**Net 3068 CCNA Security Name: Andrew Koenig Lab: # 8.7.4**

**Follow the instructions down below for the lab itself. Anything you type on this document needs to be in blue font. Ensure you put your name and lab number at the top of the document (in blue). For the questions right below, answer in complete sentences. If this is a self-grading packet tracer. Ensure you paste the screen shot of your score page at the bottom of this document. Ensure you upload the packet tracer file along with this document. Let the instructor know if you have any questions.**

***Lab Analysis Report***

1. Using complete sentences summarize work you completed during the lab.

I configured ipv6 acls on multiple routers

2. Using complete sentences describe what you learned from the lab. Hint; look at the lab objectives listed at the top of the lab section.

I learned how to use ipv6 acls to block traffic on routers

***Problems Encountered***

1. Using complete sentences describe any problem(s) experienced during lab.

No problems

2. Using complete sentences describe how you solved your problem(s).

No problems

3. Using complete sentences explain if you needed any assistance with the lab; then list what you learned from that assistance. No problems

Packet Tracer - Configure IPv6 ACLs

# Addressing Table

| Device | Interface | IPv6 Address/Prefix | Default Gateway |
| --- | --- | --- | --- |
| PC1 | NIC | 2001:db8:1:10::10/64 | fe80::1 |
| PC2 | NIC | 2001:db8:1:11::11/64 | fe80::1 |
| Server3 | NIC | 2001:db8:1:30::30/64 | fe80::30 |

1. Blank Line, No additional information

# Objectives

Part 1: Configure, Apply, and Verify an IPv6 ACL

Part 2: Configure, Apply, and Verify a Second IPv6 ACL

# Instructions

## Configure, Apply, and Verify an IPv6 ACL

Logs indicate that a computer on the 2001:db8:1:11::0/64 network is repeatedly refreshing a web page. This is causing a Denial-of-Service (DoS) attack against **Server3**. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list.

### Configure an ACL that will block HTTP and HTTPS access.

Configure an ACL named **BLOCK\_HTTP** on **R1** with the following statements.

* + 1. Block HTTP and HTTPS traffic from reaching **Server3**.

R1(config)# **deny tcp any host 2001:db8:1:30::30 eq www**

R1(config)# **deny tcp any host 2001:db8:1:30::30 eq 443**

* + 1. Allow all other IPv6 traffic to pass.

### Apply the ACL to the correct interface.

Apply the ACL on the interface closest to the source of the traffic to be blocked.

### Verify the ACL implementation.

Verify that the ACL is operating as intended by conducting the following tests:

* Open the **web browser** of **PC1** to http://2001:db8:1:30::30 or https://2001:db8:1:30::30. The website should appear.
* Open the **web browser** of **PC2** to http://2001:db8:1:30::30 or https://2001:db8:1:30::30. The website should be blocked.
* Ping from **PC2** to 2001:db8:1:30::30. The ping should be successful.

## Configure, Apply, and Verify a Second IPv6 ACL

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

### Create an access list to block ICMP.

Configure an ACL named **BLOCK\_ICMP** on **R3** with the following statements:

* + - 1. Block all ICMP traffic from any hosts to any destination.
      2. Allow all other IPv6 traffic to pass.

### Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source. To ensure that ICMP traffic is blocked, regardless of its source or any changes that occur to the network topology, apply the ACL closest to the destination.

### Verify that the proper access list functions.

* + - 1. Ping from **PC2** to 2001:db8:1:30::30. The ping should fail.
      2. Ping from **PC1** to 2001:db8:1:30::30. The ping should fail.
      3. Open the **web browser** of **PC1** to http://2001:db8:1:30::30 or https://2001:db8:1:30::30. The website should display.

### A screenshot of a computer Description automatically generated