Packet Filter

You will use a packet filter (firewall) as a mitigation tool. More specifically, we will use the IPTables tool (via a GUI) to configure the firewall to block connections to your Web server running in your VM. All the necessary tools are available on your VM.

GOAL: Block connection from a <GIVEN IP> to your Web Server.

You should use the tool '*gufw*' (ufw stands for 'uncomplicated firewall') already installed in your VM to manage the firewall rules.

First start the graphical tool:

```
$ sudo gufw
```

Fig. 1: Firewall Configuration Interface

This will open the graphical interface (Figure 1) that will be used to configure the Linux firewall. In this interface, you can see that the firewall is disabled (**Status**). Additionally, you can see the options **Ingoing** and **Outgoing**. These options represent the default firewall policy. For instance, in Figure 2, the firewall is denying all the incoming traffic and allowing all the outgoing traffic.

Since we want to provide access to the Web server but deny for a particular host, this is not how we should configure the firewall. In this lab you have to configure the firewall in order to block the connections from a specific IP but enabling regular traffic from other to your Web server.
So, **blocking all connections to your VM or blocking all connections to the Web server (80/TCP) is not a reasonable solution.**

You should find a configuration that enables access to your Web server but blocks connections from a particular IP address. As Figure 6 shows, you can add rules by clicking on the **Rules** tab and then by clicking on the plus sign. (You do need to enable the firewall (status) for your rules to take effect.)

Fig. 2: Add a new packet filter rule

For example, as shown in Figure 3, you can add a firewall rule for a specific application, such as SSH. This rule will then show up in the Rules tab.

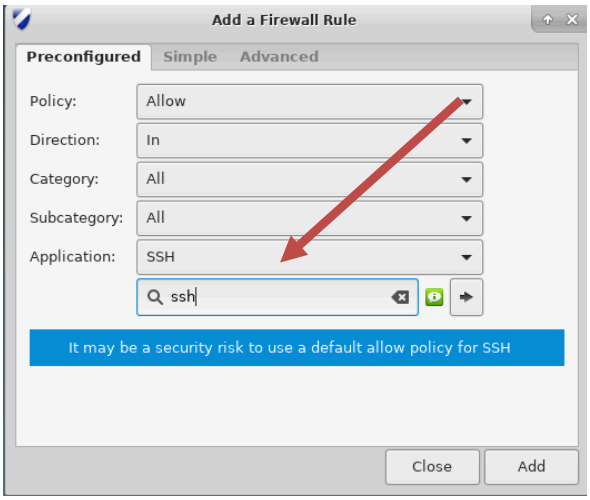

Fig. 3: Rule associated with a specific service

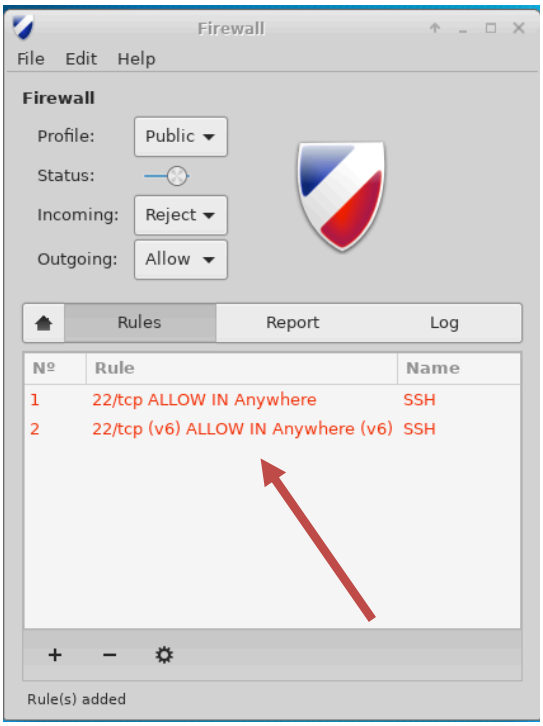

Figure 1: add rules

The default firewall policy (Incoming, Outgoing) comes into play after all the rules have been processed. If a packet is not processed by a rule in the table, it gets processed by the default policy. This default policy has 4 different options:

- Allow - accept the packets (send it to the next layer in the stack, or forward, etc)
- Deny - deny the packet (this simply discards the packet. This policy is also known as Drop)
- Reject – reject the packet (this policy will send an ICMP packet back to the source notifying that the connection has been rejected)
- Limit - deny traffic if an IP tried several connections (this is a bit of a tricky one, it is not rate-limiting)

Once you have defined the firewall rule, ask for the instructor to connect to your Web Server and check the effectivity of your rule.