**Report: Configuring ACLs in a Cisco Packet Tracer Network**

**1. Introduction**

In this project, we used Cisco Packet Tracer to configure and implement Access Control Lists (ACLs) to control traffic in a simulated network environment. The goal of the exercise was to enhance security by managing traffic flow between different network segments and preventing unauthorized access.

**2. Network Topology**

The network consists of two main routers: one located at the headquarters (HQ) and another at a branch office (Branch). Each router connects to different LAN segments and is responsible for managing traffic between the HQ, the Branch, the internet, and various internal devices such as servers and PCs.

The addressing scheme is as follows:

| **Device** | **Interface** | **IP Address** |
| --- | --- | --- |
| HQ Router | G0/0/0 | 192.168.1.1/26 |
| HQ Router | G0/0/1 | 192.168.1.65/29 |
| HQ Router | S0/1/0 | 192.0.2.1/30 |
| HQ Router | S0/1/1 | 192.168.3.1/30 |
| Branch Router | G0/0/0 | 192.168.2.1/27 |
| Branch Router | G0/0/1 | 192.168.2.33/28 |
| Branch Router | S0/1/1 | 192.168.3.2/30 |
| PC-1 (HQ LAN 1) | NIC | 192.168.1.10/26 |
| PC-2 (HQ LAN 1) | NIC | 192.168.1.20/26 |
| PC-3 (HQ LAN 1) | NIC | 192.168.1.30/26 |
| Admin PC (HQ LAN 2) | 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 |

Below is the visual representation of the network setup:

A computer screen shot of a computer

Description automatically generated

**3. ACL Configuration**

The following ACLs were configured on the HQ and Branch routers to meet specific communication requirements:

**Router HQ Configurations**

**ACL 101:**

* Block FTP access to the Enterprise Web Server from the Internet.
* Block FTP Access from Internet User to Branch Server.
* Block all ICMP traffic from the Internet to the HQ LAN.
* Permit all other traffic.

access-list 101 deny tcp any host 192.168.1.70 eq ftp

access-list 101 deny tcp any host 192.168.2.45 eq ftp

access-list 101 deny icmp any 192.168.1.0 0.0.0.63

access-list 101 permit ip any any

**ACL 111:**

* Block access to the Branch Server from HQ LAN 1.
* Permit all other traffic.

access-list 111 deny ip any host 192.168.2.45

access-list 111 permit ip any any

**Standard Named ACL (vty\_block):**

* Restrict VTY access to the HQ router to only HQ LAN 2.

ip access-list standard vty\_block

permit 192.168.1.64 0.0.0.7

**ACL Application on Interfaces:**

interface GigabitEthernet0/0/0

ip access-group 111 in

interface Serial0/1/0

ip access-group 101 in

line vty 0 4

access-class vty\_block in

**Router Branch Configurations**

**Extended Named ACL (branch\_to\_hq):**

* Block access from both Branch LANs (LAN 1 and LAN 2) to HQ LAN 1.
* Permit all other traffic.

ip access-list extended branch\_to\_hq

deny ip 192.168.2.0 0.0.0.31 192.168.1.0 0.0.0.63

deny ip 192.168.2.32 0.0.0.15 192.168.1.0 0.0.0.63

permit ip any any

**ACL Application on Interfaces:**

interface Serial0/1/1

ip access-group branch\_to\_hq out

**4. Connectivity Tests**

I performed various connectivity tests to ensure that the ACLs were working as expected.

**Test 1: Ping from Branch PC to Enterprise Web Server**

* **Result**: The ping was successful, as all traffic except FTP is allowed.
* **ACL Statement**: The traffic was permitted by the final line in ACL 101 on the HQ router.

**Test 2: Ping from HQ PC-1 to Branch Server**

* **Result**: The ping was unsuccessful, as traffic to the Branch Server is blocked.
* **ACL Statement**: The traffic was denied by the first line of ACL 111 on the HQ router.

**Test 3: HTTP Access from External Web Server to Enterprise Web Server**

* **Result**: The web page was successfully accessed, as only FTP traffic is blocked.
* **ACL Statement**: HTTP traffic was permitted by line 20 in ACL 101 on the HQ router.

**5. Conclusion**

The ACLs were successfully implemented to meet the given communication requirements. All rules were applied to the appropriate router interfaces, and connectivity tests confirmed that the ACLs are functioning as expected. Further adjustments may be necessary for additional security, such as blocking FTP access from the Internet to the Branch Server.

This report summarizes the configuration of the ACLs and their impact on network traffic control. The setup enhances network security by preventing unauthorized access while allowing necessary communications to take place.