Packet Tracer - IPv4 ACL Implementation Challenge

Addressing Table

Device	Interface	IP Address
HQ	G0/0/0	192.168.1.1/26
	G0/0/1	192.168.1.65/29
	S0/1/0	192.0.2.1/30
	S0/1/1	192.168.3.1/30
Branch	G0/0/0	192.168.2.1/27
	G0/0/1	192.168.2.33/28
	S0/1/1	192.168.3.2/30
PC-1	NIC	192.168.1.10/26
PC-2	NIC	192.168.1.20/26
PC-3	NIC	192.168.1.30/26
Admin	NIC	192.168.1.67/29
Enterprise Web Server	NIC	192.168.1.70/29
Branch PC	NIC	192.168.2.17/27
Branch Server	NIC	192.168.2.45/28
Internet User	NIC	198.51.100.218/24
External Web Server	NIC	203.0.113.73/24

Objectives

- Configure a router with standard named ACLs.
- Configure a router with extended named ACLs.
- Configure a router with extended ACLs to meet specific communication requirements.
- Configure an ACL to control access to network device terminal lines.
- Configure the appropriate router interfaces with ACLs in the appropriate direction.
- Verify the operation of the configured ACLs.

Background / Scenario

In this activity you will configure extended, standard named, and extended named ACLs to meet specified communication requirements.

Instructions

Step 1: Verify Connectivity in the New Company Network

First, test connectivity on the network as it is before configuring the ACLs. All hosts should be able to ping all other hosts.

Step 2: Configure Standard and Extended ACLs per Requirements.

Configure ACLs to meet the following requirements:

Important guidelines:

- Do **not** use explicit deny any statements at the end of your ACLs.
- Use shorthand (**host** and **any**) whenever possible.
- Write your ACL statements to address the requirements in the order that they are specified here.
- Place your ACLs in the most efficient location and direction.

ACL 1 Requirements

- Create ACL **101**.
- Explicitly block FTP access to the Enterprise Web Server from the internet.
- No ICMP traffic from the internet should be allowed to any hosts on HQ LAN 1
- Allow all other traffic.

ACL 2 Requirements

- Use ACL number **111**
- No hosts on HQ LAN 1 should be able to access the Branch Server.
- All other traffic should be permitted.

ACL 3: Requirements

- Create a named standard ACL. Use the name **vty_block**. The name of your ACL must match this name exactly.
- Only addresses from the HQ LAN 2 network should be able to access the VTY lines of the HQ router.

ACL 4: Requirements

- Create a named extended ACL called **branch_to_hq**. The name of your ACL must match this name exactly.
- No hosts on either of the Branch LANs should be allowed to access HQ LAN 1. Use one access list statement for each of the Branch LANs.
- All other traffic should be allowed.

Step 3: Verify ACL Operation.

a. Perform the following connectivity tests between devices in the topology. Note whether or not they are successful.

Note: Use the **show ip access-lists** command to verify ACL operation. Use the **clear access list counters** command to reset the match counters.

Send a ping request from Branch PC to the Enterprise Web Server. Was it successful? Explain.

Which ACL statement permitted or denied the ping between these two devices? List the access list name or number, the router on which it was applied, and the specific line that the traffic matched.

Attempt to ping from PC-1 on the HQ LAN 1 to the Branch Server. Was it successful? Explain.

Which ACL statement permitted or denied the ping between these two devices?

Open a web browser on the External Server and attempt to bring up a web page stored on the Enterprise Web Server. Is it successful? Explain.

Which ACL statement permitted or denied the ping between these two devices?

b. Test connections to an internal server from the internet.

From the command line on the Internet User PC, attempt to make an FTP connection to the Branch Server. Is the FTP connection successful?

Which access list should be modified to prevent users from the Internet to make FTP connections to the Branch Server?

Which statement(s) should be added to the access list to deny this traffic?