Hacettepe University
Department of Computer Engineering
BBM465 Information Security Laboratory
Experiment 3

Subject: Firewall Configurations, Iptables
Due Date: 10/12/2019 - 23:59

1 Introduction

The goal of this experiment is to enable you the use of the iptables service that provides the firewall configurations of devices in a network. Note that, "iptables" command exists in Linux based OS. Throughout the experiment, you will be supposed to make some tasks based on the network topology given in Figure 1 below.

A firewall separately provides security and control for its own local network and defines the rules while interacting with "outer" real world. Regarding to Figure 1, it should be kept in mind that, in addition to the central firewall, all devices have their own firewalls too. In order to complete the assignment, you may utilize Ubuntu and other Debian based operating systems along with "GNS3" network testing software.

2 General Rules

Each of the following tasks must be carried out independently from each other. Only the devices requiring settings must be involved during configuration stage. In other words, you should avoid to configure unnecessary devices. As a result, you will provide iptables configuration lines for necessary devices in order to achieve the given task. Further, in your report, you must justify your each command line by explaining why you have typed that line. It will also be a good way to explain the parameters of the command.

The default policy of all the chains belonging to the tables of iptables for each device will be considered as "DROP". Moreover, in each task, the old rules in the chains of iptables' tables to be used will be deleted whereas the rules of unused chains will not be erased. At the end of each configuration process, iptables commands will be saved into a text file named as iptables-taskX.txt

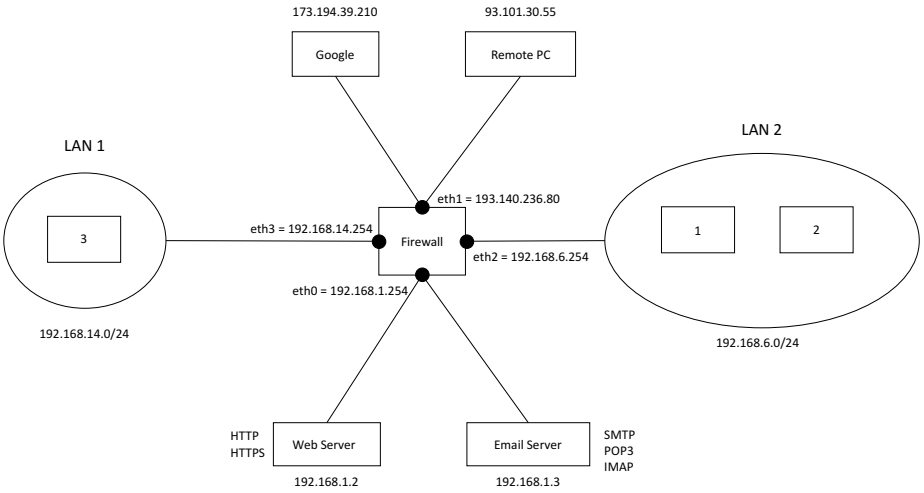

Figure 1: The Topology of the sample network

3 Tasks

1. Write the necessary configurations so that computer 1 can ping to computer 3 only.

2. Write the necessary configurations so that computer 3 can ping all of the computers in LAN 1 (Note: This will be done using ipset).

3. Write the necessary configurations so that the computers in LAN 1 and LAN 2 can only access to the Google server.

4. Write the necessary configurations for the Web Server so that no more than 8 computers can access to the same port over https. (pay attention that the configuration will be done on the Firewall device, not on the Web Server).

5. Write the necessary configurations for the Mail Server in order to prevent it from DDoS attacks. (The configuration will be done on the Firewall device, not on the Mail Server.)

6. Suppose that the Apache has been installed as the Web Server. In order to gain access to the web pages on the Apache by the 3rd party computer (by using the web browser), write the configuration to be done on Web Server. (There will be no configuration for the 3-way firewall and the firewall that routes packets.) (The ports used by the web browser and the Apache server are required.)

4 Notes

1. You need to submit a detailed lab report (i.e report.pdf) to describe what you have done and what you have observed, including screenshots and related iptables configuration lines. It is a good habit to explain the iptables based configuration lines in order to make people gain insight.

2. For each task, prepare a "iptables-taskX.txt" file.

3. You also need to provide explanation to the observations that are interesting or surprising. You are encouraged to pursue further investigation, beyond what is required by the lab description.

4. You can ask questions about the experiment via Piazza group (`piazza.com/hacettepe.edu.tr/fall2019/bbm465`).

5. Late submission will not be accepted!

6. You are going to submit your experiment to online submission system: `www.submit.cs.hacettepe.edu.tr`

   The submission format is given below:
   <Group id>.zip
   −tasks/
   iptables-task1.txt
   iptables-task2.txt
   iptables-task3.txt
   iptables-task4.txt
   iptables-task5.txt
   iptables-task6.txt
   −report/
   report.pdf

5 Policy

All work on assignments must be done with your own group unless stated otherwise. You are encouraged to discuss with your classmates about the given assignments, but these discussions should be carried out in an abstract way.

That is, discussions related to a particular solution to a specific problem (either in actual code or in the pseudocode) will not be tolerated. In short, turning in someone else's work(from internet), in whole or in part, as your own will be considered as a violation of academic integrity. Please note that the former condition also holds for the material found on the web as everything on the web has been written by someone else.
The content of this assignment can be partially changed by the instructor. However, all modifications will be reported into the Piazza system. Therefore, do not forget to keep an eye on Piazza for potential changes.