Module Practice and Quiz

4.5.1

What did I learn in this module?

Purpose of ACLs

Several tasks performed by routers require the use of ACLs to identify traffic. An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. A router does not have any ACLs configured by default. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if the packet can be forwarded. An ACL uses a sequential list of permit or deny statements, known as ACEs. Cisco routers support two types of ACLs: standard ACLs and extended ACLs. An inbound ACL filters packets before they are routed to the outbound interface. If the packet is permitted by the ACL, it is then processed for routing. An outbound ACL filters packets after being routed, regardless of the inbound interface. When an ACL is applied to an interface, it follows a specific operating procedure:

1. The router extracts the source IPv4 address from the packet header.
2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE in a sequential order.
3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.

Wildcard Masks

An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol. A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, they differ in the way they match binary 1s and 0s. **Wildcard mask bit 0** matches the corresponding bit value in the address. **Wildcard mask bit 1** ignores the corresponding bit value in the address. A wildcard mask is used to filter traffic for one host, one subnet, and a range IPv4 addresses. A shortcut to calculating a wildcard mask is to subtract the subnet mask from 255.255.255.255. Working with decimal representations of binary wildcard mask bits can be simplified by using the Cisco IOS keywords **host** and **any** to identify the most common uses of wildcard masking. Keywords reduce ACL keystrokes and make it easier to read the ACE.

Guidelines for ACL creation

There is a limit on the number of ACLs that can be applied on a router interface. For example, a dual-stacked (i.e, IPv4 and IPv6) router interface can have up to four ACLs applied. Specifically, a router interface can have one outbound IPv4 ACL, one inbound IPv4 ACL, one inbound IPv6 ACL , and one outbound IPv6 ACL. ACLs do not have to be configured in both directions. The number of ACLs and their direction applied to the interface will depend on the security policy of the organization. Basic planning is required before configuring an ACL and includes the following best practices:

- Base ACLs on the organizational security policies.
- Write out what you want the ACL to do.
- Use a text editor to create, edit, and save all of your ACLs.
- Document the ACLs using the **remark** command.
- Test the ACLs on a development network before implementing them on a production network.

Types of IPv4 ACLs

There are two types of IPv4 ACLs: standard ACLs and Extended ACLs. Standard ACLs permit or deny packets based only on the source IPv4 address. Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more. ACLs number 1 -to 99, or 1300 to 1999, are standard ACLs. ACLs number 100-199, or 2000 to 2699, are extended ACLs. Named ACLs is the preferred method to use when configuring ACLs. Specifically, standard and extended ACLs can be named to provide information about the purpose of the ACL.

The following summarizes the rules to follow for named ACLs:

- Assign a name to identify the purpose of the ACL.
- Names can contain alphanumeric characters.
- Names cannot contain spaces or punctuation.
- It is suggested that the name be written in CAPITAL LETTERS.
- Entries can be added or deleted within the ACL.

Every ACL should be placed where it has the greatest impact on efficiency. Extended ACLs should be located as close as possible to the source of the traffic to be filtered. This way, undesirable traffic is denied close to the source network without crossing the network infrastructure. Standard ACLs should be located as close to the destination as possible. If a standard ACL was placed at the source of the traffic, the "permit" or "deny" will occur based on the given source address no matter where the traffic is destined. Placement of the ACL may depend on the extent of organizational control, bandwidth of the networks, and ease of configuration.

4.5.2

Module Quiz - ACL Concepts

1. Which two conditions would cause a router to drop a packet? (Choose two.)
   - [x] The packet source address does not match the source as permitted in a standard inbound ACE.
   - [ ] The ACL that is affecting the packet does not contain at least one deny ACE.
   - [ ] No outbound ACL exists on the interface where the packet exits the router.
   - [x] No routing table entry exists for the packet destination, but the packet matches a permitted address in an outbound ACL.
   - [ ] No inbound ACL exists on the interface where the packet enters the router.
2. A network administrator configures an ACL with the command R1(config)# **access-list 1 permit 172.16.0.0 0.0.15.255**. Which two IP addresses will match this ACL statement? (Choose two.)
   - [x] 172.16.0.255
   - [x] 172.16.15.36
   - [ ] 172.16.65.21
   - [ ] 172.16.31.24
   - [ ] 172.16.16.12
3. Which two statements describe appropriate general guidelines for configuring and applying ACLs? (Choose two.)
   - [ ] If a single ACL is to be applied to multiple interfaces, it must be configured with a unique number for each interface.
   - [x] The most specific ACL statements should be entered first because of the top-down sequential nature of ACLs.
   - [ ] Standard ACLs are placed closest to the source, whereas extended ACLs are placed closest to the destination.
   - [ ] Multiple ACLs per protocol and per direction can be applied to an interface.
   - [x] If an ACL contains no permit statements, all traffic is denied by default.
4. What single access list statement matches all of the following networks?
   192.168.16.0
   192.168.17.0
   192.168.18.0
   192.168.19.0
   - ( ) **access-list 10 permit 192.168.16.0 0.0.0.255**
   - ( ) **access-list 10 permit 192.168.16.0 0.0.15.255**
   - ( ) **access-list 10 permit 192.168.0.0 0.0.15.255**
   - (•) **access-list 10 permit 192.168.16.0 0.0.3.255**
5. Which three statements describe ACL processing of packets? (Choose three.)
   - [x] Each statement is checked only until a match is detected or until the end of the ACE list.
   - [ ] Each packet is compared to the conditions of every ACE in the ACL before a forwarding decision is made.
   - [x] An implicit **deny any** rejects any packet that does not match any ACE.
   - [ ] A packet that has been denied by one ACE can be permitted by a subsequent ACE.
   - [ ] A packet that does not match the conditions of any ACE will be forwarded by default.
   - [x] A packet can either be rejected or forwarded as directed by the ACE that is matched.
6. A network administrator is configuring an ACL to restrict access to certain servers in the data center. The intent is to apply the ACL to the interface connected to the data center LAN. What happens if the ACL is incorrectly applied to an interface in the inbound direction instead of the outbound direction?
   - ( ) All traffic is permitted.
   - ( ) All traffic is denied.
   - ( ) The ACL will analyze traffic after it is routed to the outbound interface.
   - (•) The ACL does not perform as designed.
7. Which scenario would cause an ACL misconfiguration and deny all traffic?
   - (•) Apply an ACL that has all **deny** ACE statements.
   - ( ) Apply a standard ACL using the **ip access-group out**command.
   - ( ) Apply a named ACL to a VTY line.
   - ( ) Apply a standard ACL in the inbound direction.
8. In applying an ACL to a router interface, which traffic is designated as outbound?
   - (•) traffic that is leaving the router and going toward the destination host
   - ( ) traffic that is going from the destination IP address into the router
   - ( ) traffic that is coming from the source IP address into the router
   - ( ) traffic for which the router can find no routing table entry
9. When creating an ACL, which keyword should be used to document and interpret the purpose of the ACL statement on a Cisco device?
   - ( ) **description**
   - (•) **remark**
   - ( ) **eq**
   - ( ) **established**
10. Which location is recommended for extended numbered or extended named ACLs?
    - ( ) a location as close to the destination of traffic as possible
    - (•) a location as close to the source of traffic as possible
    - ( ) a location centered between traffic destinations and sources to filter as much traffic as possible
    - ( ) if using the **established** keyword, a location close to the destination to ensure that return traffic is allowed
11. Which range represents all the IP addresses that are affected when network 10.120.160.0 with a wildcard mask of 0.0.7.255 is used in an ACE?
    - (•) 10.120.160.0 to 10.120.167.255
    - ( ) 10.120.160.0 to 10.127.255.255
    - ( ) 10.120.160.0 to 10.120.168.0
    - ( ) 10.120.160.0 to 10.120.191.255

Check

Show Me

Reset