ESCUELA COLOMBIANA DE INGENIERIA
JULIO GARAVITO

IT SECURITY AND PRIVACY
GROUP 1L

LABORATORY 14

SUBMITTED BY:
JUAN PABLO FERNANDEZ GONZALES
MARIA VALENTINA TORRES MONSALVE

SUBMITTED TO:
Eng. DANIEL ESTEBAN VELA LOPEZ

BOGOTÁ D.C.
DATE:
12/05/2025

Introduction

This lab aims to provide a hands-on introduction to the use of **pfSense**, an open-source router and firewall platform widely used in network environments. During the activity, we will learn how to install and configure pfSense within a virtualized environment using **VirtualBox**.

We will focus on establishing pfSense as a **router with active DHCP services**, and implementing firewall rules that allow or block network traffic. This includes not only system installation, but also interface configuration, IP address assignment, and connectivity testing.

To validate and test this configuration, we will use two virtual machines: **Kali Linux**, a distribution aimed at penetration testing and security auditing, and **Remnux**, a distribution specialized in malware analysis and incident response. Both machines will be connected to the **internal network managed by pfSense** and should automatically receive IP addresses via DHCP.

Throughout the lab, we'll perform tests such as pings, route checks, and firewall rule configurations to ensure pfSense works as expected, properly managing traffic between WAN and LAN interfaces. This process will allow you to acquire key skills in network administration, security services, and traffic management in simulated environments.

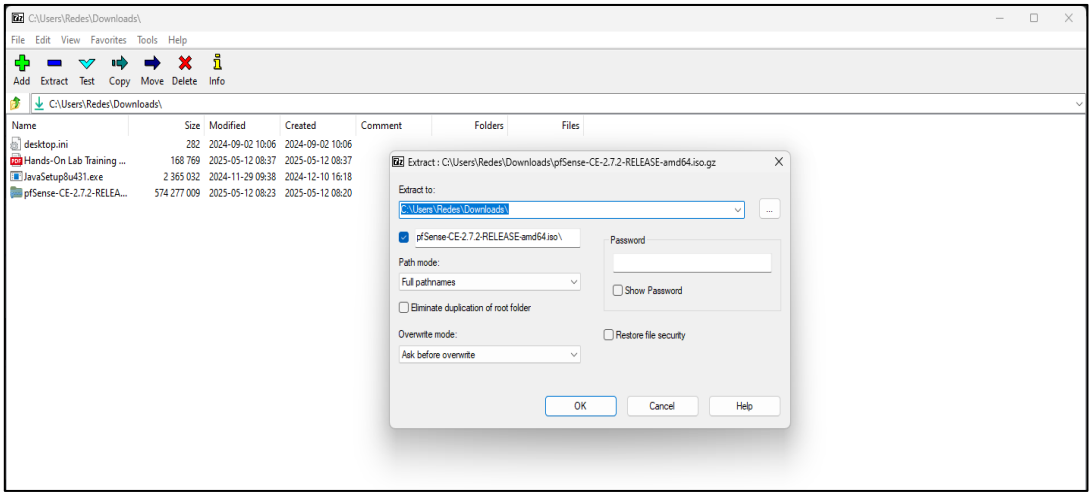
pfSense (router & DHCP)

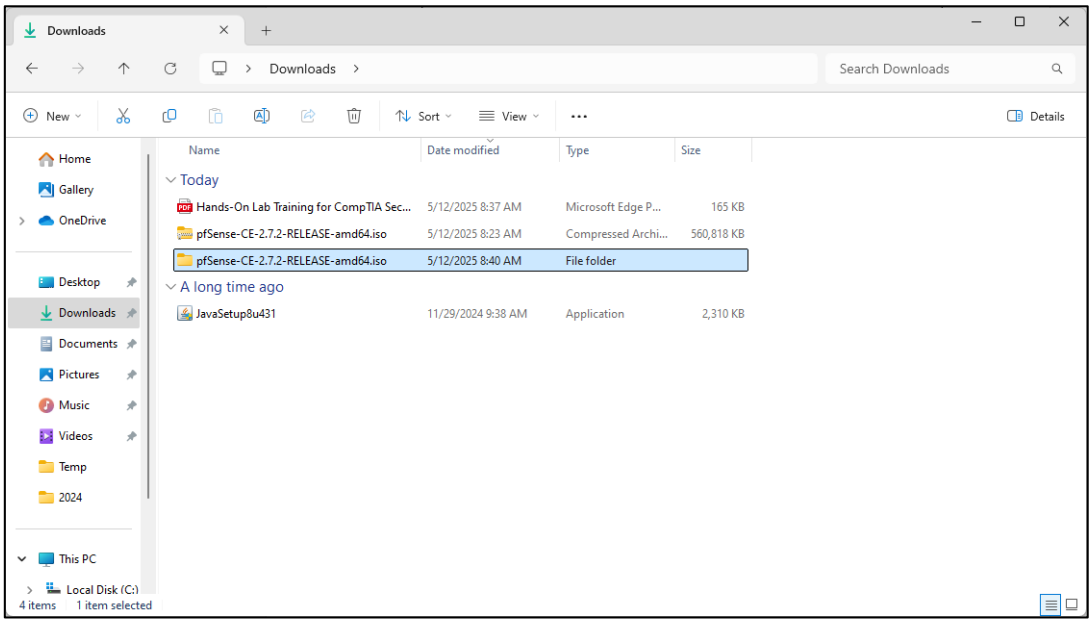
- Creating the Virtual Machine

  The first thing we will do is download the image to create the virtual machine from the link and we will be using the ***pfSense-CE-2.7.2-RELEASE-amd64.iso.gz version*** after the download from the 7zip program we will be able to extract the content of the gz to be able to obtain the ISO.

Index of /mirror/downloads/

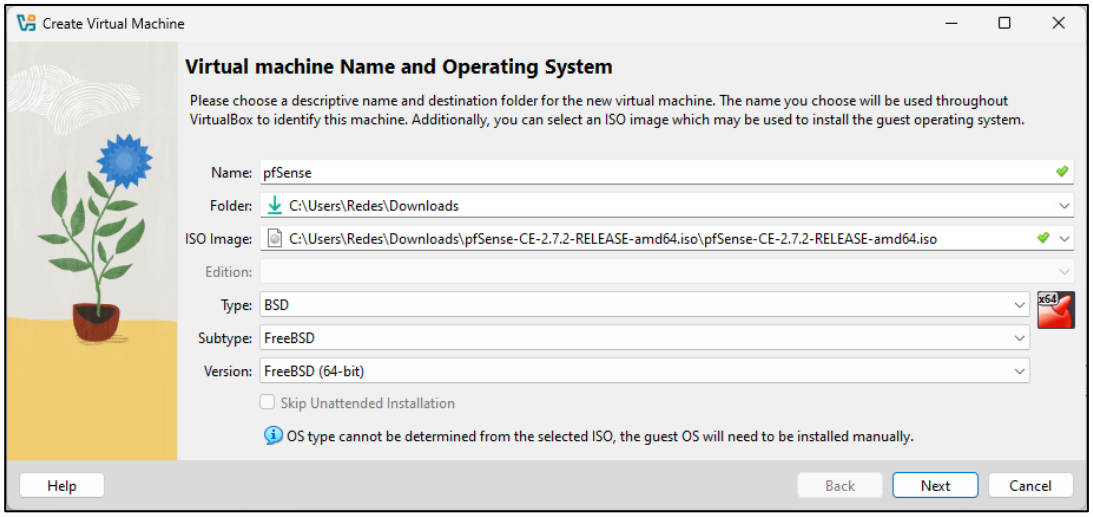
../		
old/	06-Jun-2024 19:18	-
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz	31-Jan-2022 20:31	437073513
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz.sha256	31-Jan-2022 20:32	114
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz	29-Jun-2023 20:11	495733706
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz.sha256	29-Jun-2023 20:11	114
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz	17-Nov-2023 00:47	574639430
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz.sha256	17-Nov-2023 00:47	114
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz	08-Dec-2023 18:27	574277009
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.sha256	08-Dec-2023 18:27	114
pfSense-CE-memstick-2.6.0-RELEASE-amd64.img.gz	31-Jan-2022 20:40	438161574
pfSense-CE-memstick-2.6.0-RELEASE-amd64.img.gz...>	31-Jan-2022 20:40	123
pfSense-CE-memstick-2.7.0-RELEASE-amd64.img.gz	29-Jun-2023 20:11	499043832
pfSense-CE-memstick-2.7.0-RELEASE-amd64.img.gz...>	29-Jun-2023 20:11	123



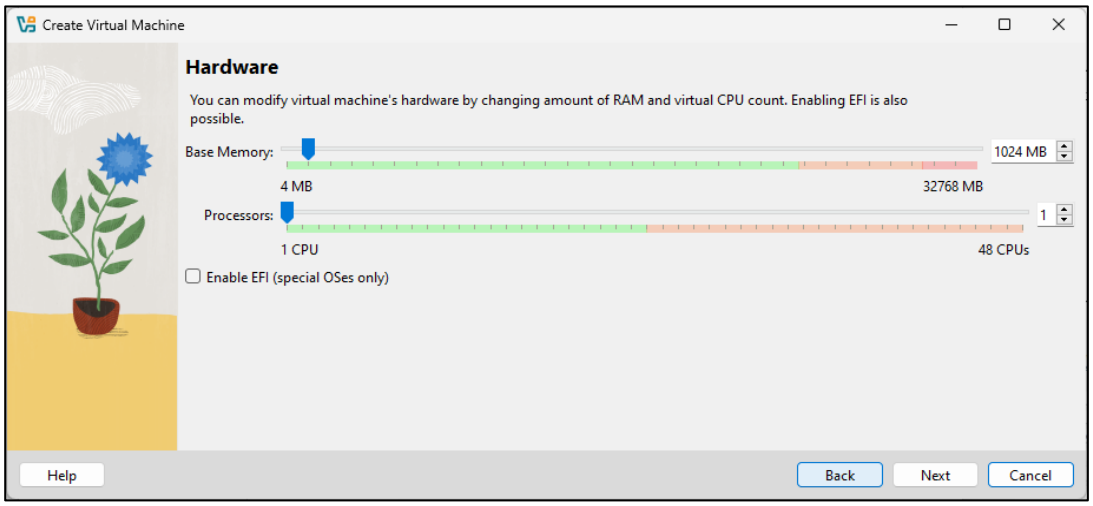


Once with the ISO we will go to VirtualBox and select the option to create new virtual machine and we will add the following configurations:

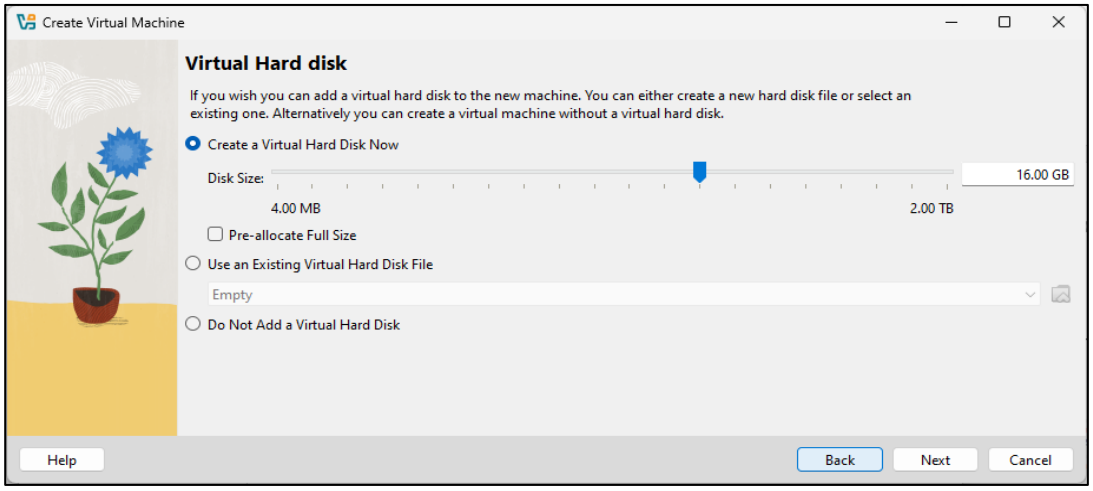
- Name: pfSense (can be any)
- Folder: Where you want to store
- ISO Image: Iso downloaded in the previous step
- Type: BSD
- Version: FreeBSD (64-bit)



- We will give you 1024MB in memory size

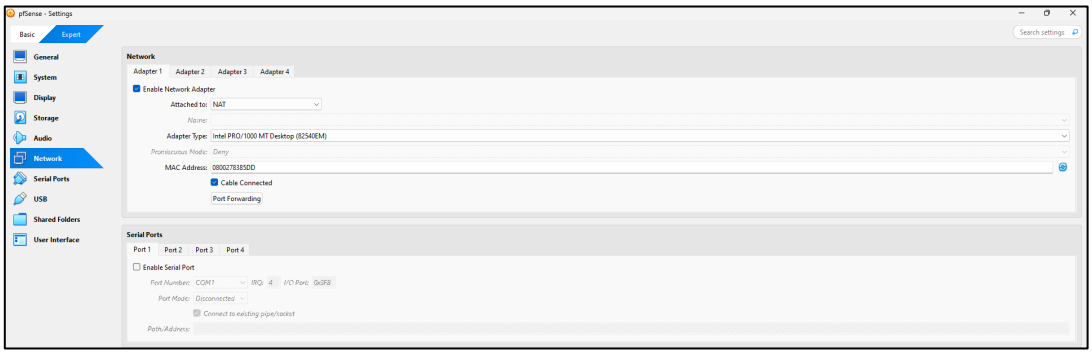


- We will be assigning the size of the disk 16.00 GB

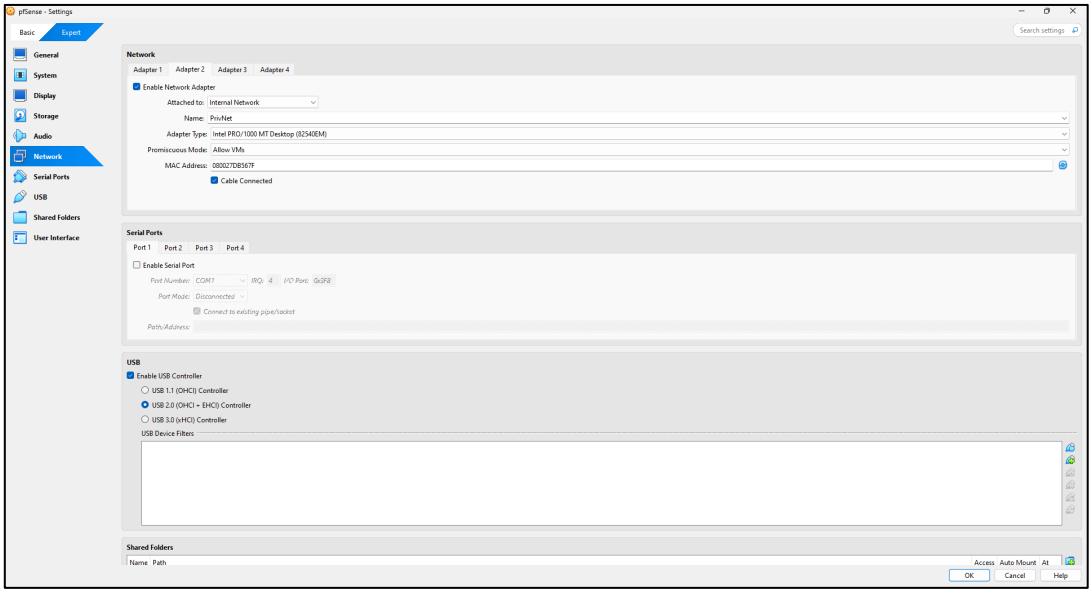


- Configuring network interfaces.

  In the settings section specifically in the Network section we will change adapter 1 to ***Bridged Adapter***.

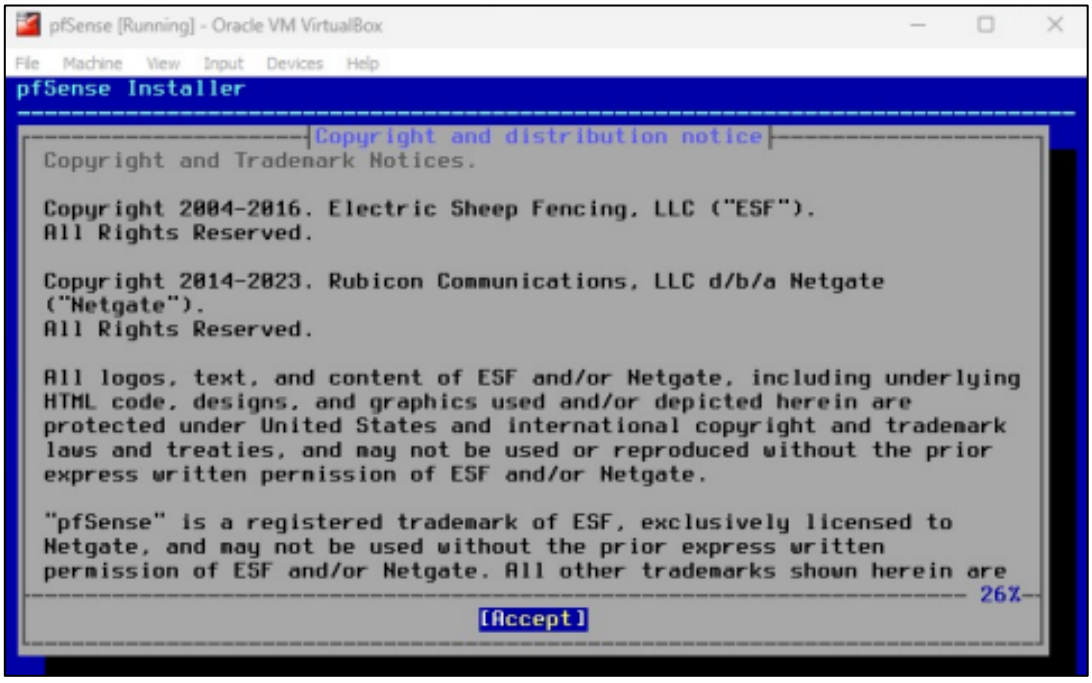


Set Adapter 2 to ***Internal Network*** and rename the network to **PrivNet**. This will be the LAN adapter for internal connectivity. Then, set promiscuous mode to ***Allow all VMs***, and click **OK**.

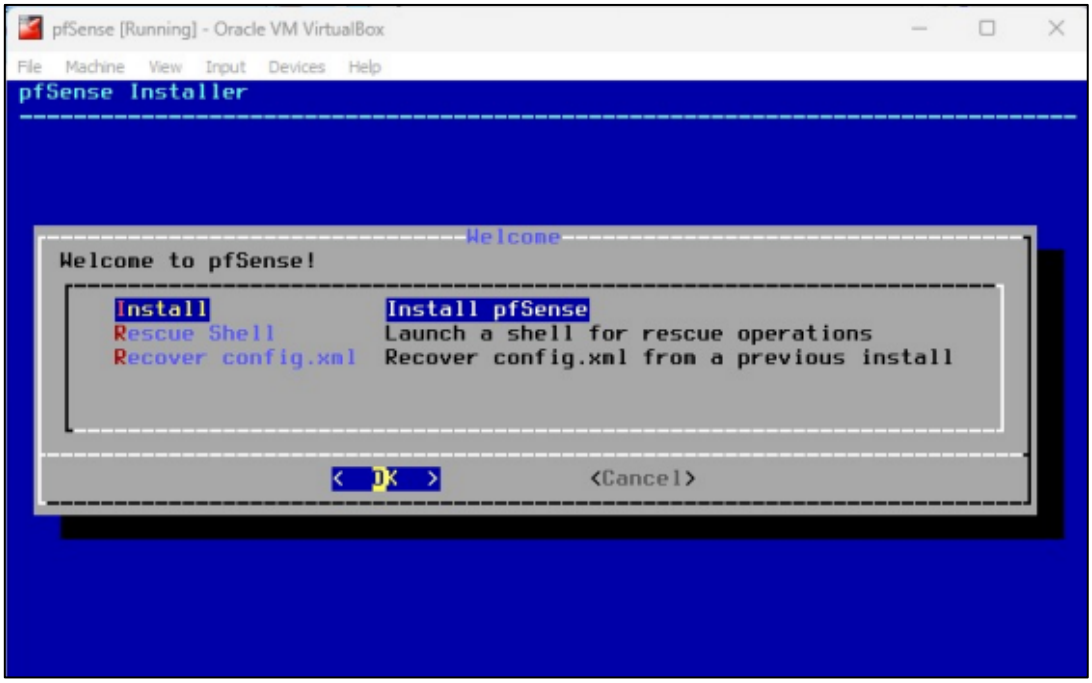


- Install pfSense

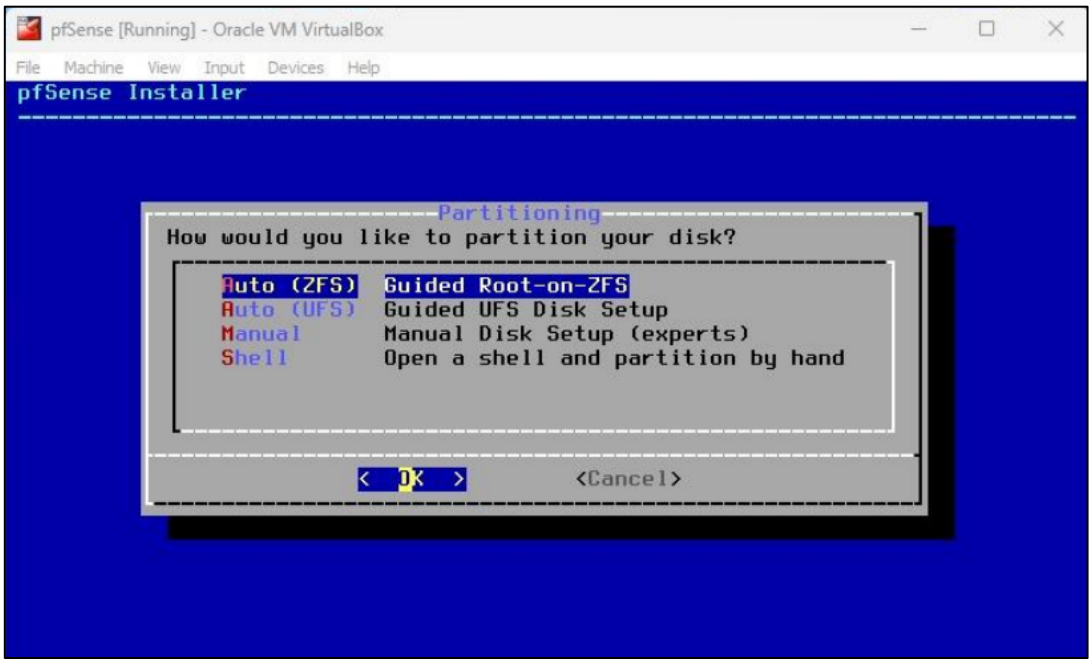
Click **Start** to begin the pfSense installation process and agree to the **copyright and distribution** notice.



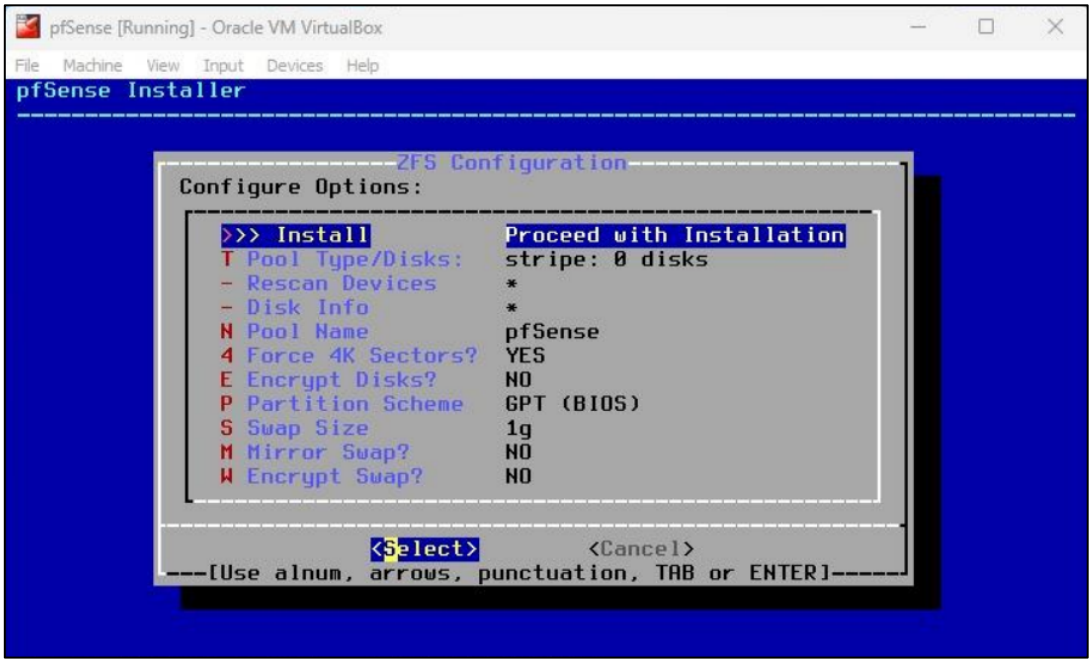
Select the option of ***Install à Install pfSensey*** then enter in the ***OK option***



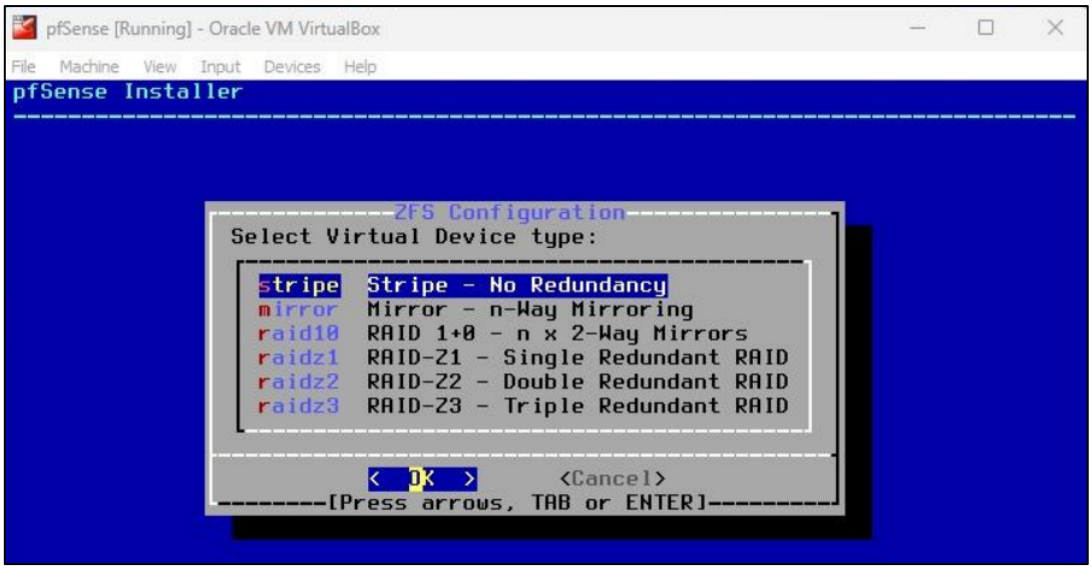
Now we must choose the type of installation. Select the "Auto (ZFS)" option and then click OK. This option is because ZFS is an advanced file system that pfSense recommends for its stability.



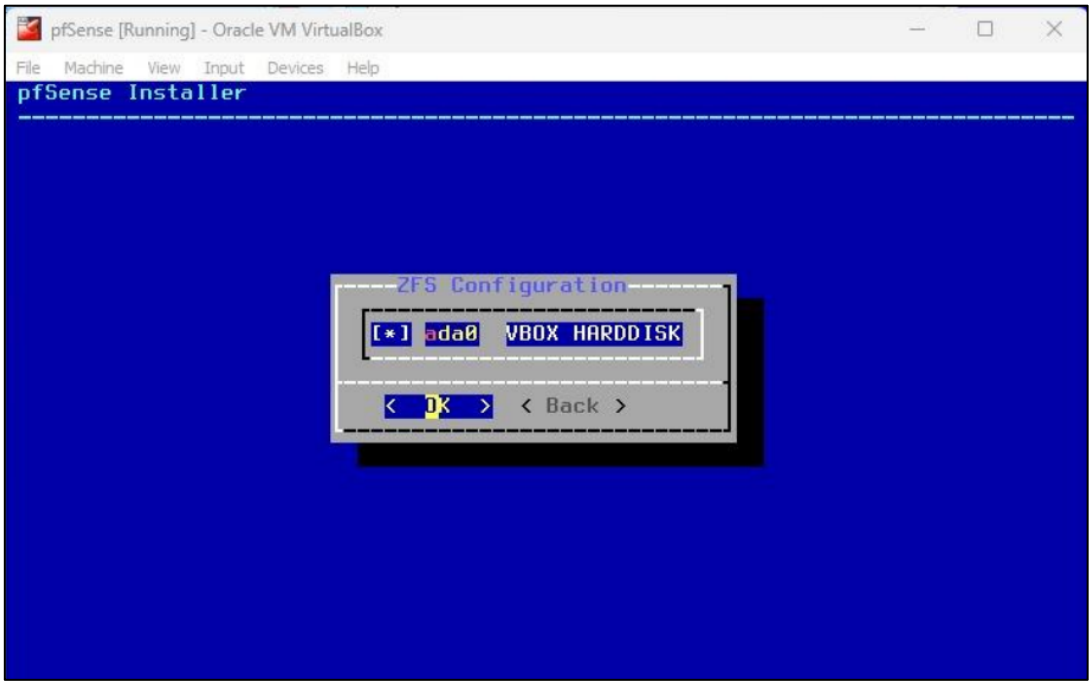
The installer will ask us on which disk we want to install pfSense. We must select the **Install** option and then click on **SELECT**. This confirms that we want to use that disk for installation.



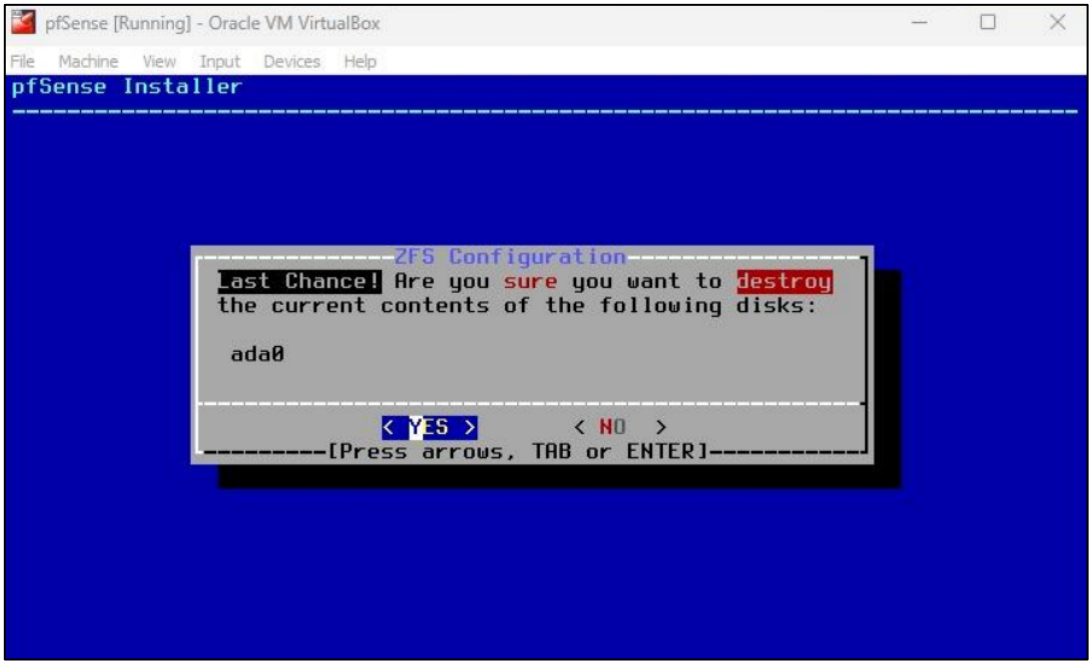
Finally, we need to choose the ***Stripe - No Redundancy*** option and then click OK**.** This configuration has no fault tolerance, but it is faster and more suitable if we are only testing.



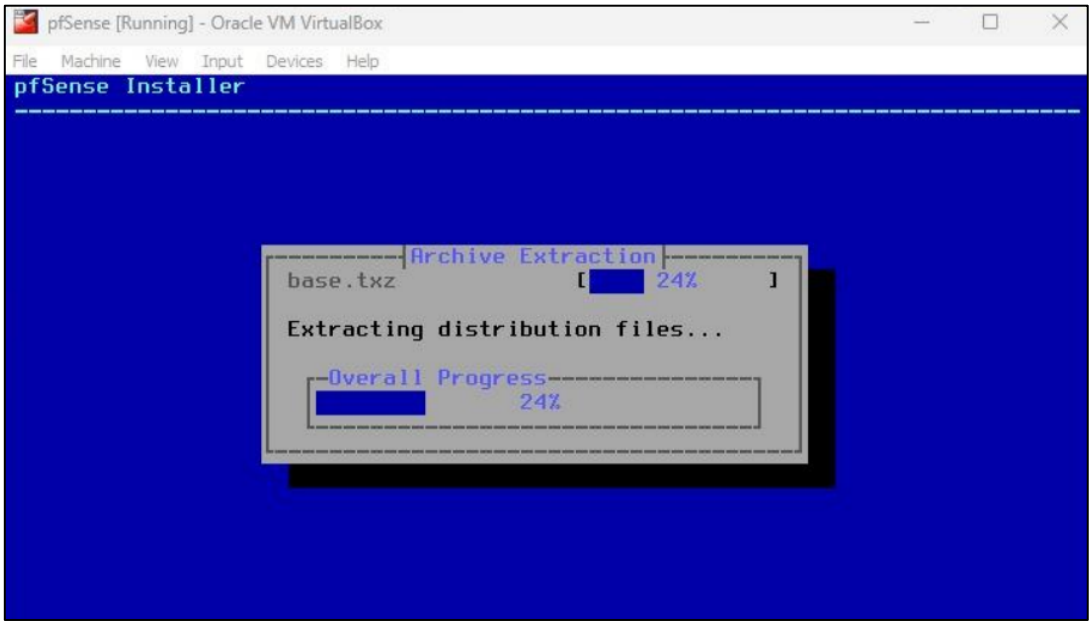
We must select the disk where pfSense will be installed, it usually appears as ***ada0 VBOX HARDDISK.*** Once selected, click ***OK***.



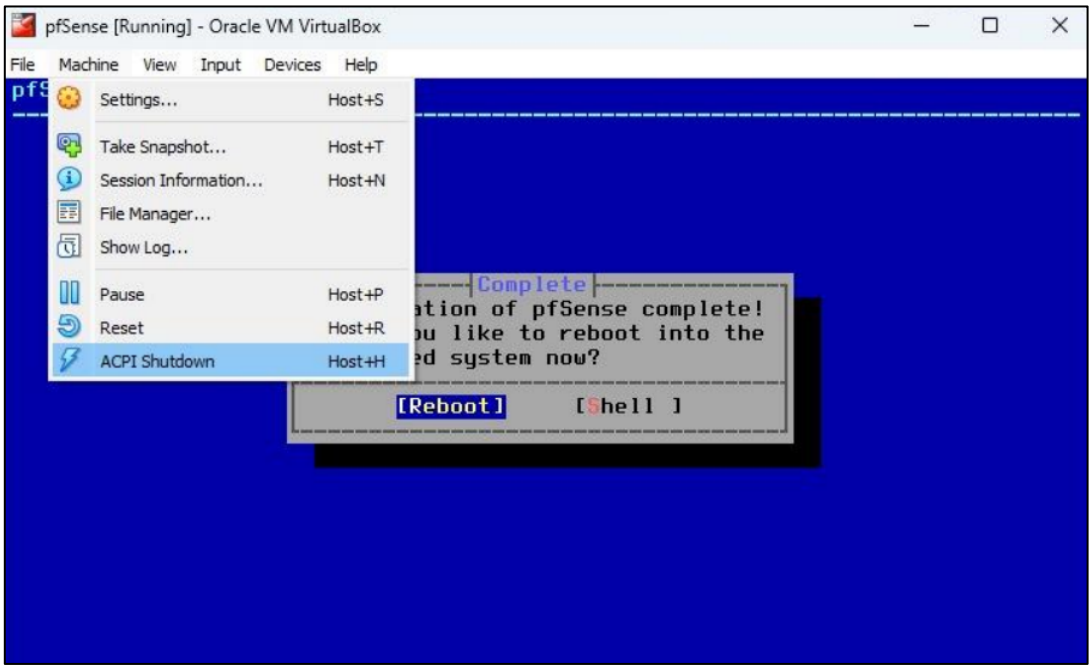
Next, we will be asked to confirm the ZFS configuration. We must select **YES** to continue with the formatting and installation.



At this point, pfSense begins to install on the selected disk. We must wait a few minutes while the files are copied and the systems are configured.



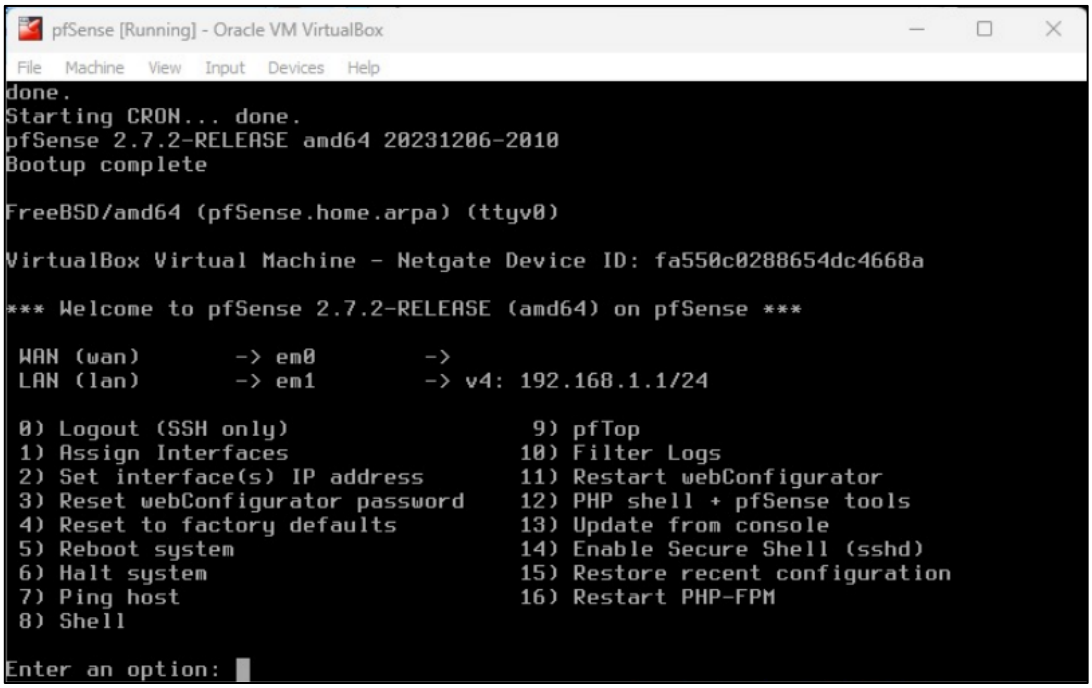
Once the installation is complete, we must shut down the virtual machine from the **VirtualBox Manager**. We do this by selecting the VM, right-clicking, and choosing **"Shut Down" or "Close → Shut Down."**



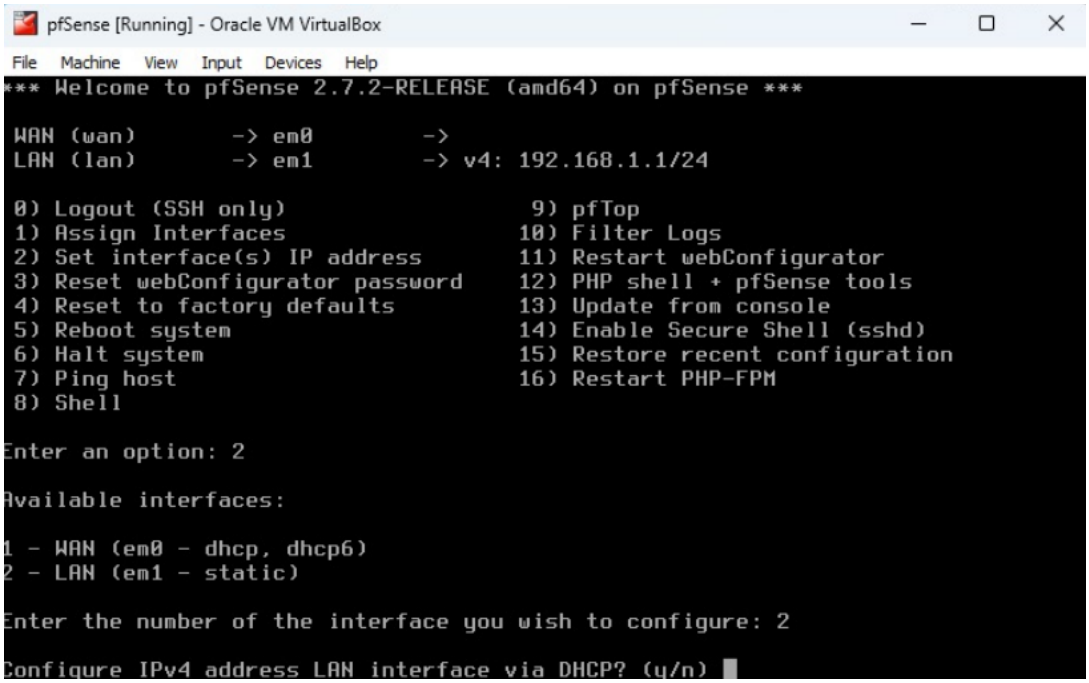
A rather important step To prevent the installation process from being repeated when rebooting, we need **to remove the ISO file** from the virtual disk reader.

- **Configure network interfaces**

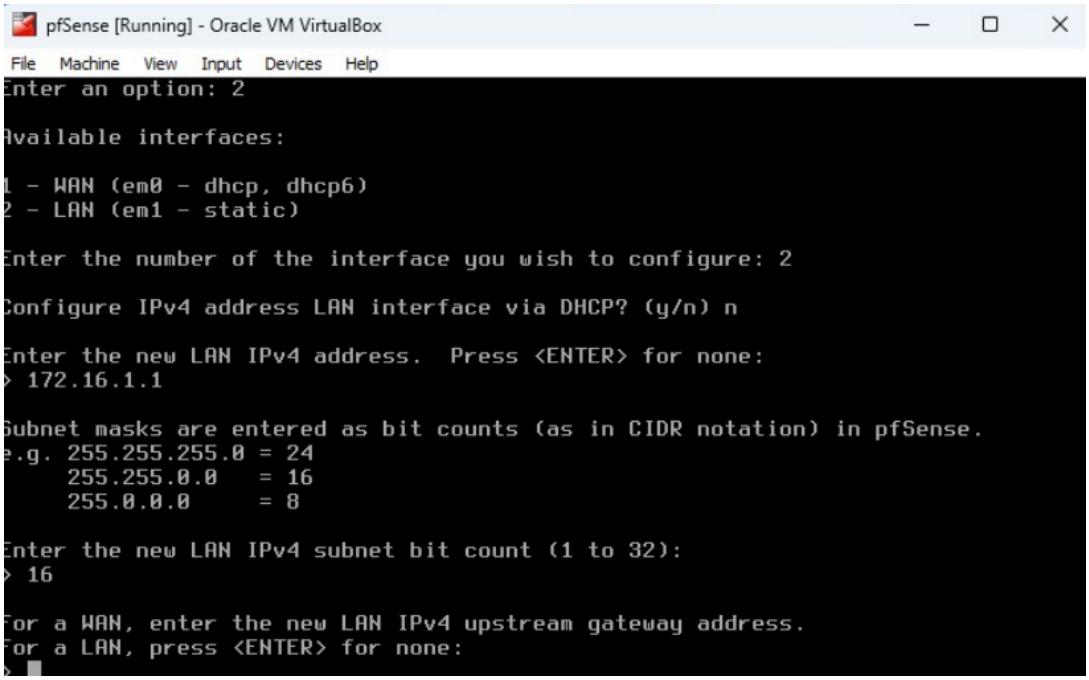
We need to start the pfSense VM from the **VirtualBox Manager**. Once the system has fully booted, the main settings menu will be displayed in the console.



In the main menu, we select option **2)** to configure IP addresses. Then we chose **option 2)** again to configure the **LAN interface (e.g. em1).** When it asks us if we want to use DHCP, we type **"n"** and press Enter.

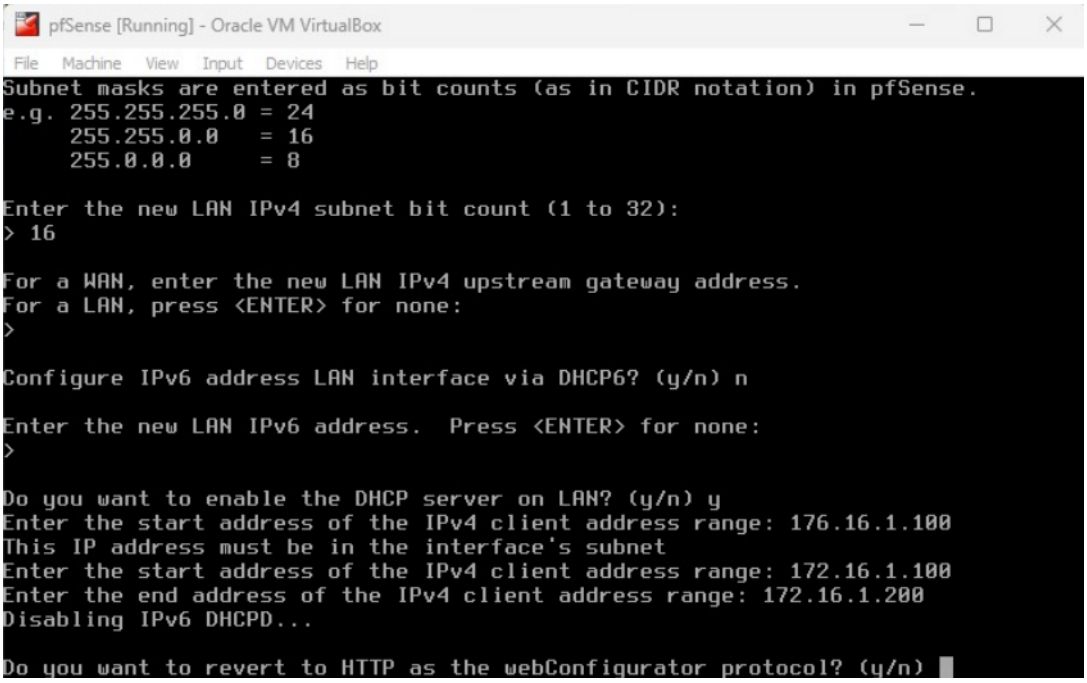


We must type the address **172.16.1.1** and press Enter. Then we type **16** as the subnet mask (Class B) and press Enter.

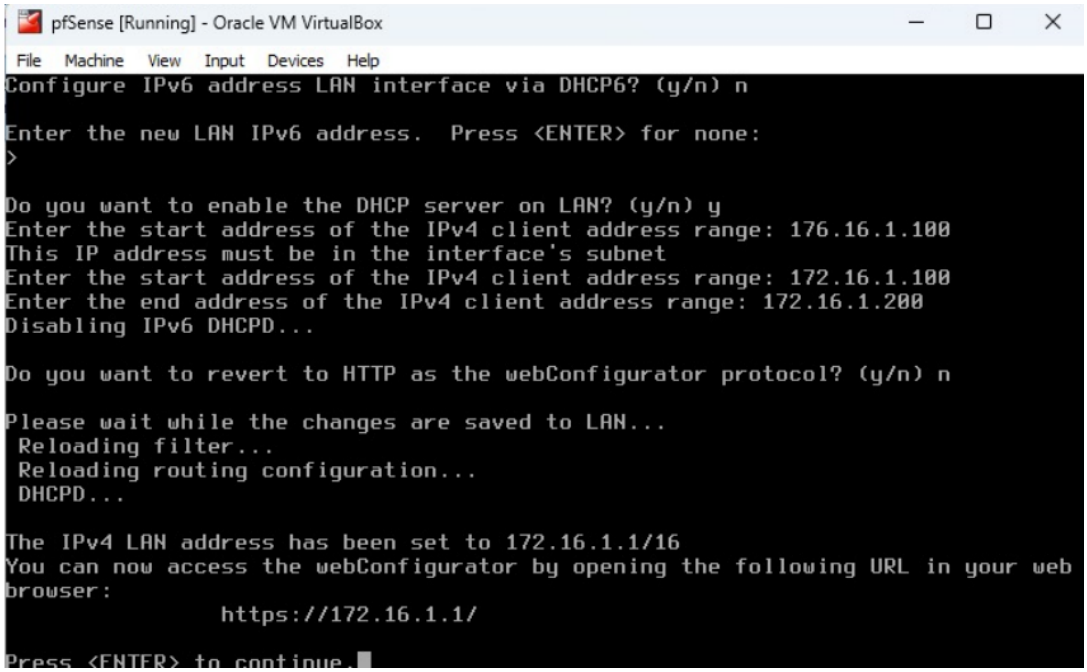


When you ask us if you want to set up an IPv6 address, we answer **"n".** Then we type **"and"** to enable the DHCP server on the LAN. Enter the address range:

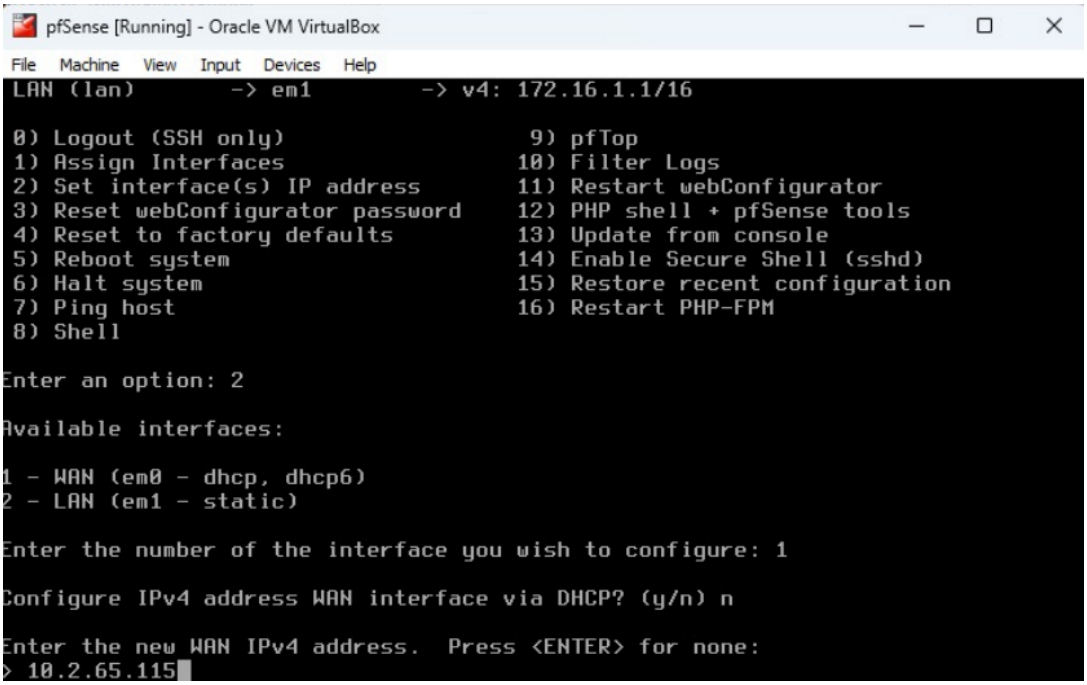
- **Start** → 172.16.1.100
- **End** → 172.16.1.200



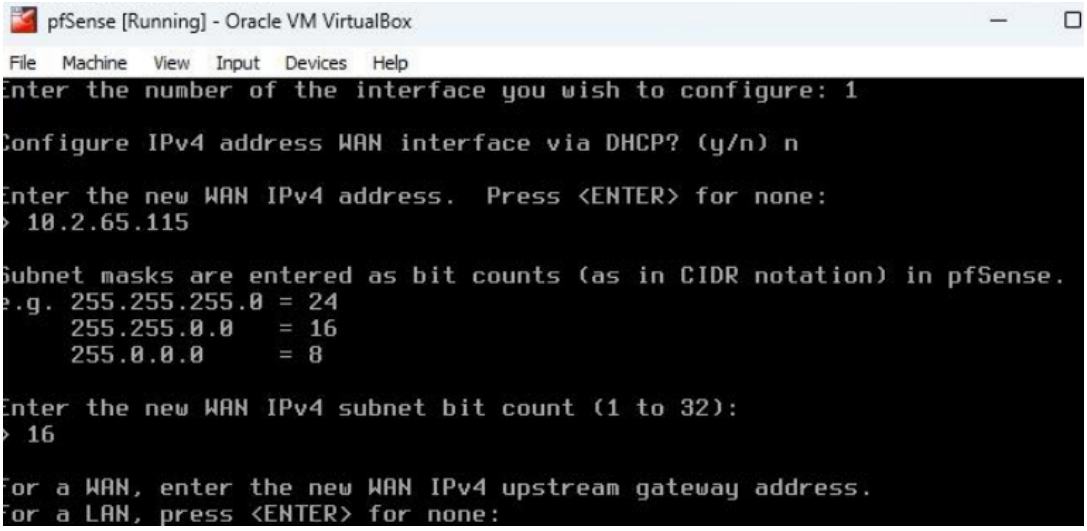
It will ask us if we want to go back to the HTTP protocol. We must type **"n"** to maintain access over HTTPS.



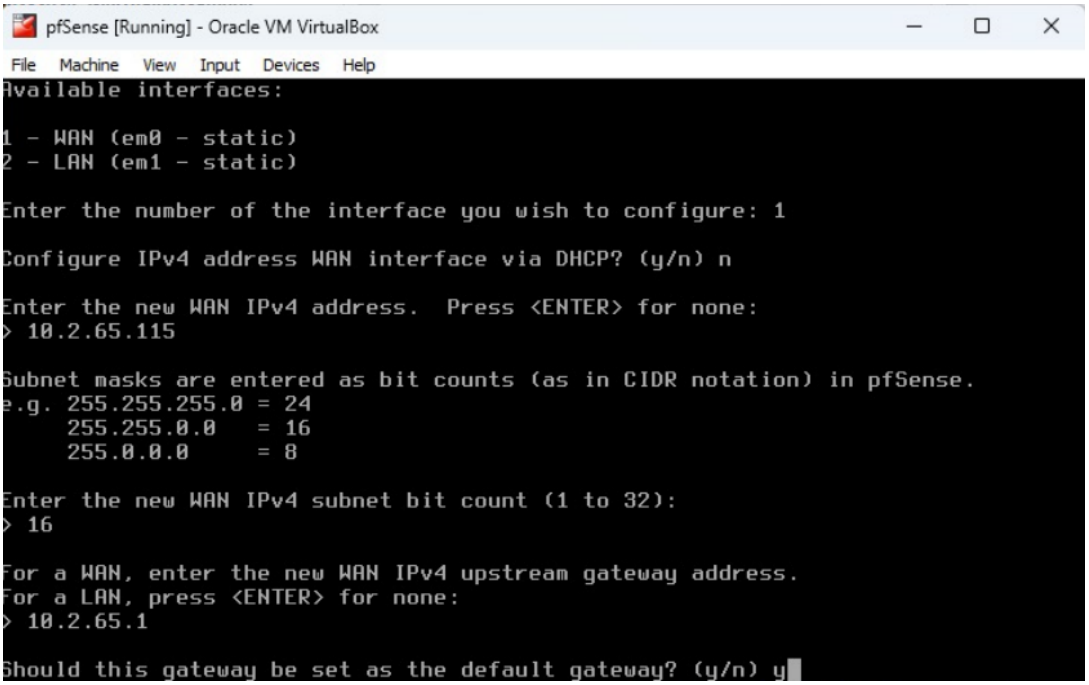
Again we select option **2)** to configure IP addresses. This time we chose option **1)** to configure the **WAN interface (e.g. em0).** We answer **"n"** when you ask us if we want to use DHCP.



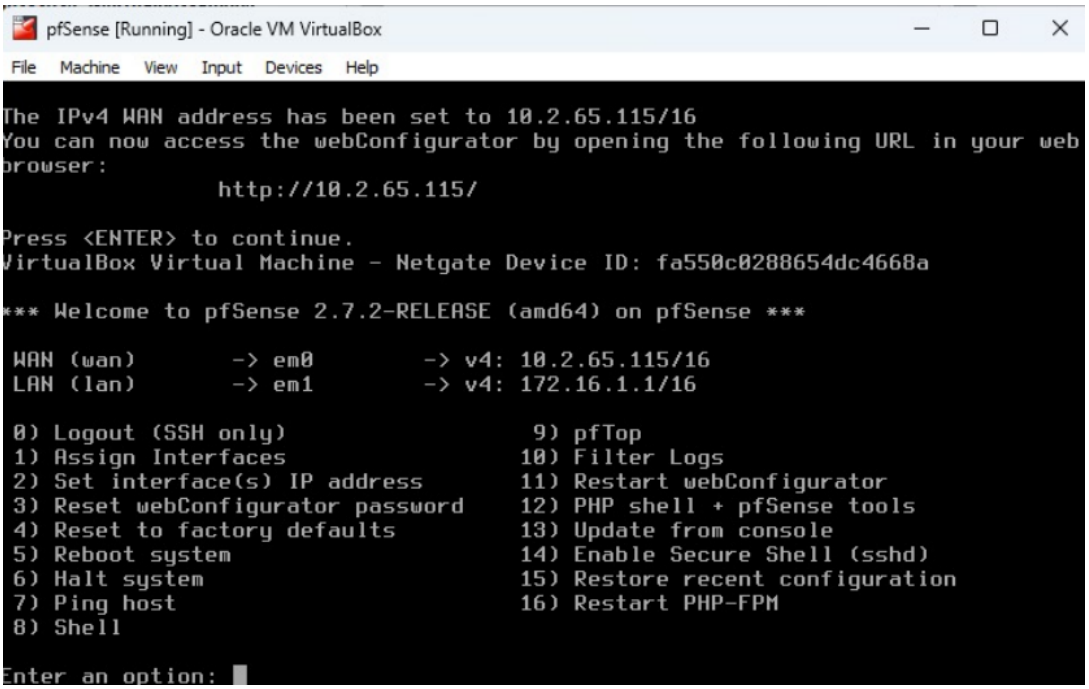
We enter the address **10.2.65.115** as the WAN IP. Then we type **16** as the subnet mask (Class B) and press Enter.



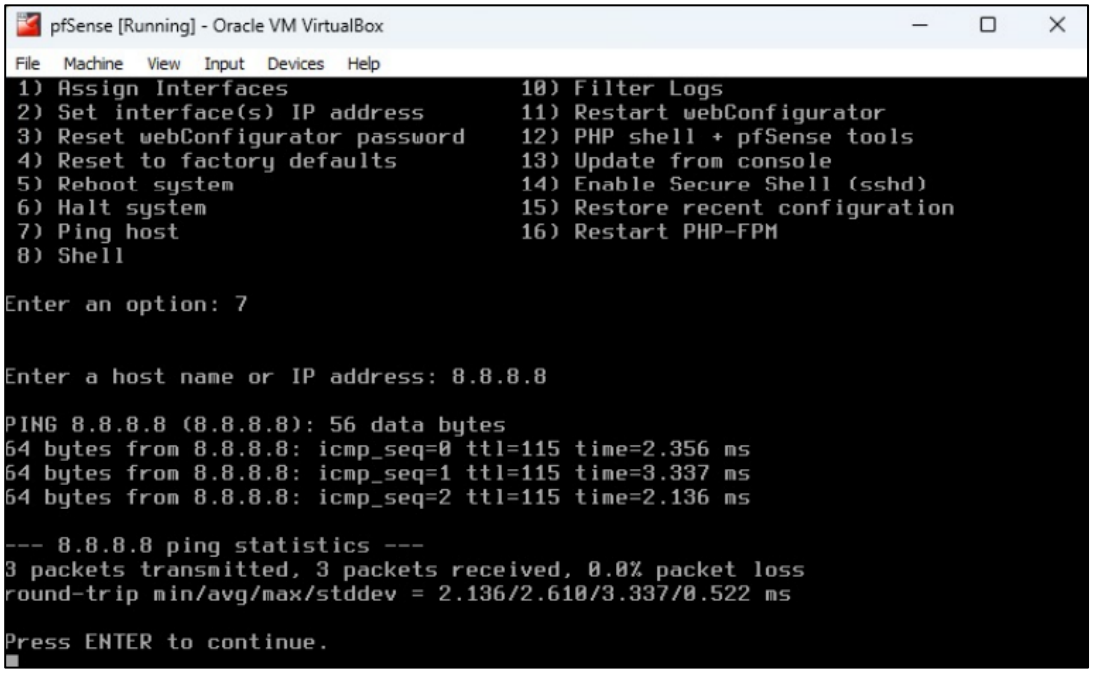
It will ask us for the gateway. We type **10.2.65.1** and press Enter. Next, type **"and"** to set this gateway as the default.



After configuring both interfaces, we need to check again that the **WAN and LAN** IP addresses are correctly assigned.



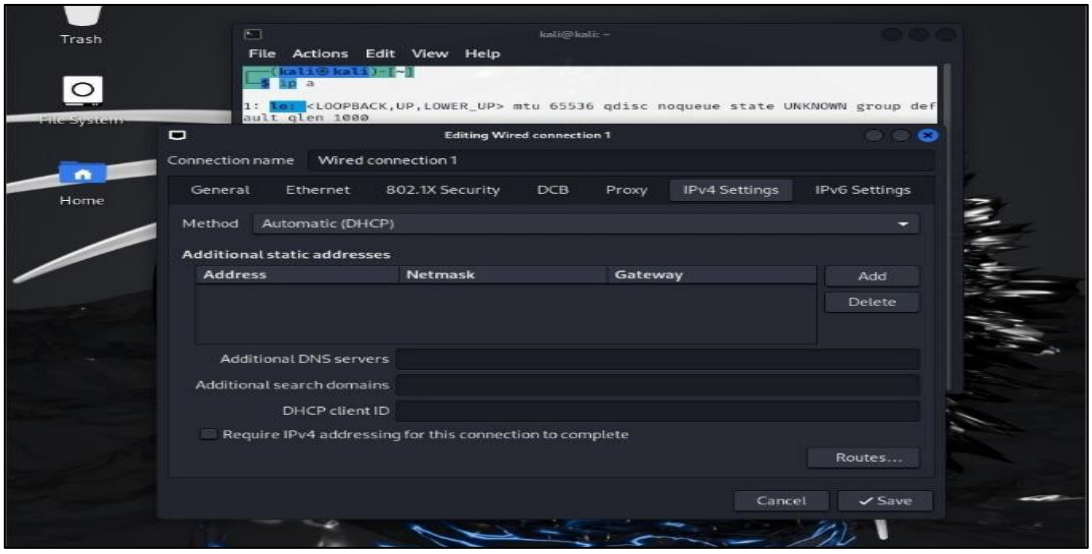
Finally, we select option **7)** in the menu to do a ping test. We type **8.8.8.8** (Google DNS) and press Enter to verify the internet connection. As we got a successful response from the ping made and this indicates that it is working well.



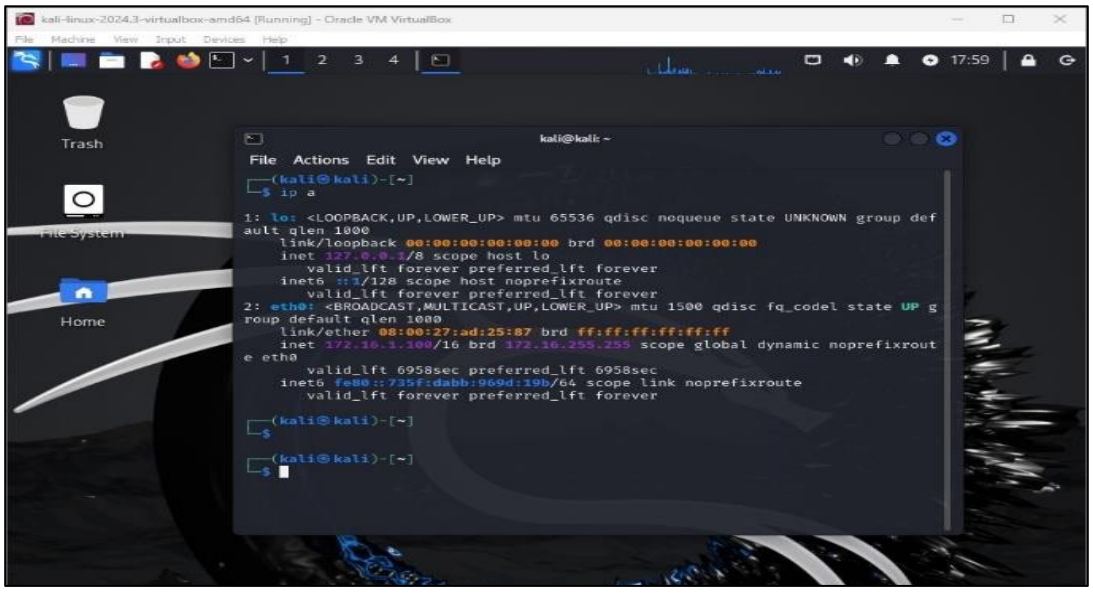
- **DHCP Assignment Verification from pfSense to Kali Linux**

  First, we need to make sure that the **Kali Linux VM** is on the same internal network as pfSense. To do this, we open **VirtualBox**, select Kali's machine and go to the configuration option. Then, in the **Network** section, we verify that **Adapter 1** is connected to an **Internal Network**, and that the **network name** is the same as the one we use in pfSense ***PrivNet***.

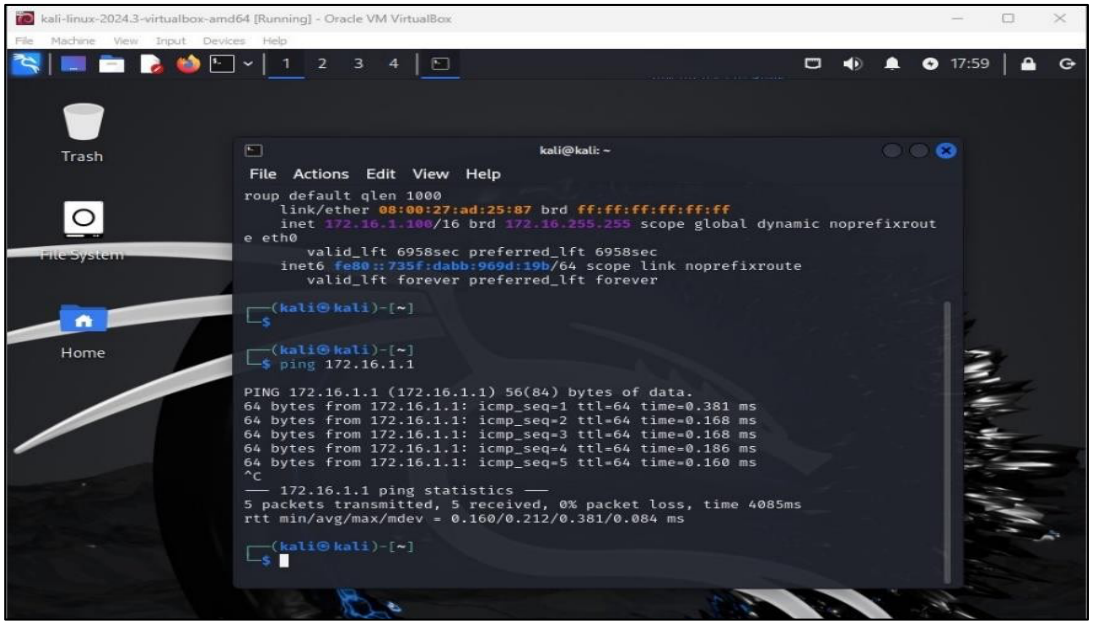
  After verifying the network, we started the **Kali Linux** virtual machine. Once inside the graphical environment, click on the **network icon** in the upper right. Select the available wired connection, and enter the settings. On the **IPv4 tab**, we changed the method to **Automatic (DHCP).** This will allow Kali to request an IP from the pfSense server. We save the changes and restart the network connection.



Then, we open a terminal in Kali Linux to check if a valid IP address has been received. We run the ip a command and look for the wired interface. The assigned IP address should be within the range **172.16.1.100 - 172.16.1.200**, which corresponds to the range previously defined on the pfSense DHCP server.



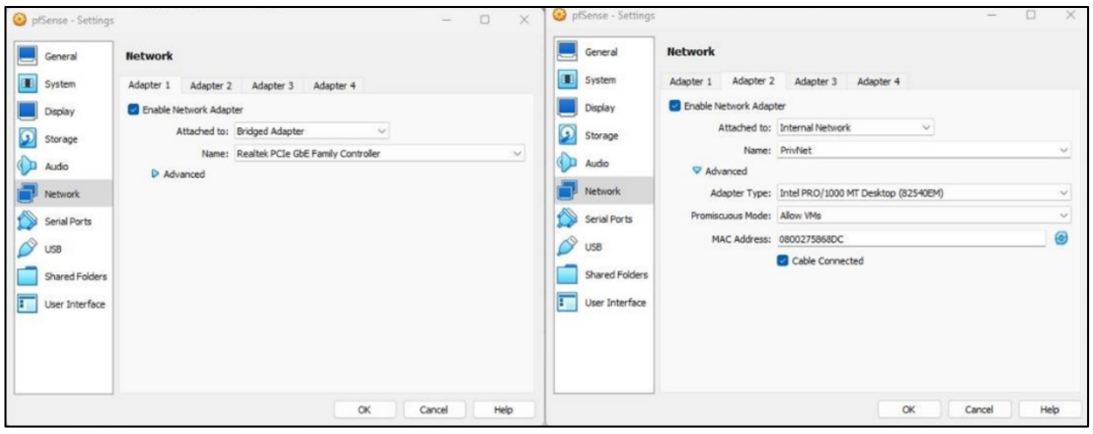
Finally, we must verify that Kali can communicate with pfSense. To do this, in the same terminal we run the ping command 172.16.1.1, which is the address of the pfSense LAN interface. If the ping responses are successful, it means that the DHCP server is working properly and that the internal network has been configured well.



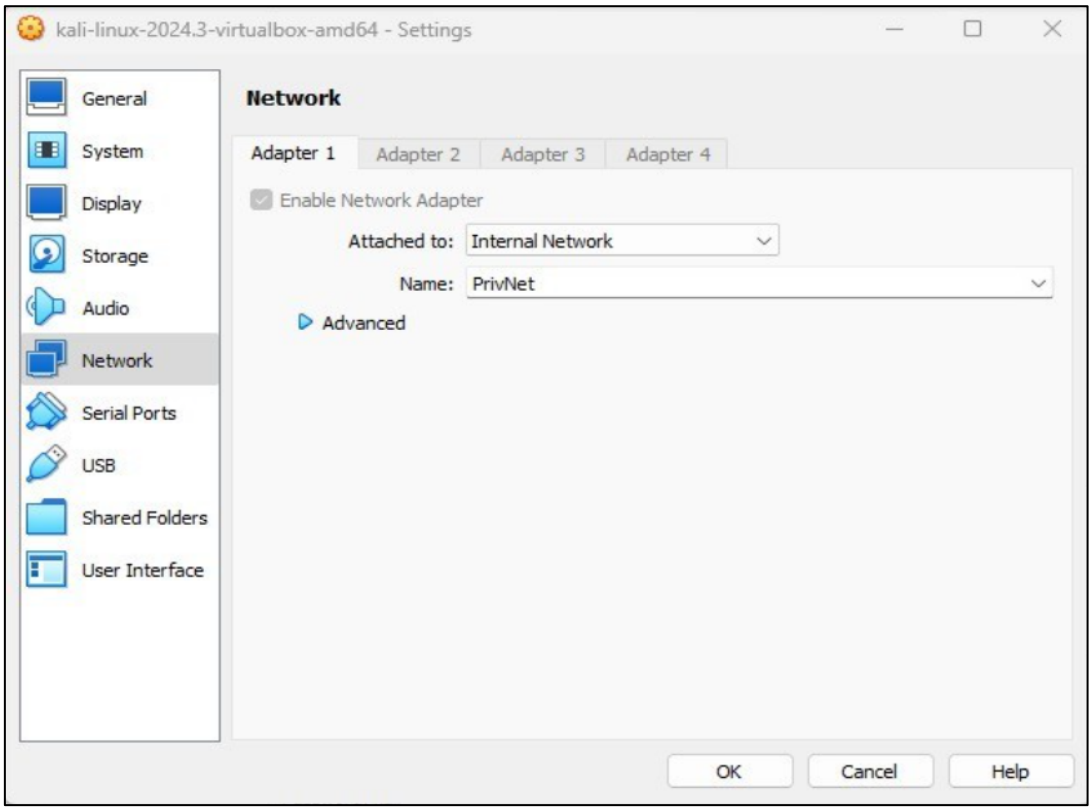
With this, we have verified that **pfSense assigns IPs correctly via DHCP** and that Kali Linux can communicate with it on the internal network.

- **Verification of the virtual machine environment.**

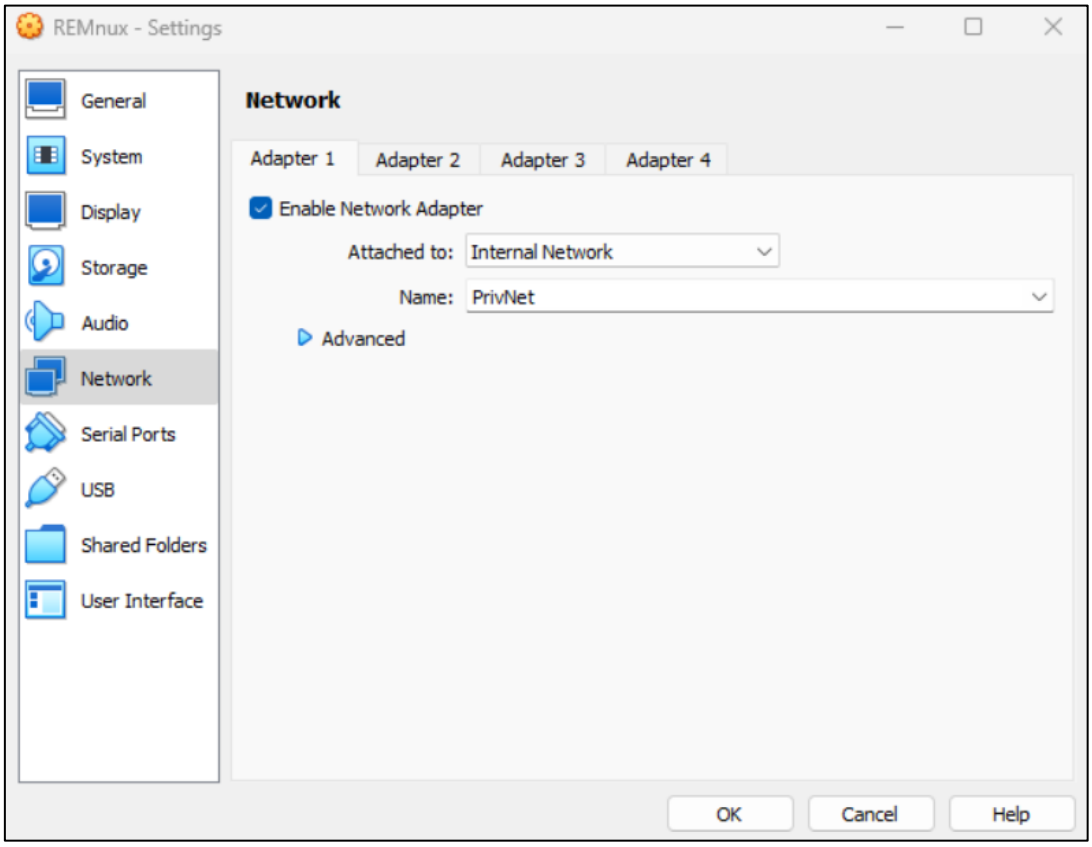
  It is necessary to verify that the Pfsense virtual machine has 2 interfaces. One put on bridged adapter and the other on PrivNet.



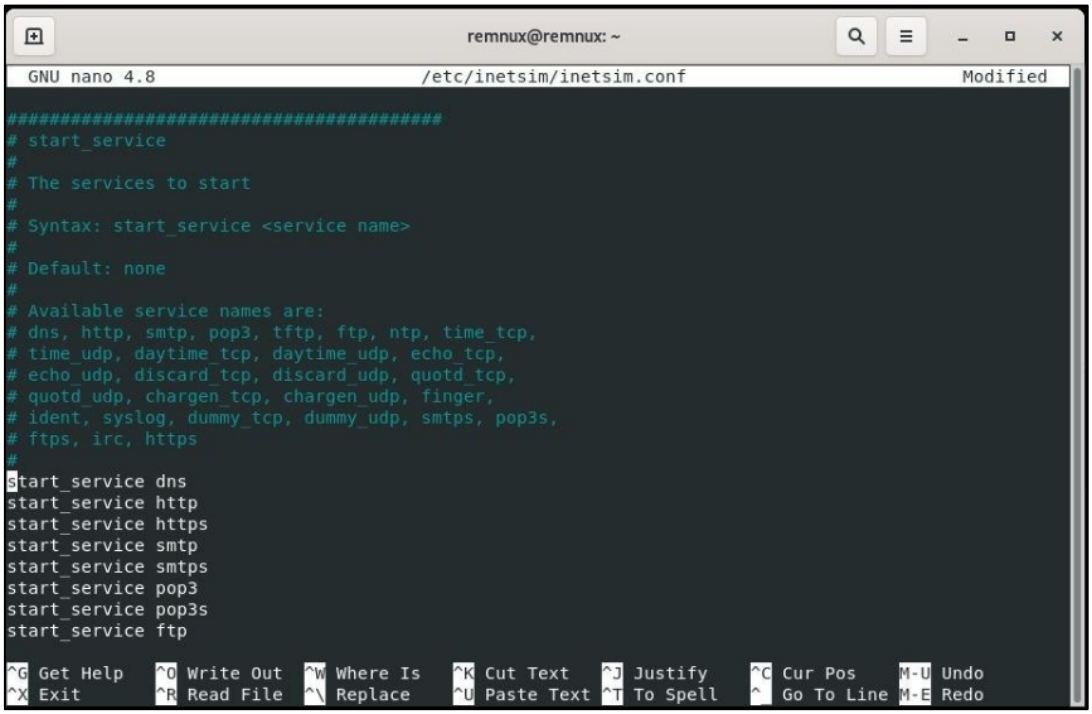
- Now we will have to verify that on Kali's machine the interface is set to Private Internal Network



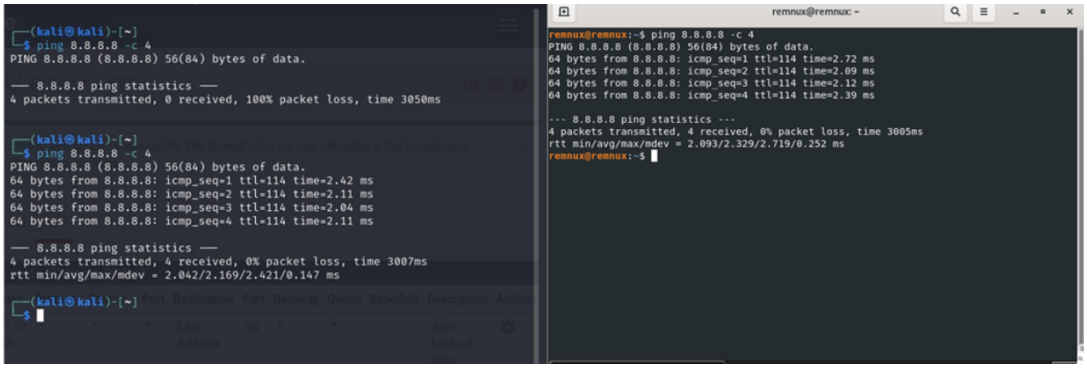
- Now we will have to verify that the Ubuntu virtual machine is also on the Private Internal Network.



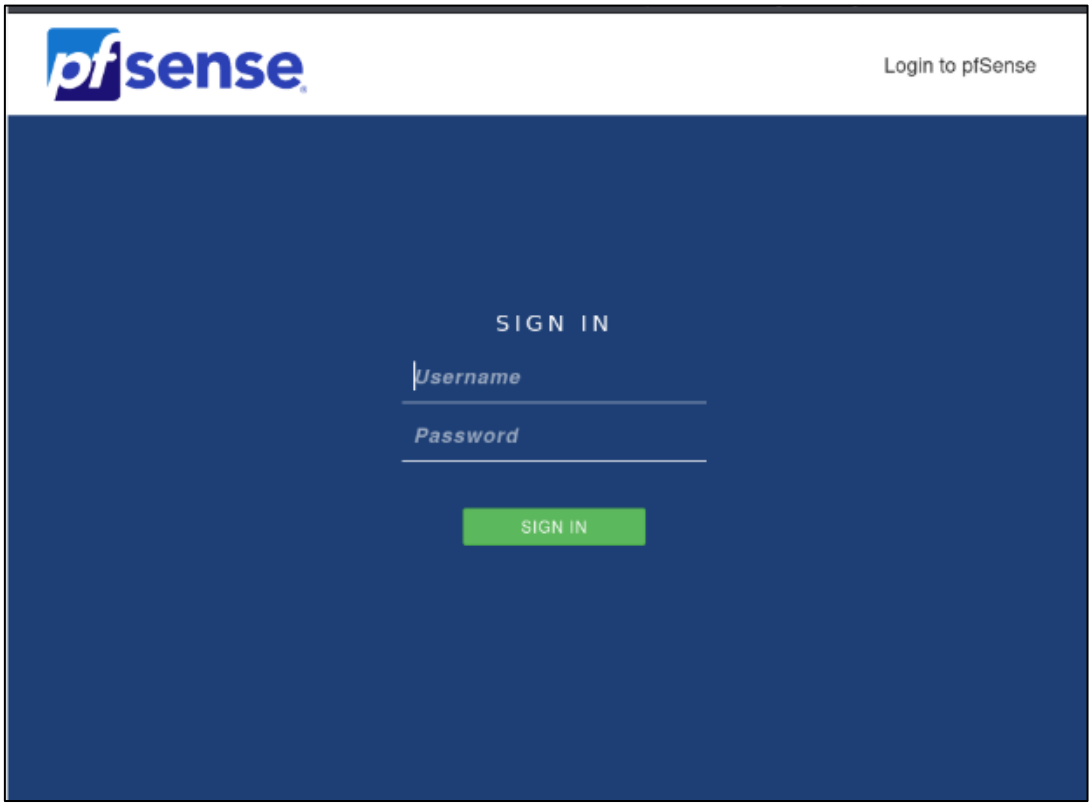
- Now we will have to turn on the DHCP service by modifying the configuration file and uncommenting a line. Specifically the line "dns start_service"



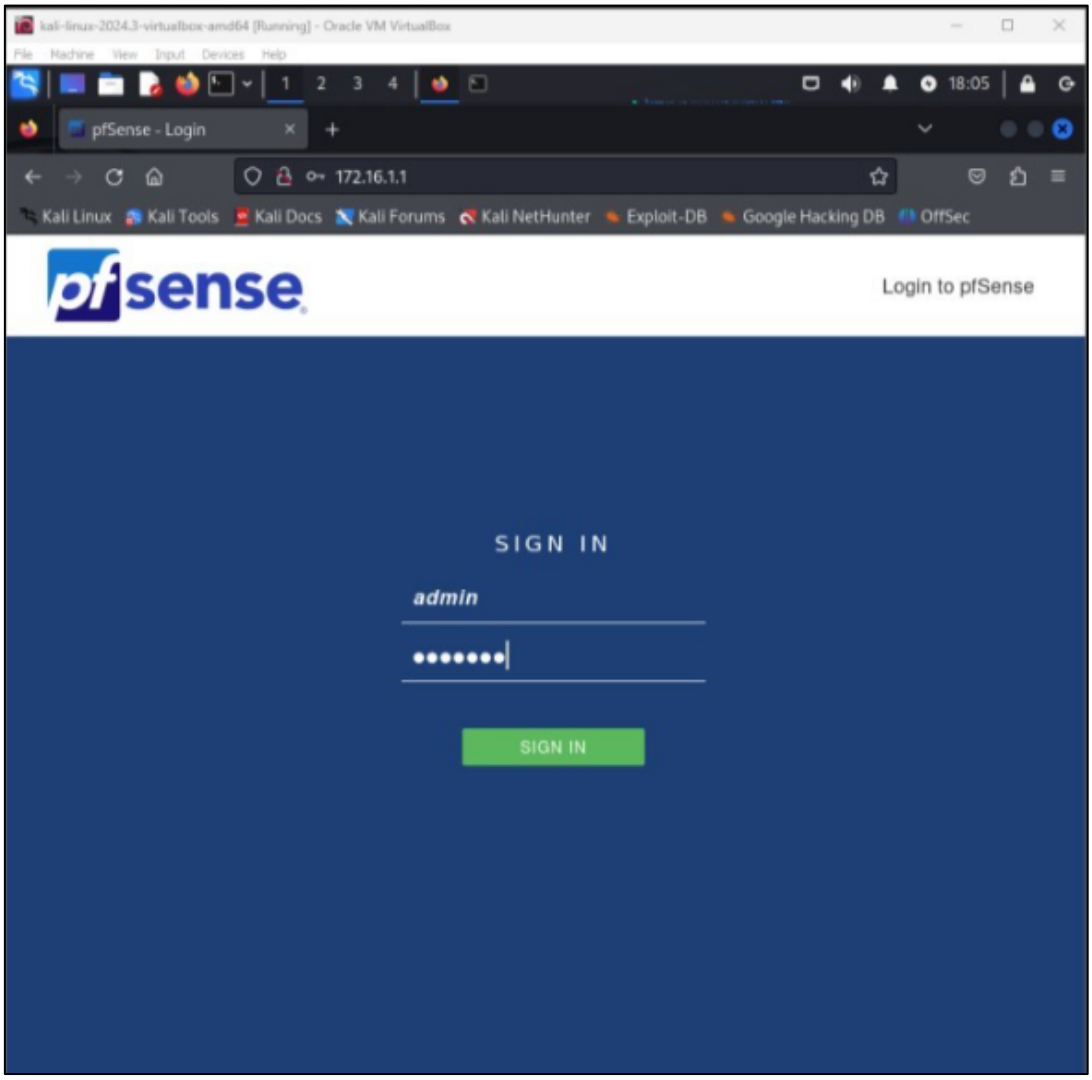
- Connectivity between virtual machines is verified.



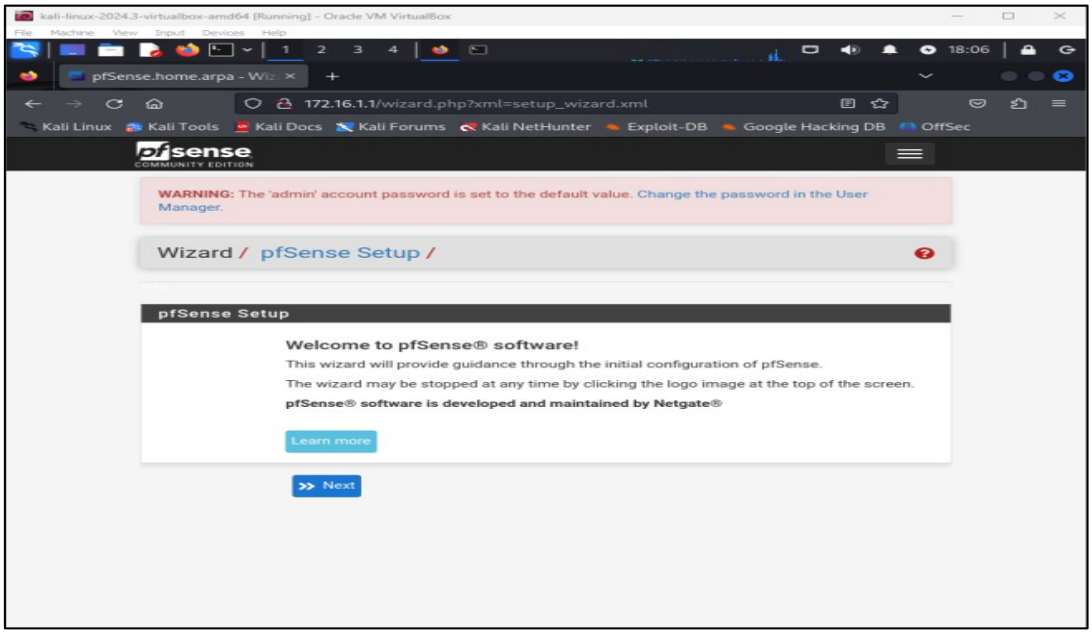
- Complete the installation of Pfsense. On the Kali Linux machine, the pfSense web console is accessed via a browser using the pfSense LAN IP 172.16.1.1 interface.



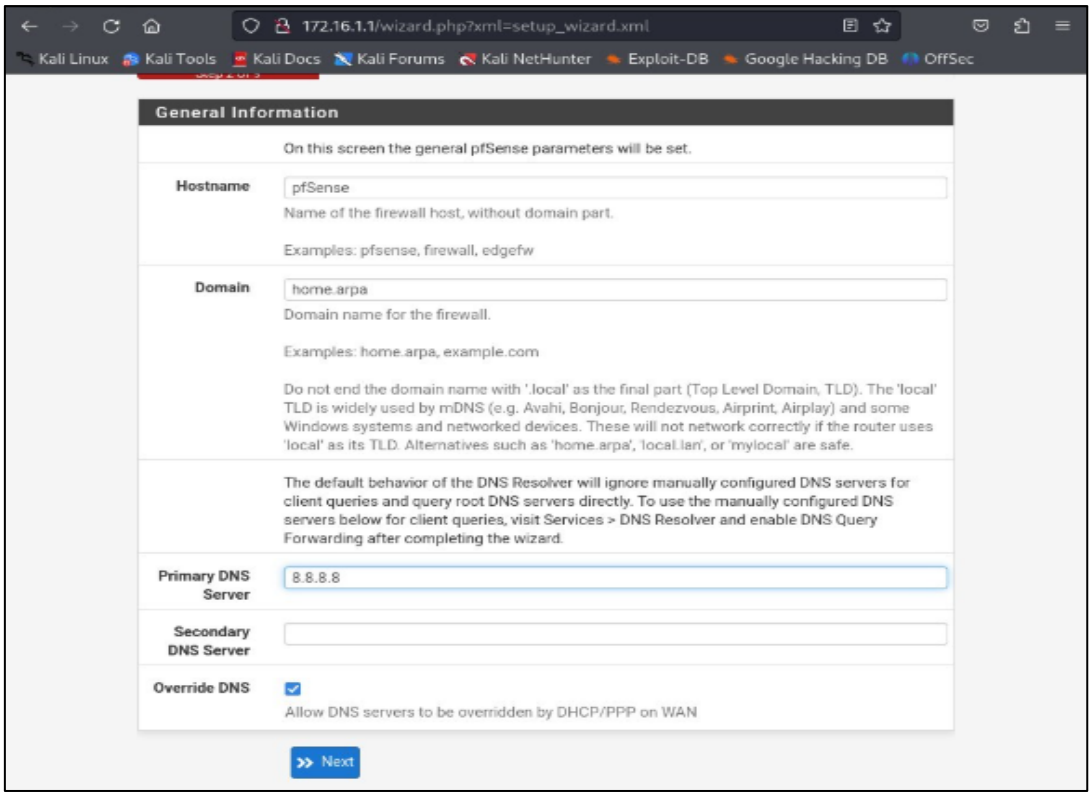
- These are the following credentials:
    - Username: admin
    - Password: pfsense

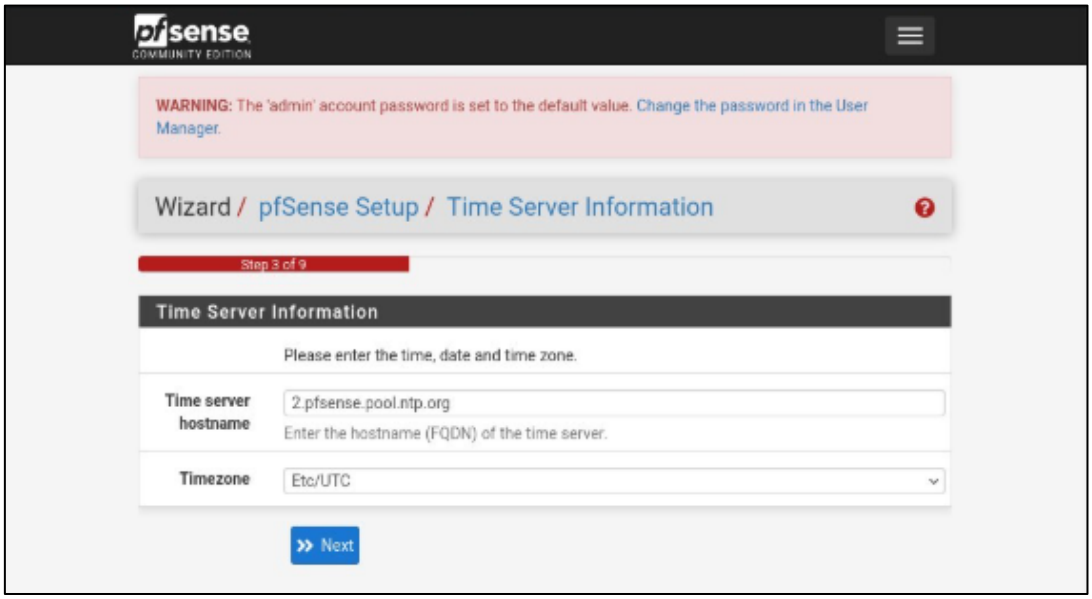


Now the welcome screen will appear and the assistant will tell us step by step what we have to do.

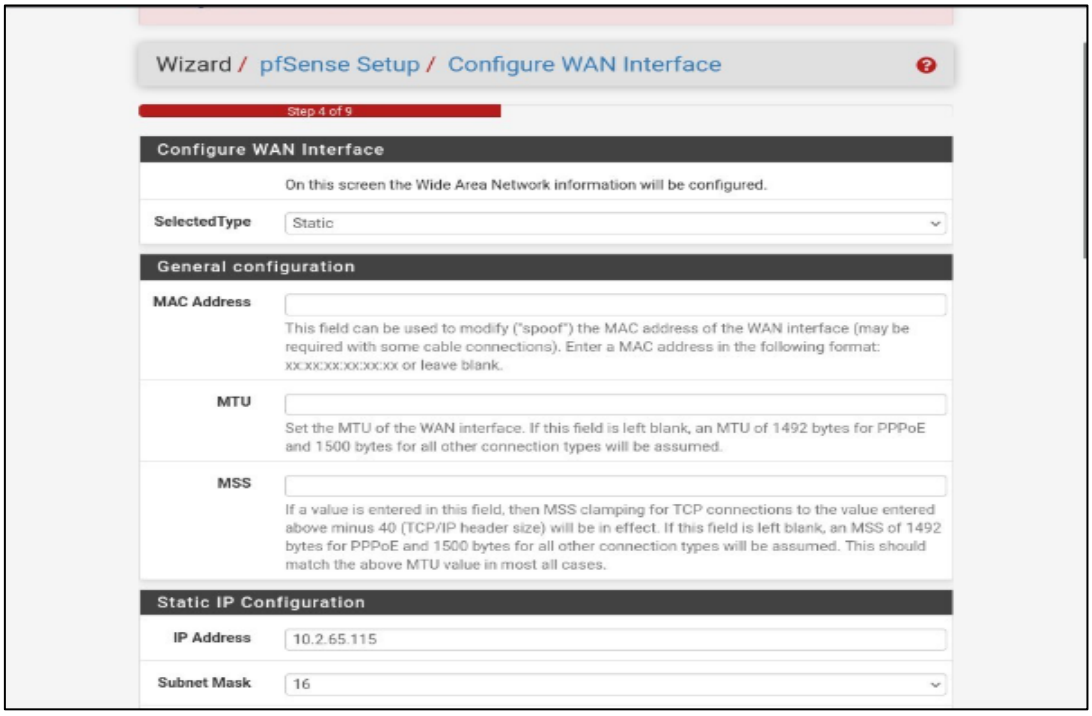


- The general pfsense parameters are configured. The primary DNS server is 8.8.8.8.

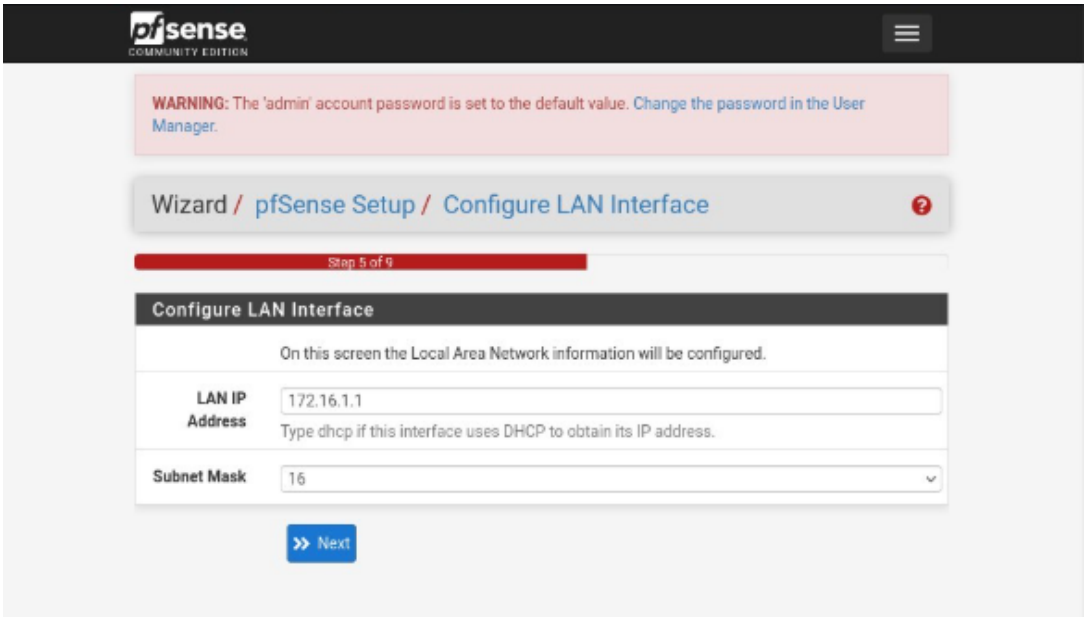




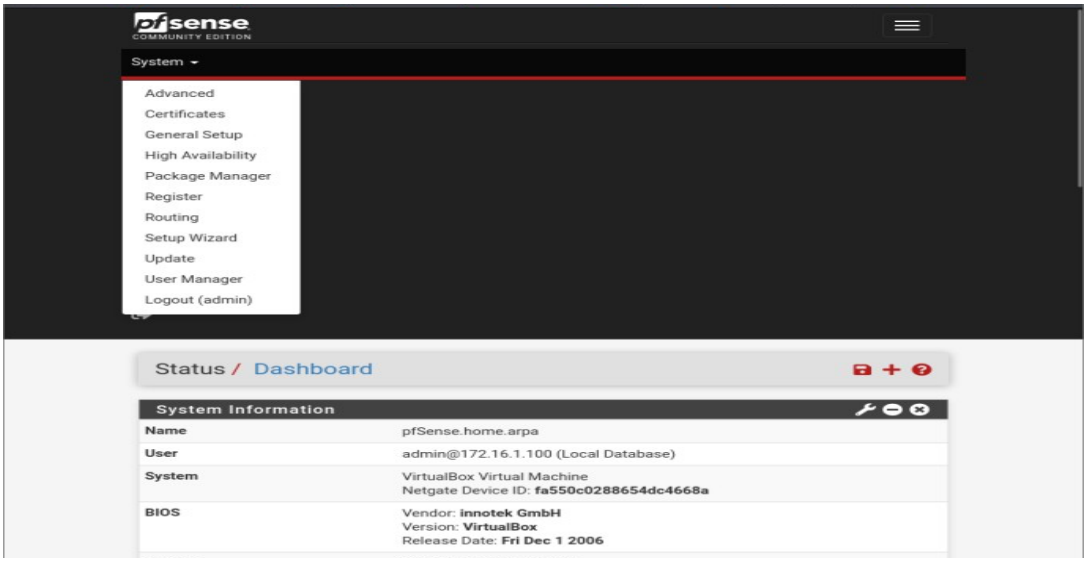
- No changes were made to the proposed configurations.
- Now we will need to change the WAN configuration. For this, 10.2.65.115 is set as the IP address and 16 as the subnet mask.



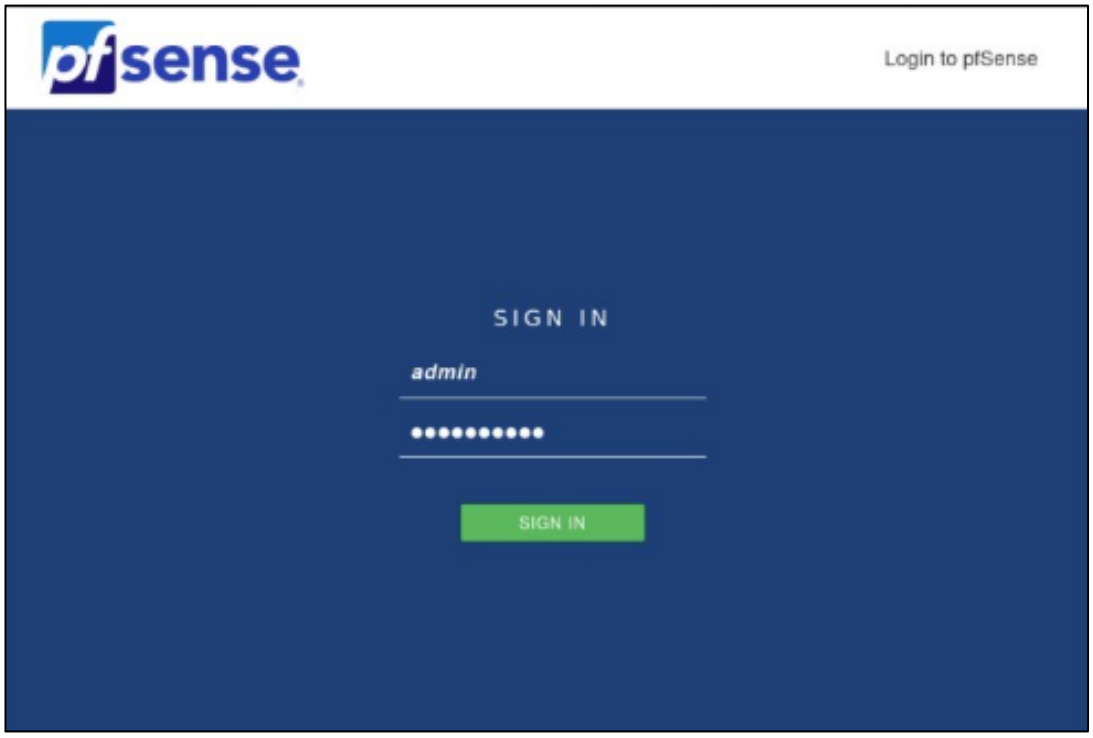
- And now with the LAN.



- We will have to look for updates in the system tab section and there we will select log out option.

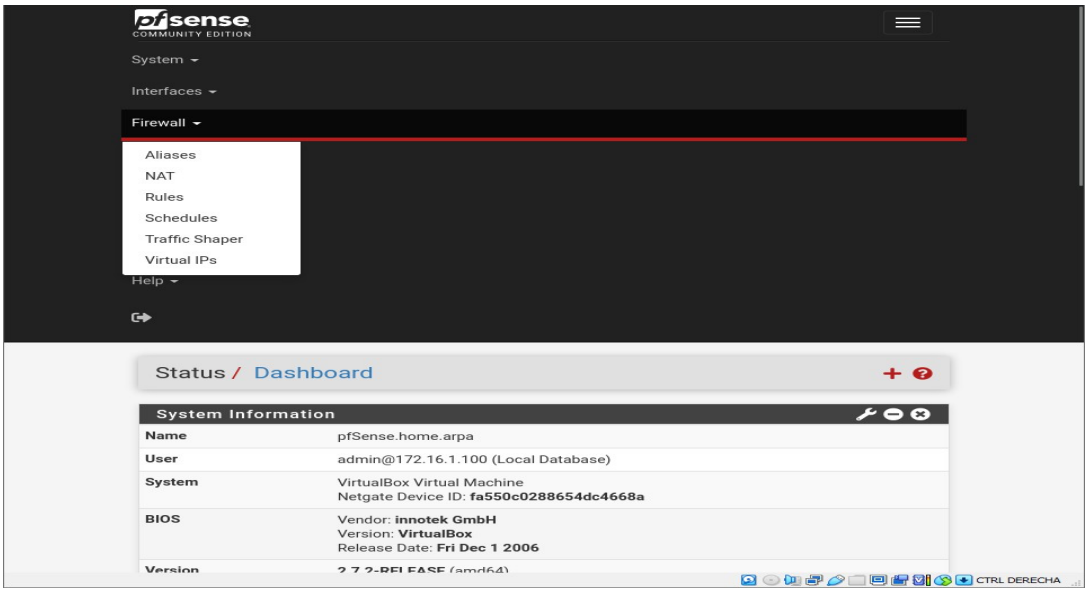


- The following credentials will now be entered
    - Username: admin
    - Password: JuanValent



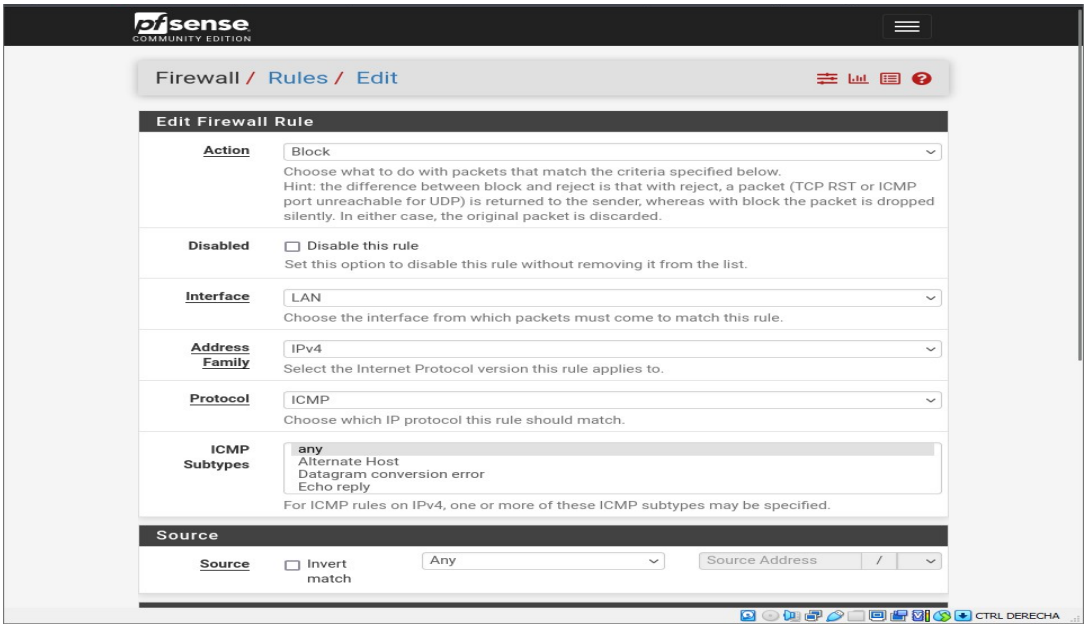
- **Configuring pfSense to block or allow ping packets through the web interface.**

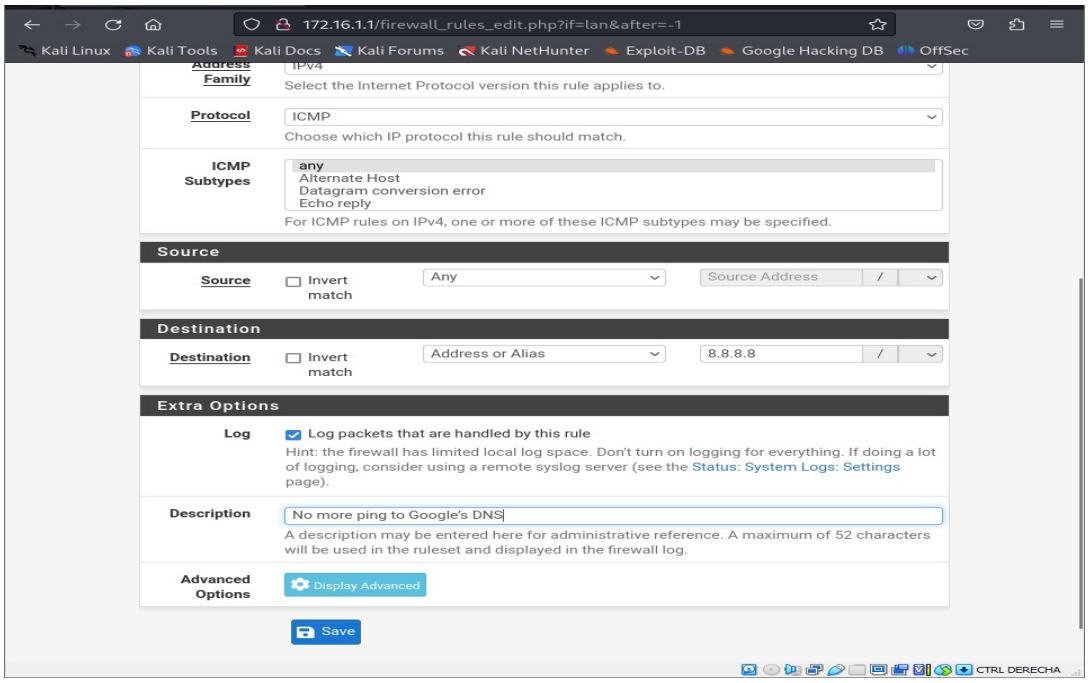
Now we will have to click on the up arrow, and enter the following parameters.



  - Action: Block
  - Interface: LAN

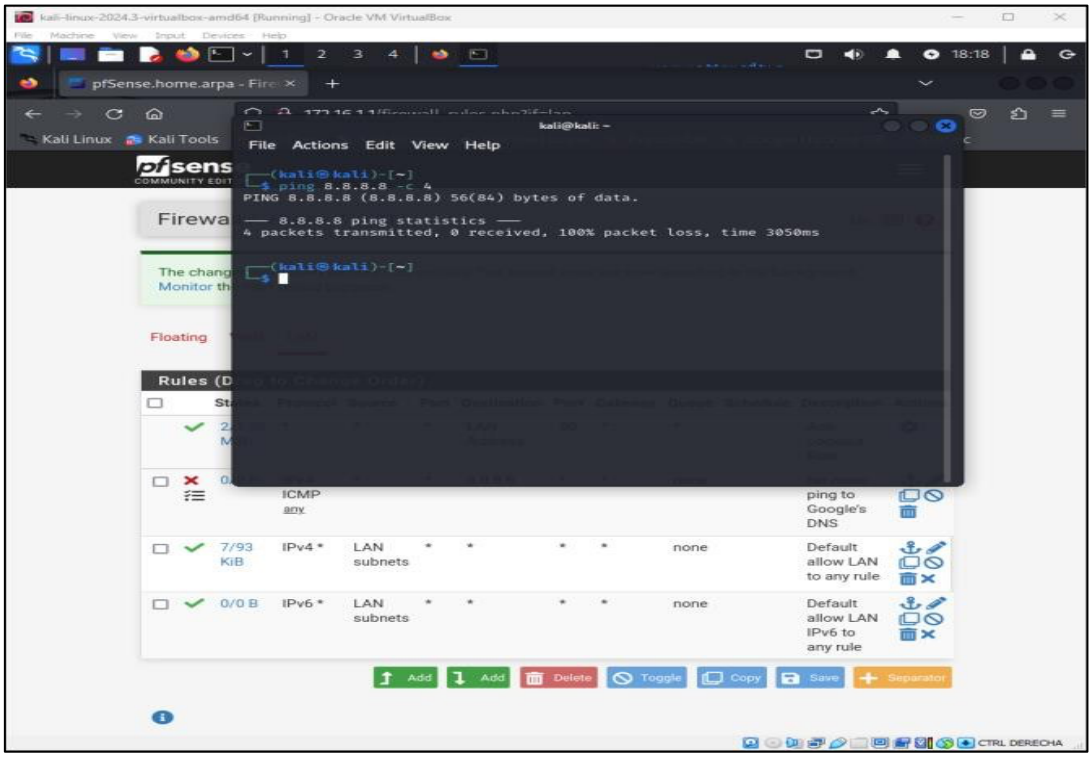
- Address Family: IPv4
- Protocol: ICMP
- ICMP Subtypes : any
- Source: any
- Destination: Single host or alias > 8.8.8.8
- Enable Log packets that are handled by this rule
- Description: No more ping to Google's DNS

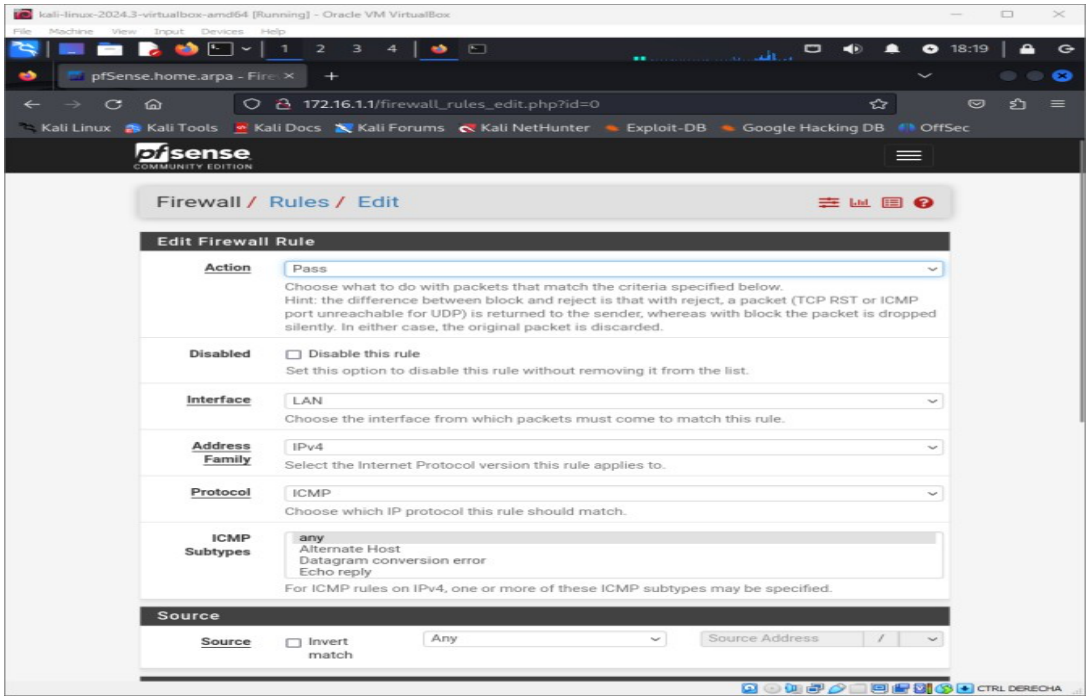




Now we'll have to test the firewall rule

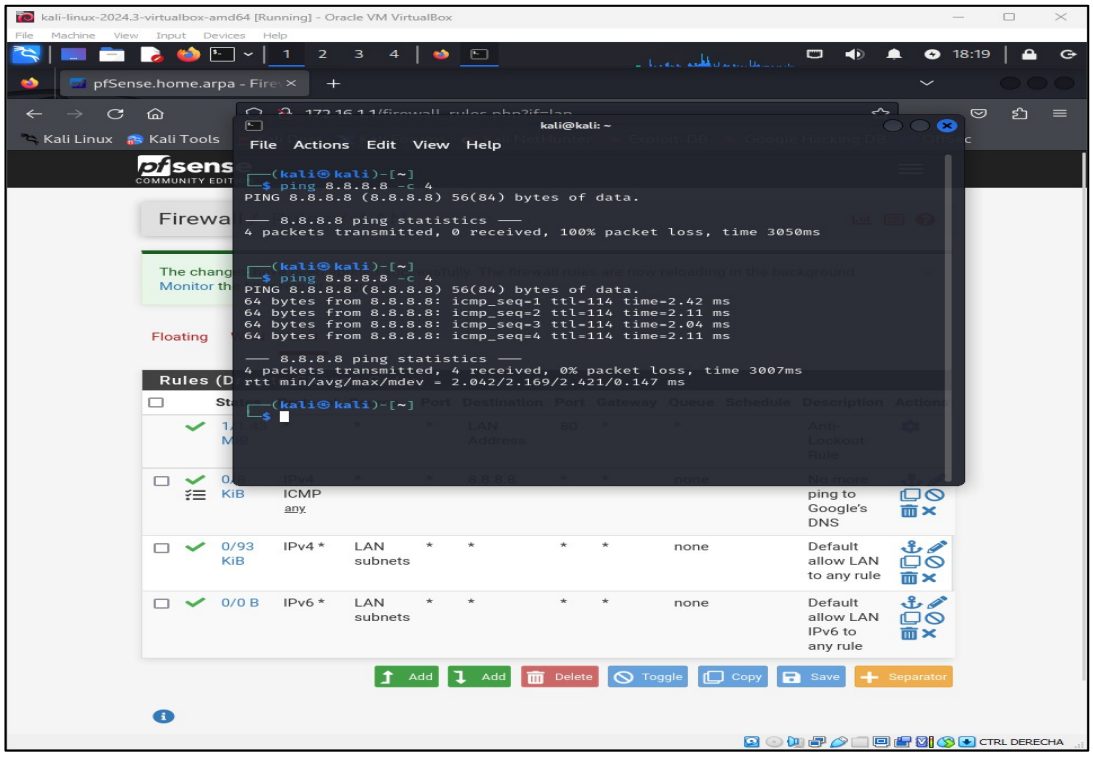
The changes are implemented and a test is performed to verify the operation of the new rule. A ping is run from the Kali Linux machine to the 8.8.8.8 address, and the response is checked. If the rule was configured correctly, the 8.8.8.8 host should be unreachable as a destination.



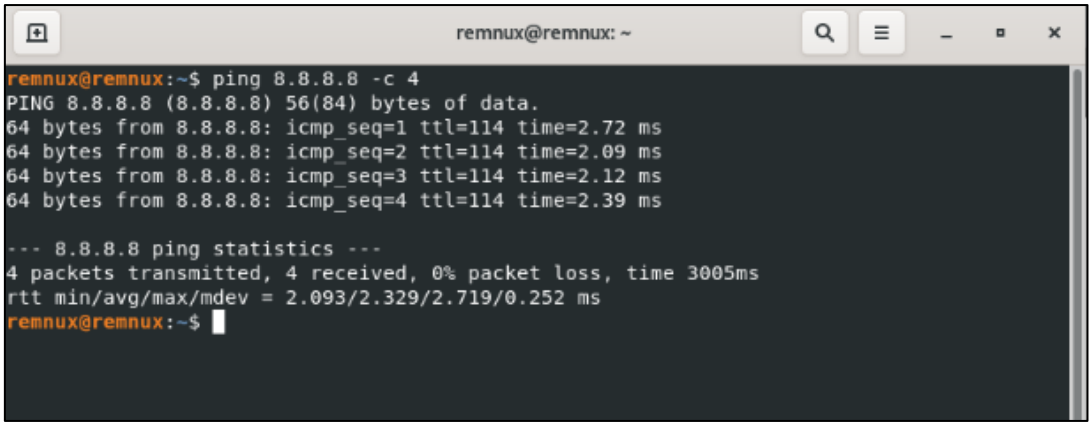


- Rule changed to pass

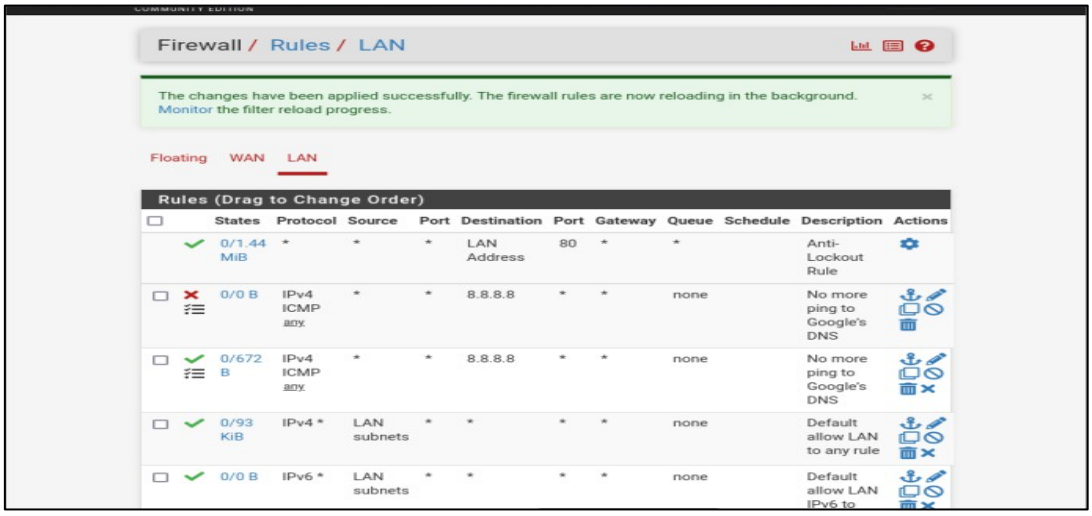
- Now we observe the answer in kali



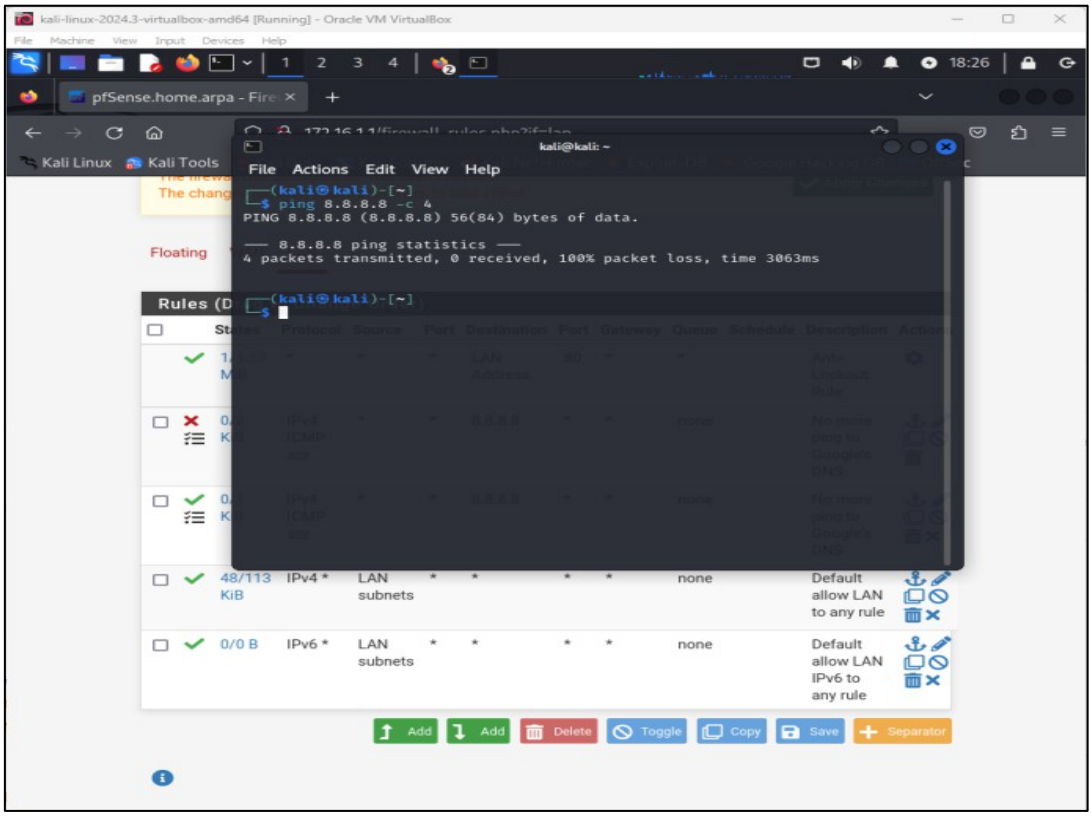
And now on the REMux virtual machine



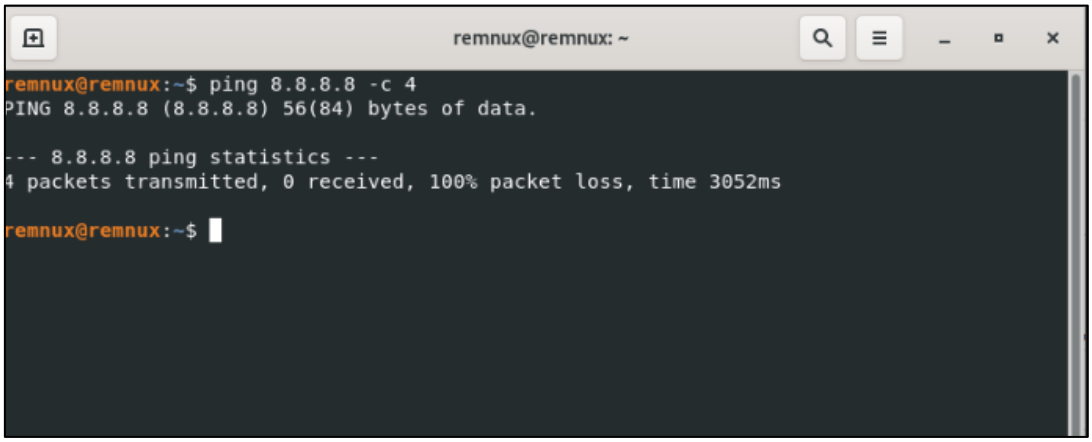
- Duplicate the permission rule and rearrange the order of the rules by dragging the lock rule to place it before the permission rule. Once done, save your changes at the bottom of the page and click "Apply Changes."



- Now we ping 8.8.8.8 and let's see the result



And finally the REMux virtual machine



Conclusion

In this laboratory, it was possible to install and configure pfsense as a router and DHCP server in a virtualized environment. Kali Linux and REMnux machines were successfully connected to the internal network, verifying automatic Ips assignment and connectivity. Also, firewall rules were implemented and tested to block or allow ICMP traffic to 8.8.8.8, demonstrating how the order of the rules affects firewall behavior. This practice allowed them to reinforce key networking and security concepts, and gain experience in traffic management and service configuration in pfsense.