# CSSE 490 -- Network Security

# Rose-Hulman Institute of Technology

# Mini Lab 06: Stateful Firewalls

## Learning Objectives

**At the end of this lab, you should be able to:**

- Define how a stateful firewall works in the context of a Linux box.
- Experiment with different stateful rules that are based on network connections, rather than individual packets.

Name: _____

| Question | Points | Score |
|---|---|---|
| **Question 1** | 5 | |
| **Question 2** | 5 | |
| **Question 3** | 5 | |
| **Question 4** | 5 | |
| **Question 5** | 5 | |
| **Question 6** | 10 | |
| **Question 7** | 5 | |
| **Question 8** | 5 | |
| **Question 9** | 5 | |
| **Question 10** | 5 | |
| **Question 11** | 5 | |
| **Question 12** | 10 | |
| **Question 13** | 5 | |
| **Question 14** | 5 | |
| **Question 15** | 5 | |
| **Question 16** | 5 | |
| **Question 17** | 10 | |
| Total: | 100 | |

# 1 A stateful firewall

The question below refer to the first section `A stateful firewall`.

**Question 1**. (5 points) Is the `telnet` session from `client1` still active?

**Question 2**. (5 points) Can you access the `server` from `client2`?

**Question 3**. (5 points) Next, get another terminal on client1 (do not kill the telnet session) and attempt to access the server again. First, attempt to ping the server using `ping -c1 server`.

Are you able to `ping` the server from `client1`?

**Question 4**. (5 points) Also, try to start a new `telnet` session from `client1`, are you able to do so?

**Question 5**. (5 points) Next, kill the `telnet` session on `client1` and then attempt to restart it immediately.

Are you able to reestablish the `telnet` connection from `client1` to the `server`?

Based on all of your observations from above, answer the following question:

**Question 6**. (10 points) What do you think the rule `ct state established,related counter accept` is doing?

## 2 Experiment 1

The questions below refer to the lab questions concerning experiment 1.

**Question 7**. (5 points) What do you expect the behavior of this firewall to be?

**Question 8**. (5 points) Next, while the telnet session is still active, install the firewall rules on the firewall container, then answer the following questions.

What happens to the active `telnet` session (you can try to input anything or run any command to test it)? Why do you think that happened?

**Question 9**. (5 points) Next, let's try to establish a new connection on from either clients to the server. From `client2`, try to `telnet server` to attempt to establish the connection.

Was the `telnet` connection setup successful?

**Question 10**. (5 points) Let's examine what happened even further. On the firewall container, run a packet capture on the `eth1` interface (i.e., the one connected to the server subnet) and examine the packets that are flowing through. Then, please answer the following question about the `telnet` connection.

Does the SYN packets sent from the client to the server reach the server?

**Question 11**. (5 points) Does the server reply to the packet? And does that packet ever make it back to the client?

**Question 12**. (10 points) Based on your answers to the above two questions, explain the difference between this experiment (where we accept everything except established connections) and the one from the first section (where we drop everything except established connections). Specifically, we are interested in the answer to the question of *when are packets dropped* by the firewall?

## 3 Experiment 2

The questions below refer to the lab questions concerning experiment 2. With your firewall rules installed and your packet capture running on the server, connect the `netcat` server from either of the client containers, do not send any packets after the connection is established.

On the firewall, observe the content of the table (`nft list table fw_tbl`). Answer the following questions.

**Question 13**. (5 points) How many packets show up in the `established` rule?

**Question 14**. (5 points) How many packets show up in the `ct direction original` rule?

**Question 15**. (5 points) How many packets show up in the packet capture on the `server`?

**Question 16**. (5 points) Do the number of those packets add up? If not, why do you think so?

## 4 Motivation thought experiment

**Question 17**. (10 points) Say now you are designing your network and you have a web server running on TCP port 80. Since port 80 is a standard port, it is easy for attacker to find out about it by doing a simple network scan, for example using `nmap`. But we don't want that to happen, we would like to block port scans from seeing the presence of port 80 on our protected network.

The first thing you can do is install a firewall at the perimeter of the subnetwork hosting the web server, but that is not enough since port 80 is still exposed to the outside and still be reached by attackers attempting to perform a port scan. We need something more.

In the space below, describe a way to hide port 80 away from everyone except those that really know about it. Please note that we cannot filter based on `IPv4` addresses since we cannot really tell from where our clients might be coming from, so that is off the table.

Here's an analogy. I am hiding from `CSSE332` students in my office and I do not want to open the door except for students from the network security class, can you suggest a way for me to only open the door is I know that the student at the door is not a `CSSE332` student and rather one from this class?