Packet Tracer - Configuring Extended ACLs - Scenario 2

Topology



 RIP V2

1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | Fa0/0 | 172.22.34.65 | 255.255.255.224 | N/A |
| Fa1/0 | 172.22.34.97 | 255.255.255.224 | N/A |
| S2/0 | 172.20.10.1 | 255.255.255.252 | N/A |
| R2 | Fa0/0 | 172.22.34.1 | 255.255.255.224 | N/A |
| S2/0 | 172.20.10.2 | 255.255.255.252 | N/A |
| S3/0 | 172.20.20.1 | 255.255.255.252 | N/A |
| R3 | Fa0/0 | 172.22.34.129 | 255.255.255.224 | N/A |
| S2/0 | 172.20.20.2 | 255.255.255.252 | N/A |
| Server | NIC | 172.22.34.10 | 255.255.255.192 | 172.22.30.1 |
| PC1 | NIC | 172.22.34.66 | 255.255.255.224 | 172.22.34.65 |
| PC2 | NIC | 172.22.34.99 | 255.255.255.224 | 172.22.34.97 |
| PC1 | NIC | 172.22.34.130 | 255.255.255.224 | 172.22.34.129 |
| PC2 | NIC | 172.22.34.135 | 255.255.255.224 | 172.22.34.129 |

1. Objectives

Part 1: Configure, Apply and Verify an Extended Numbered ACL

Part 2: Configure, Apply and Verify an Extended Named ACL

1. Background / Scenario

Two employees need access to services provided by the server. **PC1** only needs FTP access while **PC2** only needs web access. Both computers are able to ping the server, but not each other.

1. Configure, Apply and Verify an Extended Numbered ACL
	1. Configure an ACL to permit FTP and ICMP.
		1. From global configuration mode on**R1**, enter the following command to determine the first valid number for an extended access list.

R1(config)# **access-list ?**

<1-99> IP standard access list

<100-199> IP extended access list

* + 1. Add **100** to the command,followed by a question mark.

R1(config)# **access-list 100 ?**

deny Specify packets to reject

permit Specify packets to forward

remark Access list entry comment

* + 1. To permit FTP traffic, enter **permit,**followed by a question mark.

R1(config)# **access-list 100 permit ?**

ahp Authentication Header Protocol

eigrp Cisco's EIGRP routing protocol

esp Encapsulation Security Payload

gre Cisco's GRE tunneling

icmp Internet Control Message Protocol

ip Any Internet Protocol

ospf OSPF routing protocol

tcp Transmission Control Protocol

udp User Datagram Protocol

* + 1. This ACL permits FTP and ICMP. ICMP is listed above, but FTP is not, because FTP uses TCP. So you enter TCP. Enter **tcp** to further refine the ACL help.

R1(config)# **access-list 100 permit tcp ?**

A.B.C.D Source address

anyAny source host

host A single source host

* + 1. Notice that we could filter just for **PC1** by using the **host**keywordor we could allow **any** host. In this case, any device is allowed that has an address belonging to the 172.22.34.64/27 network. Enter the network address, followed by a question mark.

R1(config)# **access-list 100 permit tcp 172.22.34.64 ?**

A.B.C.D Source wildcard bits

* + 1. Calculate the wildcard maskdetermining the binary opposite of a subnet mask.

**11111111.11111111.11111111.111**00000 = 255.255.255.224

00000000.00000000.00000000.000**11111** = 0.0.0.31

* + 1. Enter the wildcard mask, followed by a question mark.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?**

A.B.C.D Destination address

anyAny destination host

eq Match only packets on a given port number

gt Match only packets with a greater port number

host A single destination host

lt Match only packets with a lower port number

neq Match only packets not on a given port number

range Match only packets in the range of port numbers

* + 1. Configure the destination address. In this scenario, we are filtering traffic for a single destination, the server. Enter the**host** keywordfollowed by the server’s IP address.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.10 ?**

dscp Match packets with given dscp value

eq Match only packets on a given port number

established established

gt Match only packets with a greater port number

lt Match only packets with a lower port number

neq Match only packets not on a given port number

precedence Match packets with given precedence value

range Match only packets in the range of port numbers

<cr>

* + 1. Notice that one of the options is **<cr>**(carriage return). In other words, you canpress **Enter** and the statement would permit all TCP traffic. However, we are only permitting FTP traffic; therefore, enter the **eq**keyword,followed by a question mark to display the available options. Then, enter **ftp** and press **Enter**.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.10 eq ?**

<0-65535> Port number

ftp File Transfer Protocol (21)

pop3 Post Office Protocol v3 (110)

smtp Simple Mail Transport Protocol (25)

telnetTelnet (23)

www World Wide Web (HTTP, 80)

R1(config)#**access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp**

* + 1. Create a second access list statement to permit ICMP (ping, etc.) traffic from **PC1** to **Server**. Note that the access list number remains the same and a specific type of ICMP traffic does not need to be specified.

R1(config)# **access-list 100 permit icmp172.22.34.64 0.0.0.31 host 172.22.34.10**

* + 1. All other traffic is denied, by default.
	1. Apply the ACL on the correct interface to filter traffic.

From **R1**’s perspective, the traffic that ACL 100 applies to is inbound from the network connected to Gigabit Ethernet 0/0 interface. Enter interface configuration mode and apply the ACL.

R1(config)# **interface fastEthernet 0/0**

R1(config-if)# **ip access-group 100 in**