Pedro Luis González Roa
A01651517

Lab 9.3.2.13 - Configuring and Verifying Extended ACLs

Part 2: Configure Devices and Verify Connectivity

Step 7: Verify connectivity between devices.

   a. From PC-A ping PC-C and the loopback on R3

```
Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

   b. From R1, ping PC-C and the loopback on R3.

```
R1#ping 192.168.30.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/26/44 ms

R1#ping 192.168.40.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/21/39 ms
```

   c. From PC-C, ping PC-A and the loopback on R1.

```
Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

   d. From R3, ping PC-A and the loopback on R1.

```
R3#ping 192.168.10.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/20/43 ms

R3#ping 192.168.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/19 ms
```

e. From PC-A, ping the loopback interfaces on the ISP.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

f. From PC-C, ping the loopback interfaces on the ISP.

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Part 3: Configure and Verify Extended Numbered and Named ACLs

Step 1: Configure a numbered extended ACL on R1 for security policy numbers 1 and 2.

What does the 80 signify in the command output listed above? **80 is the port that http uses.**

To what interface should ACL 100 be applied? In what direction should ACL 100 be applied? **On the s0/1/0 interface, with an *out* direction.**

1. Establish an ssh connection from PC-A to R3 using 10.2.2.1 for the IP address. Log in with admin and class for your credentials. *ssh -l admin 10.2.2.1*

```
C:\>ssh -l admin 10.2.2.1

Password:
% Login invalid


Password:




R3#
```

2. From the PC-A command prompt, issue a ping to 10.2.2.1. Explain your results.

Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

The ping was not successful because the only port that is allowed for 10.2.2.1 is 22 (ssh).

Step 2: Configure a named extended ACL on R3 for security policy number 3.

From R3 privileged EXEC mode command prompt, issue the show ip interface s0/0/1 command. What, if any, is the name of the ACL? **WEB-POLICY.** In what direction is the ACL applied? ***Out.***

From PC-C command prompt, ping 209.165.200.225.
```
Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

From PC-C command prompt, ping 10.1.1.1.
```
Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

From PC-C command prompt, ping 209.165.201.1.
```
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

From PC-C command prompt, ping PC-A.
```
Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

From PC-A command prompt, ping 209.165.200.225.
```
Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

From PC-A command prompt, ping 209.165.201.1.
```
Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

From PC-A command prompt, ping 10.1.1.1.
```
Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Part 4: Modify and Verify Extended ACLs

Step 1: Modify ACL 100 on R1

From R1 privileged EXEC mode, issue the show access-lists command. How many lines are there in this access list? **2 lines.**

<modifications>

Where did the new line that you just added appear in ACL 100? **As the third line.**

Step 2: Modify ACL WEB-POLICY on R3

From R3 privileged EXEC mode, issue the show access-lists command. How many lines are there in the access list? **2 lines**

<modifications>

Step 3: Verify modified ACLs

From PC-A, ping the IP address of PC-C.

```
Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

From PC-C, ping the IP address of PC-A.

```
Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Reflection

Why is careful planning and testing of ACLs required? **Because it is very easy to block any important traffic that did not need to be blocked.**

Which type of ACL is better; standard or extended? **Both have their applications, standard is easier for general rules and extended for specific rules.**