C, ping the R2 interface S0/0/1 at IP address 10.2.2.2.

C:\> **ping 10.2.2.2**

Were the pings successful? Explain.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Yes. ICMP echo replies are allowed by the ccp-permit-icmpreply policy.

* + 1. From R2, ping PC-C.
       1. From external router R2, ping PC-C at IP address 192.168.3.3.

R2# **ping 192.168.3.3**

* + - 1. Were the pings successful? Explain.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

No. The ping was initiated from outside R2 S0/0/1 and was blocked.

* + 1. Telnet from R2 to R3.

From router R2, telnet to R3 at IP address 10.2.2.1.

R2# **telnet 10.2.2.1**

Trying 10.2.2.1 ... Open

Trying 10.2.2.1 ...

% Connection timed out; remote host not responding

Why was Telnet unsuccessful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telnet was initiated from outside R2 S0/0/1 and was blocked.

* + 1. Telnet from internal PC-C to external router R2.
       1. From PC-C on the R3 internal LAN, telnet to R2 at IP address 10.2.2.2 and log in.

C:\> **telnet 10.2.2.2**

User Access verification

Password: **ciscovtypass**

* + - 1. Issue the **show policy-map type inspect zone-pair sessions** command on R3. Continue pressing **Enter** until you see an Inspect Established Session section toward the end. Your output should look similar to the following.

R3# **show policy-map type inspect zone-pair sessions**

<output omitted>

Inspect

Number of Established Sessions = 1

Established Sessions

Session 657344C0 (192.168.3.3:1274)=>(10.2.2.2:23) tacacs:tcp SIS\_OPEN

Created 00:01:20, Last heard 00:01:13

Bytes sent (initiator:responder) [45:65]

<output omitted>

* + - 1. In the Established Sessions in the output, what is the source IP address and port number for your Established Sessions?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

192.168.3.3 and port 1247. The port number may vary.

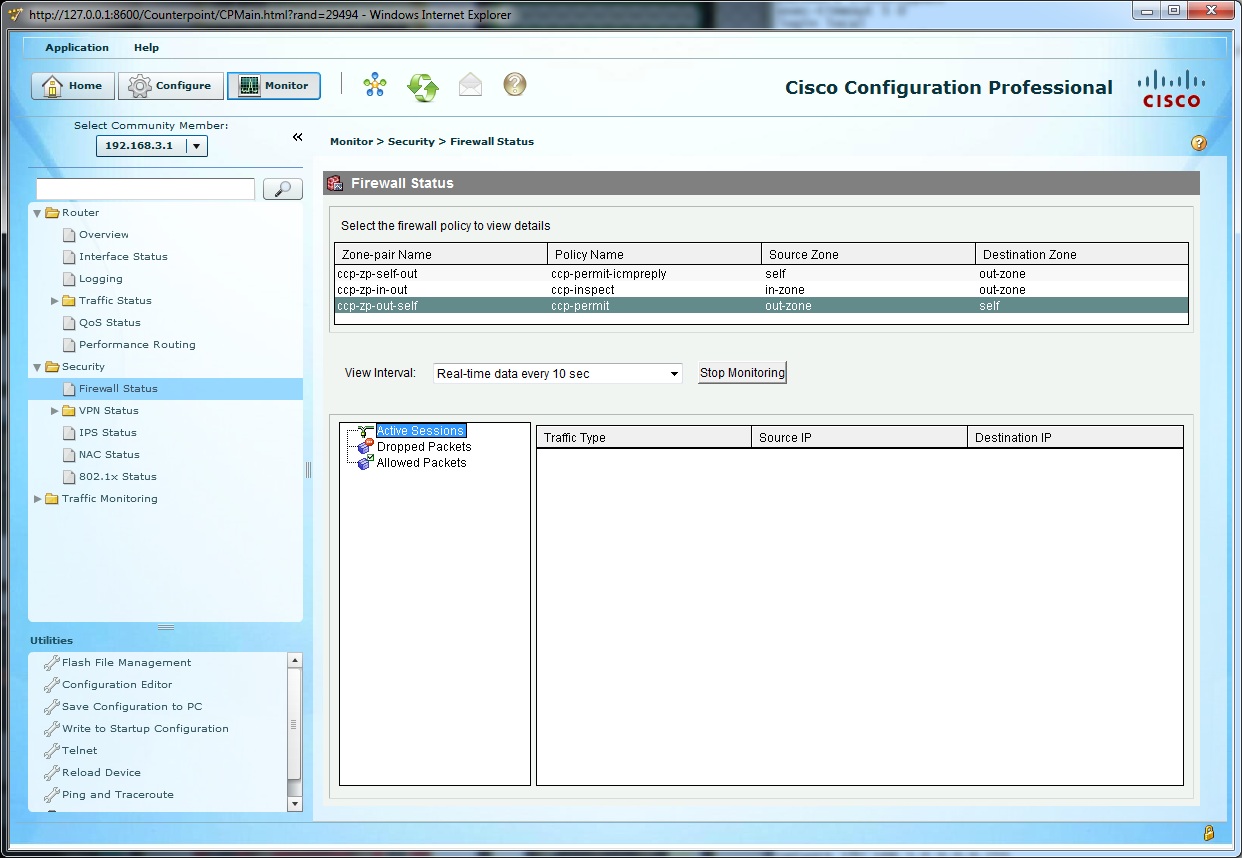
* + - 1. What is the destination IP address and port number for your established sessions?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

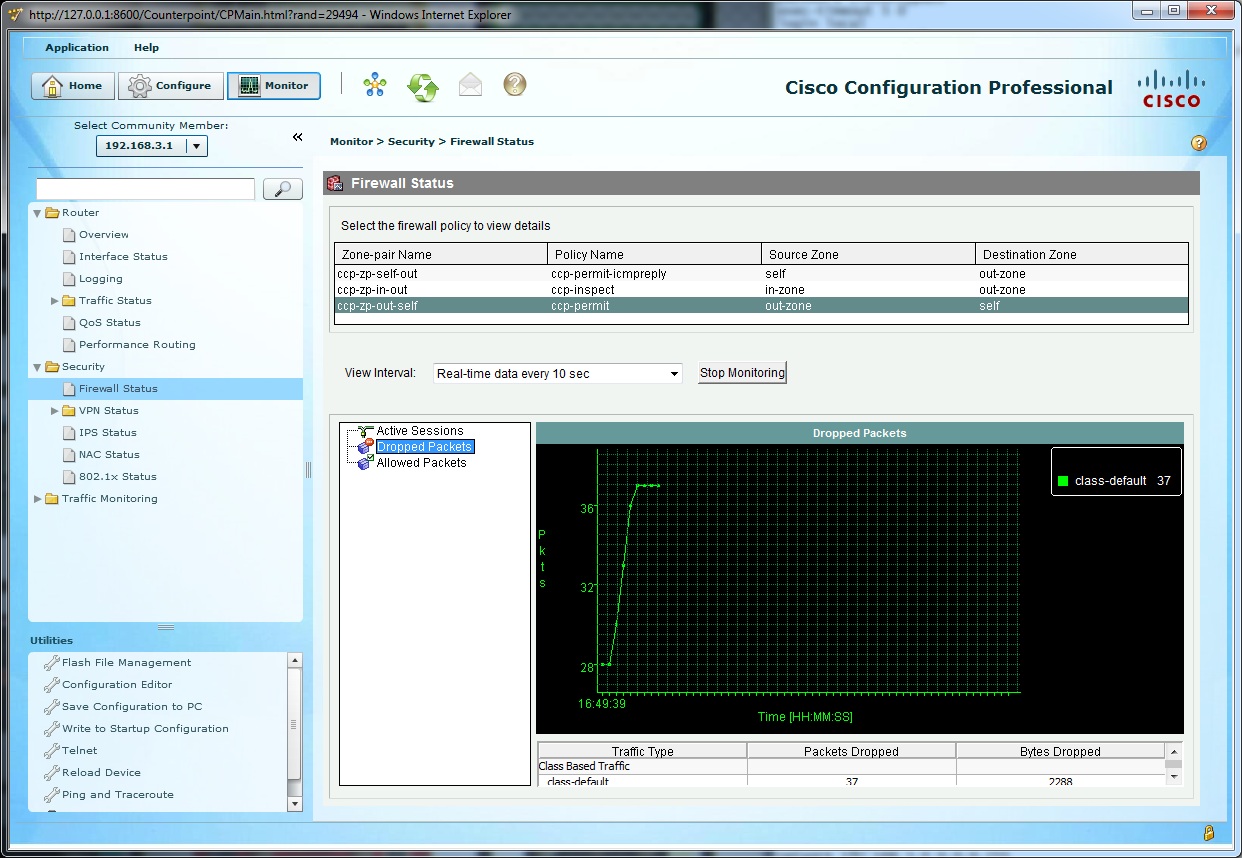
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10.2.2.2 and port 23 (telnet).

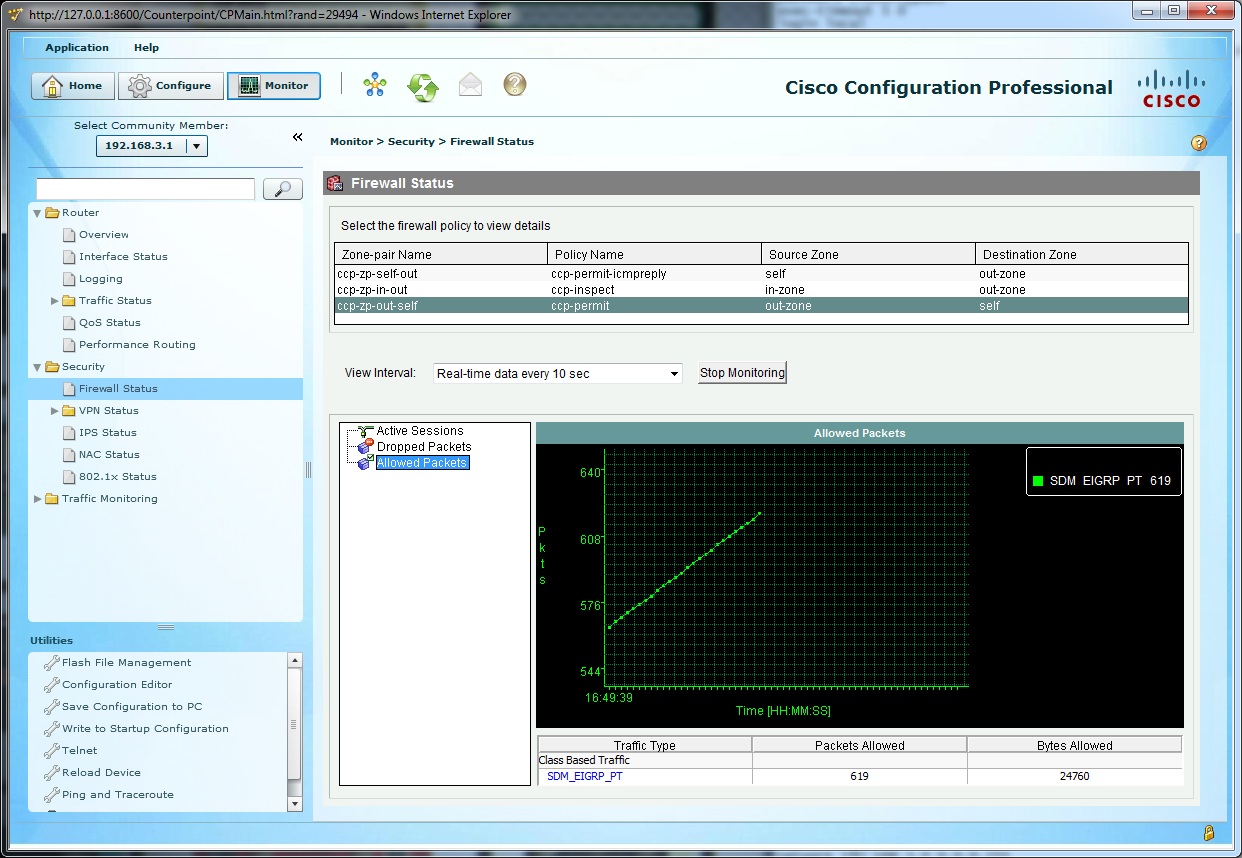
* + 1. Use CCP Monitor to verify the ZBF function.
       1. From CCP, click the **Monitor** button at the top of the screen and choose **Security** > **Firewall Status**.
       2. Choose the **ccp-zp-out-self** policy from the list of policies. This policy applies to traffic from the outside zone to the router (self) zone.
       3. Verify that **Active Sessions** is selected and that the view interval is set to **Real-time data every 10 sec**. Click the **Monitor Policy** button to start monitoring traffic from outside the zone to inside the zone.



* + - 1. From the R2 CLI, ping the R3 S0/0/1 interface at IP address **10.2.2.1**. The pings should fail.
      2. From the R2 CLI, telnet to the R3 S0/0/1 interface at IP address **10.2.2.1**. The Telnet attempt should fail.
      3. Click the **Dropped Packets** option and observe the graph showing the number of dropped packets resulting from the failed ping and Telnet attempts. Your screen should look similar to the one below.



* + - 1. Click the **Allowed Packets** option and observe the graph showing the number of OSPF packets received from router R3. This number will continue to grow at a steady pace as OSPF updates are received from R2.



* + - 1. Click the **Stop Monitoring** button and close CCP.

1. Reflection

What are some factors to consider when configuring firewalls using traditional manual CLI methods compared to using the CCP Firewall wizard GUI methods?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answers will vary but could include the following:

Traditional CLI methods are time-consuming and prone to keystroke errors. They also require the administrator to have an extensive knowledge of ACLs and Cisco IOS security command syntax.

CCP gives the maximum flexibility and greatly simplifies firewall configuration, especially for multiple routers with multiple interfaces and where DMZ services are needed.

1. 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. | | | | |

1. Basic Router Configs - Part 1

**Note**: ISR G2 devices have GigabitEthernet interfaces instead of FastEthernet Interfaces.

1. Router R1 after Part 1

R1# **show run**

Building configuration...

Current configuration : 1385 bytes

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

logging message-counter syslog

!

no aaa new-model

dot11 syslog

ip source-route

!

ip cef

no ip domain lookup

!

no ipv6 cef

multilink bundle-name authenticated

!

!

!

archive

log config

hidekeys

!

interface FastEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet0/1/0

!

interface FastEthernet0/1/1

!

interface FastEthernet0/1/2

!

interface FastEthernet0/1/3

!

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

clock rate 2000000

!

router ospf 1

log-adjacency-changes

network 10.1.1.0 0.0.0.3 area 0

network 192.168.1.0 0.0.0.255 area 0

!

ip forward-protocol nd

ip http server

ip http secure-server

!

control-plane

!

line con 0

exec-timeout 5 0

password 7 14141B180F0B29242A38322631

logging synchronous

login

line aux 0

exec-timeout 5 0

password 7 045802150C2E4D5B1109040401

login

line vty 0 4

exec-timeout 5 0

password 7 05080F1C2243581D0015160118

login

!

scheduler allocate 20000 1000

end

1. Router R2 after Part 1

R2# **show run**

Building configuration...

Current configuration : 1369 bytes

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

logging message-counter syslog

!

no aaa new-model

dot11 syslog

ip source-route

!

ip cef

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

!

archive

log config

hidekeys

!

interface FastEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet0/1

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

!

router ospf 1

log-adjacency-changes

network 10.1.1.0 0.0.0.3 area 0

network 10.2.2.0 0.0.0.3 area 0

!

ip forward-protocol nd

no ip http server

no ip http secure-server

!

!

control-plane

!

line con 0

exec-timeout 5 0

password 7 05080F1C22434D061715160118

logging synchronous

login

line aux 0

exec-timeout 5 0

password 7 104D000A0618131E14142B3837

login

line vty 0 4

exec-timeout 5 0

password 7 02050D4808091935555E080A16

login

!

scheduler allocate 20000 1000

end

1. Router R3 after Part 1

R3# **show run**

Building configuration...

Current configuration : 1347 bytes

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R3

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

logging message-counter syslog

!

no aaa new-model

dot11 syslog

ip source-route

!

ip cef

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

!

archive

log config

hidekeys

!

interface FastEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 192.168.3.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

!

router ospf 1

log-adjacency-changes

network 10.2.2.0 0.0.0.3 area 0

network 192.168.3.0 0.0.0.255 area 0

!

ip forward-protocol nd

ip http server

no ip http secure-server

!

control-plane

!

line con 0

exec-timeout 5 0

password 7 01100F17580405002F5C4F1A0A

logging synchronous

login

line aux 0

exec-timeout 5 0

password 7 094F471A1A0A1607131C053938

login

line vty 0 4

exec-timeout 5 0

password 7 14141B180F0B3C3F3D38322631

login

!

scheduler allocate 20000 1000

end

1. Router R3 after Part 2

R3# **show run**

Building configuration...

Current configuration : 6267 bytes

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R3

!

boot-start-marker

boot system usbflash0:c1841-advipservicesk9-mz.124-24.T8.bin

boot-end-marker

!

security passwords min-length 10

logging message-counter syslog

enable secret 5 $1$oO2u$.uF0cRnoBIjrUFVmU.bHc1

!

no aaa new-model

memory-size iomem 15

dot11 syslog

ip source-route

!

ip cef

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

crypto pki token default removal timeout 0

!

crypto pki trustpoint TP-self-signed-3204056323

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-3204056323

revocation-check none

rsakeypair TP-self-signed-3204056323

!

crypto pki certificate chain TP-self-signed-3204056323

certificate self-signed 01

3082023A 308201A3 A0030201 02020101 300D0609 2A864886 F70D0101 04050030

31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

69666963 6174652D 33323034 30353633 3233301E 170D3039 30323037 30323132

35375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649

4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 32303430

35363332 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281

8100A6F5 48106BE2 E85C3E1D 620F21F5 9D458C5D A50A4DD7 C915904F C87A9A77

91EF2175 9F3107EC 44BDF2A3 10A69717 643FA74A 97668C41 5893A05B 523C9E7A

0F1912C3 94B9C7CF F1D7986B 5C3FD781 ED0D53C9 DFE6E169 265CCE28 566D1C27

9281C2F4 2B22A6F5 2302C5BC E90B5423 37EA1353 9F4EE2BB 0DCDD199 7CE6DF66

9B270203 010001A3 62306030 0F060355 1D130101 FF040530 030101FF 300D0603

551D1104 06300482 02523330 1F060355 1D230418 30168014 79522D04 DBD7C96D

9E605DB4 9CD5EC3A BB7C5568 301D0603 551D0E04 16041479 522D04DB D7C96D9E

605DB49C D5EC3ABB 7C556830 0D06092A 864886F7 0D010104 05000381 810070E5

48D84F8A F4DF287C BFACFC96 0CE7B88D 928D8DF5 88CE3466 3A1091F3 E5FE4642

32DFFBD3 47AEFA38 2F60E8DB D3FE827B ED5D4E35 70F0F46E CD2BB5CA 62A0BB32

75C69791 DFAF41BF ACA15824 CD654935 E8180FD6 441F0BB4 CE7A01B5 9B90AFA8

807F0AA8 56A755C8 2CF7C07D 483FCFCA DE1BA13C 1BF17851 32070758 C588

quit

!

username admin privilege 15 secret 5 $1$IIJe$y70/S3F40l43w18k0yDEY0

archive

log config

hidekeys

!

class-map type inspect match-any ccp-skinny-inspect

match protocol skinny

class-map type inspect match-any SDM\_OSPF

match access-group name SDM\_OSPF

class-map type inspect match-any ccp-cls-insp-traffic

match protocol cuseeme

match protocol dns

match protocol ftp

match protocol https

match protocol icmp

match protocol imap

match protocol pop3

match protocol netshow

match protocol shell

match protocol realmedia

match protocol rtsp

match protocol smtp extended

match protocol sql-net

match protocol streamworks

match protocol tftp

match protocol vdolive

match protocol tcp

match protocol udp

class-map type inspect match-all ccp-insp-traffic

match class-map ccp-cls-insp-traffic

class-map type inspect match-any SDM\_OSPF\_TRAFFIC

match class-map SDM\_OSPF

class-map type inspect match-any ccp-h323nxg-inspect

match protocol h323-nxg

class-map type inspect match-any ccp-cls-icmp-access

match protocol icmp

match protocol tcp

match protocol udp

class-map type inspect match-any ccp-h225ras-inspect

match protocol h225ras

class-map type inspect match-any ccp-h323annexe-inspect

match protocol h323-annexe

class-map type inspect match-all SDM\_OSPF\_PT

match class-map SDM\_OSPF\_TRAFFIC

class-map type inspect match-any ccp-h323-inspect

match protocol h323

class-map type inspect match-all ccp-invalid-src

match access-group 100

class-map type inspect match-all ccp-icmp-access

match class-map ccp-cls-icmp-access

class-map type inspect match-any ccp-sip-inspect

match protocol sip

class-map type inspect match-all ccp-protocol-http

match protocol http

!

policy-map type inspect ccp-permit-icmpreply

class type inspect ccp-icmp-access

inspect

class class-default

pass

policy-map type inspect ccp-inspect

class type inspect ccp-invalid-src

drop log

class type inspect ccp-protocol-http

inspect

class type inspect ccp-insp-traffic

inspect

class type inspect ccp-sip-inspect

inspect

class type inspect ccp-h323-inspect

inspect

class type inspect ccp-h323annexe-inspect

inspect

class type inspect ccp-h225ras-inspect

inspect

class type inspect ccp-h323nxg-inspect

inspect

class type inspect ccp-skinny-inspect

inspect

class class-default

drop

policy-map type inspect ccp-permit

class type inspect SDM\_OSPF\_PT

pass

class class-default

drop

!

zone security in-zone

zone security out-zone

zone-pair security ccp-zp-self-out source self destination out-zone

service-policy type inspect ccp-permit-icmpreply

zone-pair security ccp-zp-in-out source in-zone destination out-zone

service-policy type inspect ccp-inspect

zone-pair security ccp-zp-out-self source out-zone destination self

service-policy type inspect ccp-permit

!

interface FastEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface FastEthernet0/1

description $FW\_INSIDE$

ip address 192.168.3.1 255.255.255.0

zone-member security in-zone

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

description $FW\_OUTSIDE$

ip address 10.2.2.1 255.255.255.252

zone-member security out-zone

!

router ospf 1

log-adjacency-changes

network 10.2.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

!

ip forward-protocol nd

ip http server

ip http authentication local

ip http secure-server

!

ip access-list extended SDM\_OSPF

remark CCP\_ACL Category=1

permit ospf any any

!

access-list 100 remark CCP\_ACL Category=128

access-list 100 permit ip host 255.255.255.255 any

access-list 100 permit ip 127.0.0.0 0.255.255.255 any

access-list 100 permit ip 10.2.2.0 0.0.0.3 any

!

control-plane

!

line con 0

exec-timeout 5 0

password 7 05080F1C22434D061715160118

logging synchronous

login

line aux 0

exec-timeout 5 0

password 7 0822455D0A1604020A1B0D1739

login

line vty 0 4

exec-timeout 5 0

password 7 045802150C2E5A5A1009040401

login

transport input all

!

scheduler allocate 20000 1000

end