Packet Tracer - Configure Extended IPv4 ACLs - Scenario 2 (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Answers: 26.2.2 Packet Tracer - Configure Extended IPv4 ACLs - Scenario 2

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RT1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	
PC1	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC2	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC3	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server1	NIC	64.101.255.254	**255.254.0.0**	**64.100.1.1**
Server2	NIC	64.103.255.254	**255.254.0.0**	**64.102.1.1**

Objectives

Part 1: Configure a Named Extended ACL

Part 2: Apply and Verify the Extended ACL

Background / Scenario

In this scenario, specific devices on the LAN are allowed to various services on servers located on the internet.

Instructions

Part 1: Configure a Named Extended ACL

Configure one named ACL to implement the following policy:

- Block HTTP and HTTPS access from **PC1** to **Server1** and **Server2**. The servers are inside the cloud and you only know their IP addresses.
- Block FTP access from **PC2** to **Server1** and **Server2**.
- Block ICMP access from **PC3** to **Server1** and **Server2**.

Note: For scoring purposes, you must configure the statements in the order specified in the following steps.

Step 1: Deny PC1 access to HTTP and HTTPS services on Server1 and Server2.

a. Create a named extended IP access list on router RT1 which will deny **PC1** access to the HTTP and HTTPS services of **Server1** and **Server2**. Four access control statements are required.

What is the command to begin the configuration of an extended access list with the name **ACL**?

```
ip access-list extended ACL
```

b. Begin the ACL configuration with a statement that denies access from **PC1** to **Server1**, only for HTTP (port 80). Refer to the addressing table for the IP address of **PC1** and **Server1**.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 80
```

c. Next, enter the statement that denies access from **PC1** to **Server1**, only for HTTPS (port 443).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
```

d. Enter the statement that denies access from **PC1** to **Server2**, only for HTTP. Refer to the addressing table for the IP address of **Server 2.**

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 80
```

e. Enter the statement that denies access from **PC1** to **Server2**, only for HTTPS.

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
```

Step 2: Deny PC2 to access FTP services on Server1 and Server2.

Refer to the addressing table for the IP address of **PC2**.

a. Enter the statement that denies access from **PC2** to **Server1**, only for FTP (port 21 only).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.101.255.254 eq 21
```

b. Enter the statement that denies access from **PC2** to **Server2**, only for FTP (port 21 only).

```
RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.103.255.254 eq 21
```

Step 3: Deny PC3 to ping Server1 and Server2.

Refer to the addressing table for the IP address of **PC3.**

a. Enter the statement that denies ICMP access from **PC3** to **Server1**.

```
RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.101.255.254
```

b. Enter the statement that denies ICMP access from **PC3** to **Server2**.

```
RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.103.255.254
```

Step 4: Permit all other IP traffic.

By default, an access list denies all traffic that does not match any rule in the list. Enter the command that permits all traffic that does not match any of the configured access list statements.

```
RT1(config-ext-nacl)# permit ip any any
```

Step 5: Verify the access list configuration before applying it to an interface.

Before any access list is applied, the configuration needs to be verified to make sure that there are no typographical errors and that the statements are in the correct order. To view the current configuration of the access list, use either the **show access-lists** or the **show running-config** command.

```
RT1# show access-lists
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
```

```
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254
    90 permit ip any any

RT1# show running-config | begin access-list
ip access-list extended ACL
 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
 deny icmp host 172.31.1.103 host 64.101.255.254
 deny icmp host 172.31.1.103 host 64.103.255.254
 permit ip any any
```

Note: The difference between the output of the **show access-lists** command and the output of the **show running-config** command is that the **show access-lists** command includes the sequence numbers assigned to the configuration statements. These sequence numbers enable the editing, deleting, and inserting of single lines within the access list configuration. Sequence numbers also define the processing order of individual access control statements, starting with the lowest sequence number.

Part 2: Apply and Verify the Extended ACL

The traffic to be filtered is coming from the 172.31.1.96/27 network and is destined for remote networks. Appropriate ACL placement depends on the relationship of the traffic with respect to **RT1**. In general, extended access lists should be placed on the interface closest to the source of the traffic.

Step 1: Apply the ACL to the correct interface and in the correct direction.

Note: In an actual operational network, an untested ACL should never be applied to an active interface. This is not a good practice and can disrupt network operation.

On which interface should the named ACL be applied, and in which direction?

Interface Gigabit Ethernet 0/0, in.

Enter the configuration commands to apply the ACL to the interface.

```
RT1(config)# interface g0/0
RT1(config-f)# ip access-group ACL in
```

Step 2: Test access for each PC.

a. Access the websites of **Server1** and **Server2** using the web browser of **PC1**. Use both the HTTP and HTTPS protocols. Use the **show access-lists** command to view which access list statement permitted or denied the traffic. The output of the **show access-lists** command displays the number of packets that match each statement since the last time the counters were cleared, or the router rebooted.

Note: To clear the counters on an access list, use the **clear access-list counters** command.

```
RT1# show ip access-lists
Extended IP access list ACL
    10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (12 match(es))
    20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))
    30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
    40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
    50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
    60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
    70 deny icmp host 172.31.1.103 host 64.101.255.254
    80 deny icmp host 172.31.1.103 host 64.103.255.254
    90 permit ip any any
```

b. Access FTP of **Server1** and **Server2** using **PC1**. The username and password is **cisco**.

c. Ping **Server1** and **Server2** from **PC1**.

d. Repeat Step 2a to Step 2c with **PC2** and **PC3** to verify proper access list operation.

Answer Configuration

Router RT1

```
enable
configure terminal
ip access-list extended ACL
 deny tcp host 172.31.1.101 host 64.101.255.254 eq www
 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443
 deny tcp host 172.31.1.101 host 64.103.255.254 eq www
 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443
 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp
 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp
 deny icmp host 172.31.1.103 host 64.101.255.254
 deny icmp host 172.31.1.103 host 64.103.255.254
 permit ip any any
interface GigabitEthernet0/0
 ip access-group ACL in
end
```