PT Activity: Configuring a Zone-Based Policy Firewall (ZPF)

**Addressing Table**

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- |
| R1 | Fa0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| S0/0/0 | 10.1.1.1 | 255.255.255.252 | N/A |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| S0/0/1 | 10.2.2.2 | 255.255.255.252 | N/A |
| R3 | Fa0/1 | 192.168.3.1 | 255.255.255.0 | N/A |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 |

**Learning Objectives**

·         Verify connectivity among devices before firewall configuration.

·         Configure a zone-based policy (ZPF) firewall on router R3

·         Verify ZPF firewall functionality using ping, Telnet and a web browser.

**Introduction**

Zone-based policy (ZPF) firewalls are the latest development in the evolution of Cisco firewall technologies. In this activity, you configure a basic ZPF on an edge router R3 that allows internal hosts access to external resources and blocks external hosts from accessing internal resources. You then verify firewall functionality from internal and external hosts.

The routers have been pre-configured with the following:

·         Console password: **ciscoconpa55**

·         Password for vty lines: **ciscovtypa55**

·         Enable password: **ciscoenpa55**

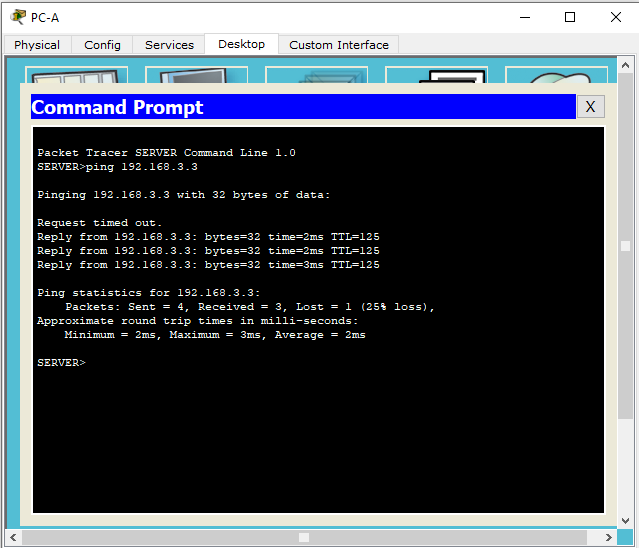
·         Host names and IP addressing

·         Static routing

**Task 1: Verify Basic Network Connectivity**

Verify network connectivity prior to configuring the zone-based policy firewall.

**Step 1. From the PC-A command prompt, ping PC-C at 192.168.3.3.**

****

**Step 2. From the PC-C command prompt, Telnet to the Router R2 S0/0/1 interface at 10.2.2.2. Exit the Telnet session.**

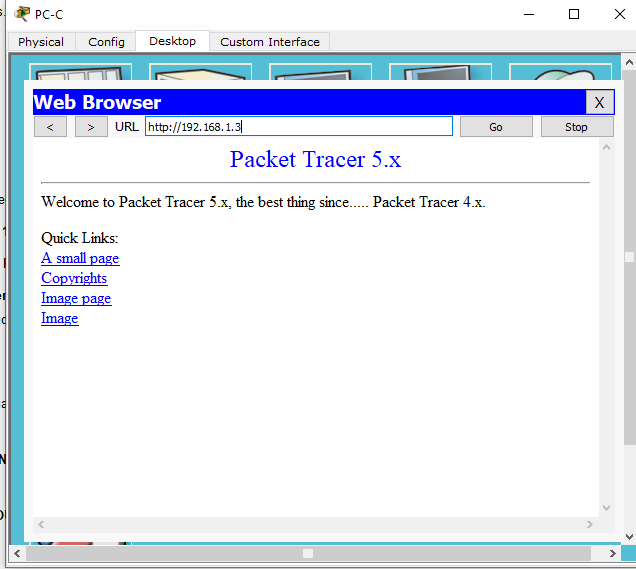
**A screenshot of a computer

Description automatically generated**

**Step 3. From PC-C, open a web browser to the PC-A server.**

Click the **Desktop** tab and click the **Web Browser** application. Enter the PC-A IP address 192.168.1.3 as the URL. The Packet Tracer 5.x welcome page from the web server should be displayed.

Close the browser on PC-C.



**Task 2: Create the Firewall Zones on Router R3**

**Note**: For all configuration tasks, be sure to use the exact names as specified.

**Step 1. Create an internal zone.**

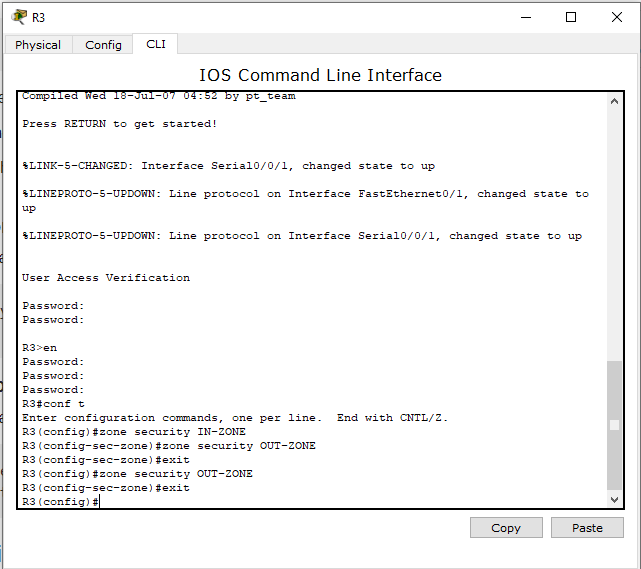
Use the **zone security** command to create a zone named **IN-ZONE**.

Graphical user interface, text, application, email

Description automatically generated

**Step 2. Step 2. Create an external zone.**

Use the **zone security** command to create a zone named **OUT-ZONE**.



**Task 3: Define a Traffic Class and Access List**

**Step 1. Create an ACL that defines internal traffic.**

Use the **access-list** command to create extended ACL **101**to permit all IP protocols from the **192.168.3.0/24** source network to any destination.

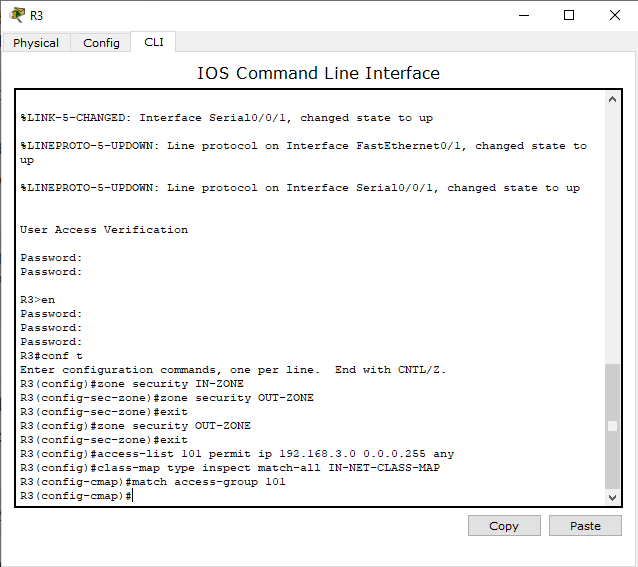
Graphical user interface, text, application, email

Description automatically generated

**Step 2. Create a class map referencing the internal traffic ACL.**

Use the **class map type inspect** command with the match-all option to create a class map named **IN-NET-CLASS-MAP**. Use the **match access-group** command to match ACL **101**.

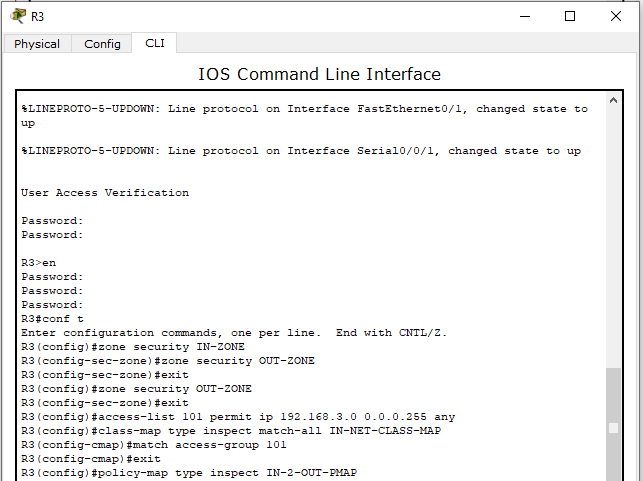
**Note:** Although not supported in this Packet Tracer exercise, individual protocols (HTTP, FTP, etc.) can be specific to be matched using the **match-any** option in order to provide more precise control over what type of traffic is inspected.



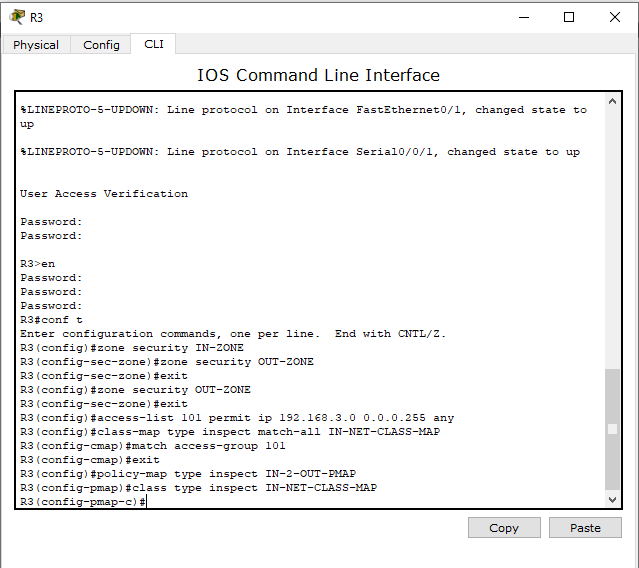
**Task 4: Specify Firewall Policies**

**Step 1. Create a policy map to determine what to do with matched traffic.**

Use the **policy-map type inspect** command and create a policy map named **IN-2-OUT-PMAP**.



**Step 2. Specify a class type of inspect and reference class map IN-NET-CLASS-MAP.**

****

**Step 3. Specify the action of inspect for this policy map .**

The use of the **inspect** command invokes context-based access control (other options include pass and drop).

R3(config-pmap-c)# **inspect**

%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be inspected.

Graphical user interface, text, application

Description automatically generated

Issue the **exit** command twice to leave **config-pmap-c** mode and return to **config** mode.

R3(config-pmap-c)# **exit**

R3(config-pmap)# **exit**

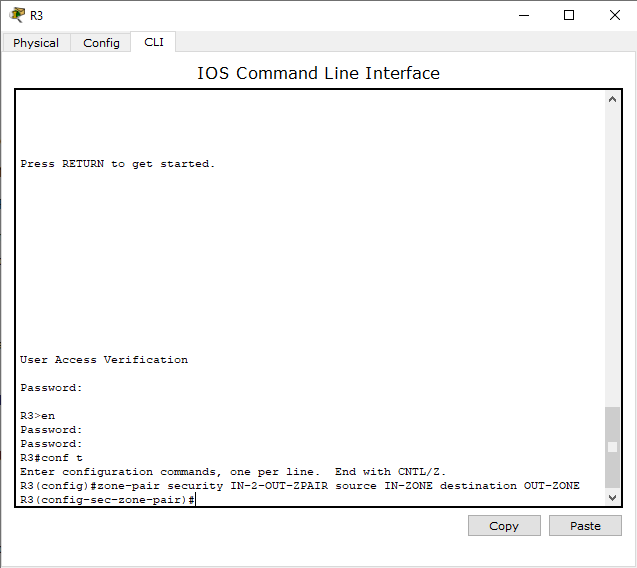
**Graphical user interface, text, application

Description automatically generated**

**Task 5: Apply Firewall Policies**

**Step 1. Create a pair of zones.**

Using the **zone-pair security** command, create a zone pair named **IN-2-OUT-ZPAIR**. Specify the source and destination zones that were created in Task 1.



**Step 2. Specify the policy map for handling the traffic between the two zones.**

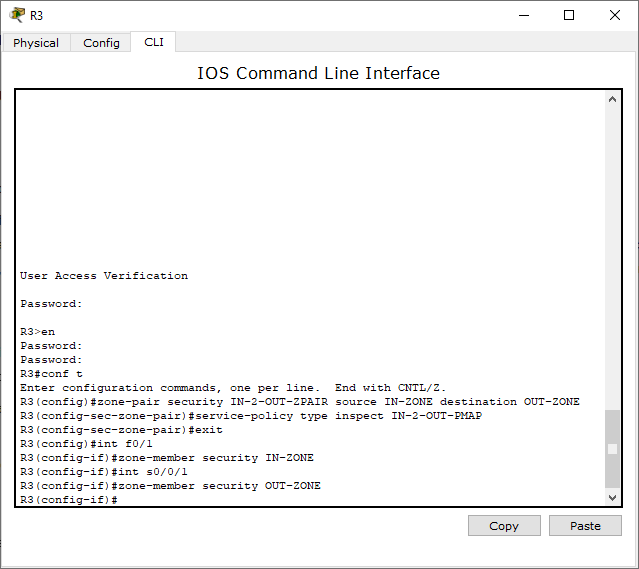
Attach a policy-map and its associated actions to the zone pair using the **service-policy type inspect** command and reference the policy map previously created, **IN-2-OUT-PMAP**.

Graphical user interface, text, application, email

Description automatically generated

**Step 3. Assign interfaces to the appropriate security zones.**

Use the **zone-member security** command in interface config mode to assign Fa0/1 to **IN-ZONE** and S0/0/1 to **OUT-ZONE**.



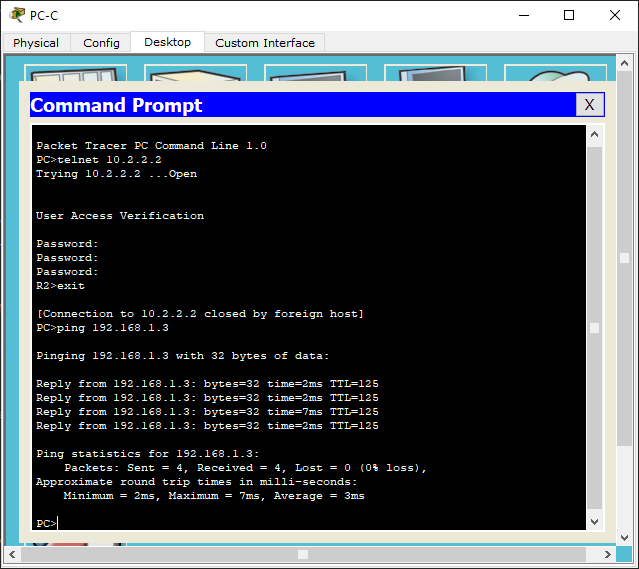
**Step 4. Copy the running config to the startup config.**

**Task 6: Test Firewall Functionality from IN-ZONE to OUT-ZONE**

Verify that internal hosts can still access external resources after configuring the zone-based policy firewall.

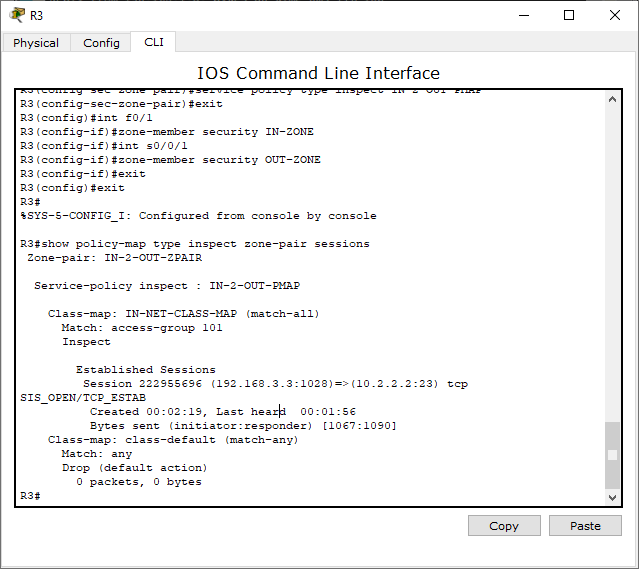
**Step 1. From internal PC-C, ping the external PC-A server.**

From the PC-C Command Prompt, ping PC-A at 192.168.1.3. The ping should succeed.



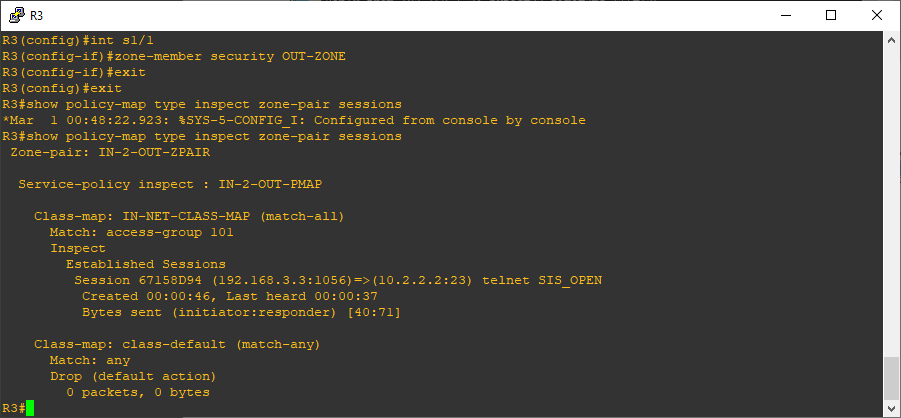
**Step 2. From internal PC-C, Telnet to the router R2 S0/0/1 interface.**

From the PC-C Command Prompt, telnet to R2 at 10.2.2.2 and provide the vty password **ciscovtypa55**. The telnet should succeed. While the Telnet session is active, issue the command **show policy-map type inspect zone-pair sessions** on R3 to view established sessions.



What is the source IP address and port number? 192.168.3.3:1028

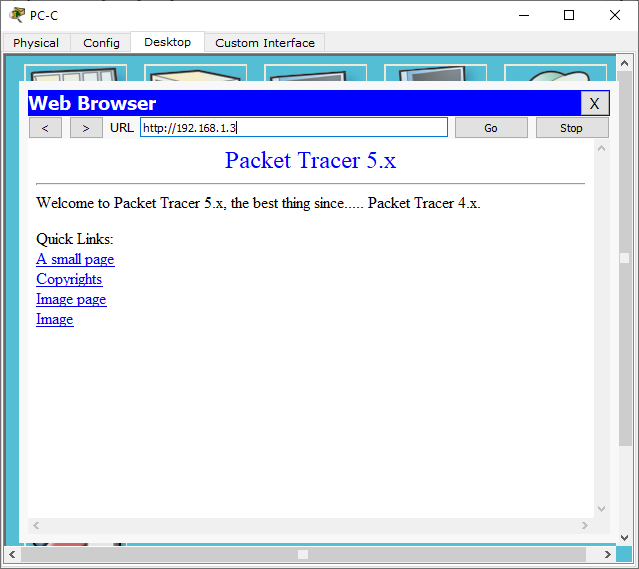
What is the destination IP address and port number? 10.2.2.2:23

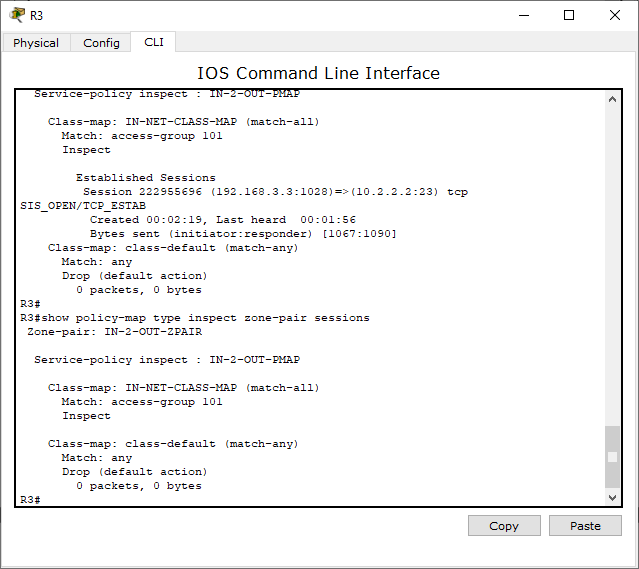


**Step 3. From PC-C, exit the Telnet session on R2 and close the Command Prompt window.**

**Step 4. From internal PC-C, open a web browser to the PC-A server web page.**

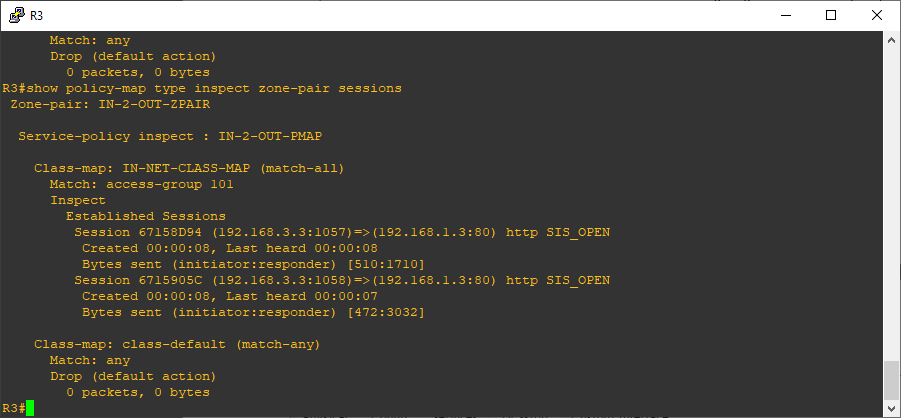
Enter the server IP address 192.168.1.3 in the browser URL field and click **Go**. The HTTP session should succeed. While the HTTP session is active, issue the command **show policy-map type inspect zone-pair sessions** on R3 established sessions.





What is the source IP address and port number?

What is the destination IP address and port number?



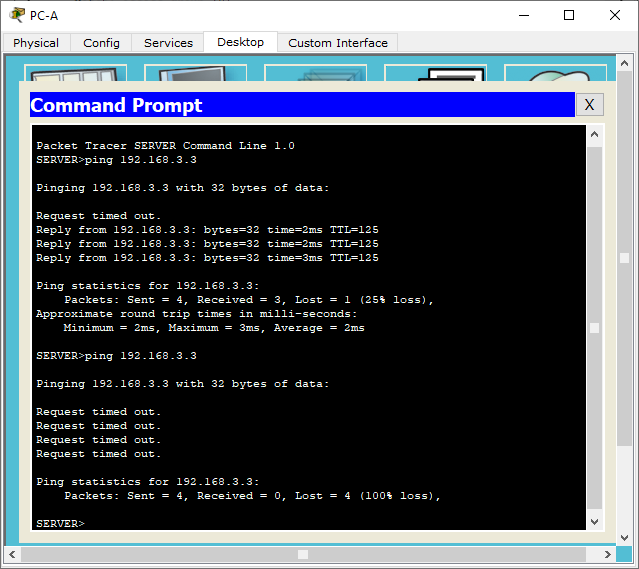
**Step 5. Close the Browser on PC-C.**

**Task 7: Test Firewall Functionality from OUT-ZONE to IN-ZONE**

Verify that external hosts CANNOT access internal resources after configuring the zone-based policy firewall.

**Step 1. From the PC-A server command prompt, ping PC-C.**

From the PC-A Command Prompt, ping PC-C at 192.168.3.3. The ping should fail.



**Step 2. From router R2, ping PC-C.**

From R2, ping PC-C at 192.168.3.3. The ping should fail.

Graphical user interface, text, application, email

Description automatically generated

**Step 3. Check results.**

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

Application

Description automatically generated with medium confidence

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.