PT Activity: Configuring Context-Based Access Control (CBAC)

**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 an IOS firewall with CBAC on router R3

·         Verify CBAC functionality using ping, Telnet, and HTTP.

**Introduction**

Context-Based Access Control (CBAC) is used to create an IOS firewall. In this activity, you will create a basic CBAC configuration on edge router R3. R3 provides access to resources outside of the network for hosts on the inside network. R3 blocks external hosts from accessing internal resources. After the configuration is complete, you will verify firewall functionality from internal and external hosts.

The routers have been pre-configured with the following:

·         Enable password: **ciscoenpa55**

·         Password for console: **ciscoconpa55**

·         Password for vty lines: **ciscovtypa55**

·         IP addressing

·         Static routing

·         All switch ports are in VLAN 1 for switches S1 and S3.

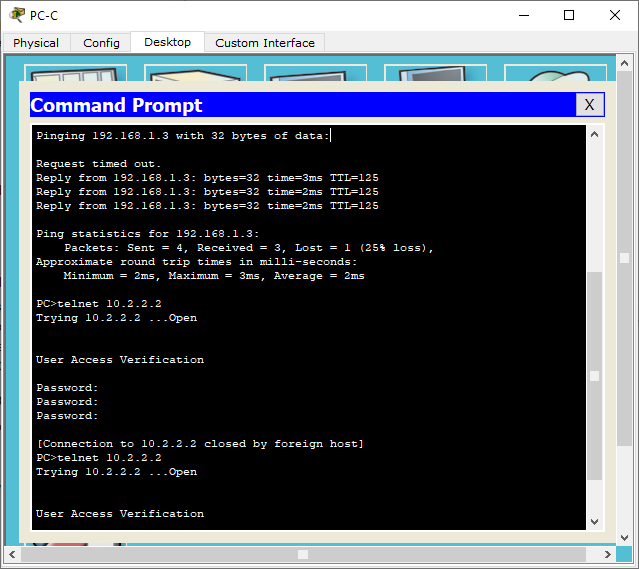
**Task 1: Block Traffic From Outside**

**Step 1. Verify Basic Network Connectivity.**

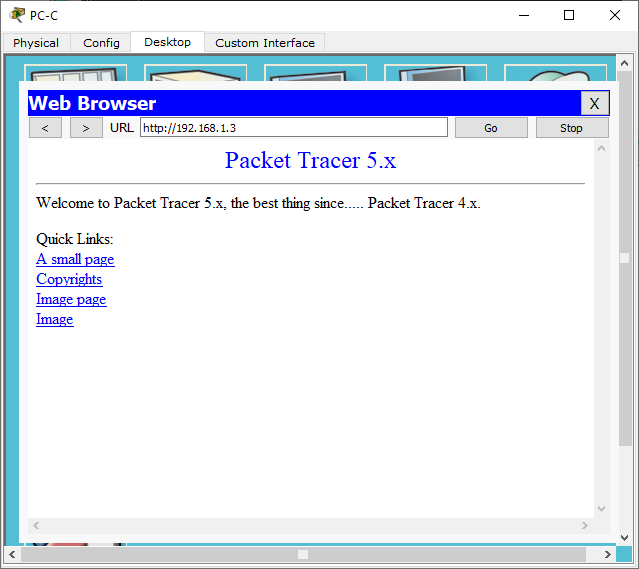
Verify network connectivity prior to configuring the IOS firewall.

·         From the PC-C command prompt, ping the PC-A server.

·         From the PC-C command prompt, Telnet to the Router R2 S0/0/1 interface: IP address 10.2.2.2. Exit the Telnet session.



·         From PC-C, open a web browser to the PC-A server to display the web page. Close the browser on PC-C.



·         From the PC-A server command prompt, ping PC-C.

A screenshot of a computer

Description automatically generated

**Step 2. Configure a named IP ACL on R3 to block all traffic originating from the outside network.**

Use the **ip access-list extended** command to create a named IP ACL.

**Step 3. Apply the ACL to interface Serial 0/0/1.**

**Step 4. Confirm that traffic entering interface Serial 0/0/1 is dropped.**

From the PC-C command prompt, ping the PC-A server. The ICMP echo replies are blocked by the ACL.

Graphical user interface, text, application

Description automatically generated

**Task 2: Create a CBAC Inspection Rule**

**Step 1. Create an inspection rule to inspect ICMP, Telnet, and HTTP traffic.**

**Step 2. Turn on time-stamped logging and CBAC audit trail messages.**

Use the **ip inspect audit-trail** command to turn on CBAC audit messages to provide a record of network access through the firewall, including illegitimate access attempts. Enable logging to the syslog server, 192.168.1.3, with the **logging**command. Make sure that logged messages are timestamped.

Graphical user interface, text

Description automatically generated

**Step 3. Apply the inspection rule to egress traffic on interface S0/0/1.**

**Step 4. Verify that audit trail messages are being logged on the syslog server.**

·         From PC-C, test connectivity to PC-A with ping, Telnet, and HTTP. All should be successful. Note that PC-A will reject the Telnet session.

Graphical user interface, text, application, email

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

·         From PC-A, test connectivity to PC-C with ping and Telnet. All should be blocked.

Graphical user interface, text

Description automatically generated

·         Review the syslog messages on server PC-A: click the **Config** tab and then click the **SYSLOG** option.

**Task 3: Verify Firewall Functionality**

**Step 1. Open a Telnet session from PC-C to R2.**

The Telnet should succeed. While the Telnet session is active, issue the command **show ip inspect sessions**on R3. This command displays the existing sessions that are currently being tracked and inspected by CBAC.

Graphical user interface, text

Description automatically generated

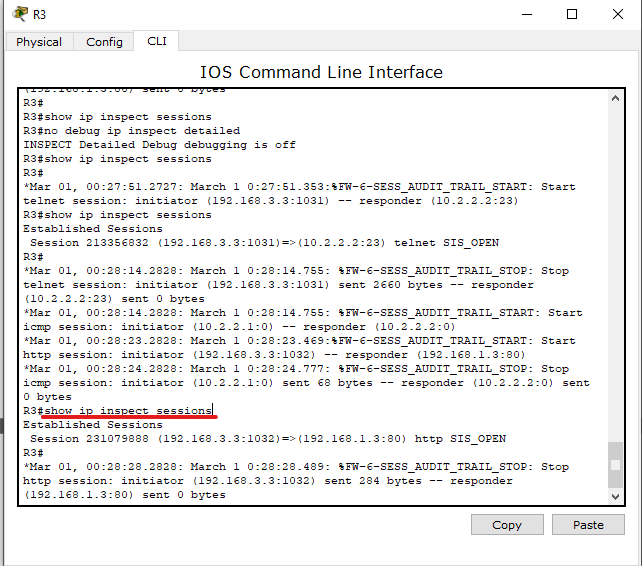
What is the source IP address and port number?

What is the destination IP address and port number?

**Exit** the Telnet session.

**Step 2. From PC-C, open a web browser to the PC-A server web page using the server IP address.**

The HTTP session should succeed. While the HTTP session is active, issue the command **show ip inspect sessions**on R3.

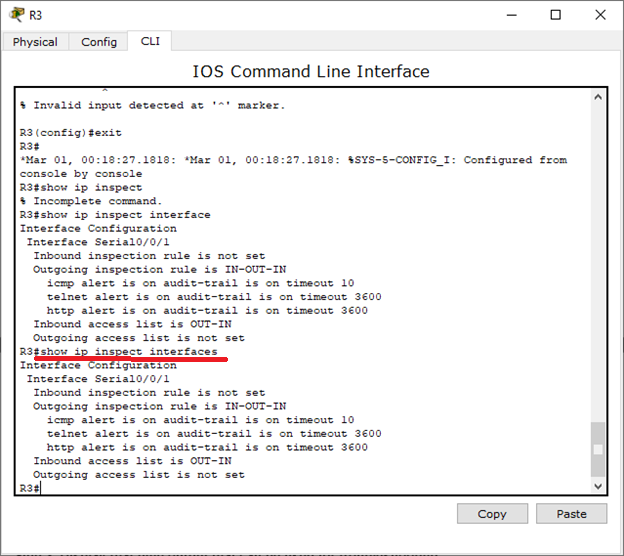


What is the source IP address and port number?

What is the destination IP address and port number?

**Close** the browser on PC-C.

**Step 3. View the interface configuration and inspection rule timers.**

****

Enter the **show ip inspect** interfaces command on R3.

The output shows existing sessions that are currently being tracked and inspected by CBAC.

**Task 4: Review CBAC Configuration**

**Step 1. Display CBAC configuration.**

Enter the **show ip inspect config**command on R3 to display the complete CBAC inspection configuration.

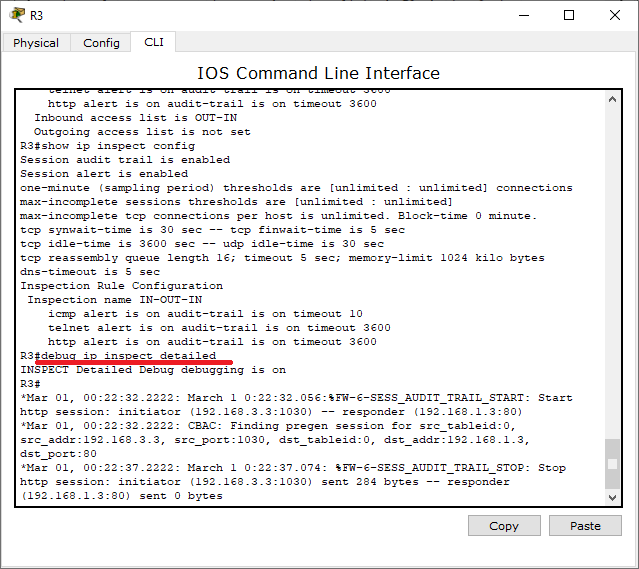
Text

Description automatically generated

**Step 2. Display real-time output that can be used for troubleshooting.**

Enter the **debug ip inspect detailed**command on R3 to display detailed messages about CBAC software events, including information about CBAC packet processing.

From PC-C, open a web browser on PC-C; enter the PC-A (server) IP address: 192.168.1.3.



**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.

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