Packet Tracer - Configure a ZPF Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Descriptions
R-01	G0/0	192.168.1.1	255.255.255.0	N/A	SW-01
	G0/1	192.168.2.1	255.255.255.0	N/A	SW-02
	S0/0/0	10.1.1.2	255.255.255.252	N/A	R-02
R-02	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	R-01
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	R-03
R-03	G0/0	192.168.3.1	255.255.255.0	N/A	SW-03
	S0/0/1	10.2.2.2	255.255.255.252	N/A	R-02
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	SW-01
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1	SW-01
PC-C	NIC	192.168.2.10	255.255.255.0	192.168.2.1	SW-02
PC-D	NIC	192.168.2.11	255.255.255.0	192.168.2.1	SW-02
DNS-Server	NIC	192.168.3.10	255.255.255.0	192.168.3.1	SW-03
Web-Server	NIC	192.168.3.11	255.255.255.0	192.168.3.1	SW-03

Objectives

- Verify connectivity among devices before firewall configuration.
- Configure a zone-based policy (ZPF) firewall on R-02.
- Verify ZPF firewall functionality using ping, DNS and Web.

Background/Scenario

You Have to configure Routers as the following:

- Console password: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- Host names and IP addressing
- SSH Configurations
    - Local username: Admin
    - Secret: Adminpa55
    - RSA Crypto key Module: 1024
    - Domain-name: sltsc.lk
- OSPF-10 area-0

Instructions

Part 1: Verify Basic Network Connectivity

Step 1: From the PC-A command prompt, ping PC-C at 192.168.3.10.

Step 2: Access R2 using SSH.

Part 2: Create the Firewall Zones on R3

Step 1: Create an internal zone.

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

Step 2: Create an external zone.

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

Part 3: Identify Traffic Using a Class-Map

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 **192.168.1.0/24** and 192.168.2.0/24 given source to given protocols only.

PC-A can access Ping, DNS and Web

PC-B can access Ping,

PC-C can access Ping, DNS and Web

PC-D can access DNS and Web

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**.

Part 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).

Part 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 previously.

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**.

Step 3: Assign interfaces to the appropriate security zones.

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

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

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

Verify that internal hosts can still access external resources after configuring the ZPF.

Step 1: From internal PC-D, ping the external Web-Server.

Step 2: From internal PC-B, Web zRequest the external Web-Server.