Networking Academy

Toff Darell Vergara

T135 October 14, 2025

Packet Tracer - Configure IP ACLs to Mitigate Attacks

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252		N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252		
	G0/0	209.165.200.225	255.255.255.224		
	Lo0	192.168.2.1	255.255.255.0		
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252		N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectives

- Verify connectivity among devices before firewall configuration.
- Use ACLs to ensure remote access to the routers is available only from management station PC-C.
- Configure ACLs on R1 and R3 to mitigate attacks.
- Verify ACL functionality.

Background/Scenario

Access to routers R1, R2, and R3 should only be permitted from PC-C, the management station. PC-C is also used for connectivity testing to PC-A, which is a server providing DNS, SMTP, FTP, and HTTPS services.

Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and destination IP address. In this activity, you will create ACLs on edge routers R1 and R3 to achieve this goal. You will then verify ACL functionality from internal and external hosts.

The routers have been pre-configured with the following:

- Enable password: **ciscoenpa55**
- Password for console: **ciscoconpa55**
- SSH logon username and password: **SSHadmin/ciscosshpa55**
- IP addressing
- Static routing

Part 1: Verify Basic Network Connectivity

Verify network connectivity prior to configuring the IP ACLs.

Step 1: From PC-A, verify connectivity to PC-C and R2.

a. From the command prompt, ping **PC-C** (192.168.3.3).

b. From the command prompt, establish an SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

```
SERVER> ssh -l SSHadmin 192.168.2.1
```

Step 2: From PC-C, verify connectivity to PC-A and R2.

a. From the command prompt, ping **PC-A** (192.168.1.3).

b. From the command prompt, establish an SSH session to **R2** Lo0 interface (192.168.2.1) using username **SSHadmin** and password **ciscosshpa55**. Close the SSH session when finished.

c. Establish another SSH session to R2 G0/0 interface (209.165.200.225) using username **SSHadmin** and password **ciscosshpa55**. When finished, exit the SSH session.

d. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page. Close the browser when done.

Part 2: Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

a. Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**.

Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

Step 3: Verify exclusive access from management station PC-C.

a. Establish an SSH session to 192.168.2.1 from **PC-C** (should be successful).

b. Establish an SSH session to 209.165.200.225 from **PC-C** (should be successful).

c. Establish an SSH session to 192.168.2.1 from **PC-A** (should fail).

Part 3: Create a Numbered IP ACL 120 on R1

Create an IP ACL numbered 120 with the following rules:

- Permit any outside host to access DNS, SMTP, and FTP services on server **PC-A.**
- Deny any outside host access to HTTPS services on **PC-A.**
- Permit **PC-C** to access **R1** via SSH.

Note: Check Results will not show a correct configuration for ACL 120 until you modify it in Part 4.

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server **PC-A**.

Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

Step 3: Apply the ACL to interface S0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.

Part 4: Modify an Existing ACL on R1

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to **R1**). Deny all other incoming ICMP packets.

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.

Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

Step 3: Verify that PC-A can successfully ping the loopback interface on R2.

Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP addresses on **R3**.

Step 1: Configure ACL 110 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.

Step 2: Apply the ACL to interface G0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface G0/1.

Part 6: Create a Numbered IP ACL 100 on R3

On **R3**, block all packets containing the source IP address from the following pool of addresses: any RFC 1918 private addresses, 127.0.0.0/8, and any IP multicast address. Because **PC-C** is being used for remote administration, permit SSH traffic from the 10.0.0.0/8 network to return to the host **PC-C**.

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address. In this activity, your internal address space is part of the private address space specified in RFC 1918.

Use the **access-list** command to create a numbered IP ACL.

Step 2: Apply the ACL to interface Serial 0/0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is handled correctly.

a. From the PC-C command prompt, ping the PC-A server. The ICMP echo replies are blocked by the ACL because they are sourced from the 192.168.0.0/16 address space.

b. Establish an SSH session to 192.168.2.1 from **PC-C**. (should fail)

c. Establish an SSH session to 209.165.200.225. (should be successful).

Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

Router 1

```
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#
R1(config)#hostname R1
R1(config)#enable secret ciscoenpa55
R1(config)#line console 0
R1(config-line)#password ciscoconpa55
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#
R1(config)#ip domain-name local.lab
R1(config)#crypto key generate rsa modulus 1024
                                ^
% Invalid input detected at '^' marker.

R1(config)#username SSHadmin password ciscosshpa55
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#
R1(config)#
R1(config)#interface gigabitEthernet0/1
R1(config-if)#description to_S1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#interface serial0/1/0
R1(config-if)#description to_R2
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

```
R1(config)#interface serial0/1/0
R1(config-if)#description to_R2
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#
R1(config)#ip route 192.168.3.0 255.255.255.0 10.1.1.2
R1(config)#ip route 192.168.2.0 255.255.255.0 10.1.1.2
R1(config)#
R1(config)#
R1(config)#access-list 10 permit host 192.168.3.3
R1(config)#access-list 10 deny any
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#
R1(config)#
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq https
                                                           ^
% Invalid input detected at '^' marker.

R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 permit ip host 192.168.3.3 any
R1(config)#access-list 120 deny ip any any
R1(config)#
R1(config)#interface serial0/1/0
R1(config-if)#ip access-group 120 in
R1(config-if)#exit
```

ROUTER 2

```
Router>en
Router#
Router#
Router#enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#hostname R2
R2(config)#enable secret ciscoenpa55
R2(config)#line console 0
R2(config-line)#password ciscoconpa55
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#
R2(config)#ip domain-name local.lab
R2(config)#crypto key generate rsa modulus 1024
                                   ^
% Invalid input detected at '^' marker.

R2(config)#username SSHadmin password ciscosshpa55
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#access-class 10 in
R2(config-line)#exit
R2(config)#
R2(config)#
R2(config)#interface serial0/1/0
R2(config-if)#description to_R1
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#interface serial0/1/1
R2(config-if)#description to_R3
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#clock rate 64000
This command applies only to DCE interfaces
```

```
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#interface gigabitEthernet0/0
R2(config-if)#description to_ISP
R2(config-if)#ip address 209.165.200.225 255.255.255.224
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#interface loopback0

R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#exit
R2(config)#
R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1
R2(config)#
R2(config)#
R2(config)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

Router 3

```
R3#enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#
R3(config)#
R3(config)#hostname R3
R3(config)#enable secret ciscoenpa55
R3(config)#line console 0
R3(config-line)#password ciscoconpa55
R3(config-line)#login
R3(config-line)#exit
R3(config)#
R3(config)#
R3(config)#ip domain-name local.lab
R3(config)#crypto key generate rsa modulus 1024
                                  ^
% Invalid input detected at '^' marker.

R3(config)#username SSHadmin password ciscosshpa55
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#access-class 10 in
R3(config-line)#exit
R3(config)#
R3(config)#
R3(config)#interface gigabitEthernet0/1
R3(config-if)#description to_S3
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
R3(config)#interface serial0/1/1
R3(config-if)#description to_R2
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
R3(config-if)#exit
R3(config)#
```

```
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
R3(config-if)#exit
R3(config)#
R3(config)#ip route 192.168.1.0 255.255.255.0 10.2.2.2
R3(config)#ip route 192.168.2.0 255.255.255.0 10.2.2.2
R3(config)#
R3(config)#
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#access-list 110 deny ip any any
R3(config)#interface gigabitEthernet0/1
R3(config-if)#ip access-group 110 out
R3(config-if)#exit
R3(config)#
R3(config)#
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit tcp any host 192.168.3.3 eq ssh
                                                              ^
% Invalid input detected at '^' marker.

R3(config)#access-list 100 deny ip any any
R3(config)#interface serial0/1/1
R3(config-if)#ip access-group 100 in
R3(config-if)#exit
R3(config)#
```