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

## Build the Network and Configure Basic Device Settings.

### Cable the network as shown in the topology.

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

### Configure basic settings for each router.

Open configuration window

* + - 1. Assign a device name to the router.
      2. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
      3. Assign **class** as the privileged EXEC encrypted password.
      4. Assign **cisco** as the console password and enable login.
      5. Assign **cisco** as the VTY password and enable login.
      6. Encrypt the plaintext passwords.
      7. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
      8. Save the running configuration to the startup configuration file.

Close configuration window

### Configure basic settings for each switch.

Open configuration window

* + - 1. Assign a device name to the switch.
      2. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
      3. Assign **class** as the privileged EXEC encrypted password.
      4. Assign **cisco** as the console password and enable login.
      5. Assign **cisco** as the VTY password and enable login.
      6. Encrypt the plaintext passwords.
      7. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
      8. Save the running configuration to the startup configuration file.

Close configuration window

## Configure VLANs on the Switches

### Create VLANs on both switches.

Open configuration window

* + - 1. Create and name the required VLANs on each switch from the table above.
      2. Configure the management interface and default gateway on each switch using the IP address information in the Addressing Table.
      3. 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.

### Assign VLANs to the correct switch interfaces.

* + - 1. Assign used ports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.
      2. Issue the **show vlan** **brief** command and verify that the VLANs are assigned to the correct interfaces.

Close configuration window

## Configure Trunking

### Manually configure trunk interface F0/1.

Open configuration window

* + - 1. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.
      2. 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.
      3. As another part of trunk configuration, specify that VLANs 10, 20, 30, and 1000 are allowed to cross the trunk.
      4. Issue the **show interfaces trunk** command to verify trunking ports, the Native VLAN and allowed VLANs across the trunk.

### Manually configure S1’s trunk interface F0/5.

* + - 1. Configure S1’s interface F0/5 with the same trunk parameters as F0/1. This is the trunk to the router.
      2. Save the running configuration to the startup configuration file.
      3. Issue the **show interfaces trunk** command to verify trunking.

Close configuration window

## Configure Routing

### Configure Inter-VLAN Routing on R1.

Open configuration window

* + - 1. Activate interface G0/0/1 on the router.
      2. 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.
      3. Configure interface Loopback 1 on R1 with addressing from the table above.
      4. Use the **show ip interface brief** command to verify the sub-interfaces are operational.

### 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

Close configuration window

## Configure Remote Access

### Configure all network devices for basic SSH support.

Open configuration window

* + - 1. Create a local user with the username SSHadmin and the encrypted password $cisco123!
      2. Use **ccna-lab.com** as the domain name.
      3. Generate crypto keys using a 1024-bit modulus.
      4. Configure the first five VTY lines on each device to support SSH connections only and to authenticate to the local user database.

### Enable secure, authenticated web services on R1.

* + - 1. Enable the HTTPS server on R1.

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

* + - 1. Configure R1 to authenticate users attempting to connect to the web server.

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

Close configuration window

## Verify Connectivity

### Configure PC hosts.

Refer to the Addressing Table for PC host address information.

### 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 |

## 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.

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

### Develop and apply extended access lists that will meet the security policy statements.

### 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 |

End of document