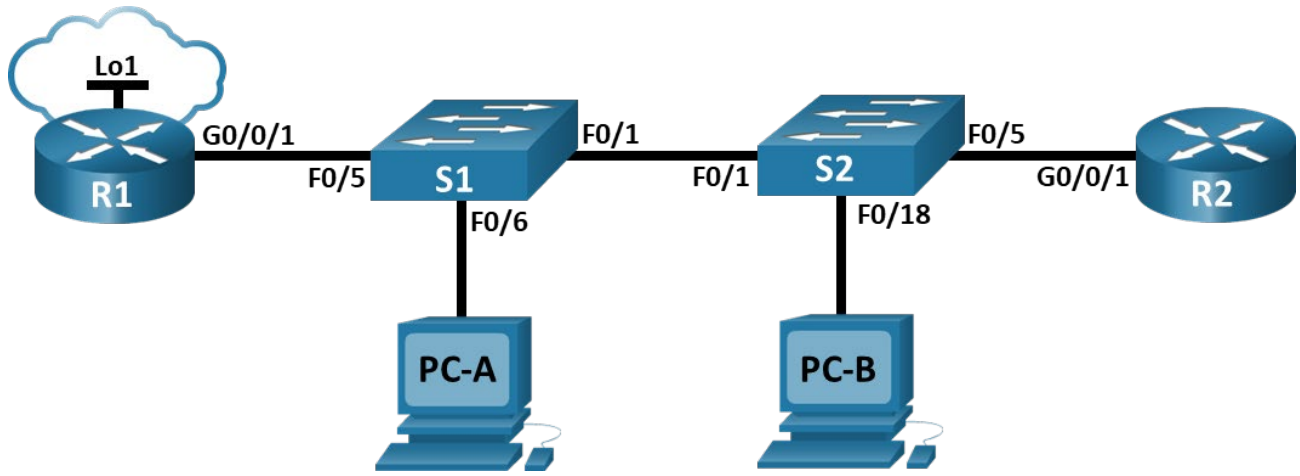
Lab - Configure and Verify Extended IPv4 ACLs

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	
	Loopback1	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

VLAN Table

VLAN	Name	Interface Assigned
20	Management	S2: F0/5
30	Operations	S1: F0/6
40	Sales	S2: F0/18

VLAN	Name	Interface Assigned
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 and Verify Extended Access Control Lists

Background / Scenario

You have been tasked with configuring access control lists on 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 (simulated by interface Loopback 1) and sharing the default route information to R2. After initial configuration is complete, the company has some specific traffic security requirements that you are responsible for implementing.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Build the Network and Configure Basic Device Settings.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

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 and enable login.

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 and enable login.

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 table above.

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 is helpful 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 above) 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.

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 the router.

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

c. Issue the **show interfaces trunk** command to verify trunking.

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 IP 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 Loopback 1 on R1 with addressing from the table above.

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

Step 2: Configure the R2 interface g0/0/1 using the address from the 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 the encrypted password $cisco123!

```
R1(config)# username SSHadmin secret $cisco123!
```

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

```
R1(config)# ip domain name ccna-lab.com
```

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

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

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

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
```

Step 2: Enable secure, authenticated web services on R1.

a. Enable the HTTPS server on R1.

```
R1(config)# ip http secure-server
```

b. Configure R1 to authenticate users attempting to connect to the web server.

```
R1(config)# ip http authentication local
```

Part 6: Verify Connectivity

Step 1: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

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

Note: You may have to disable the PC firewall for pings to be successful.

From	Protocol	Destination
PC-A	Ping	10.40.0.10
PC-A	Ping	10.20.0.1
PC-B	Ping	10.30.0.10
PC-B	Ping	10.20.0.1
PC-B	Ping	172.16.1.1
PC-B	HTTPS	10.20.0.1
PC-B	HTTPS	172.16.1.1
PC-B	SSH	10.20.0.1
PC-B	SSH	172.16.1.1

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 IP addresses in the Management network using any web protocol (HTTP/HTTPS). The Sales Network is also not allowed to access R1 interfaces using any web protocol. All other web traffic is allowed (note – Sales can access the Loopback 1 interface on R1).

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: Analyze the network and the security policy requirements to plan ACL implementation.

The requirements listed above require two extended access lists to be implemented. Following the guidance of placing extended access lists as close to the source of the traffic to be filtered as possible, these ACLs will go on interfaces G0/0/0.30 and G0/0/0.40.

Step 2: Develop and apply extended access lists that will meet the security policy statements.

```
R1(config)# access-list 101 remark ACL 101 fulfills policies 1, 2, and 3
```

Deny SSH from VLAN 20 to 40

```
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255
eq 22
```

Deny HTTP from VLAN 40 to 20

```
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255
eq 80
```

Deny HTTP from VLAN 40 to 30

```
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.30.0.1 0.0.0.0 eq
80
```

Deny HTTP from VLAN 40 to 10.40.0.1

```
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.40.0.1 0.0.0.0 eq
80
```

Deny HTTPs from VLAN 40 to 20

```
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255
eq 443
```

Deny HTTPs from VLAN 40 to 30

```
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.30.0.1 0.0.0.0 eq
443
```

Deny HTTPs from VLAN 40 to 10.40.0.1

```
R1(config)# access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.40.0.1 0.0.0.0 eq
443
```

Deny ICMP-echo from VLAN 40 to 20

```
R1(config)# access-list 101 deny icmp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255
echo
```

Deny ICMP-echo from VLAN 40 to 30

```
R1(config)# access-list 101 deny icmp 10.40.0.0 0.0.0.255 10.30.0.0 0.0.0.255
echo
```

Permit anything else

```
R1(config)# access-list 101 permit ip any any
```

Apply to interface g0/0/1.40 inbound

```
R1(config)# interface g0/0/1.40
R1(config-subif)# ip access-group 101 in

R1(config)# access-list 102 remark ACL 102 fulfills policy 4
```

Deny ICMP-echo from VLAN 30 to 40

```
R1(config)# access-list 102 deny icmp 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255
echo
```

Permit anything else

```
R1(config)# access-list 102 permit ip any any
```

Apply to interface g0/0/1.30 inbound

```
R1(config)# interface g0/0/1.30
R1(config-subif)# ip access-group 102 in
```

Step 3: Verify security policies are being enforced by the deployed access lists.

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

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	10.20.0.1	Fail
PC-B	HTTPS	172.16.1.1	Success
PC-B	SSH	10.20.0.4	Fail
PC-B	SSH	172.16.1.1	Success