Module Practice and Quiz

5.5.1

Packet Tracer - IPv4 ACL Implementation Challenge

In this Packet Tracer challenge, you will configure extended, standard named, and extended named IPv4 ACLs to meet specified communication requirements.

IPv4 ACL Implementation Challenge

IPv4 ACL Implementation Challenge

5.5.2

Lab - Configure and Verify Extended IPv4 ACLs

Skills Practice Opportunity

You have the opportunity to practice the following skills:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure and Verify Extended IPv4 ACLs

You can practice these skills using the Packet Tracer or lab equipment, if available.

Packet Tracer - Physical Mode (PTPM)

Configure and Verify Extended IPv4 ACLs - Physical Mode

Configure and Verify Extended IPv4 ACLs - Physical Mode

Lab Equipment

Configure and Verify Extended IPv4 ACLs

5.5.3

What did I learn in this module?

Configure Standard IPv4 ACLs

All access control lists (ACLs) must be planned, especially for ACLs requiring multiple access control entries (ACEs). When configuring a complex ACL, it is suggested that you use a text editor and write out the specifics of the policy to be implemented, add the IOS configuration commands to accomplish those tasks, include remarks to document the ACL, copy and paste the commands on a lab device, and always thoroughly test an ACL to ensure that it correctly applies the desired policy. To create a numbered standard ACL, use the **ip access-list** *access-list-number* global configuration command. Use the **no access-list** *access-list-number* global configuration command to remove a numbered standard ACL. Use the **show ip interface** command to verify if an interface has an ACL applied to it. In addition to standard numbered ACLs, there are named standard ACLs. ACL names are alphanumeric, case sensitive, and must be unique. Capitalizing ACL names is not required but makes them stand out when viewing the running-config output. To create a named standard ACL, use the **ip access-list standard** *access-list-name* global configuration command. Use the **no ip access-list standard** *access-list-name* global configuration command to remove a named standard IPv4 ACL. After a standard IPv4 ACL is configured, it must be linked to an interface or feature. To bind a numbered or named standard IPv4 ACL to an interface, use the **ip access-group** {*access-list-number* | *access-list-name*} { **in** | **out** } global configuration command. To remove an ACL from an interface, first enter the **no ip access-group** interface configuration command. To remove the ACL from the router, use the **no access-list** global configuration command.

Modify IPv4 ACLs

To modify an ACL, use a text editor or use sequence numbers. ACLs with multiple ACEs should be created in a text editor. This allows you to plan the required ACEs, create the ACL, and then paste it into the router interface. An ACL ACE can also be deleted or added using the ACL sequence numbers. Sequence numbers are automatically assigned when an ACE is entered. These numbers are listed in the **show access-lists** command. The **show running-config** command does not display sequence numbers. Named ACLs can also use sequence numbers to delete and add ACEs. The **show access-lists** command shows statistics for each statement that has been matched. The **clear access-list counters** command to clear the ACL statistics.

Secure VTY Ports with a Standard IPv4 ACL

ACLs typically filter incoming or outgoing traffic on an interface. However, a standard ACL can also be used to secure remote administrative access to a device using the vty lines. The two steps to secure remote administrative access to the vty lines are to create an ACL to identify which administrative hosts should be allowed remote access and to apply the ACL to incoming traffic on the vty lines. The **in** keyword is the most commonly used option to filter incoming vty traffic. The **out** parameter filters outgoing vty traffic and is rarely applied. Both named and numbered access lists can be applied to vty lines. Identical restrictions should be set on all the vty lines, because a user can attempt to connect to any of them. After the ACL to restrict access to the vty lines is configured, it is important to verify that it is working as expected. Use the **show ip interface** command to verify if an interface has an ACL applied to it. To verify the ACL statistics, issue the **show access-lists** command.

Configure Extended IPv4 ACLs

Extended ACLs are used more often than standard ACLs because they provide a greater degree of control. They can filter on source address, destination address, protocol (i.e., IP, TCP, UDP, ICMP), and port number. This provides a greater range of criteria on which to base the ACL. Like standard ACLs, extended ACLs can be created as numbered extended ACL and named extended ACL. Numbered Extended ACLs are created using the same global configuration commands that are used for standard ACLs. The procedural steps for configuring extended ACLs are the same as for standard ACLs. However, the command syntax and parameters are more complex to support the additional features provided by extended ACLs. To create a numbered extended ACL, use the Router(config)# **access-list** *access-list-number* {**deny** | **permit** | **remark** *text*} *protocol source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**log**] global configuration command. Extended ACLs can filter on many different types of Internet protocols and ports. Selecting a *protocol* influences *port* options. For instance, selecting the **tcp** protocol would provide TCP related ports options. Configuring the port number is required when there is not a specific *protocol* name listed such as SSH (port number 22) or HTTPS (port number 443). TCP can also perform basic stateful firewall services using the TCP **established** keyword. The keyword enables inside traffic to exit the inside private network and permits the returning reply traffic to enter the inside private network. After an ACL has been configured and applied to an interface, use Cisco IOS **show** commands to verify the configuration. The **show ip interface** command is used to verify the ACL on the interface and the direction in which it was applied.

5.5.4

Module Quiz - ACLs for IPv4 Configuration

1. The computers used by the network administrators for a school are on the 10.7.0.0/27 network. Which two commands are needed at a minimum to apply an ACL that will ensure that only devices that are used by the network administrators will be allowed Telnet access to the routers? (Choose two.)

- [x] **access-class 5 in**
- [ ] **access-list 5 deny any**
- [x] **access-list 5 permit 10.7.0.0 0.0.0.31**
- [ ] **ip access-group 5 in**
- [ ] **access-list standard VTY**
  permit 10.7.0.0 0.0.0.127
- [ ] **ip access-group 5 out**

2. Consider the configured access list.

R1# **show access-lists**
extended IP access list 100
deny tcp host 10.1.1.2 host 10.1.1.1 eq telnet
deny tcp host 10.1.2.2 host 10.1.2.1 eq telnet
permit ip any any (15 matches)

What are two characteristics of this access list? (Choose two.)

- [x] Any device on the 10.1.1.0/24 network (except the 10.1.1.2 device) can telnet to the router that has the IP address 10.1.1.1 assigned.
- [ ] Any device can telnet to the 10.1.2.1 device.
- [ ] The 10.1.2.1 device is not allowed to telnet to the 10.1.2.2 device.
- [ ] Only the 10.1.1.2 device can telnet to the router that has the 10.1.1.1 IP address assigned.
- [ ] A network administrator would not be able to tell if the access list has been applied to an interface or not.
- [x] The access list has been applied to an interface.

3. Which command will verify the number of packets that are permitted or denied by an ACL that restricts SSH access?

- ( ) **show ip ssh**
- ( ) **show ip interface brief**
- ( ) **show running-config**
- (•) **show access-lists**

4. Which access list statement permits HTTP traffic that is sourced from host 10.1.129.100 port 4300 and destined to host 192.168.30.10?

- (•) **access-list 101 permit tcp 10.1.128.0 0.0.1.255 eq 4300 192.168.30.0 0.0.0.15 eq www**
- ( ) **access-list 101 permit tcp 192.168.30.10 0.0.0.0 eq 80 10.1.0.0 0.0.255.255**
- ( ) **access-list 101 permit tcp host 192.168.30.10 eq 80 10.1.0.0 0.0.255.255 eq 4300**
- ( ) **access-list 101 permit tcp 10.1.129.0 0.0.0.255 eq www 192.168.30.10 0.0.0.0 eq www**
- ( ) **access-list 101 permit tcp any eq 4300**

5. When configuring router security, which statement describes the most effective way to use ACLs to control Telnet traffic that is destined to the router itself?

- (•) The ACL should be applied to all vty lines in the *in* direction to prevent an unwanted user from connecting to an unsecured port.
- ( ) Apply the ACL to the vty lines without the **in** or **out** option required when applying ACLs to interfaces.
- ( ) The ACL is applied to the Telnet port with the **ip access-group** command.
- ( ) The ACL must be applied to each vty line individually.

6. What packets would match the access control list statement that is shown below?

access-list 110 permit tcp 172.16.0.0 0.0.0.255 any eq 22

- (•) SSH traffic from the 172.16.0.0 network to any destination network
- ( ) SSH traffic from any source network to the 172.16.0.0 network
- ( ) any TCP traffic from any host to the 172.16.0.0 network
- ( ) any TCP traffic from the 172.16.0.0 network to any destination network

7. Consider the access list command applied outbound on a router serial interface.

access-list 100 deny icmp 192.168.10.0 0.0.0.255 any echo reply

What is the effect of applying this access list command?

- ( ) The only traffic denied is ICMP-based traffic. All other traffic is allowed.
- ( ) The only traffic denied is echo-replies sourced from the 192.168.10.0/24 network. All other traffic is allowed.
- (•) No traffic will be allowed outbound on the serial interface.
- ( ) Users on the 192.168.10.0/24 network are not allowed to transmit traffic to any other destination.

8. Consider the following output for an ACL that has been applied to a router via the **access-class in** command. What can a network administrator determine from the output that is shown?

R1# **<output omitted>**
Standard IP access list 2
10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
20 deny any (1 match)

- ( ) Traffic from one device was not allowed to come into one router port and be routed outbound a different router port.
- (•) Two devices were able to use SSH or Telnet to gain access to the router.
- ( ) Traffic from two devices was allowed to enter one router port and be routed outbound to a different router port.
- ( ) Two devices connected to the router have IP addresses of 192.168.10.x.

9. Which two commands will configure a standard ACL? (Choose two.)

- [x] Router(config)# **access-list 35 permit host 172.31.22.7**
- [ ] Router(config)# **access-list 45 permit 192.168.200.4 host**
- [ ] Router(config)# **access-list 20 permit host 192.168.5.5 any any**
- [x] Router(config)# **access-list 90 permit 192.168.10.5 0.0.0.0**
- [ ] Router(config)# **access-list 10 permit 10.20.5.0 0.255.255.255 any**

10. To facilitate the troubleshooting process, which inbound ICMP message should be permitted on an outside interface?

- ( ) router advertisement
- (•) echo reply
- ( ) time-stamp request
- ( ) echo request
- ( ) time-stamp reply

11. What two ACEs could be used to deny IP traffic from a single source host 10.1.1.1 to the 192.168.0.0/16 network? (Choose two.)

- [ ] access-list 100 deny ip 192.168.0.0 0.0.255.255 host 10.1.1.1
- [ ] access-list 100 deny ip 192.168.0.0 0.0.255.255 10.1.1.1 255.255.255.255
- [ ] access-list 100 deny ip 192.168.0.0 0.0.255.255 10.1.1.1 0.0.0.0
- [ ] access-list 100 deny ip 10.1.1.1 255.255.255.255 192.168.0.0 0.0.255.255
- [x] access-list 100 deny ip host 10.1.1.1 192.168.0.0 0.0.255.255
- [x] access-list 100 deny ip 10.1.1.1 0.0.0.0 192.168.0.0 0.0.255.255

12. An administrator has configured an access list on R1 to allow SSH administrative access from host 172.16.1.100. Which command correctly applies the ACL?

- (•) R1(config-line)# **access-class 1 in**
- ( ) R1(config-if)# **ip access-group 1 in**
- ( ) R1(config-line)# **access-class 1 out**
- ( ) R1(config-if)# **ip access-group 1 out**

Check

Show Me

Reset