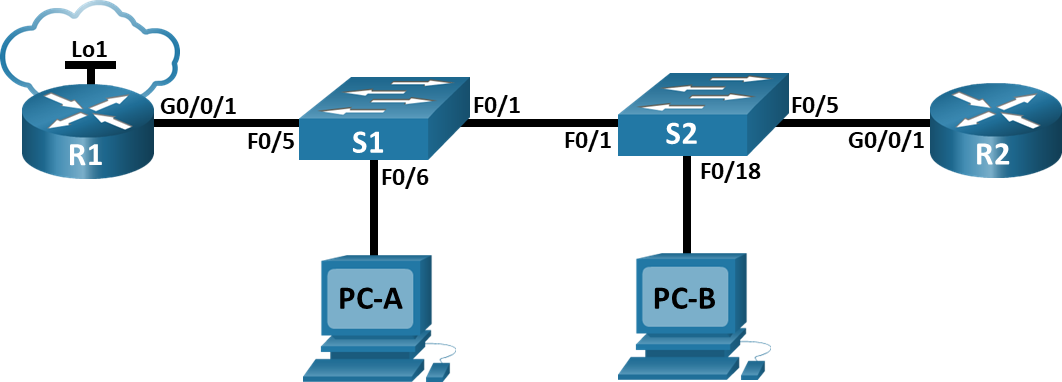
Lab - Configure and Verify Extended IPv4 ACLs

# Topology



# Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/0/1 | N/A | N/A | N/A |
| R1 | G0/0/1.20 | 10.20.0.1 | 255.255.255.0 | N/A |
| R1 | G0/0/1.30 | 10.30.0.1 | 255.255.255.0 | N/A |
| R1 | G0/0/1.40 | 10.40.0.1 | 255.255.255.0 | N/A |
| R1 | G0/0/1.1000 | N/A | N/A | N/A |
| R1 | Loopback1 | 172.16.1.1 | 255.255.255.0 | N/A |
| 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 |
| 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.

router(config)# **hostname R1**

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

R1(config)# **no ip domain lookup**

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

R1(config)# **enable secret class**

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

R1(config)# **line console 0**

R1(config-line)# **password cisco**

R1(config-line)# **login**

e. Assign **cisco** as the VTY password and enable login.

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

f. Encrypt the plaintext passwords.

R1(config)# **service password-encryption**

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

R1(config)# **banner motd $ Authorized Users Only! $**

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

R1# **copy running-config startup-config**

##### Step 3: Configure basic settings for each switch.

a. Assign a device name to the switch.

switch(config)# **hostname S1**

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

S1(config)# **no ip domain-lookup**

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

S1(config)# **enable secret class**

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

S1(config)# **line console 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

e. Assign **cisco** as the VTY password and enable login.

S1(config)# **line vty 0 15**

S1(config-line)# **password cisco**

S1(config-line)# **login**

f. Encrypt the plaintext passwords.

S1(config)# **service password-encryption**

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

S1(config)# **banner motd $ Authorized Users Only! $**

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

S1(config)# **exit**

S1# **copy running-config startup-config**

#### 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.

S1(config)# **vlan 20**

S1(config-vlan)# **name Management**

S1(config-vlan)# **vlan 30**

S1(config-vlan)# **name Operations**

S1(config-vlan)# **vlan 40**

S1(config-vlan)# **name Sales**

S1(config-vlan)# **vlan 999**

S1(config-vlan)# **name ParkingLot**

S1(config-vlan)# **vlan 1000**

S1(config-vlan)# **name Native**

S1(config-vlan)# **exit**

S2(config)# **vlan 20**

S2(config-vlan)# **name Management**

S2(config-vlan)# **vlan 30**

S2(config-vlan)# **name Operations**

S2(config-vlan)# **vlan 40**

S2(config-vlan)# **name Sales**

S2(config-vlan)# **vlan 999**

S2(config-vlan)# **name ParkingLot**

S2(config-vlan)# **vlan 1000**

S2(config-vlan)# **name Native**

S2(config-vlan)# **exit**

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

S1(config)# **interface vlan 20**

S1(config-if)# **ip address 10.20.0.2 255.255.255.0**

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

S1(config)# **ip default-gateway 10.20.0.1**

S1(config)# **end**

S2(config)# **interface vlan 20**

S2(config-if)# **ip address 10.20.0.3 255.255.255.0**

S2(config-if)# **no shutdown**

S2(config-if)# **exit**

S2(config)# **ip default-gateway 10.20.0.1**

S2(config)# **end**

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.

S1(config)# **interface range f0/2 - 4, f0/7 - 24, g0/1 - 2**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 999**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S2(config)# **interface range f0/2 - 17, f0/19 - 24, g0/1 - 2**

S2(config-if-range)# **switchport mode access**

S2(config-if-range)# **switchport access vlan 999**

S2(config-if-range)# **shutdown**

S2(config-if-range)# **end**

##### 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.

S1(config)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 30**

S2(config)# **interface f0/18**

S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 40**

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

S1# **show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/5

10 Management active

20 Sales active Fa0/6

30 Operations active

999 ParkingLot active Fa0/2, Fa0/3, Fa0/4, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

1000 Native active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S2# **show vlab brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1

10 Management active

30 Operations active

40 Sales active Fa0/18

999 ParkingLot active Fa0/2, Fa0/3, Fa0/4, Fa0/5

Fa0/6, Fa0/7, Fa0/8, Fa0/9

Fa0/10, Fa0/11, Fa0/12, Fa0/13

Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gi0/1, Gi0/2

#### 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.

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode trunk**

S2(config)# **interface f0/1**

S2(config-if)# **switchport mode trunk**

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.

S1(config-if)# **switchport trunk native vlan 1000**

S2(config-if)# **switchport trunk native vlan 1000**

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

S1(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

S2(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

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

S1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk

Fa0/1 20,30,40,1000

Port Vlans allowed and active in management domain

Fa0/1 20,30,40,1000

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 20,30,40,1000

S2# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk

Fa0/1 20,30,40,1000

Port Vlans allowed and active in management domain

Fa0/1 30,40,1000

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 30,40

##### 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.

S1(config)# **interface f0/5**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 1000**

S1(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

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

S1# **copy running-config startup-config**

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.

R1(config)# **interface g0/0/1**

R1(config-if)# **no shutdown**

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.

R1(config)# **interface g0/0/1.20**

R1(config-subif)# **description Management Network**

R1(config-subif)# **encapsulation dot1q 20**

R1(config-subif)# **ip address 10.20.0.1 255.255.255.0**

R1(config-subif)# **interface g0/0/1.30**

R1(config-subif)# **encapsulation dot1q 30**

R1(config-subif)# **description Operations Network**

R1(config-subif)# **ip address 10.30.0.1 255.255.255.0**

R1(config-subif)# **interface g0/0/1.40**

R1(config-subif)# **encapsulation dot1q 40**

R1(config-subif)# **description Sales Network**

R1(config-subif)# **ip address 10.40.0.1 255.255.255.0**

R1(config-subif)# **interface g0/0/1.1000**

R1(config-subif)# **encapsulation dot1q 1000 native**

R1(config-subif)# **description Native VLAN**

c. Configure interface Loopback 1 on R1 with addressing from the table above.

R1(config)# **interface Loopback 1**

R1(config-if)# **ip address 172.16.1.1 255.255.255.0**

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

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 unassigned YES unset administratively down down

GigabitEthernet0/0/1 unassigned YES unset up up

Gi0/0/1.20 10.20.0.1 YES manual up up

Gi0/0/1.30 10.30.0.1 YES manual up up

Gi0/0/1.40 10.40.0.1 YES manual up up

Gi0/0/1.1000 unassigned YES unset up up

Serial0/1/0 unassigned NO unset down down

Serial0/1/1 unassigned NO unset down down

GigabitEthernet0 unassigned YES unset administratively down down

Loopback1 172.16.1.1 YES manual up up

##### 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

R2(config)# **interface g0/0/1**

R2(config-if)# **ip address 10.20.0.4 255.255.255.0**

R2(config-if)# **no shutdown**

R2(config-if)# **exit**

R2(config)# **ip route 0.0.0.0 0.0.0.0 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.

##### 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 |