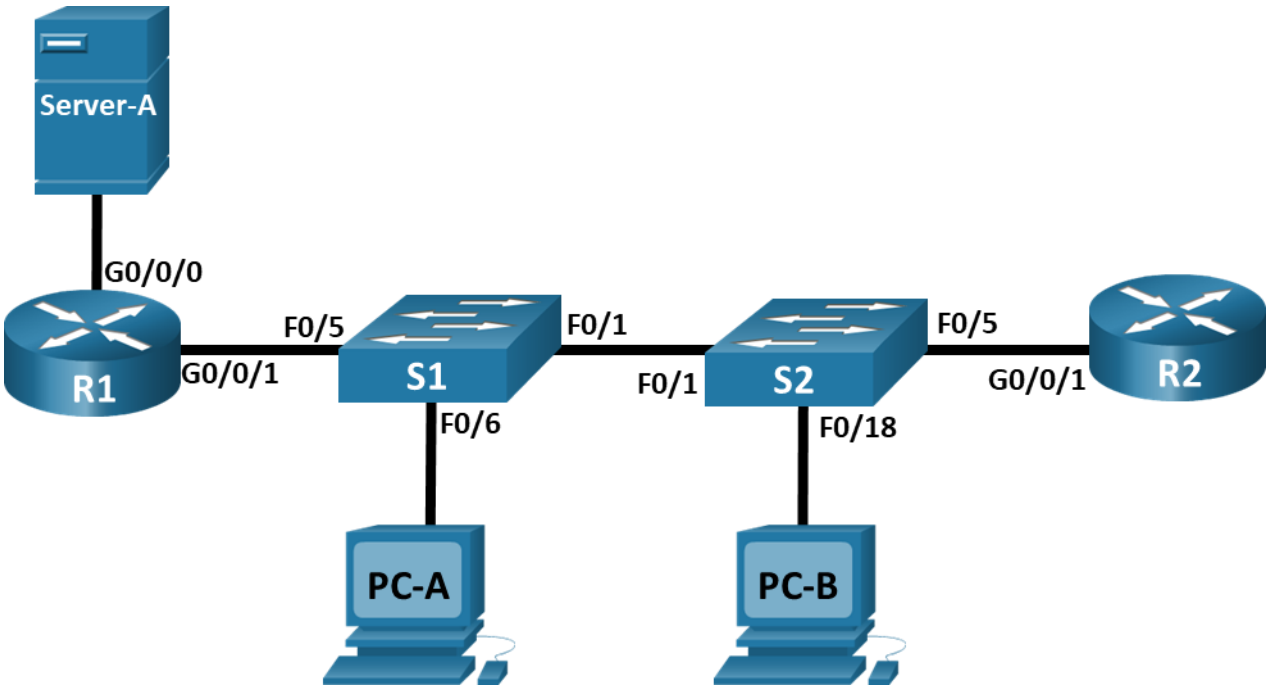
5.5.2 Packet Tracer - Configure and Verify Extended IPv4 ACLs - Physical Mode

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	N/A	N/A	N/A
	G0/0/1.20	10.20.0.1	255.255.255.0	
	G0/0/1.30	10.30.0.1	255.255.255.0	
	G0/0/1.40	10.40.0.1	255.255.255.0	
	G0/0/1.1000	N/A	N/A	
	G0/0/0	172.16.1.1	255.255.255.0	
R2	G0/0/1	10.20.0.4	255.255.255.0	N/A
S1	VLAN 20	10.20.0.2	255.255.255.0	10.20.0.1
S2	VLAN 20	10.20.0.3	255.255.255.0	10.20.0.1
PC-A	NIC	10.30.0.10	255.255.255.0	10.30.0.1
PC-B	NIC	10.40.0.10	255.255.255.0	10.40.0.1

© 2020 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Server-A	NIC	172.16.1.2	255.255.255.0	172.16.1.1

VLAN Table

VLAN	Name	Interface Assigned
20	Management	S2: F0/5
30	Operations	S1: F0/6
40	Sales	S2: F0/18
999	ParkingLot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2
1000	Native	N/A

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure VLANs on the Switches

Part 3: Configure Trunking

Part 4: Configure Routing

Part 5: Configure Remote Access

Part 6: Verify Connectivity

Part 7: Configure and Verify Extended Access Control Lists

Background / Scenario

In this Packet Tracer Physical Mode (PTPM) activity, you have been tasked with configuring access control lists (ACLs) on a small company's network. ACLs are one of the simplest and most direct means of controlling Layer 3 traffic. R1 will be hosting an internet connection and sharing the default route information to R2. After initial configuration is complete, the company has some specific traffic security requirements that you will be responsible for implementing.

Note: There are over 100 items scored in this activity. Therefore, Packet Tracer will display the number of items currently correct instead of the percentage score.

Instructions

Part 1: Build the Network and Configure Basic Device Settings

Step 1: Cable the network as shown in the topology.

a. Cable and power on the devices as shown in the topology diagram. Use a console cable to connect a **PC** to each switch or router as you configure them. To access a switch or router, you must connect a console cable between the PCs and the device you wish to configure. We recommend connecting **PC-A** to **R1** and **PC-B** to **R2**.

b. Then, when configuring the switches, connect **PC-A** to **S1** and **PC-B** to **S2**. After you have connected the console cable, click the **PC > Desktop tab** > **Terminal**, and then click **OK**, to access the command line.

© 2020 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

When changing a console cable to a new device, such as between a router and a switch, it is easier to click the end of the console cable and drag it back to the Cable Pegboard than it is to try to connect the cable directly to another device. After attaching a console cable to a different device, you must close and reopen the **Terminal** window to establish a new connection.

Step 2: Configure basic settings for each router.

a. Assign a device name to the router.

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password and enable login.

e. Assign **cisco** as the vty password. You will enable login later in this activity.

f. Encrypt the plaintext passwords.

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

h. Save the running configuration to the startup configuration file.

Step 3: Configure basic settings for each switch.

a. Assign a device name to the switch.

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password and enable login.

e. Assign **cisco** as the vty password. You will enable login later in this activity.

f. Encrypt the plaintext passwords.

g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

h. Save the running configuration to the startup configuration file.

Part 2: Configure VLANs on the Switches

Step 1: Create VLANs on both switches.

a. Create and name the required VLANs on each switch from the VLAN table.

b. Configure the management interface and default gateway on each switch using the IP address information in the Addressing Table.

c. Assign all unused ports on the switch to the Parking Lot VLAN. Configure them for static access mode, and administratively deactivate them.

Note: The **interface range** command helps to accomplish this task with as few commands as necessary.

Step 2: Assign VLANs to the correct switch interfaces.

a. Assign used ports to the appropriate VLAN (specified in the VLAN table) and configure them for static access mode.

b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

© 2020 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Part 3: Configure Trunking

Step 1: Manually configure trunk interface F0/1.

a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

b. As a part of the trunk configuration, set the native vlan to 1000 on both switches. You may see error messages temporarily while the two interfaces are configured for different Native VLANs.

c. As another part of trunk configuration, specify that VLANs 10, 20, 30, and 1000 are allowed to cross the trunk.

d. Issue the **show interfaces trunk** command to verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

Step 2: Manually configure S1's trunk interface F0/5.

a. Configure S1's interface F0/5 with the same trunk parameters as F0/1. This is the trunk to R1.

b. Save the running configuration to the startup configuration file.

Part 4: Configure Routing

Step 1: Configure Inter-VLAN Routing on R1.

a. Activate interface G0/0/1 on the router.

b. Configure sub-interfaces for each VLAN as specified in the Addressing Table. All sub-interfaces use 802.1Q encapsulation. Ensure the sub-interface for the Native VLAN does not have an IP address assigned. Include a description for each sub-interface.

c. Configure interface G0/0/1 on R1 with addressing from the Addressing Table.

d. Use the **show ip interface brief** command to verify that the sub-interfaces are operational.

Step 2: Configure the R2 interface g0/0/1 using the Addressing table and a default route with the next hop 10.20.0.1

Part 5: Configure Remote Access

Step 1: Configure all network devices for basic SSH support.

a. Create a local user with the username **SSHadmin** and **$cisco123!** as the encrypted password.

b. Use **ccna-lab.com** as the domain name.

c. Generate crypto keys using a 1024-bit modulus.

d. Configure the first five vty lines on each device to support SSH connections only and to authenticate to the local user database.

Part 6: Verify Connectivity

Step 1: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

© 2020 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

www.netacad.com

Step 2: Complete the following tests. All should be successful.

Note: If you click **Check Results**, you will see that the five highlighted **Connectivity Tests** show as incorrect. This is because you have not implemented ACLs yet. After ACLs are implemented, these five highlighted **Connectivity Tests** should successfully fail.

From	Protocol	Destination	Result
PC-A	Ping	10.40.0.10	Success
PC-A	Ping	10.20.0.1	Success
PC-B	Ping	10.30.0.10	Success
PC-B	Ping	10.20.0.1	Success
PC-B	Ping	172.16.1.1	Success
PC-B	HTTPS	172.16.1.2	Success
PC-A	HTTPS	172.16.1.2	Success
PC-B	SSH	10.20.0.4	Success
PC-B	SSH	172.16.1.1	Success

Part 7: Configure and Verify Extended Access Control Lists

When basic connectivity is verified, the company requires the following security policies to be implemented:

Policy 1: The Sales Network is not allowed to SSH to the Management Network (but other SSH is allowed).

Policy 2: The Sales Network is not allowed to access server-A using any web protocol (HTTP/HTTPS). All other web traffic is allowed.

Policy 3: The Sales Network is not allowed to send ICMP echo requests to the Operations or Management Networks. ICMP echo requests to other destinations are allowed.

Policy 4: The Operations network is not allowed to send ICMP echo requests to the Sales Network. ICMP echo requests to other destinations are allowed.

Step 1: Develop and apply extended access lists that will meet the security policy statements.

Step 2: Verify that security policies are being enforced by the deployed access lists.

Run the following tests. The expected results are shown in the table:

Note: Click **Check Results** to force Packet Tracer to run all the **Connectivity Tests** again.

From	Protocol	Destination	Result
PC-A	Ping	10.40.0.10	Fail
PC-A	Ping	10.20.0.1	Success
PC-B	Ping	10.30.0.10	Fail
PC-B	Ping	10.20.0.1	Fail
PC-B	Ping	172.16.1.1	Success
PC-B	HTTPS	172.16.1.2	Fail

© 2020 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

From	Protocol	Destination	Result
PC-A	HTTPS	172.16.1.2	Success
PC-B	SSH	10.20.0.4	Fail
PC-B	SSH	172.16.1.1	Success

© 2020 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

www.netacad.com