Part 1: Verify Basic Network Connectivity

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

Step 2: Access R2 using SSH.

1. a. From the PC-C command prompt, SSH to the S0/0/1 interface on R2 at 10.2.2.2. Use the username Admin and password Adminpa55 to log in. PC> ssh -l Admin 10.2.2.2
2. b. Exit the SSH session.

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

a. Click the Desktop tab and then click the Web Browser application. Enter the PC-A IP address

192.168.1.3 as the URL. The Packet Tracer welcome page from the web server should be displayed. b. Close the browser on PC-C.

Part 2: Create the Firewall Zones on R3

Step 1: Enable the Security Technology package.

1. a. On R3, issue the show version command to view the Technology Package license information.
2. b. If the Security Technology package has not been enabled, use the following command to enable the package.

R3(config)# license boot module c1900 technology-package securityk9

1. c. Accept the end-user license agreement.

# do copy run start

Step 2: Create an internal zone.

R3(config)# zone security IN-ZONE

R3(config-sec-zone) exit

Step 3: Create an external zone.

R3(config-sec-zone)# zone security OUT-ZONE

R3(config-sec-zone)# exit

Part 3: Identify Traffic Using a Class-Map

Step 1: Create an ACL that defines internal traffic.

create extended ACL 101 to permit all IP protocols from the 192.168.3.0/24 source network to any destination

R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any

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

R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP

R3(config-cmap)# match access-group 101

R3(config-cmap)# exit

Part 4: Specify Firewall Policies

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

R3(config)# policy-map type inspect IN-2-OUT-PMAP

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

R3(config-pmap)# class type inspect IN-NET-CLASS-MAP

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

R3(config-pmap-c)# inspect

R3(config-pmap-c)# exit

R3(config-pmap)# exit

Part 5: Apply Firewall Policies

Step 1: Create a pair of zones.

R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUTZONE

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

R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP

R3(config-sec-zone-pair)# exit

Step 3: Assign interfaces to the appropriate security zones.

R3(config)# interface g0/1

R3(config-if)# zone-member security IN-ZONE

R3(config-if)# exit

R3(config)# interface s0/0/1

R3(config-if)# zone-member security OUT-ZONE

R3(config-if)# exit

Step 4: Copy the running configuration to the startup configuration.

Part 6: Test Firewall Functionality from IN-ZONE to OUT-ZONE

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, SSH to the R2 S0/0/1 interface.

1. a. From the PC-C command prompt, SSH to R2 at 10.2.2.2. Use the username Admin and the password Adminpa55 to access R2. The SSH session should succeed.
2. b. While the SSH session is active, issue the command show policy-map type inspect zone-pair sessions on R3 to view established sessions.

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

Step 3: From PC-C, exit the SSH 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.

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

Step 5: Close the browser on PC-C.

Part 7: Test Firewall Functionality from OUT-ZONE to IN-ZONE

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 R2, ping PC-C.

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