CCNAv7: Enterprise Networking, Security, and Automation

Companion Guide

Networking Academy

Enterprise Networking, Security, and Automation Companion Guide (CCNAv7)

Cisco Press

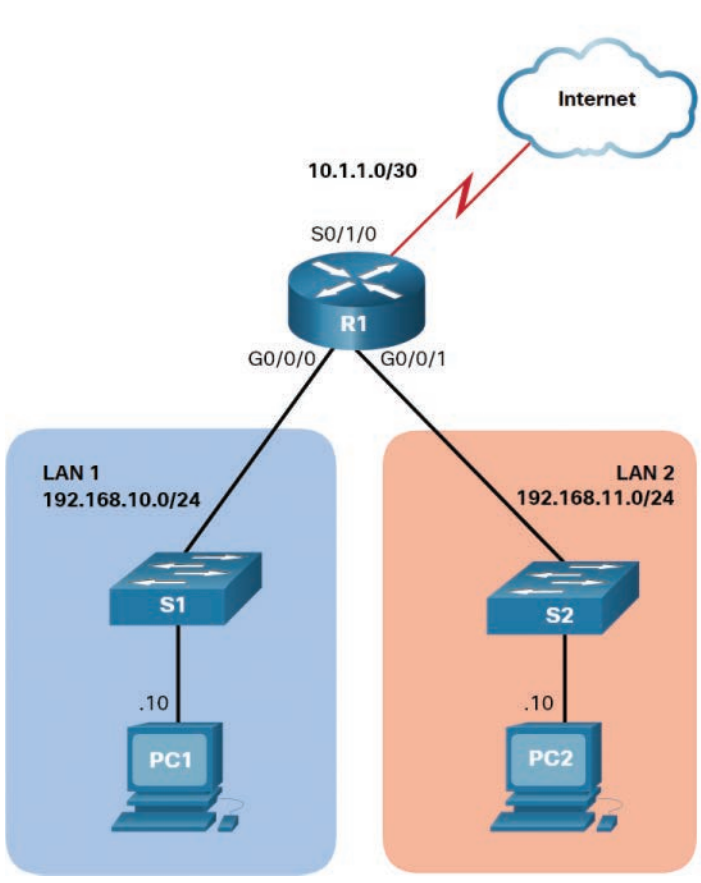

Figure 5-3 Numbered and Named Standard ACL Reference Topology

Example 5-19 Configuring and Applying an ACL to vty Lines

```
R1(config)# username ADMIN secret class
R1(config)# ip access-list standard ADMIN-HOST
R1(config-std-nacl)# remark This ACL secures incoming vty lines
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

A named standard ACL called ADMIN-HOST is created and identifies PC1. Notice that the **deny any** has been configured to track the number of times access has been denied.

The vty lines are configured to use the local database for authentication, permit Telnet traffic, and use the ADMIN-HOST ACL to restrict traffic.

In a production environment, you would set the vty lines to only allow SSH, as shown in Example 5-20.

Example 5-20 Configuring VYT Lines for SSH Access Only

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

Verify the VTY Port Is Secured (5.3.3)

After an ACL to restrict access to the vty lines is configured, it is important to verify that it is working as expected. As shown in Figure 5-4, when PC1 Telnets to R1, the host is prompted for a username and password before the user on PC1 can successfully access the command prompt.

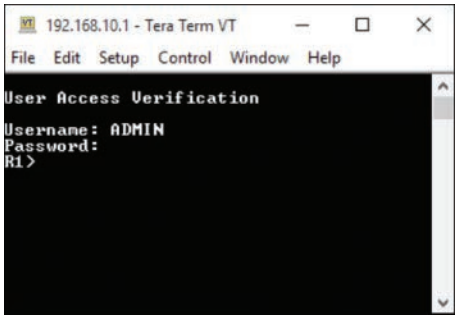

Figure 5-4 Remote Access from PC1

The R1> prompt verifies that PC1 can access R1 for administrative purposes.

Next, test the connection from PC2. As shown in Figure 5-5, when PC2 attempts to Telnet, the connection is refused.

To verify the ACL statistics, issue the **show access-lists** command. Notice the informational message displayed on the console regarding the admin user, as shown in Example 5-21. An informational console message is also generated when a user exits the vty line.

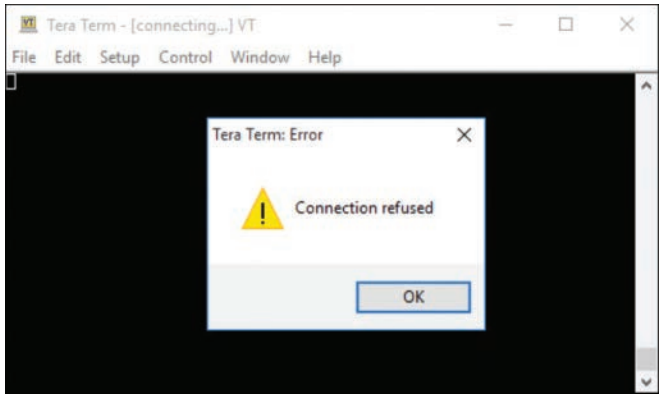

Figure 5-5 Remote Access Attempt from PC2

Example 5-21 Logging Message for Failed Login Attempt

```
R1#
Oct  9 15:11:19.544: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin]
  [Source: 192.168.10.10] [localport: 23] at 15:11:19 UTC Wed Oct 9 2019
R1#
R1# show access-lists
Standard IP access list ADMIN-HOST
    10 permit 192.168.10.10  (2 matches)
    20 deny   any  (2 matches)
R1#
```

The matches in the **permit** line of the output result from the successful Telnet connection by PC1. The matches in the **deny** statement are due to the failed attempt to create a Telnet connection by PC2, a device on the 192.168.11.0/24 network.

Interactive Graphic

Syntax Checker—Secure the VTY Ports (5.3.4)

Refer to the online course to complete this activity.

Configure Extended IPv4 ACLs (5.4)

Extended ACLs enable more control of the filter. In this section, you configure numbered and named extended IPv4 ACLs.

Extended ACLs (5.4.1)

In the previous sections, you learned how to configure and modify standard ACLs and how to secure vty ports with a standard IPv4 ACL. Standard ACLs only filter on

source address. When more precise traffic-filtering control is required, extended IPv4 ACLs can be created.

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 (that is, IP, TCP, UDP, ICMP), and port number. This provides a greater range of criteria on which to base the ACL. For example, one extended ACL can allow email traffic from a network to a specific destination while denying file transfers and web browsing.

Like standard ACLs, extended ACLs can be created as either numbered or named:

- **Numbered extended ACL:** Created using the **access-list** *access-list-number* global configuration command.
- **Named extended ACL:** Created using the **ip access-list extended** *access-list-name*.

Numbered Extended IPv4 ACL Syntax (5.4.2)

The procedural steps for configuring extended ACLs are the same as for standard ACLs. The extended ACL is first configured, and then it is activated on an interface. 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 following global configuration command:

```
Router(config)# access-list access-list-number {deny | permit | remark text}
protocol source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]] [established] [log]
```

Use the **no ip access-list extended** *access-list-name* global configuration command to remove an extended ACL.

Although there are many keywords and parameters for extended ACLs, it is not necessary to use all of them when configuring an extended ACL. Table 5-2 provides a detailed explanation of the syntax for an extended ACL.

Table 5-2 Syntax for Numbered Extended IPv4 ACLs

Parameter	Description
access-list-number	■ This is the decimal number of the ACL. ■ The extended ACL number range is 100 to 199 and 2000 to 2699.
deny	■ This denies access if the condition is matched.

Parameter	Description
permit	■ This permits access if the condition is matched.
remark *text*	■ (Optional) This adds a text entry for documentation purposes. ■ Each remark is limited to 100 characters.
protocol	■ This is the name or number of an internet protocol. ■ Common keywords include **ip**, **tcp**, **udp**, and **icmp**. ■ The **ip** keyword matches all IP protocols.
source	■ This identifies the source network or host address to filter. ■ Use the **any** keyword to specify all networks. ■ Use the **host** *ip-address* keyword or simply enter an IP address (without the **host** keyword) to identify a specific IP address.
source-wildcard	■ (Optional) This is a 32-bit wildcard mask that is applied to the source.
destination	■ This identifies the destination network or host address to filter. ■ Use the **any** keyword to specify all networks. ■ Use the **host** *ip-address* keyword or *ip-address*.
destination-wildcard	■ (Optional) This is a 32-bit wildcard mask that is applied to the destination.
operator	■ (Optional) This compares source or destination ports. ■ Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	■ (Optional) This is the decimal number or name of a TCP or UDP port.
established	■ (Optional) This is for TCP only. ■ It is a first-generation firewall feature.
log	■ (Optional) This keyword generates and sends an informational message whenever the ACE is matched. ■ This message includes ACL number, matched condition (that is, permitted or denied), source address, and number of packets. ■ This message is generated for the first matched packet. ■ This keyword should be implemented only for troubleshooting or security reasons.

The command to apply an extended IPv4 ACL to an interface is the same as the command used for standard IPv4 ACLs:

```
Router(config-if)# ip access-group access-list-name {in | out}
```

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.

Note

The internal logic applied to the ordering of standard ACL statements does not apply to extended ACLs. The order in which the statements are entered during configuration is the order in which they are displayed and processed.

Protocols and Ports (5.4.3)

Extended ACLs can filter on many different types of internet protocols and ports. The following sections provide more information about the internet protocols and ports on which extended ACLs can filter.

Protocol Options

The four highlighted protocols in Example 5-22 are the most popular options.

Note

Use the **?** to get help when entering a complex ACE.

Note

If an internet protocol is not listed, then the IP protocol number could be specified. For instance, the ICMP protocol number is 1, TCP is 6, and UDP is 17.

Example 5-22 Extended ACL Protocol Options

```
R1(config)# access-list 100 permit ?
  <0-255>        An IP protocol number
  ahp            Authentication Header Protocol
  dvmrp          dvmrp
  eigrp          Cisco's EIGRP routing protocol
  esp            Encapsulation Security Payload
  gre            Cisco's GRE tunneling
  icmp           Internet Control Message Protocol
  igmp           Internet Gateway Message Protocol
```