CPRE 431

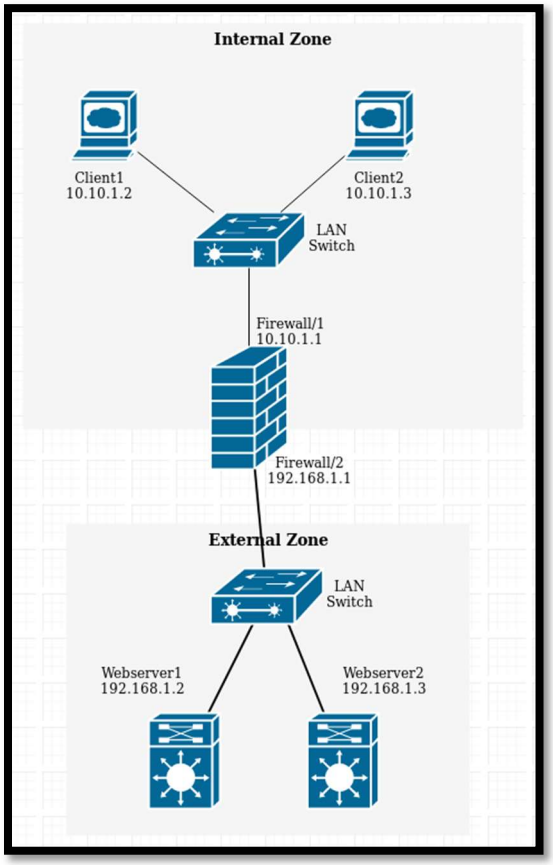
M06 Lab HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!
Please ensure that you support all your answers with the correct screenshots showing your solutions.

Notes:

- The goal of this lab is to use iptables to create simple firewall rules.
- Use the "Introduction to iptables" page on canvas to help you in the needed commands for this homework.
- This homework consists of 5 tasks. **The answer for each task requires you to record a command/result and write an explanation and support this with screenshots.**
- Use the template "M06 - Answers.txt" file (attached with the homework) as a guideline of how the answer should look like. Your answer submission must be in .pdf format ONLY!
- The tasks assume you have created the below virtual network topology on GENI platform. You can use the rspec file "M06 - rspec.xml" (attached with the homework) to create the network topology on GENI platform (if the reservation failed because there is no enough pcs, please use a different InstaGENI site).
- This virtual network consists of two zones, internal (Clients) and external (Servers). The internal zone consists of two clients (Client1 and 2) connected through a LAN switch to a Firewall that connects them to the external zone. The Firewall has two interfaces "Firewall/1" connected to the internal network, and "Firewall/2" connected to the external zone. The external zone has many servers connected through a LAN switch to the Firewall. However, we will only focus on two servers (Webserver1 and 2). The below figure has the network diagram and the needed details for the zones, clients, servers, and firewall:



- **In all your answers, try to write rules as general as possible.** For example, although we are only focusing on two servers in the external zone, try to write rules such that the policy is achieved even if there were more than two servers.
- **Always remember to flush all iptables rules between tasks** (for example: after completing task 1, make sure there are no rules before you start task 2).

Task 1: (Aim: understand the difference between INPUT, FORWARD, and OUTPUT chains):

1. Add **Rule1** to the firewall filter table that blocks ping (icmp) packets being forwarded between the two subnets.
2. Delete Rule1, and then add **Rule2** that blocks ping packets coming into the firewall.
3. Delete Rule2, and then add **Rule3** that blocks ping packets coming out of the firewall.

To test each of the above rules, try to ping between the following pairs of nodes, and observe whether it is successful or not:

- Client1 to Webserver1
- Webserver2 to Client2
- Client1 to Firewall
- Firewall to Webserver1
- Client1 to Client2

4. Record your rules' results (allowed or blocked) and an explanation of the difference between the three chains in your answer (take screenshots of webserver/client/firewall terminals to show your syntax and results of pings).

Task 2: (Aim: filter based on ports and IPs):

This task will be testing SSH connections between client and server. SSH is enabled by default on the webservers. GENI platform forces SSH through key-pair authentication only. We will need to enable SSH to use password authentication as well.

1. On Webserver1 and Webserver2, to enable password authentication for SSH, we need to change the SSH configuration as follows:

   ```
   > sudo nano /etc/ssh/sshd_config
   ```

   - Near the end of the file, search for the line having: "`PasswordAuthentication no`"
   - Change it to "`PasswordAuthentication yes`", then save the changes and exit.

2. Restart the SSH service:

   ```
   > sudo service ssh restart
   ```

3. On Webserver1, Webserver2 and the Firewall, we need to create a test user to be used in verifying the SSH connections:

   ```
   > sudo adduser test
   ```

   - Add the user password and information needed to create the user.

4. Verify that the SSH connection can be established as follows:

   - On Client1:

   ```
   > ssh test@webserver1
   ```

   - Ensure that you get a prompt for password, then enter the password for user "test" and ensure the SSH connection is successfully established.

5. Now we need to configure the Firewall to control the SSH connections. Add **Rule4** to the firewall filter table to prevent Client1 from SSHing to any outside nodes, but it can still SSH to the firewall itself.
6. Test the correctness of **Rule4**.

Task 3: (Aim: filter based on ports, understand HTTP request/response format):

The first part of this task is similar to how we setup the environment of HW04. Please refer to HW04, if you need help with the commands.

1. Install and enable the Apache webserver on both Webserver1 and Webserver2.
2. The Lynx web browser should be installed by default on both Client1 and Client2. To verify run the following command on the clients:

   ```
   > lynx -version
   ```

3. Verify that the web servers are running by connecting to them from the Lynx browsers on the clients, and you should see the Apache2 Ubuntu Default Page.

   ```
   > lynx http://webserver1
   ```

4. Use a text editor to change the index.html file to include your group number and members' names in the heading of the default webpage (use <h1> tags):

   ```
   > sudo nano /var/www/html/index.html
   ```

5. Verify that your changes are applied by connecting to the server again using the Lynx browser from the clients. Check the response and make sure it is what you expected.
6. Add **Rule5** to the Firewall filter to prevent internal zone clients from accessing the webpage on Webserver1.
7. Test the correctness of **Rule5**.

Task 4: (Aim: change default policy):

1. Up to this point, we were using the default policy of ACCEPT on the Firewall. For **task 5** we will use the default policy of DROP.
2. Change the default policy of the firewall "forwarding" table to DROP.
3. Verify that all connections tested through tasks 1 to 3 are blocked without adding their rules.

Task 5: (Aim: use Stateful Packet Inspection):

1. Enable Stateful Packet Inspection on the firewall with:

   ```
   > sudo iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
   ```

2. Add **Rule6** so that inside hosts can access outside websites
3. Add **Rule7** so that outside hosts can SSH into Client1. To enable SSH to Client1, please refer to commands used in task 2.
4. No other access should be allowed.

Hint: In iptables rules, you can use "-i" and "-o" to specify the input or output interfaces.

5. To view the SPI table, you need to install the "conntrack" package on the firewall:

```
> sudo apt-get install conntrack
```

6. Then you can view the SPI table with:

```
> sudo conntrack -L
```

7. To view the SPI entries created on the fly while testing the firewall:

```
> sudo conntrack –E
```

Hint: GENI platform uses the network 172.17.0.0/16 for internal maintenance. You can filter out these packets/connections through your analysis by using –s <Scr_IP> or –d <Dst_IP> with conntrack commands.

8. Test the correctness of **Rule6** by connecting to the webpage on Webserver1 from Client2.
9. Test the correctness of **Rule7** by SSHing to Client1 from Webserver1.
10. Test any other connections and ensure they are all blocked.