22HT-2DV702 - Internet Security
Assignment 4 - Firewalls

Configuration & Setup of Filtering Rules, IDS/IPS

Faculty of Technology
Department of Computer Science

This document builds on the work by:
Uraz Odyurt

Instructor: Paolo Molinaro
pm222py@student.lnu.se

24-03-2023

I.INTRODUCTION

The purpose of this practical work is to test different filtering rules on a firewall. You need to have at least two computers running the GNU/Linux operating system. On these computers, you are required to work with the operating system's built-in firewall tool and in this case, you will have access to *iptables*. You will also need to configure some services on these computers, namely, client-server *FTP* service. While the FTP client is available within the Terminal, the FTP server must be configured using ***vsftpd***. In the final part of this assignment, you will also take a brief look at an open-source IDS/IPS, i.e., *Suricata*.

Throughout this document, pay attention to bold terms. Namely, **manually**, i.e., `--state` parameter not allowed, no stateful filtering, and **stateful**. For all tasks involving firewalls, include the syntax you have used during the rule creation, not just a listing of the chains.

Finally, there are different ways to achieve the required results of the assignment. Try to think about the real-world implementations and make sure that your chosen solutions make sense in a production environment.

II. DEADLINE & SUBMISSION

The deadline for the fourth assignment is **Monday the 5th of June, 23:59**. The individual report should be **limited to 8 pages** and should clearly describe the steps you have taken to solve the problem for each section and answer the questions related to each task. Make sure to specify the exact setup premises you have been using to perform experiments. Describe what you had to do to make all tests work and any other remarks or findings that are relevant. To support your answers to the questions, you may need to use references, i.e., to state where you got the information from. Examples of this has been given in the document *"Introduction to Practical Work"* and also in the *"Report Template"*, which must be used for the report.

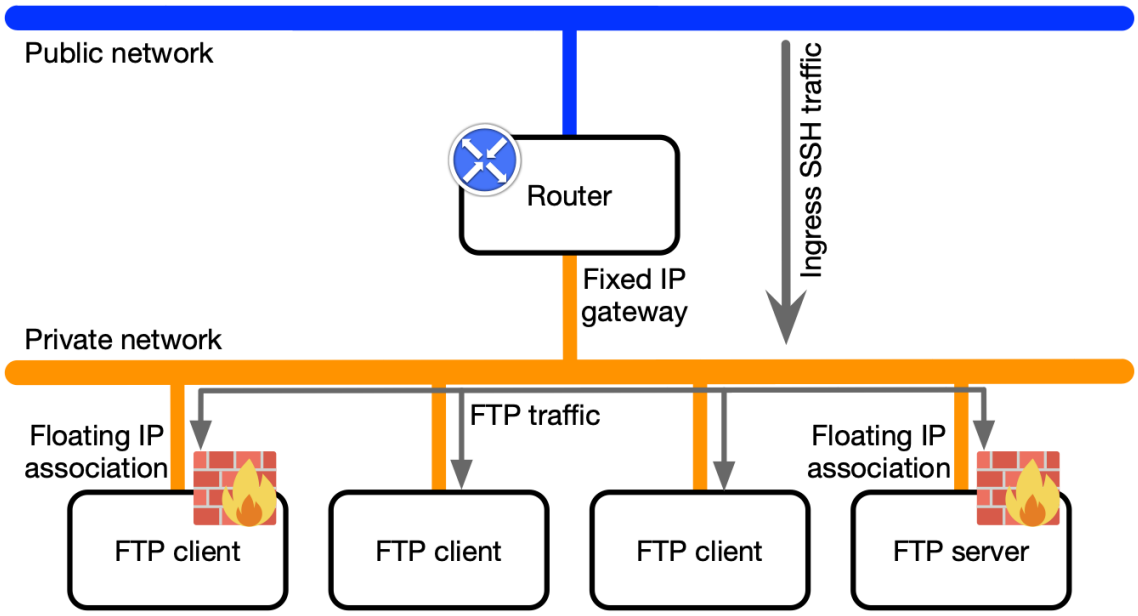
Submission of the report is done on *MyMoodle*; **observe that you must upload the report before the deadline as the system will not accept your file after this time**. Do not forget to put your name and student id on the front page of the Report Template and to convert it to `.pdf` before sending it in.

III. INITIAL SETUP

This practical work takes place over LNU's *CScloud* infrastructure, which is based on OpenStack. Necessary explanations regarding the CScloud will be given during the introductory session for this practical work.

Before you start performing the tasks, you need to setup two compute instances and connect them over a network. For this purpose, there are *Ubuntu* images available on CScloud. You also need to configure supporting mechanisms to allow your remote access via SSH to these instances. You must configure both server and client instances on the same network subnet to allow communication. You should also configure your FTP server by installing/configuring ***vsftpd***. The config file can be found at: `/etc/vsftpd.conf`

The following diagram can give you an idea about your setup for the CScloud environment, remote access, and the extra elements you need to assume in your experiments.



Note: Keep in mind that whatever changes you make to firewall rules, you should always provide SSH reachability.

IV. FIREWALL TASKS

Overall, considering the limited number of pages, prioritize listing the rules used over the screenshots. Focus on the description of the output chain with details.

1. Test the connectivity by pinging from your FTP client computer. Do you get any responses? Can you change the rules for ICMP making it possible to allow or block it in either direction? Provide rules for these. Are there other types of rules for ICMP? Give a couple of example rules. Create necessary firewall rules **manually**.

2. **With focus on the client**, make sure you can access the FTP server from the FTP client behind the firewall and get files from it. FTP is a bit special, since for the ordinary setup it requires two TCP connections, one for commands and one for data transfers. How is your firewall handling that? Can you use FTP in both **passive** and **active** modes? Test different rulesets in the FTP client's firewall. Compose separate rulesets for,
a) passive and
b) active modes.
Create necessary firewall rules **manually**.

3. **Flush the chains. Focus on the server**, make the same type of tests as in task 2, but now for incoming FTP connections from the FTP client. Which settings in the FTP server and its firewall make it possible to serve FTP for the network in different modes? Compose separate rulesets for,
a) passive and
b) active modes.
Create necessary firewall rules **manually**.

4. Refresh the chains by flushing. Now it is time to try out firewall filtering. **Block** the FTP client computer, first for both incoming and outgoing traffic. Where should this blocking happen? At the client, or at the server?
Test different protocols, e.g., ICMP and FTP, to see that everything is blocked. Then lift the restrictions to make it possible to ping in both directions. Lastly, add FTP connectivity, but only for the data channel. Do it separately for,
a) passive and
b) active modes.
Is there any difference when adding the active mode in comparison to the passive mode? Make sure to have everything other than the minimum requirements blocked.
Create necessary firewall rules **manually**.

5. Refresh the chains by flushing. This time **allow** connections to the FTP server from one specific host, the FTP client. Make sure no one else can access it and add FTP connectivity. Compose separate rulesets for,
a) passive and
b) active modes.
Create necessary firewall rules **manually**.

6. Refresh the chains by flushing one last time. Now try to use **stateful** filtering on the server and provide FTP connectivity. Make sure to test FTP functionality after setting the rules. Compose a ruleset for the passive mode. **Use stateful filtering for everything.**

V. INTRUSION DETECTION/PREVENTION SYSTEMS

1. In this part, you will write briefly on the topic of intrusion detection/prevention. Try to keep your text limited to 400 words. A longer essay does not contribute to a better grade. You are expected to include the following in your writing:
   - A taxonomy of IDS/IPS categories,
   - Describe well-known methods and explain which category they belong to. Start from the simple ones, such as *Log Monitoring,*
   - Describe *Extrusion Detection.*

2. Look into the documentation and other resources for *Suricata*, which is a network threat detection engine. Explain the purpose of the following rules and explain the meaning of every keyword/element:

```
alert tcp any any -> any ![20,21] (msg:”This should not happen!”;
flow:to_server; app-layer-protocol:ftp; sid:2271004; rev:1;)
```

```
alert tcp any any -> any [20,21] (msg:”This should not happen!”;
flow:to_server; app-layer-protocol:!ftp; sid:2271005; rev:1;)
```

Do not forget to reference your sources.