

**ESCUOLA COLOMBIANA DE INGENIERIA
JULIO GARAVITO**

**IT SECURITY AND PRIVACY
GROUP 1L**

LABORATORY 14

**SUBMITTED BY:
JUAN PABLO FERNANDEZ GONZALES
MARIA VALENTINA TORRES MONSALVE**

1

**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)

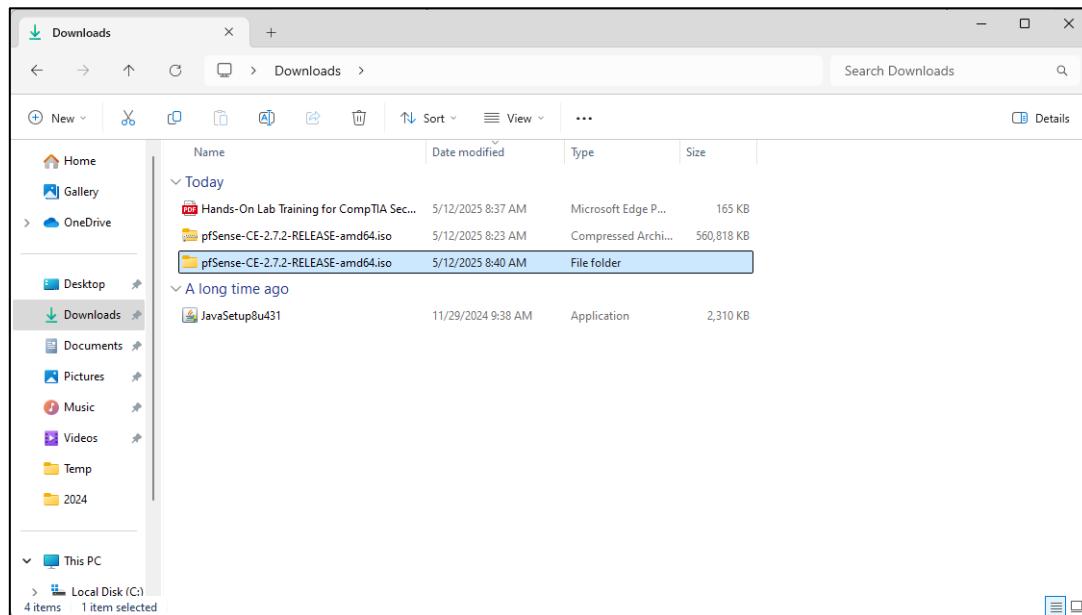
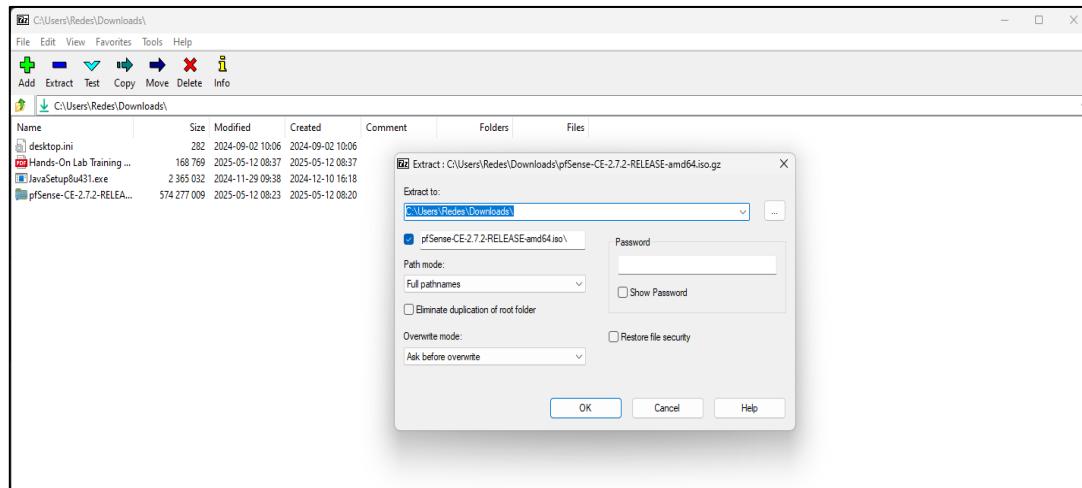
2

- 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/

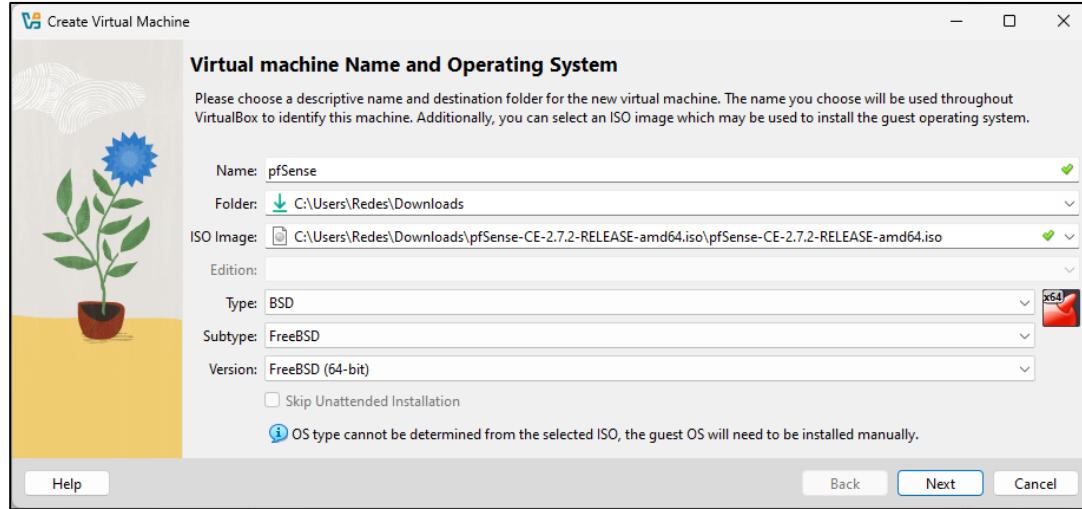
..		
old/		
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz	06-Jun-2024 19:18	-
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz.sha256	31-Jan-2022 20:31	437073513
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz	31-Jan-2022 20:32	114
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz.sha256	29-Jun-2023 20:11	495733706
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz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



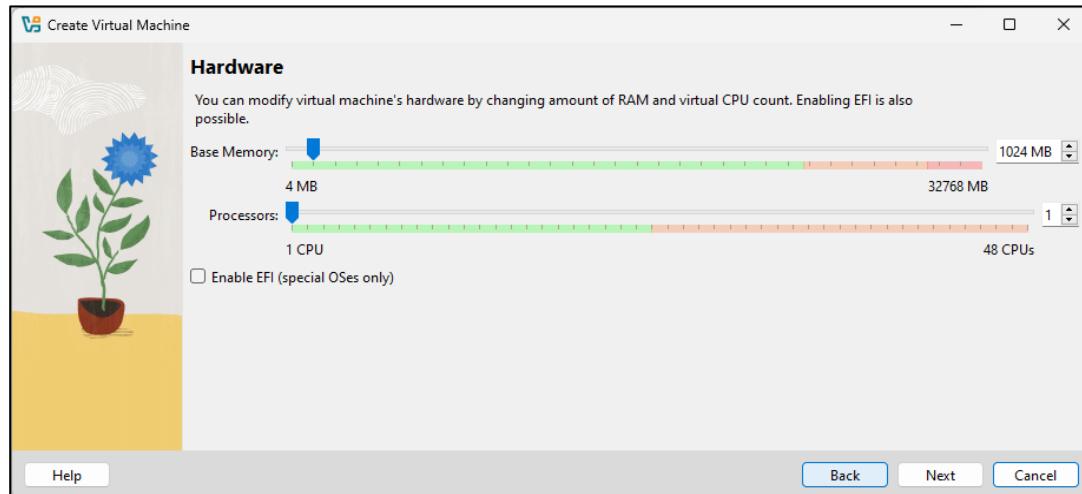
3

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:

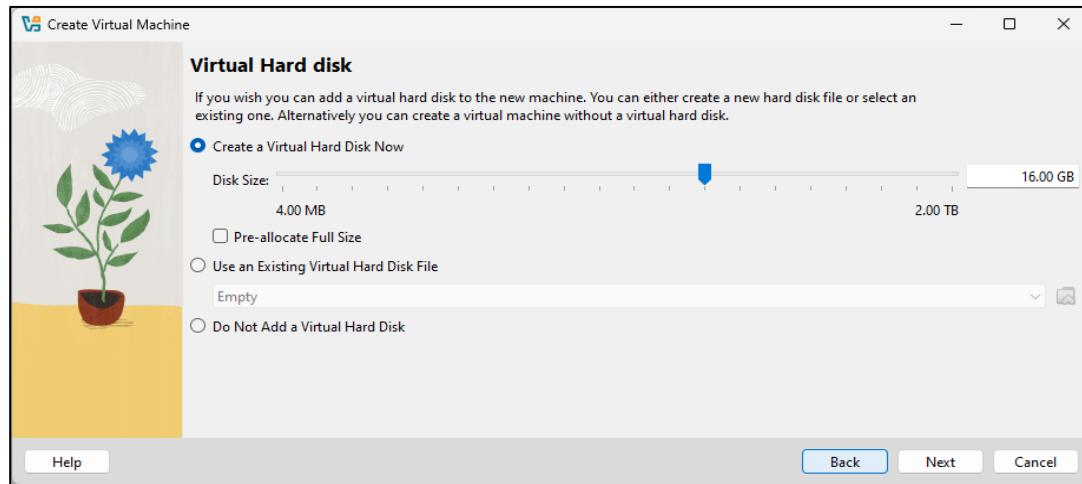
- Name: pfSense (can be any)
- Folder: Where you want to store
- ISO Image: Iso downloaded in the previous step
- Type: BSD
- Version: FreeBSD (64-bit)



- We will give you 1024MB in memory size



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

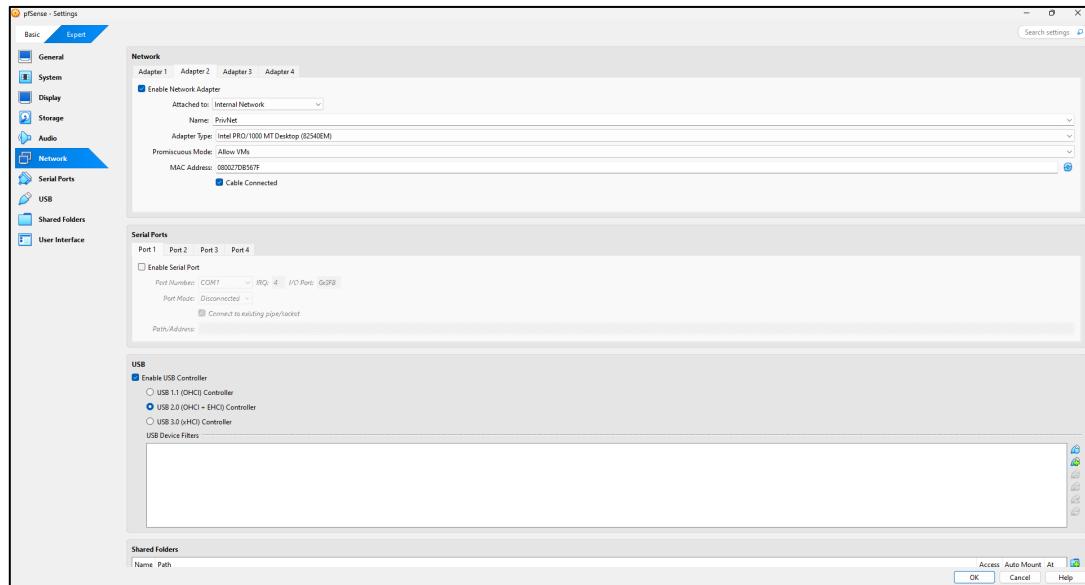


- Configuring network interfaces.

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

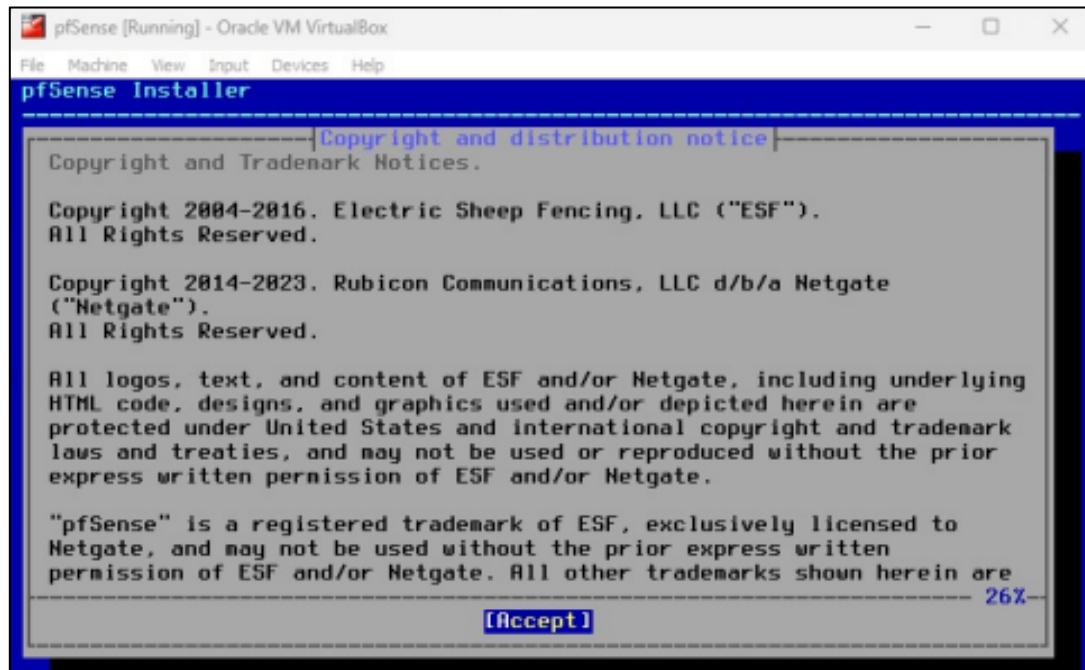


Set Adapter 2 to ***Internal Network*** and rename the network to ***PrivNet***. This will be the LAN adapter for internal connectivity. Then, set promiscuous mode to ***Allow all VMs***, and click ***OK***.

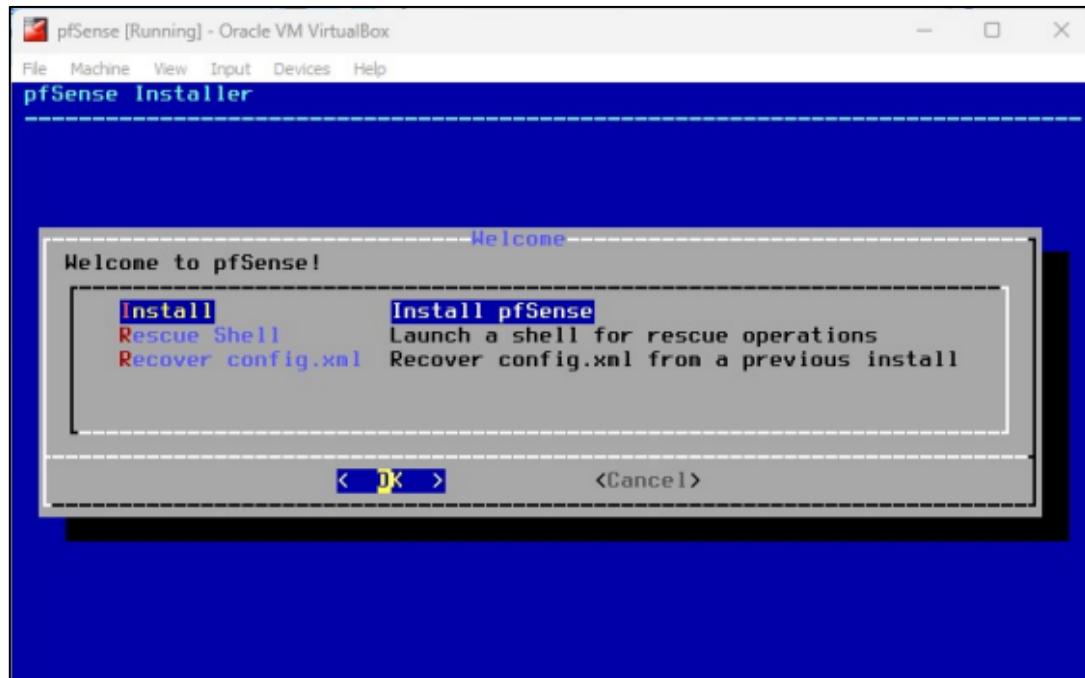


- Install pfSense

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

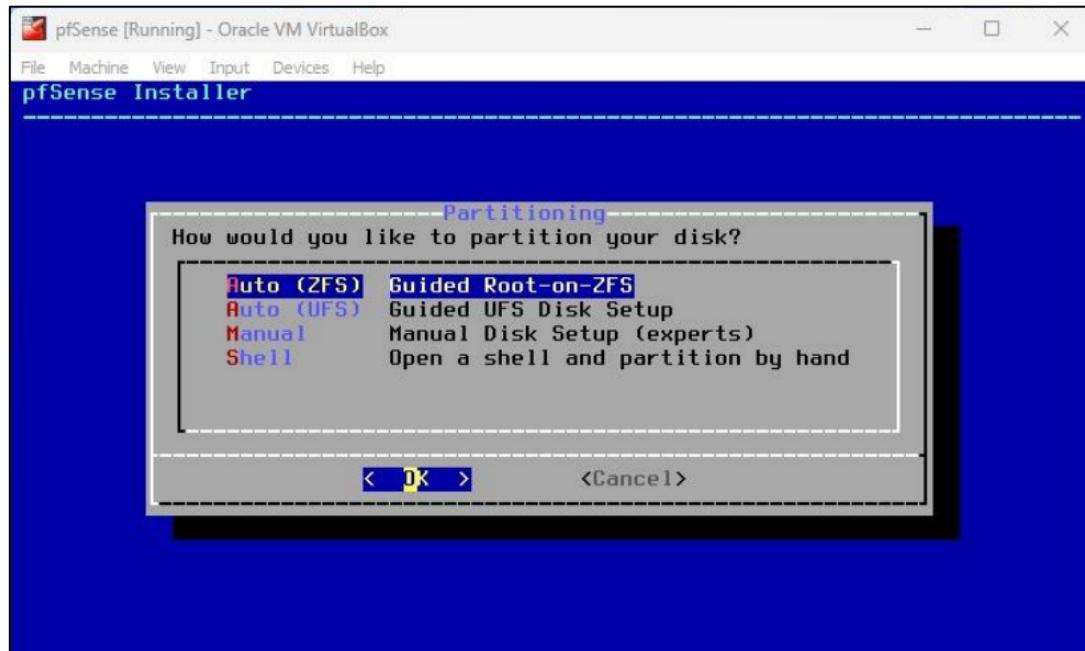


Select the option of **Install à Install pfSensey** then enter in the **OK option**

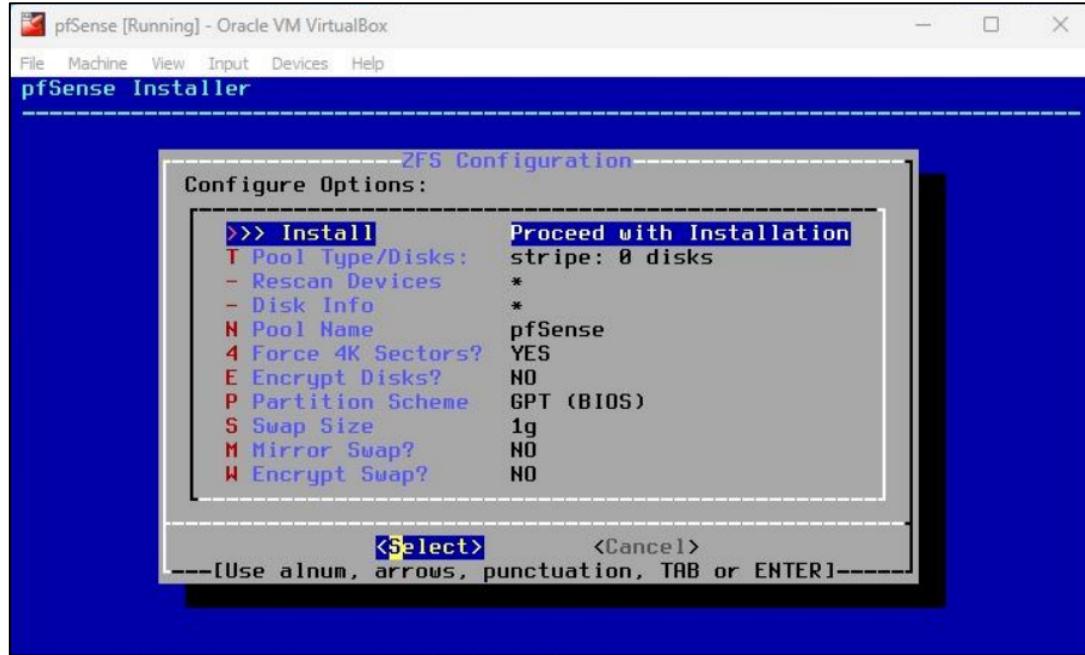


Now we must choose the type of installation. Select the "Auto (ZFS)" option and then click OK. This option is because ZFS is an advanced file system that pfSense recommends for its stability.

7

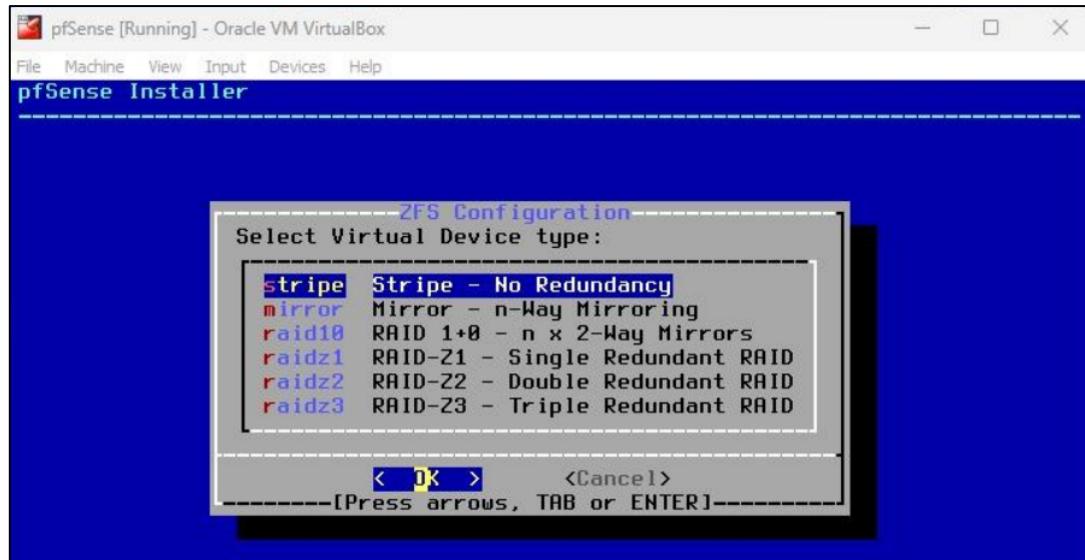


The installer will ask us on which disk we want to install pfSense. We must select the **Install** option and then click on **SELECT**. This confirms that we want to use that disk for installation.



8

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.

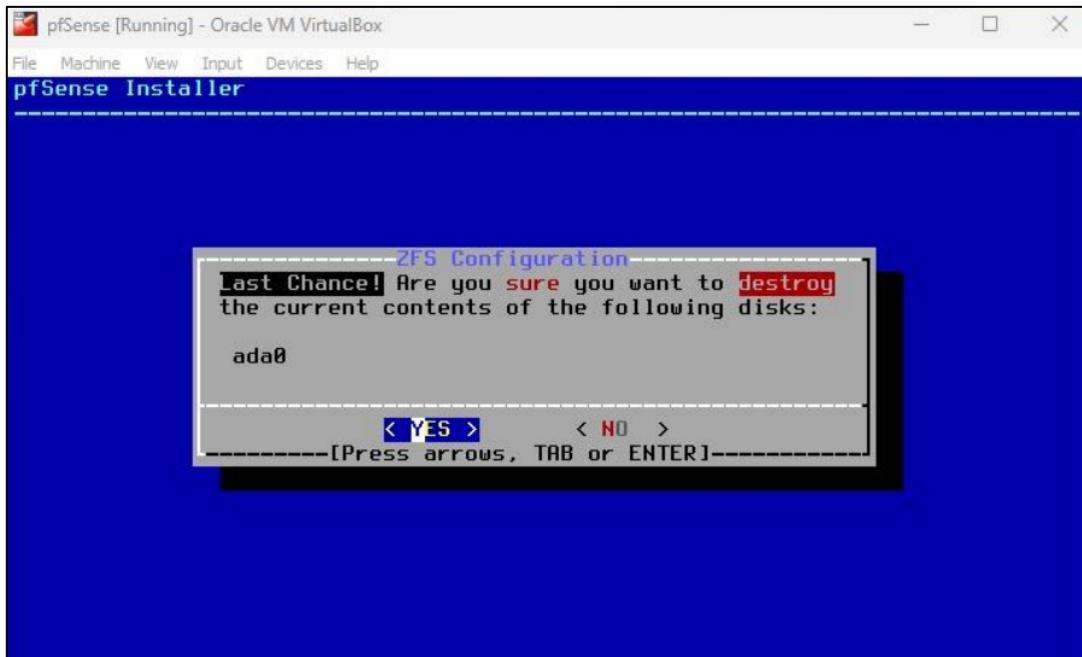


We must select the disk where pfSense will be installed, it usually appears as **ada0 VBOX HARDDISK**. Once selected, click **OK**.

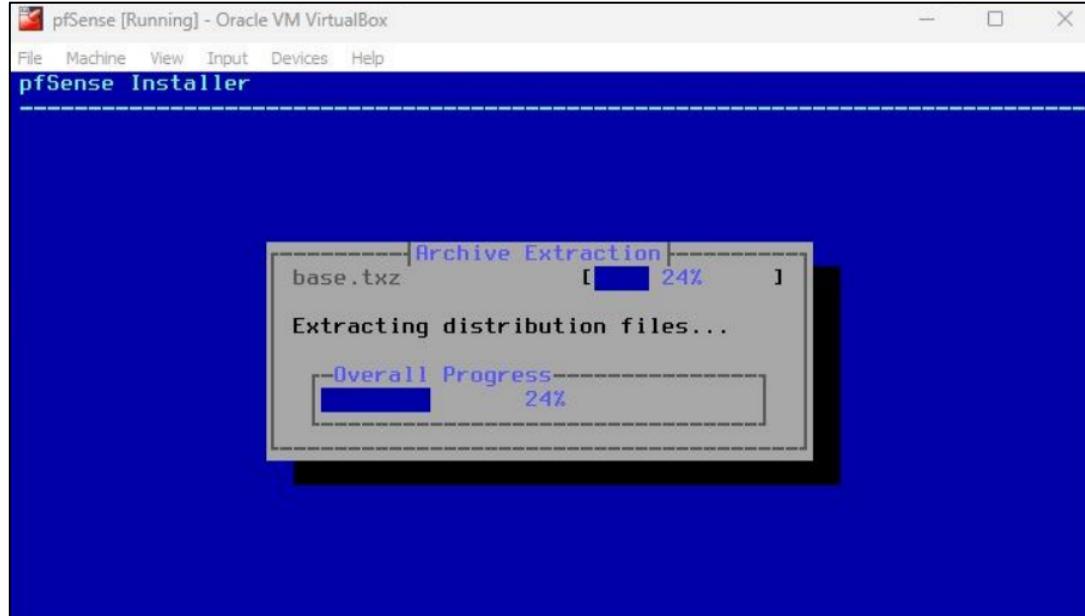


Next, we will be asked to confirm the ZFS configuration. We must select **YES** to continue with the formatting and installation.

9

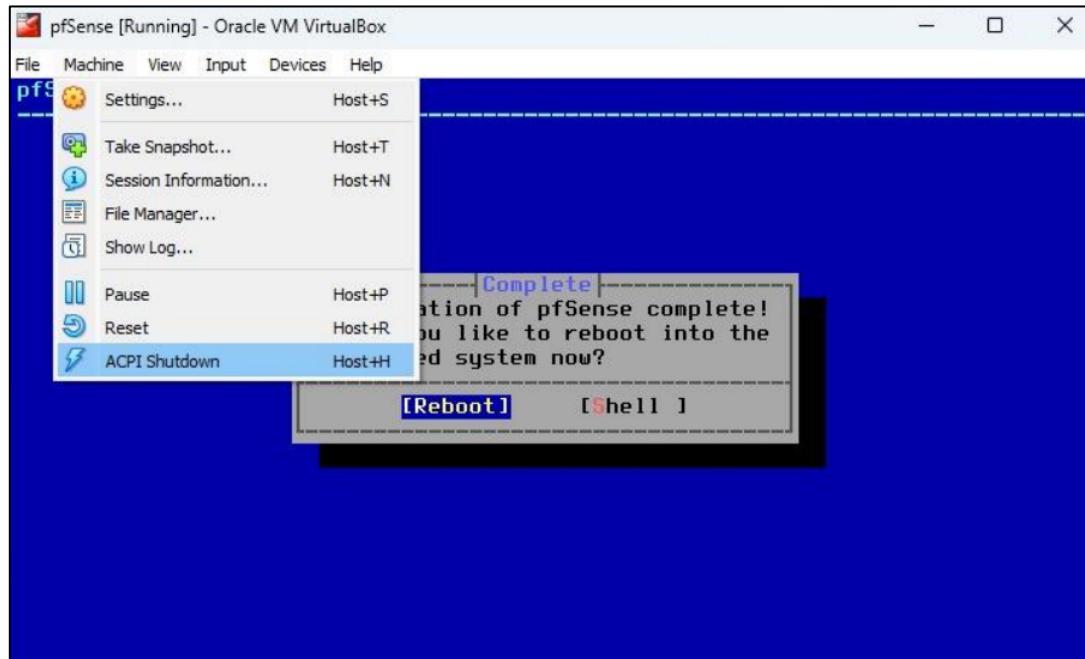


At this point, pfSense begins to install on the selected disk. We must wait a few minutes while the files are copied and the systems are configured.



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."

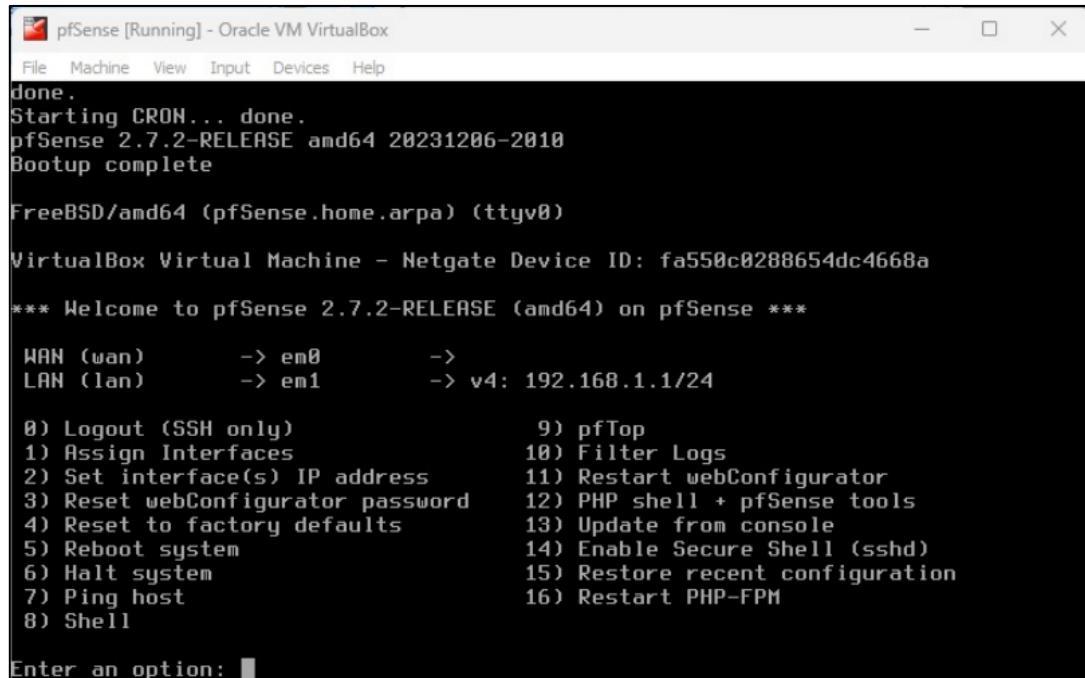
10



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.



```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: fa550c0288654dc4668a

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

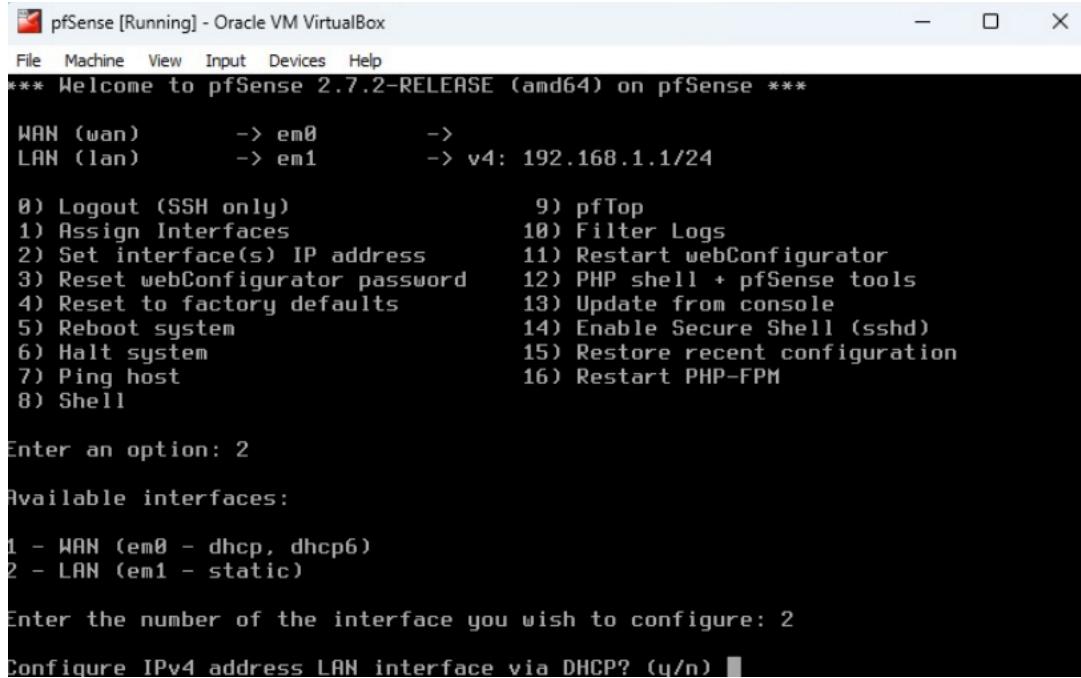
WAN (wan)      -> em0          ->
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

 0) Logout (SSH only)          9) pfTop
 1) Assign Interfaces          10) Filter Logs
 2) Set interface(s) IP address 11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults 13) Update from console
 5) Reboot system              14) Enable Secure Shell (sshd)
 6) Halt system                15) Restore recent configuration
 7) Ping host                  16) Restart PHP-FPM
 8) Shell

Enter an option: ■
```

11

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.



```

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

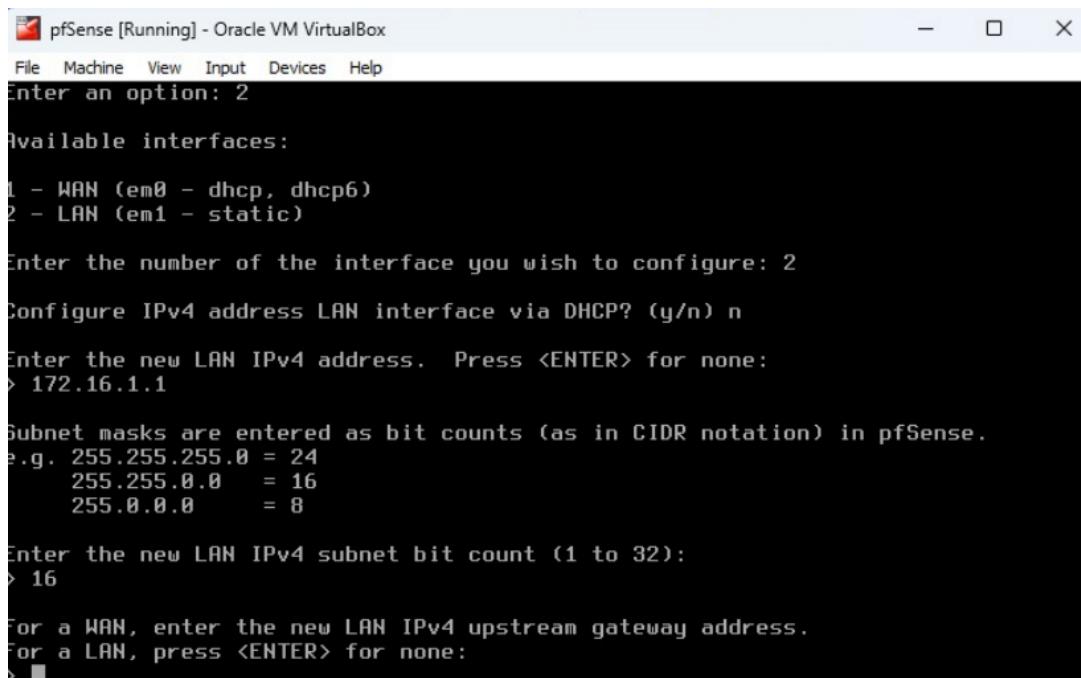
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) ■

```

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.



```

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0    = 16
     255.0.0.0      = 8

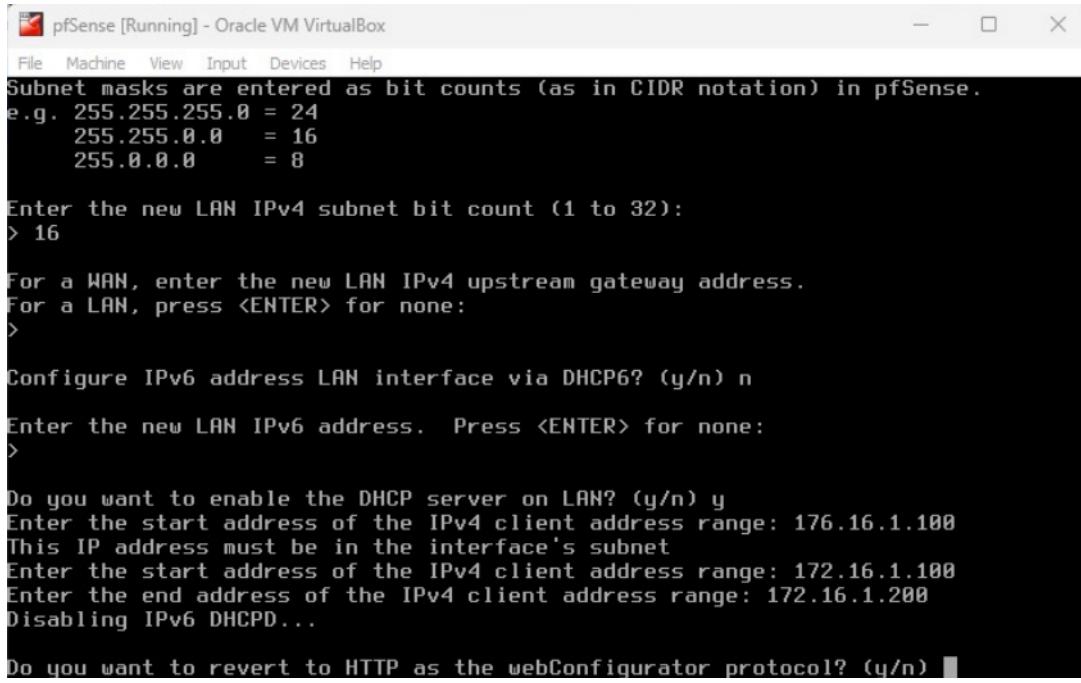
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 16

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> ■

```

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



```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 16

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

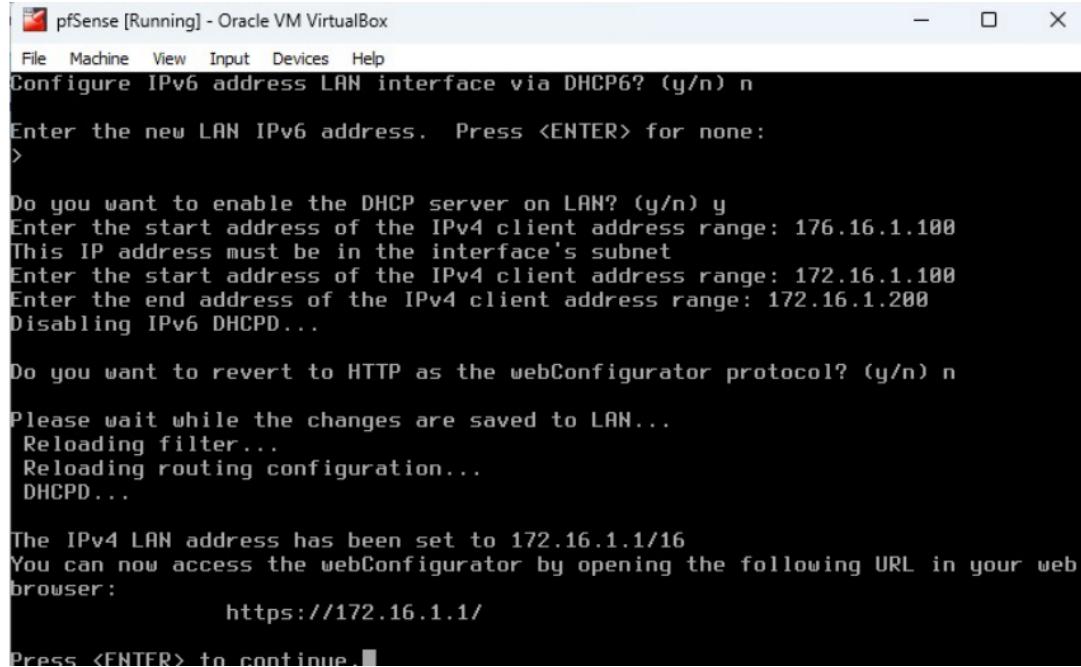
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 176.16.1.100
This IP address must be in the interface's subnet
Enter the start address of the IPv4 client address range: 172.16.1.100
Enter the end address of the IPv4 client address range: 172.16.1.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) ■
```

13

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



```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

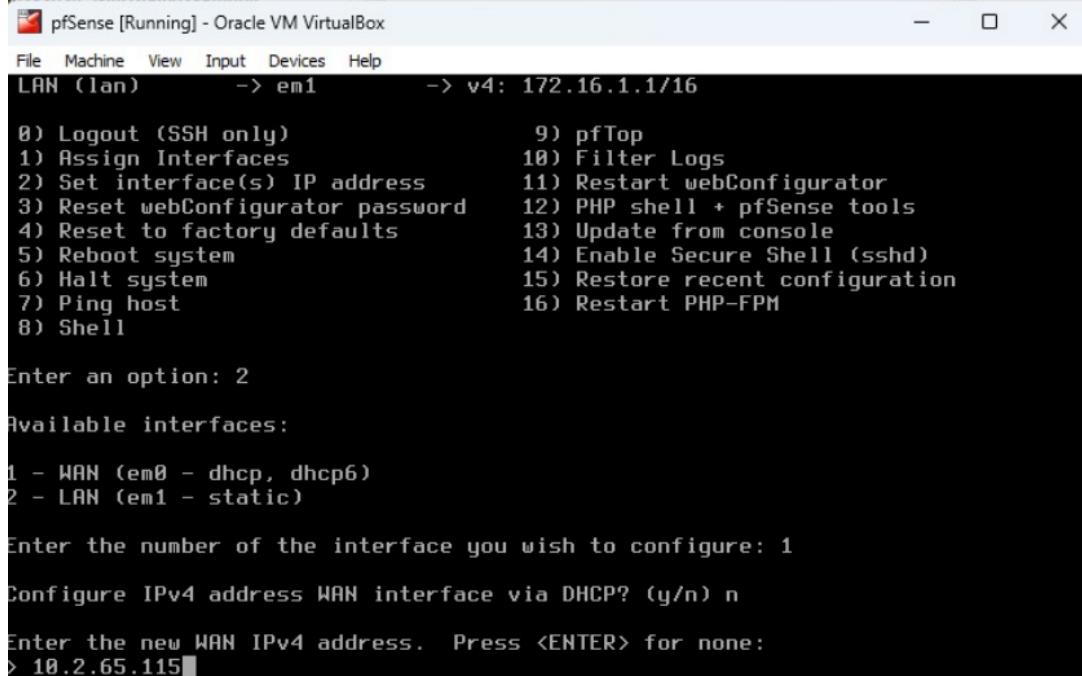
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 176.16.1.100
This IP address must be in the interface's subnet
Enter the start address of the IPv4 client address range: 172.16.1.100
Enter the end address of the IPv4 client address range: 172.16.1.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

The IPv4 LAN address has been set to 172.16.1.1/16
You can now access the webConfigurator by opening the following URL in your web
browser:
  https://172.16.1.1/
Press <ENTER> to continue.■
```

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.



```

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
LAN (lan) -> em1 -> v4: 172.16.1.1/16

8) Logout (SSH only)      9) pfTop
1) Assign Interfaces       10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system           14) Enable Secure Shell (sshd)
6) Halt system             15) Restore recent configuration
7) Ping host               16) Restart PHP-FPM

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

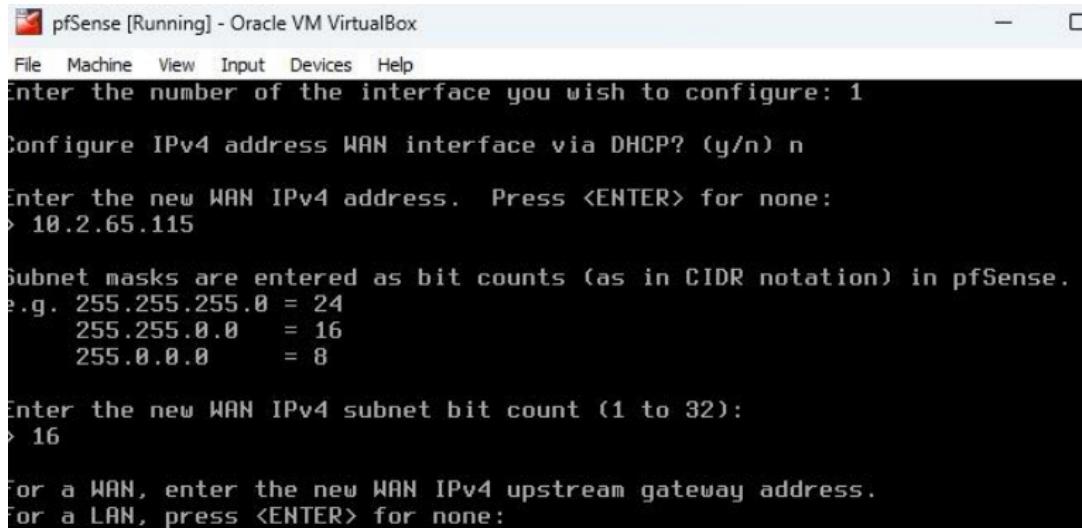
Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.2.65.115

```

14

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.



```

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.2.65.115

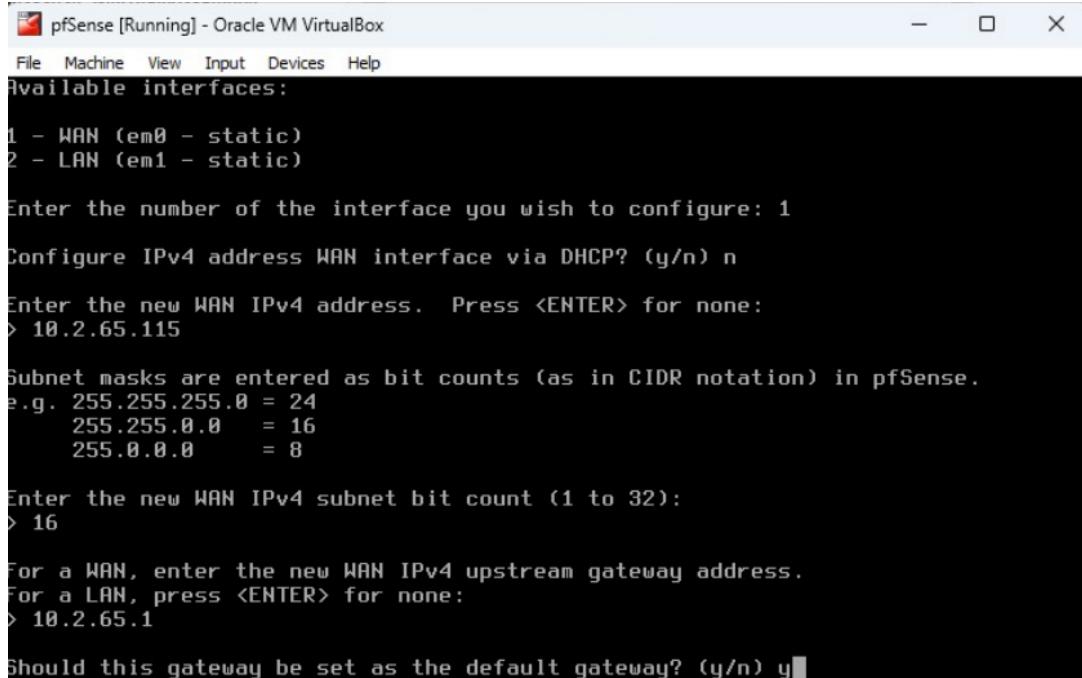
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 16

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:

```

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.



```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.2.65.115

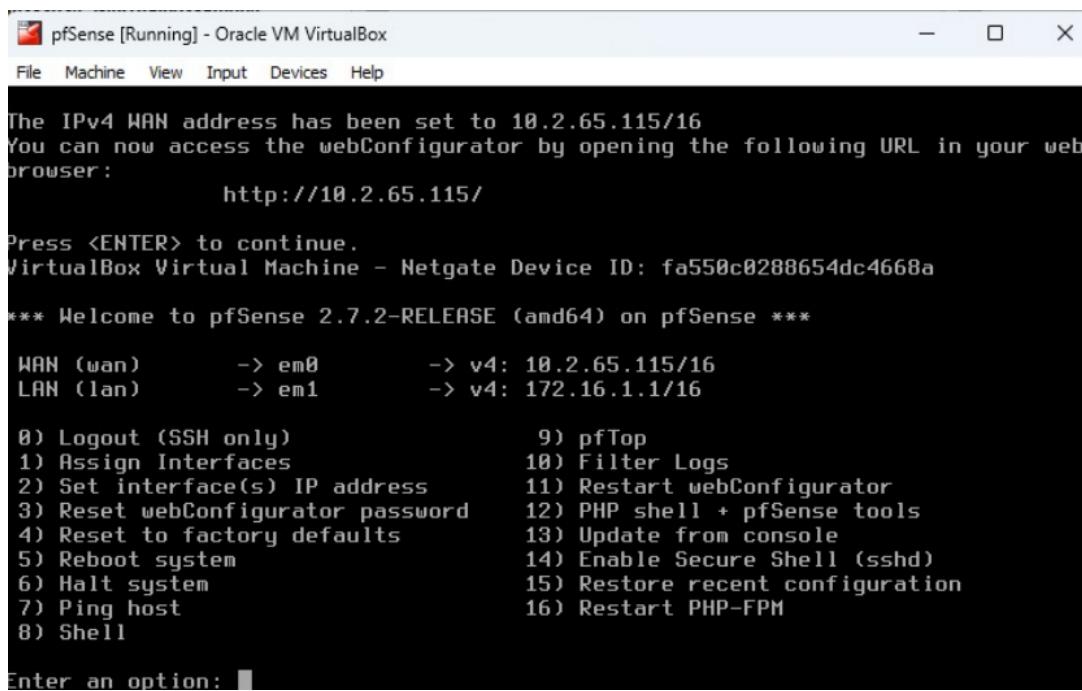
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 16

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.2.65.1

Should this gateway be set as the default gateway? (y/n) y
```

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



```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The IPv4 WAN address has been set to 10.2.65.115/16
You can now access the webConfigurator by opening the following URL in your web
browser:
http://10.2.65.115/
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: fa550c0288654dc4668a

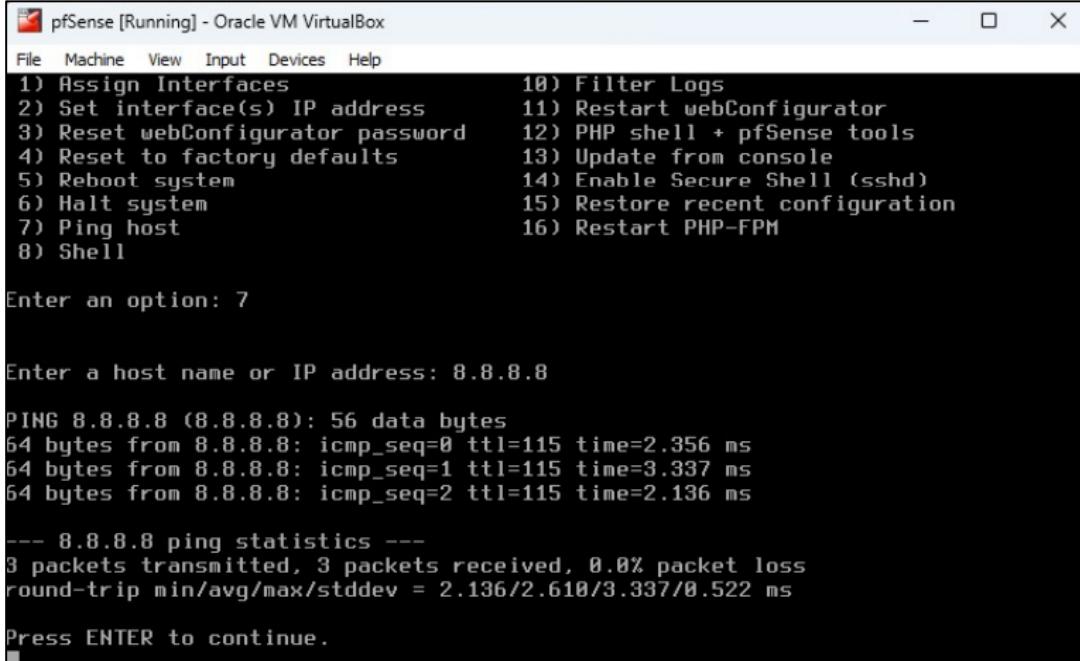
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.2.65.115/16
LAN (lan)      -> em1      -> v4: 172.16.1.1/16

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

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.



```

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1) Assign Interfaces 10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system 14) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell

Enter an option: 7

Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=2.356 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=3.337 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=2.136 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.136/2.610/3.337/0.522 ms

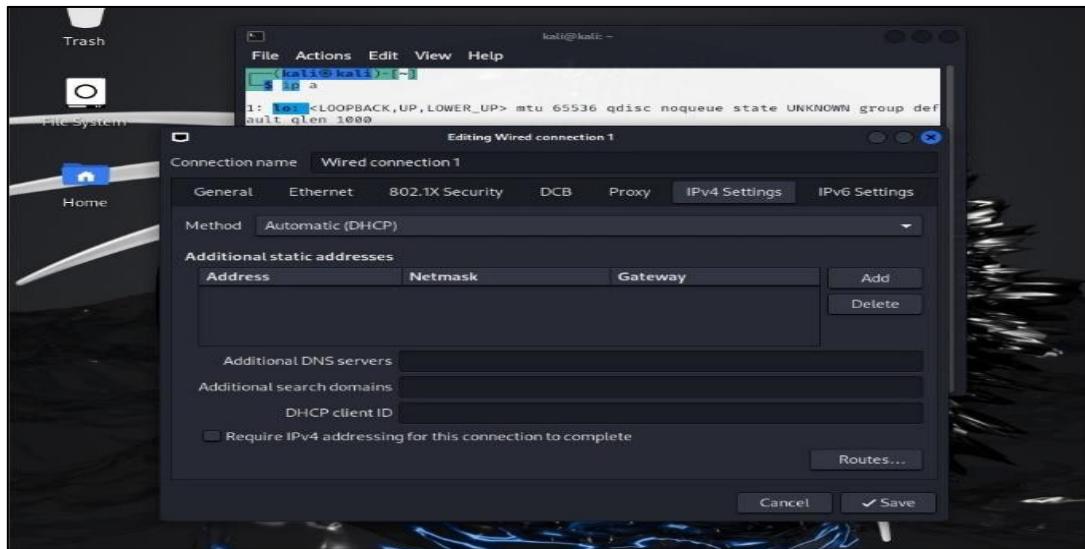
Press ENTER to continue.

```

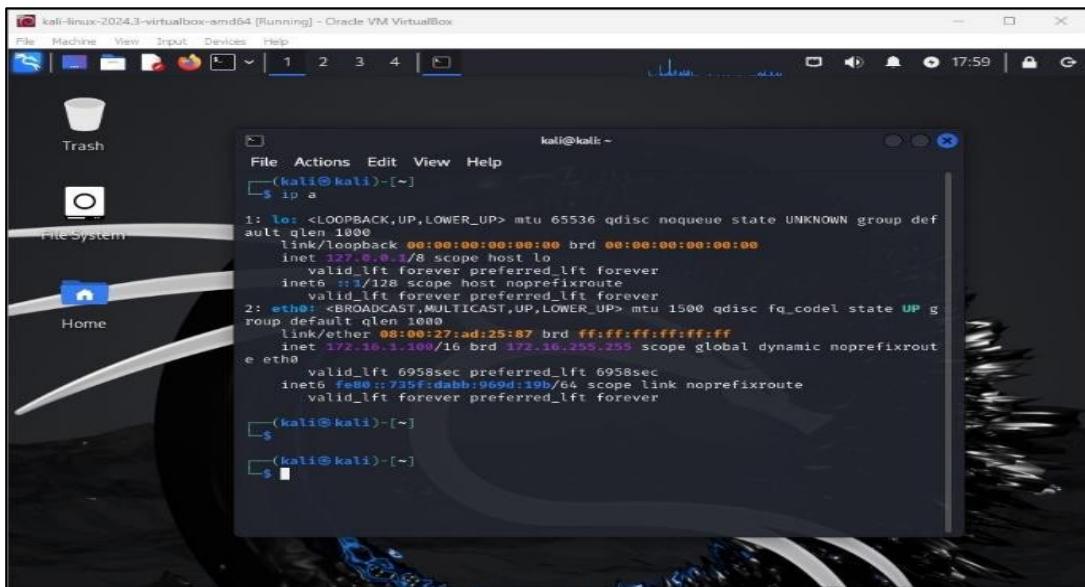
- **DHCP Assignment Verification from pfSense to Kali Linux**

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***.

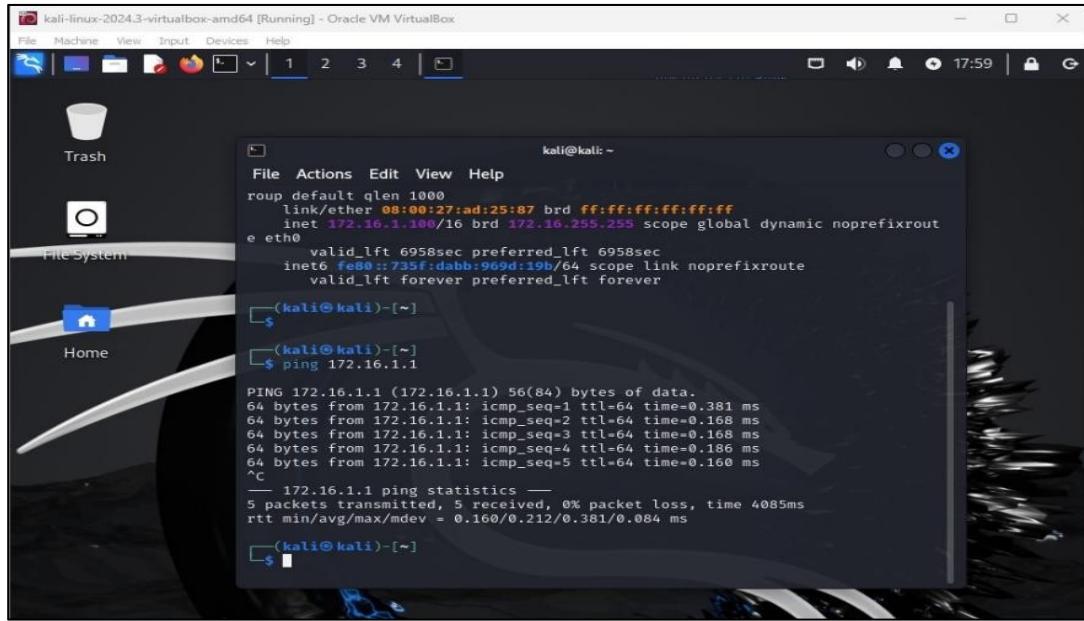
After verifying the network, we started the **Kali Linux** virtual machine. Once inside the graphical environment, click on the **network icon** in the upper right. Select the available wired connection, and enter the settings. On the **IPv4 tab**, we changed the method to **Automatic (DHCP)**. This 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.

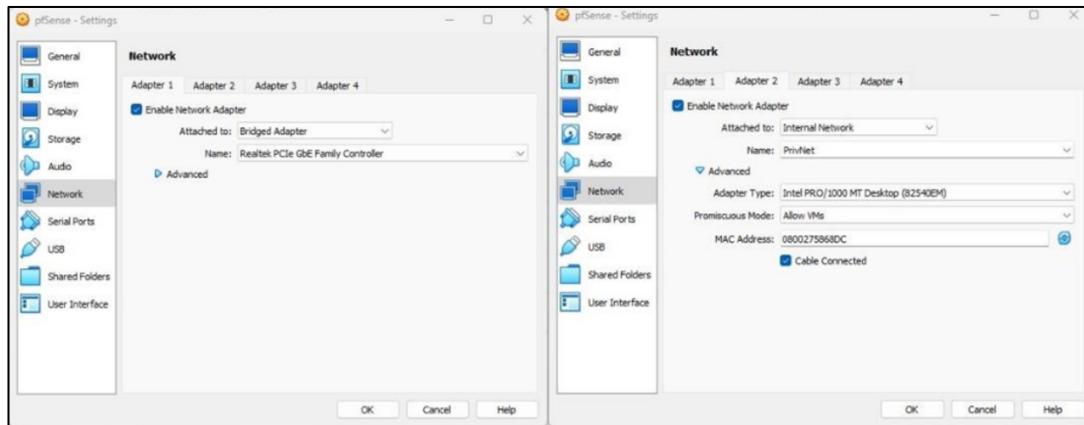


With this, we have verified that pfSense assigns IPs correctly via DHCP and that Kali Linux can communicate with it on the internal network.

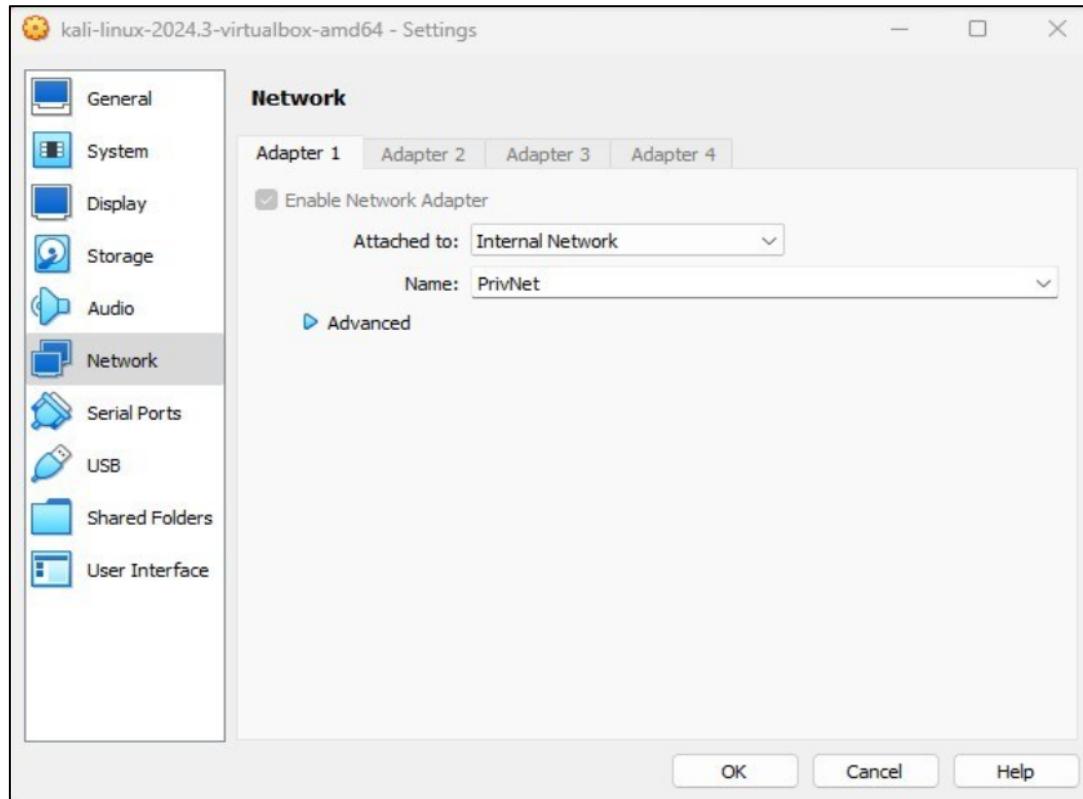
- **Verification of the virtual machine environment.**

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

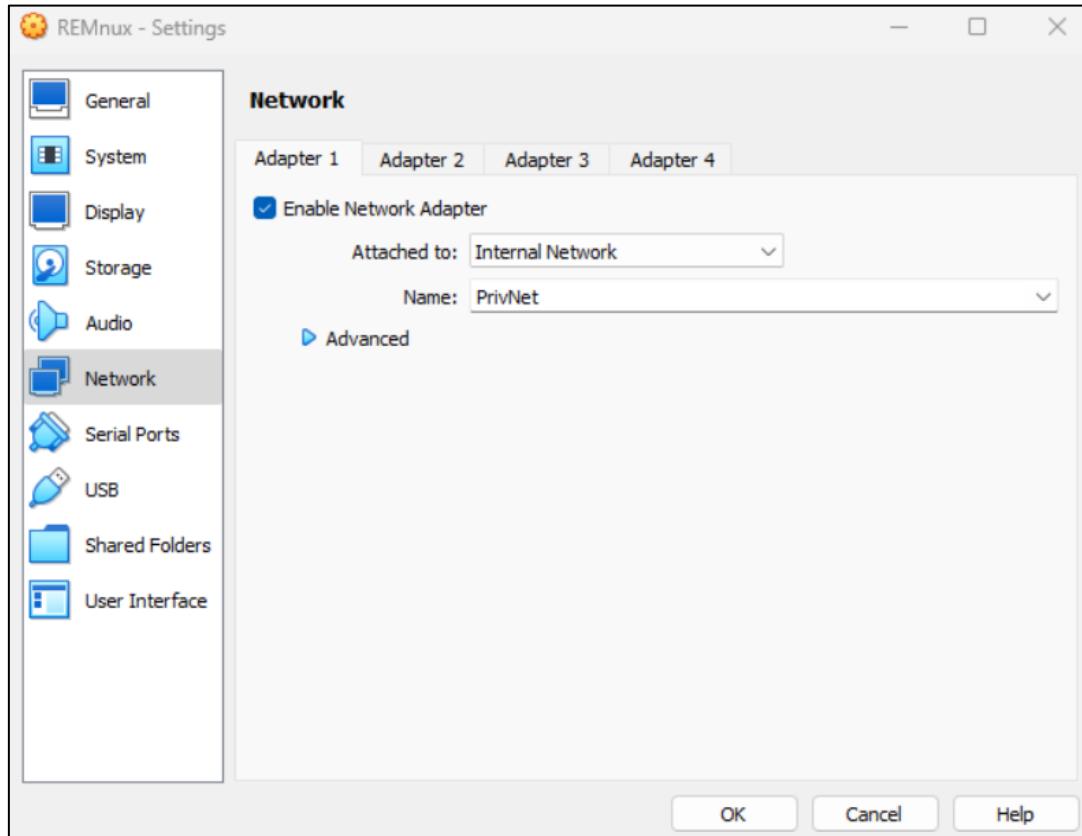
18



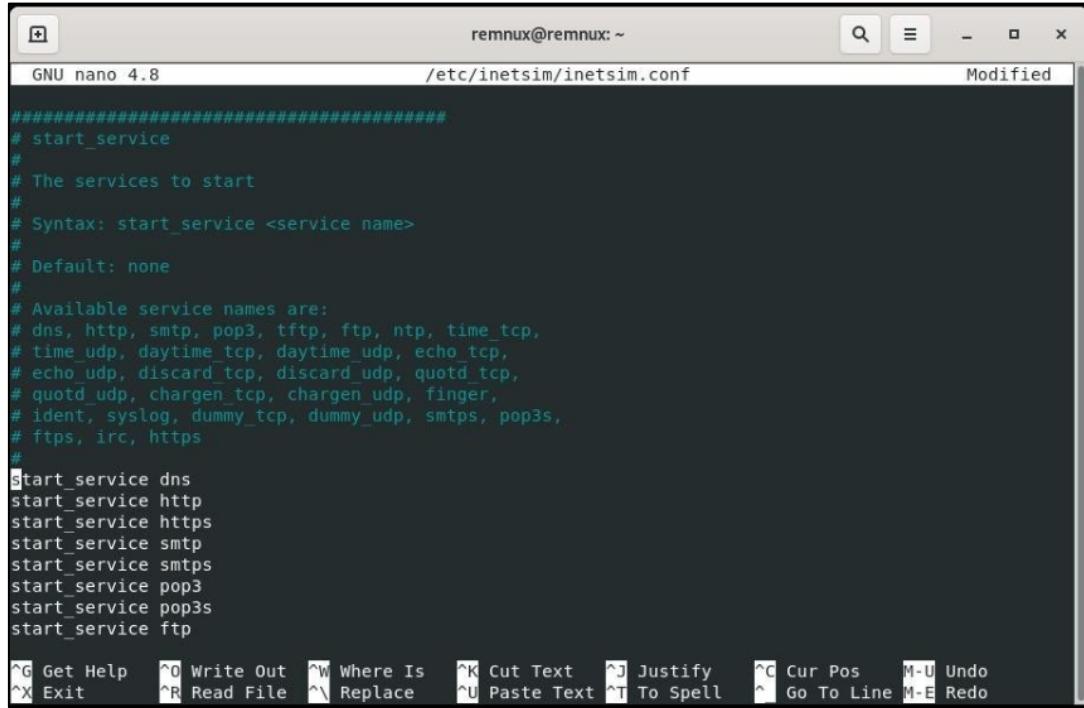
- Now we will have to verify that on Kali's machine the interface is set to Private Internal Network



- 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"

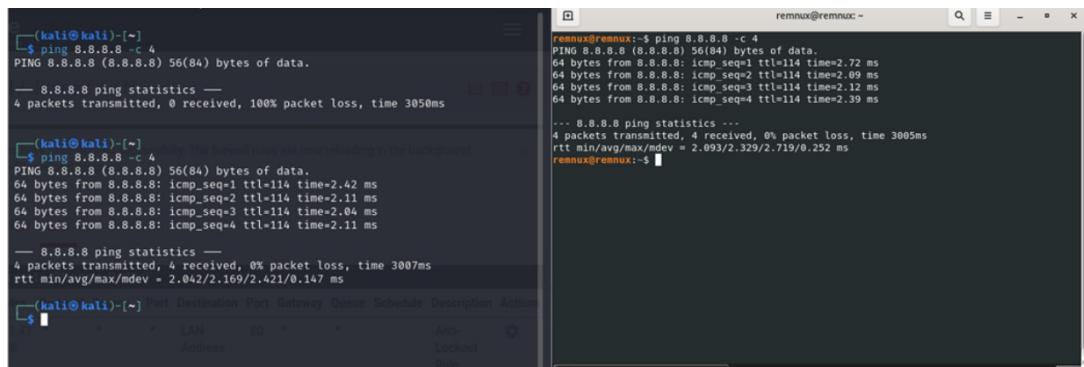


```
remnux@remnux: ~
GNU nano 4.8          /etc/inetsim/inetsim.conf          Modified

#####
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit   ^R Read File   ^U Replace   ^U Paste Text   ^T To Spell   ^ Go To Line M-E Redo
```

- Connectivity between virtual machines is verified.



```
(kali㉿kali)-[~]
└$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
4 packets transmitted, 0 received, 100% packet loss, time 3050ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3050ms

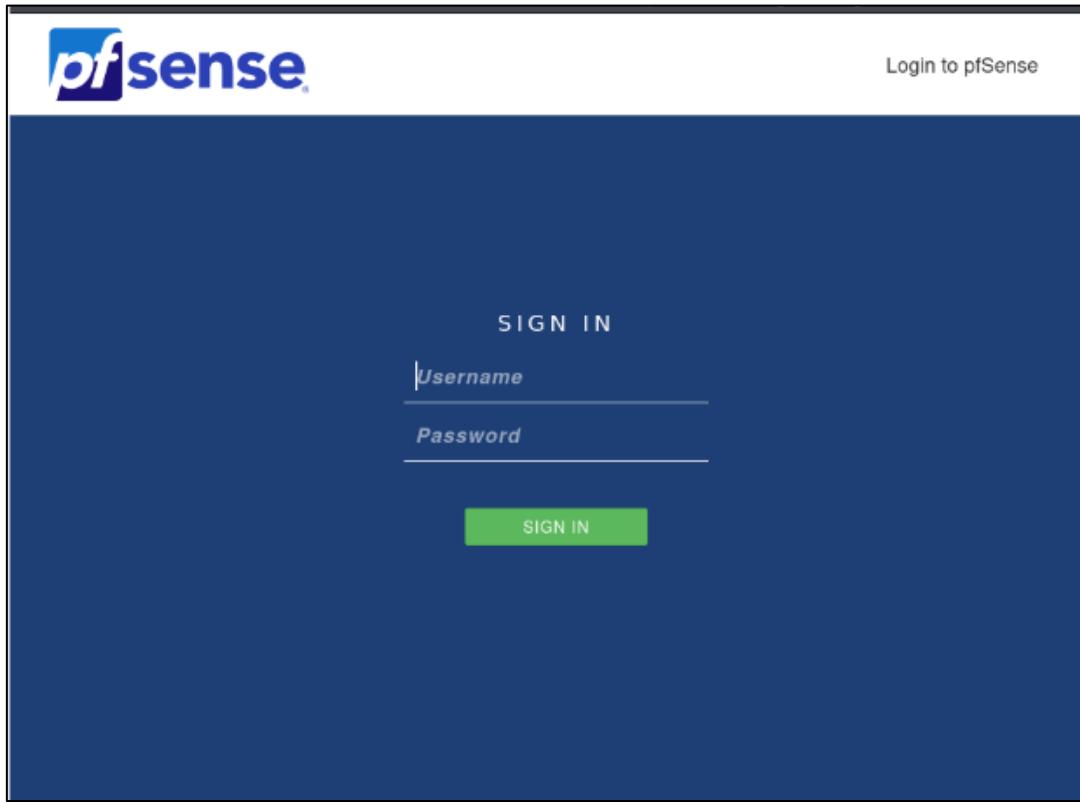
(kali㉿kali)-[~]
└$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=14 time=2.42 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=14 time=2.11 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=14 time=2.04 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=14 time=2.11 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.042/2.169/2.421/0.147 ms

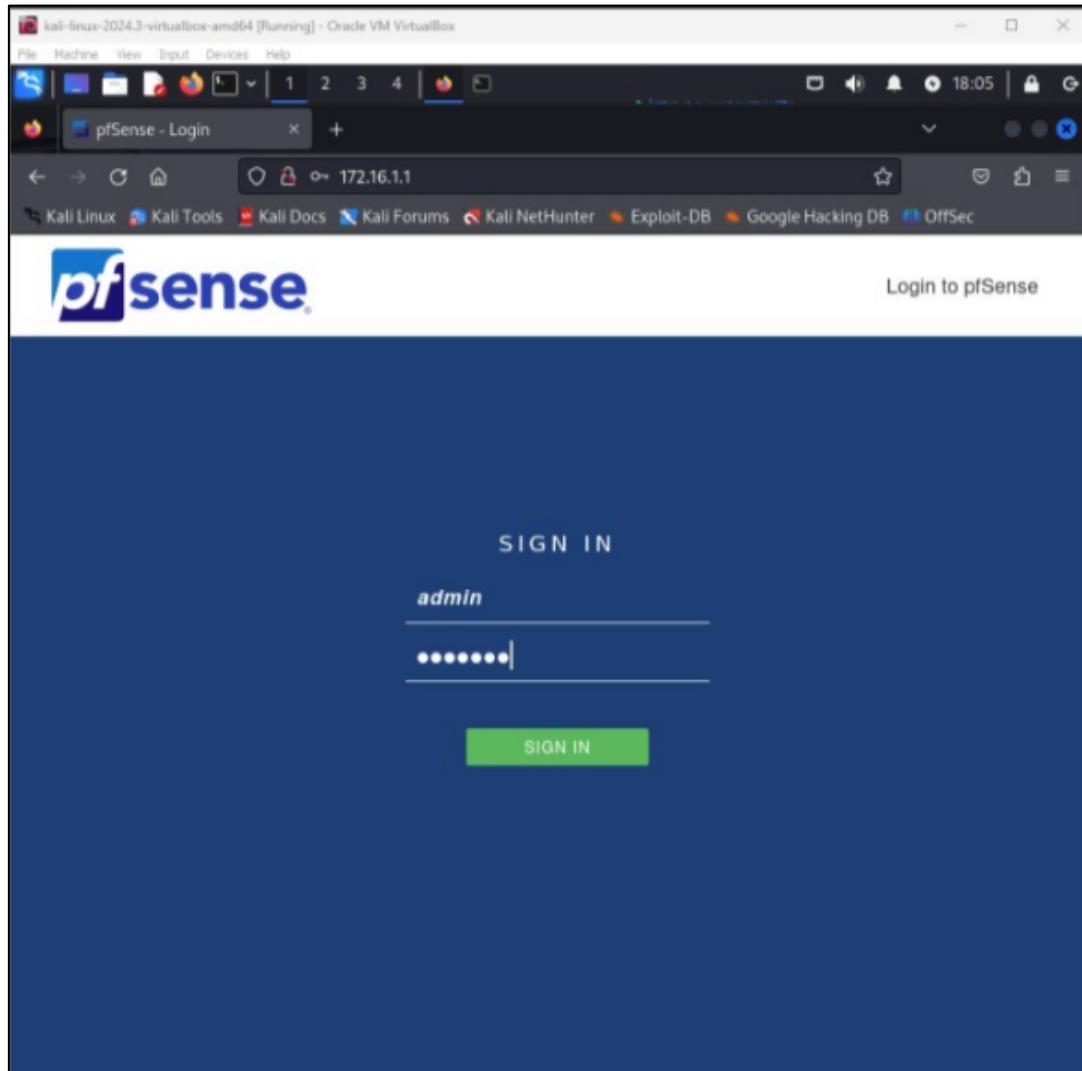
remnux@remnux: ~
└$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=14 time=2.72 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=14 time=2.69 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=14 time=2.12 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=14 time=2.39 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.093/2.329/2.719/0.252 ms
```

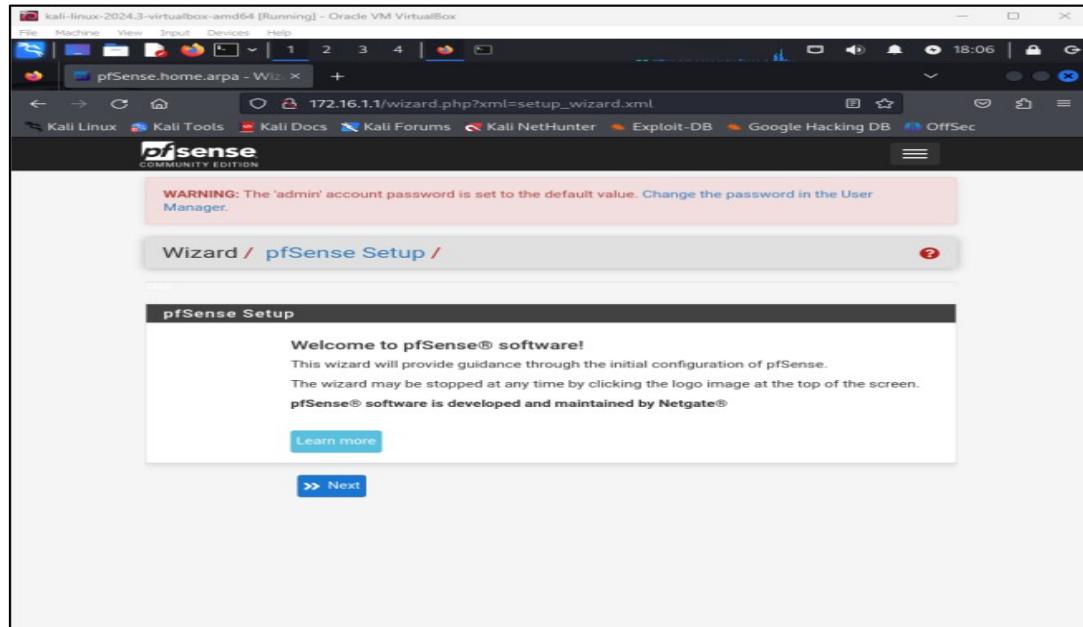
- Complete the installation of Pfsense. On the Kali Linux machine, the pfSense web console is accessed via a browser using the pfSense LAN IP 172.16.1.1 interface.



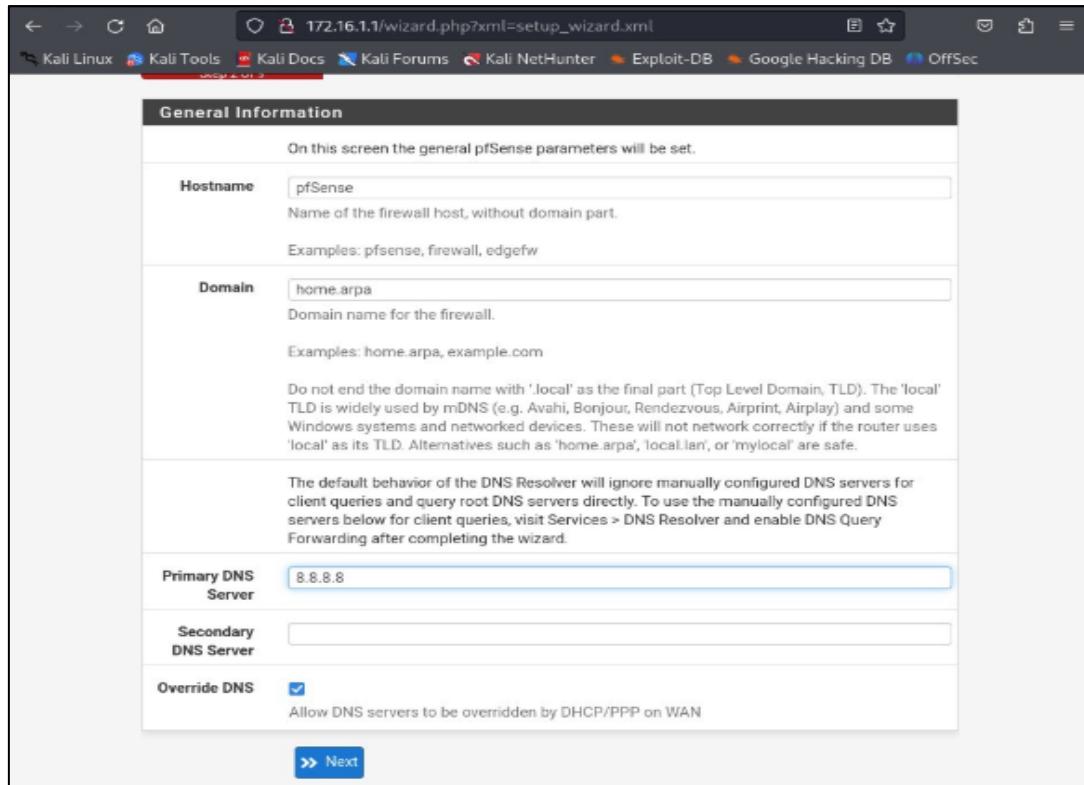
- These are the following credentials:
 - Username: admin
 - Password: pfsense



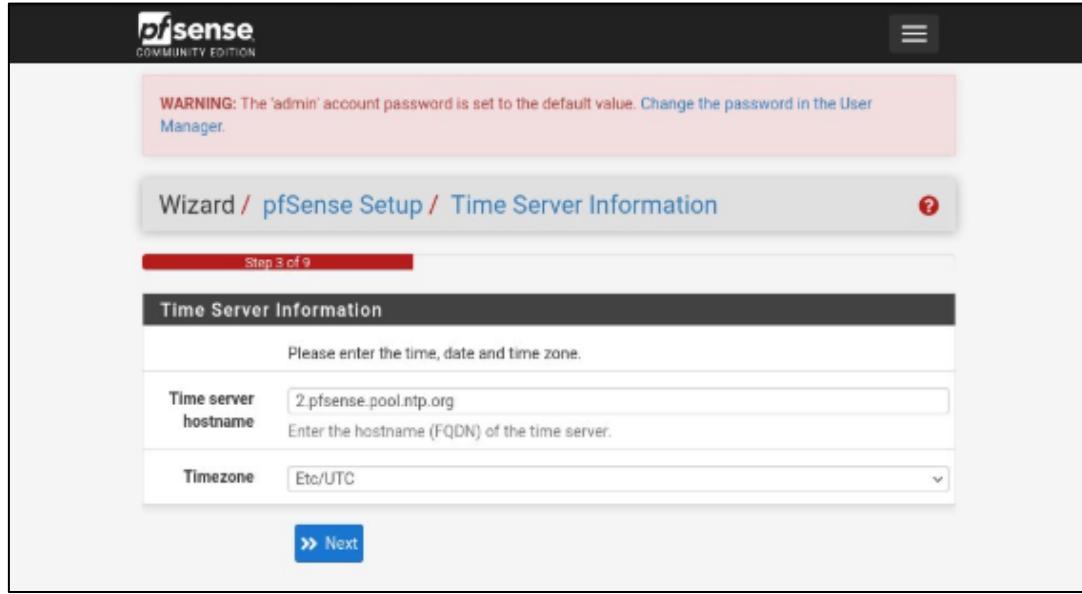
Now the welcome screen will appear and the assistant will tell us step by step what we have to do.



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



The screenshot shows the "General Information" step of the pfSense setup wizard. The URL in the address bar is `172.16.1.1/wizard.php?xml=setup_wizard.xml`. The page title is "General Information". It says: "On this screen the general pfSense parameters will be set." Under "Hostname", the value is "pfSense" with a note: "Name of the firewall host, without domain part." Examples given are "pfsense", "firewall", "edgefw". Under "Domain", the value is "home.arpa" with a note: "Domain name for the firewall." Examples given are "home.arpa", "example.com". A note below states: "Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe." Under "Primary DNS Server", the value is "8.8.8.8". Under "Secondary DNS Server", there is an empty input field. Under "Override DNS", there is a checked checkbox with the note: "Allow DNS servers to be overridden by DHCP/PPP on WAN". At the bottom is a "» Next" button.



WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

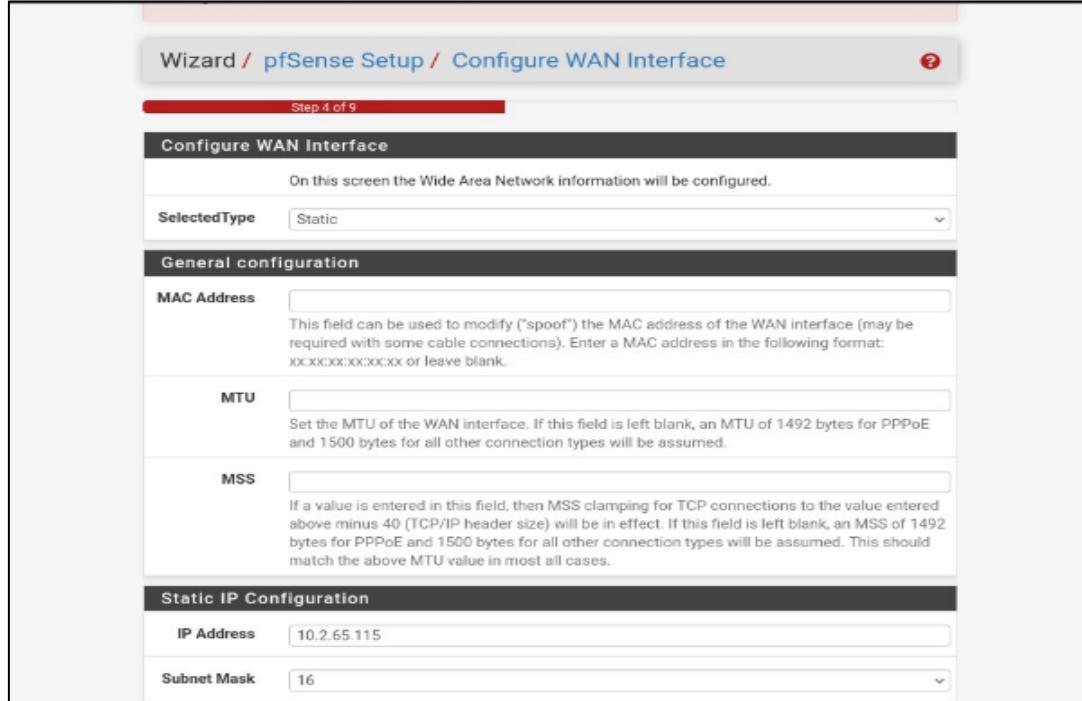
Please enter the time, date and time zone.

Time server hostname 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone Etc/UTC

>> Next

- 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.



Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

Selected Type Static

General configuration

MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: XXXXXXXX:XX:XX or leave blank.

MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

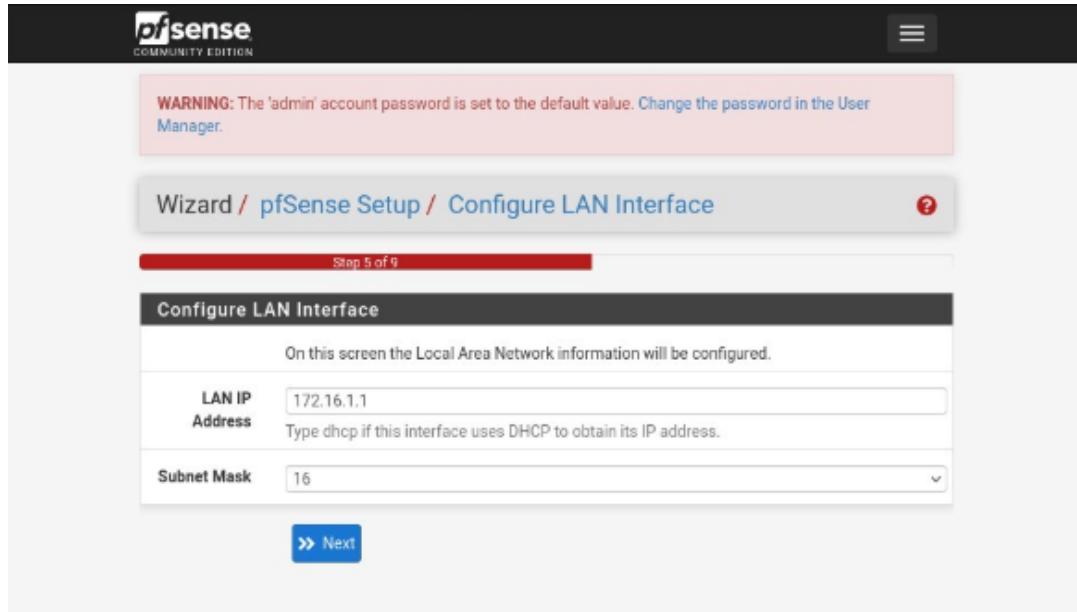
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

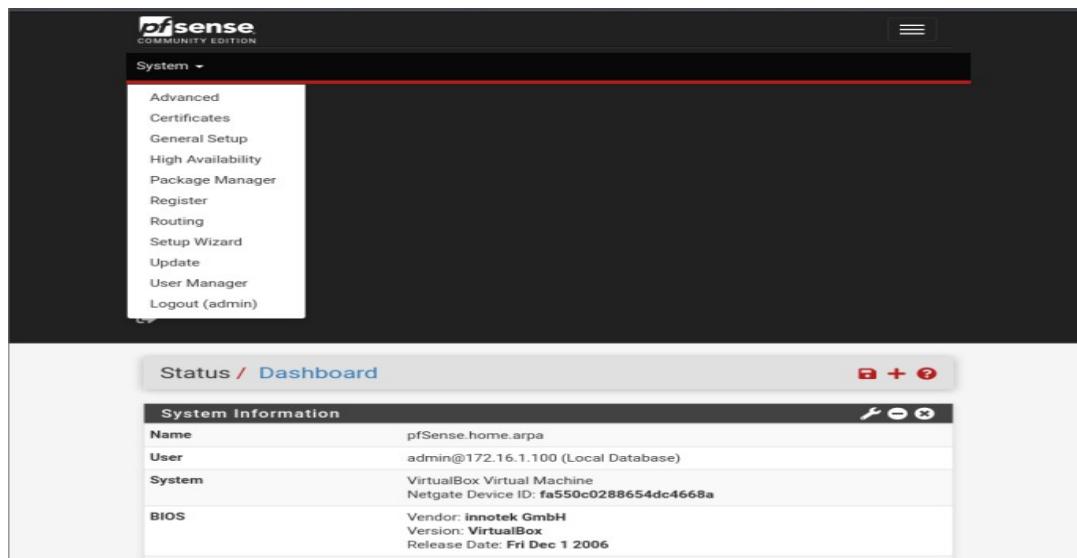
IP Address 10.2.65.115

Subnet Mask 16

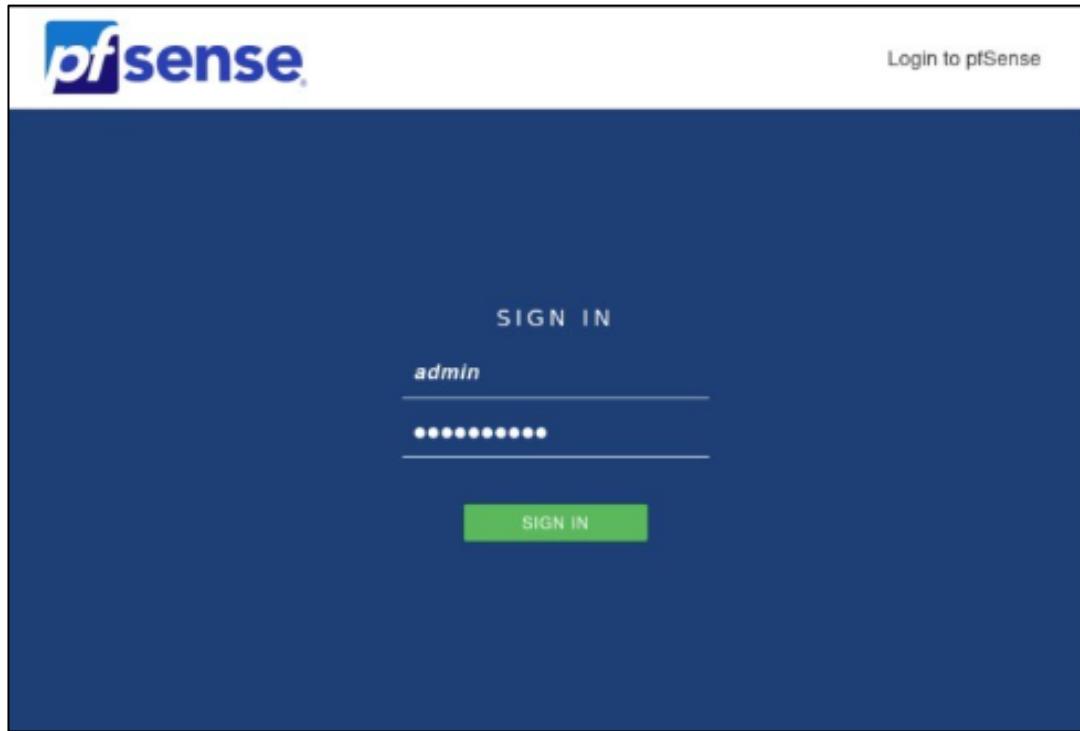
- And now with the LAN.



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



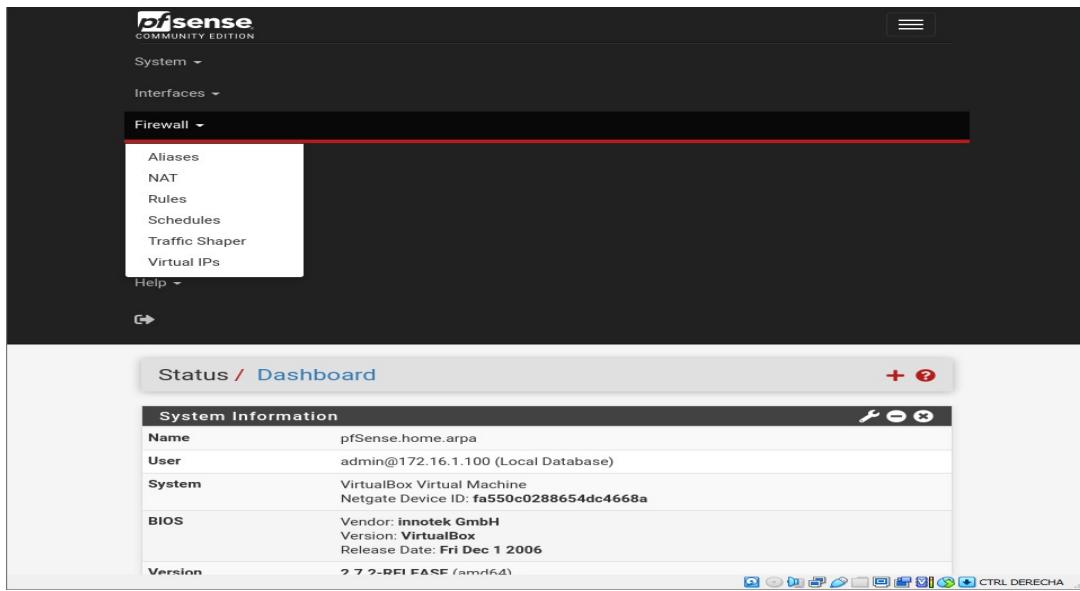
- The following credentials will now be entered
 - Username: admin
 - Password: JuanValent



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

27

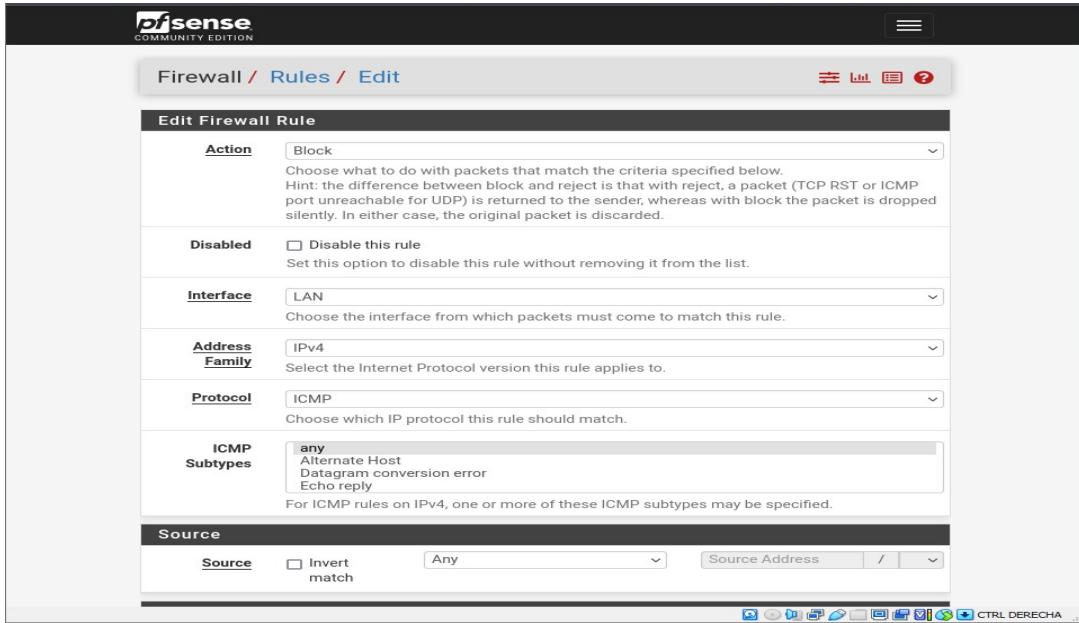
Now we will have to click on the up arrow, and enter the following parameters.



System Information	
Name	pfSense.home.arpa
User	admin@172.16.1.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: fa550c0288654dc4668a
BIOS	Vendor: innoteck GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-PFSENSE (armhf64)

- Action: Block
- Interface: LAN

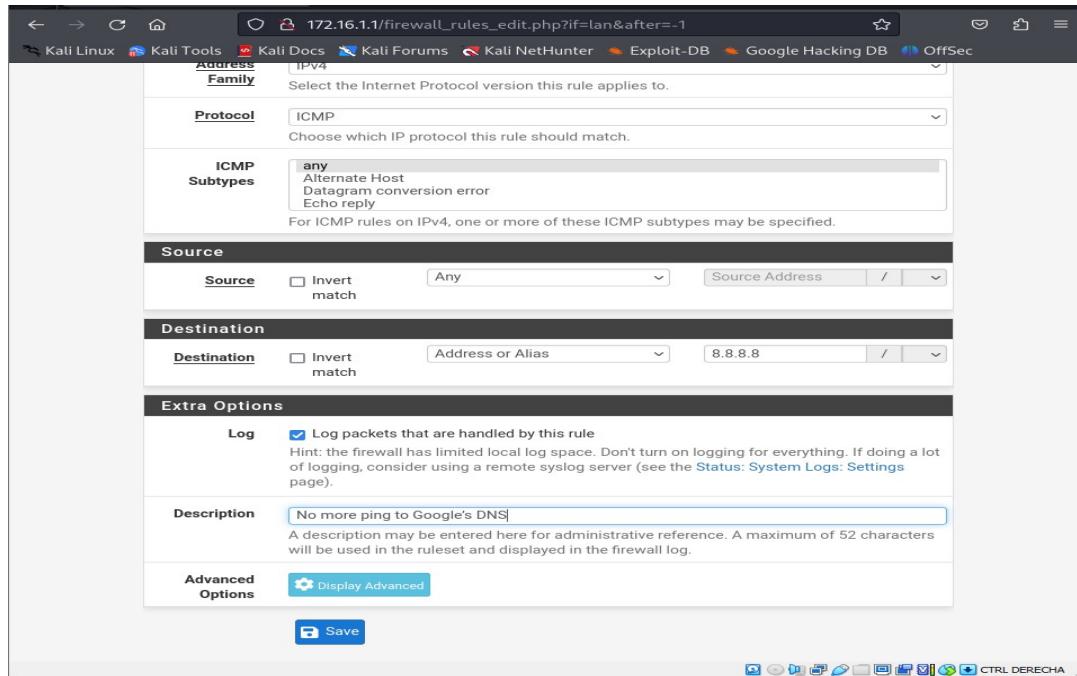
- Address Family: IPv4
- Protocol: ICMP
- ICMP Subtypes : any
- Source: any
- Destination: Single host or alias > 8.8.8.8
- Enable Log packets that are handled by this rule
- Description: No more ping to Google's DNS



The screenshot shows the pfSense Firewall Rules Edit interface. A new rule is being configured with the following settings:

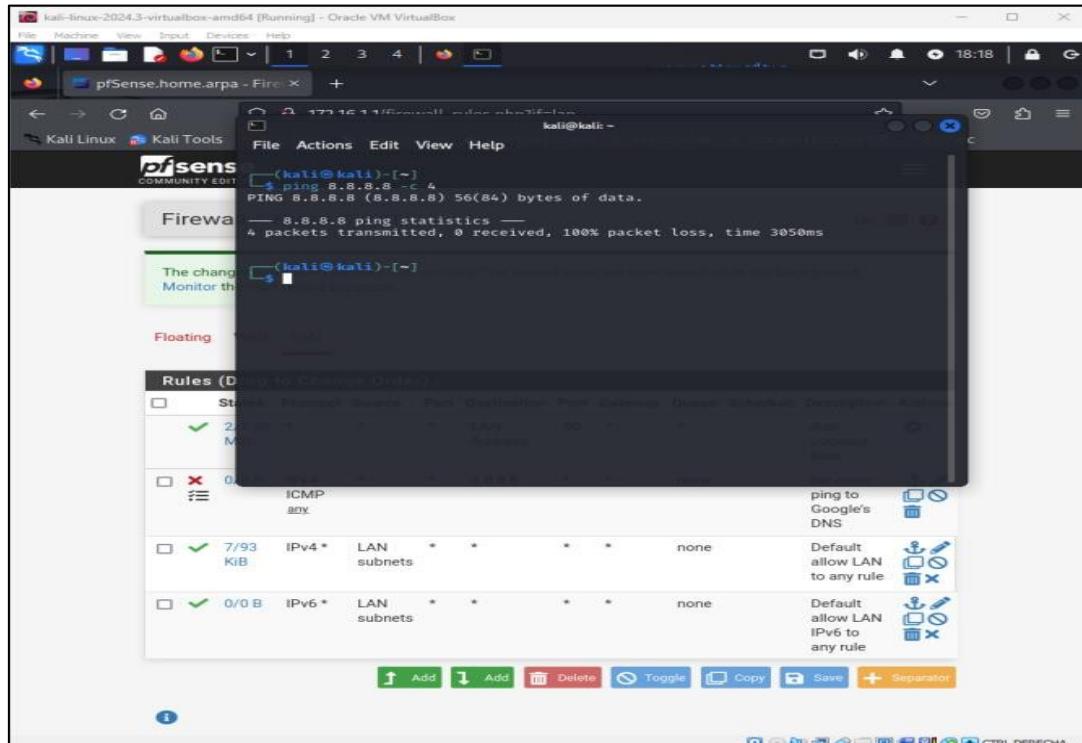
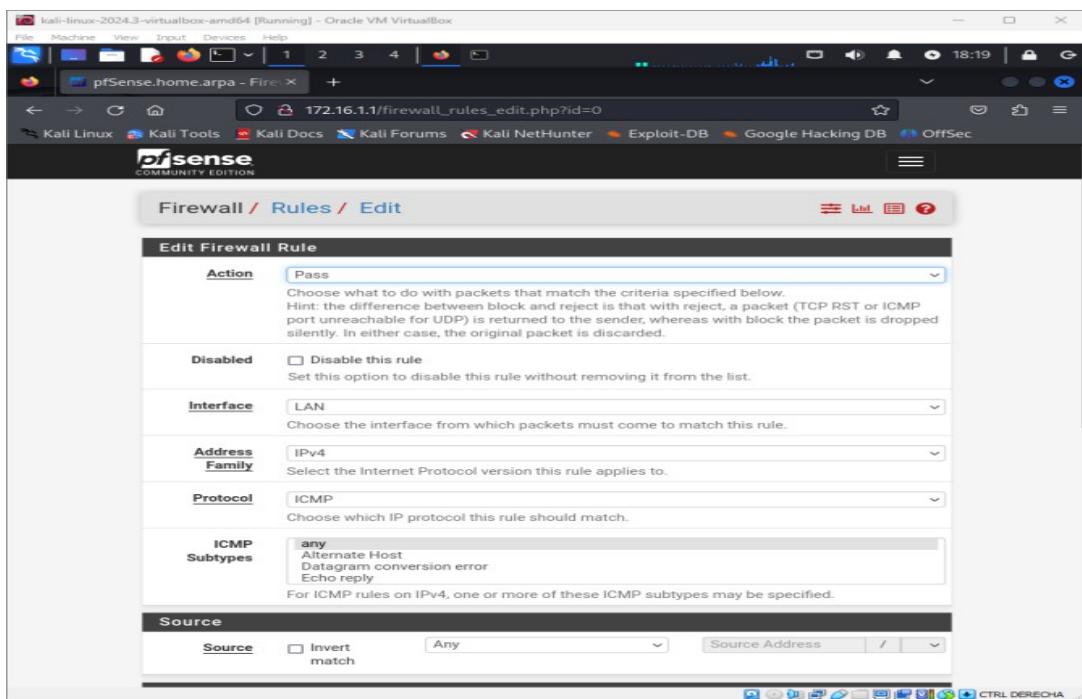
- Action:** Block
- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** ICMP
- ICMP Subtypes:** any (selected from a dropdown list which also includes Alternate Host, Datagram conversion error, and Echo reply)
- Source:** Any (selected from a dropdown list)

At the bottom right of the interface, there is a toolbar with various icons and the text "CTRL DERECHA".



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.

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: LAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: ICMP
Choose which IP protocol this rule should match.

ICMP Subtypes: any
Alternate Host
Datagram conversion error
Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

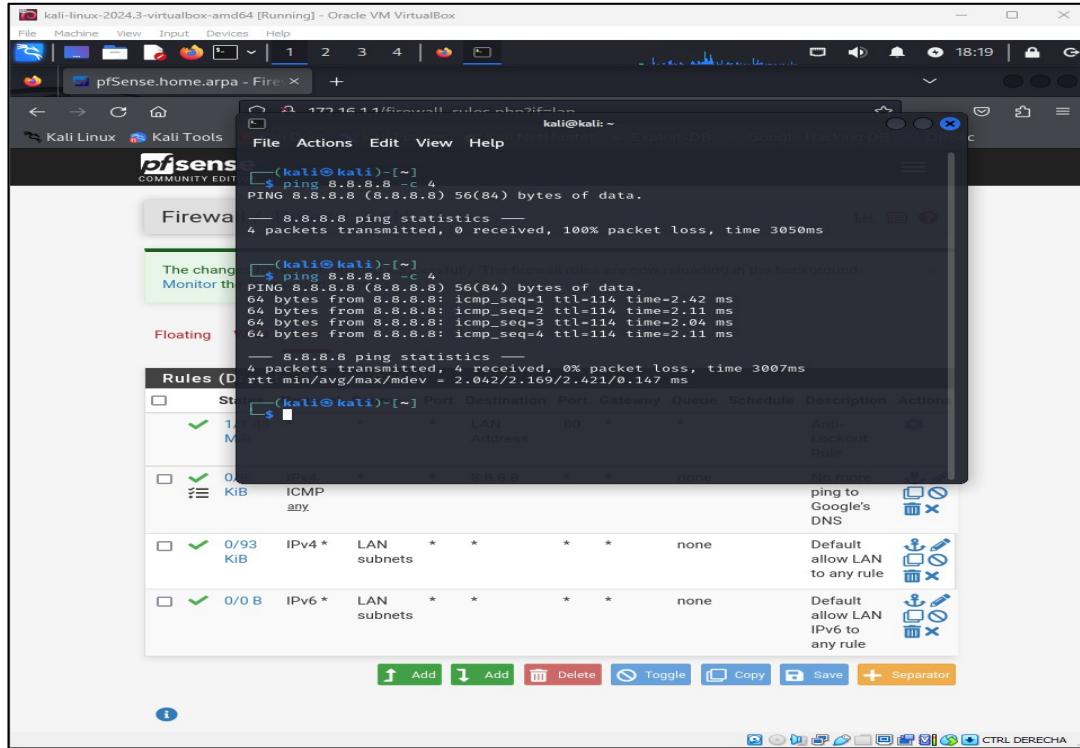
Source:

Source: Any
 Invert match

30

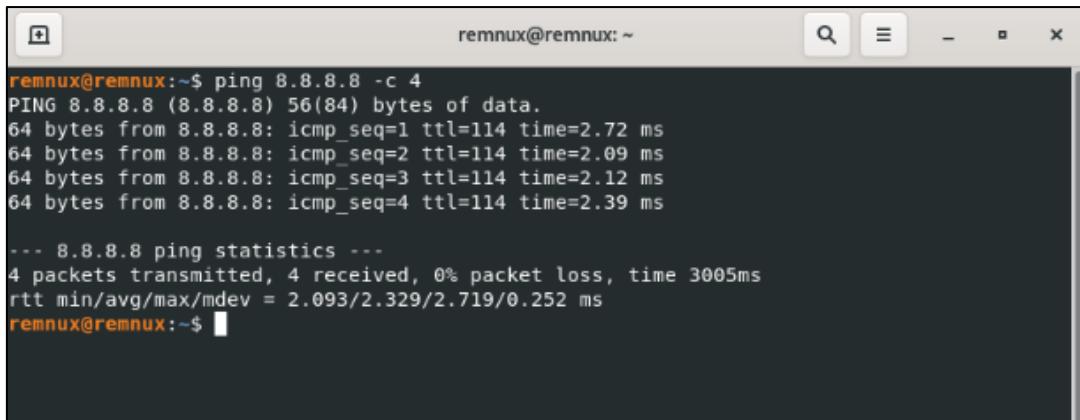
- Rule changed to pass

- Now we observe the answer in kali



31

And now on the REMux virtual machine



```
remnux@remnux:~$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=2.72 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=2.09 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=2.12 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=2.39 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.093/2.329/2.719/0.252 ms
remnux@remnux:~$
```

- 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."

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/1.44 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 ICMP any.	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input checked="" type="checkbox"/>	✓ 0/672 B	IPv4 ICMP any.	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input type="checkbox"/>	✓ 0/93 KIB	IPv4 *	LAN subnets	*	*	*	*	*	none	Default allow LAN to any rule	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

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

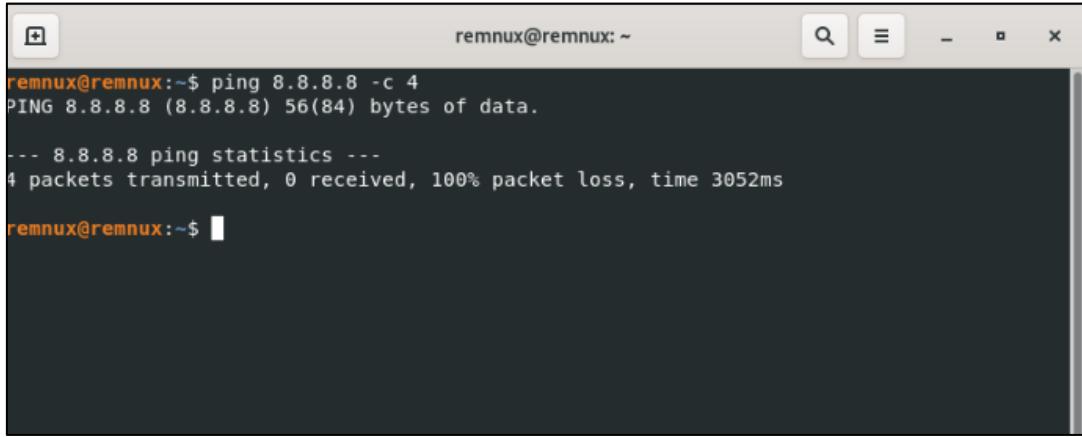
```

ping 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
PING 8.8.8.8 ping statistics
4 packets transmitted, 0 received, 100% packet loss, time 3063ms

```

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1.44 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 ICMP any.	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input checked="" type="checkbox"/>	✓ 0/672 B	IPv4 ICMP any.	*	*	8.8.8.8	*	*	none		No more ping to Google's DNS	
<input type="checkbox"/>	✓ 48/113 KIB	IPv4 *	LAN subnets	*	*	*	*	*	none	Default allow LAN to any rule	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

And finally the REMux virtual machine



```
remnux@remnux:~$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3052ms

remnux@remnux:~$
```

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 IP 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.