

[Open in app ↗](#) Medium Search Write 7 F

How to Install and Configure pfSense in a Homelab for Full LAN Internet Access



Frederick Adigun · 13 min read · Aug 21, 2025



13



...

Salut!

In this guide, we will cover:

1. Downloading and installing pfSense
2. Accessing the pfSense web interface
3. Configuring firewall rules in pfSense

I'm assuming you already have VirtualBox installed. If not, you can follow [this link](#) to learn how to install it for free.

Step 1: DOWNLOADING AND INSTALLING PFSENSE

With VirtualBox installed, the next step is to download the pfSense ISO file. Go to the official pfSense website [here](#) to get the ISO for installation (Fig. 1). You'll need to create an account to download the image. You can choose either the Community Edition or pfSense Plus, but I'll be using the Community Edition here.

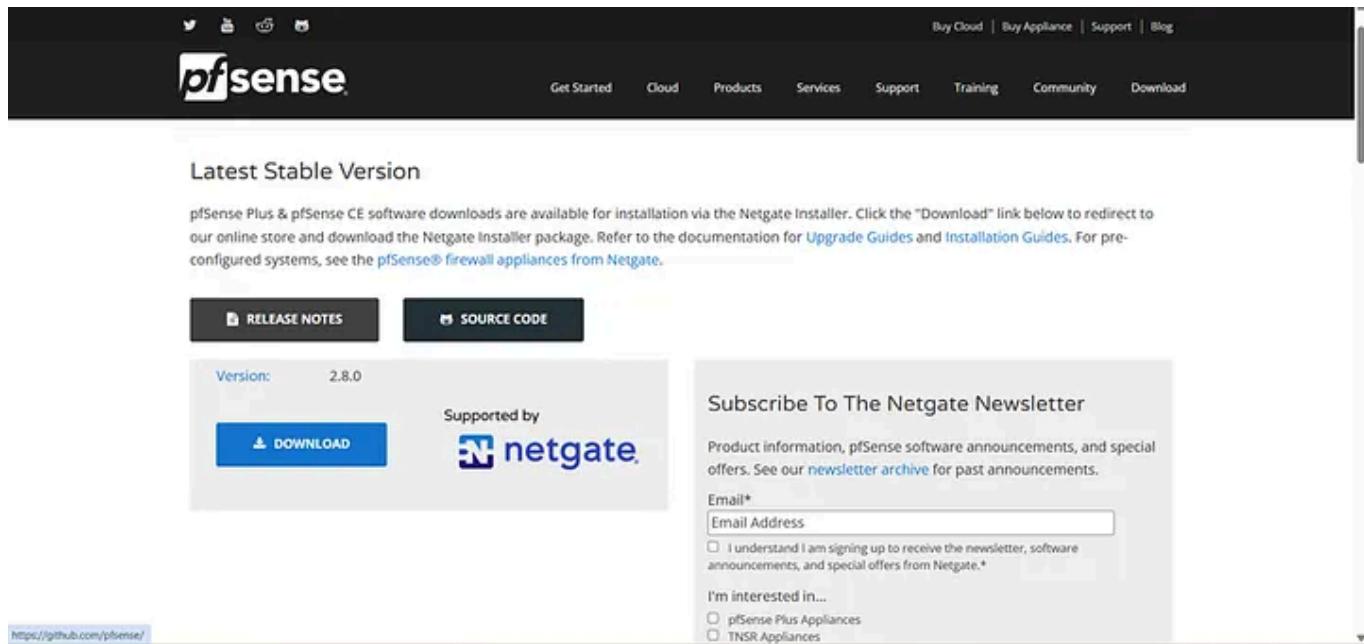


Fig. 1

Click on **DOWNLOAD**, then on the next page, select the image type as shown in the screenshot below. After, click on **ADD TO CART** to go to the checkout page (Fig. 2).

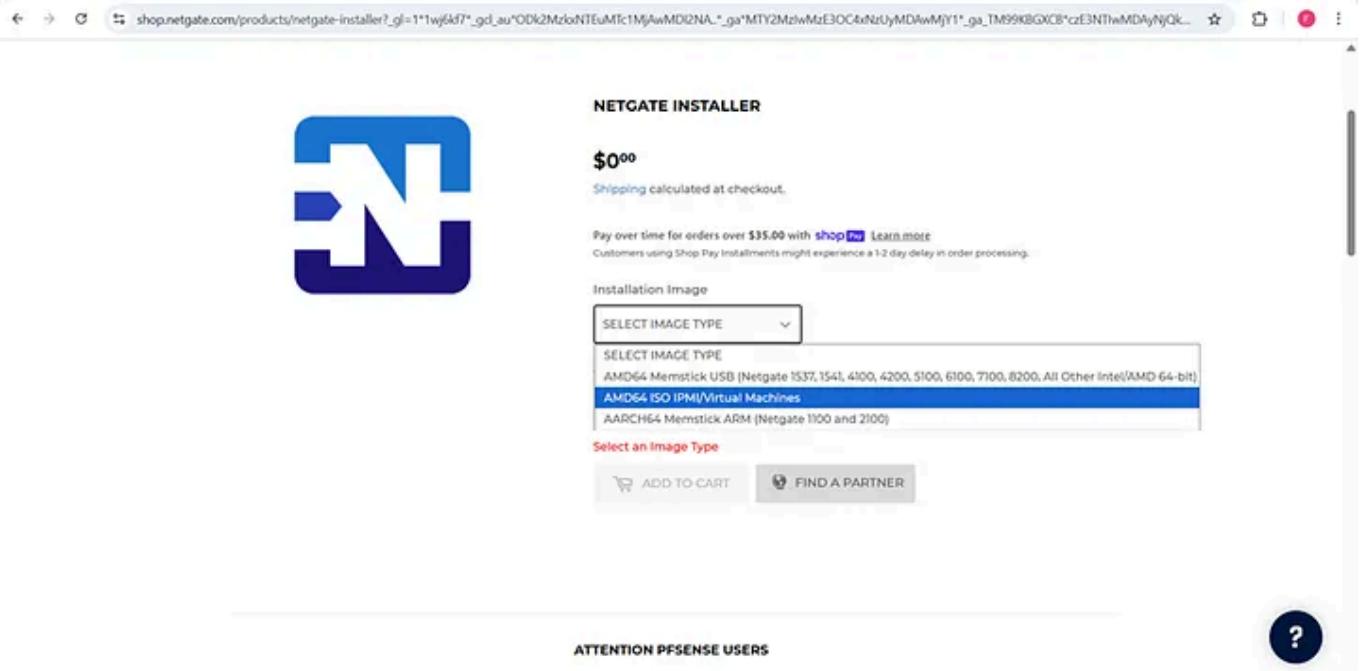


Fig. 2

On the checkout page, download the ISO file for free (Fig. 3).

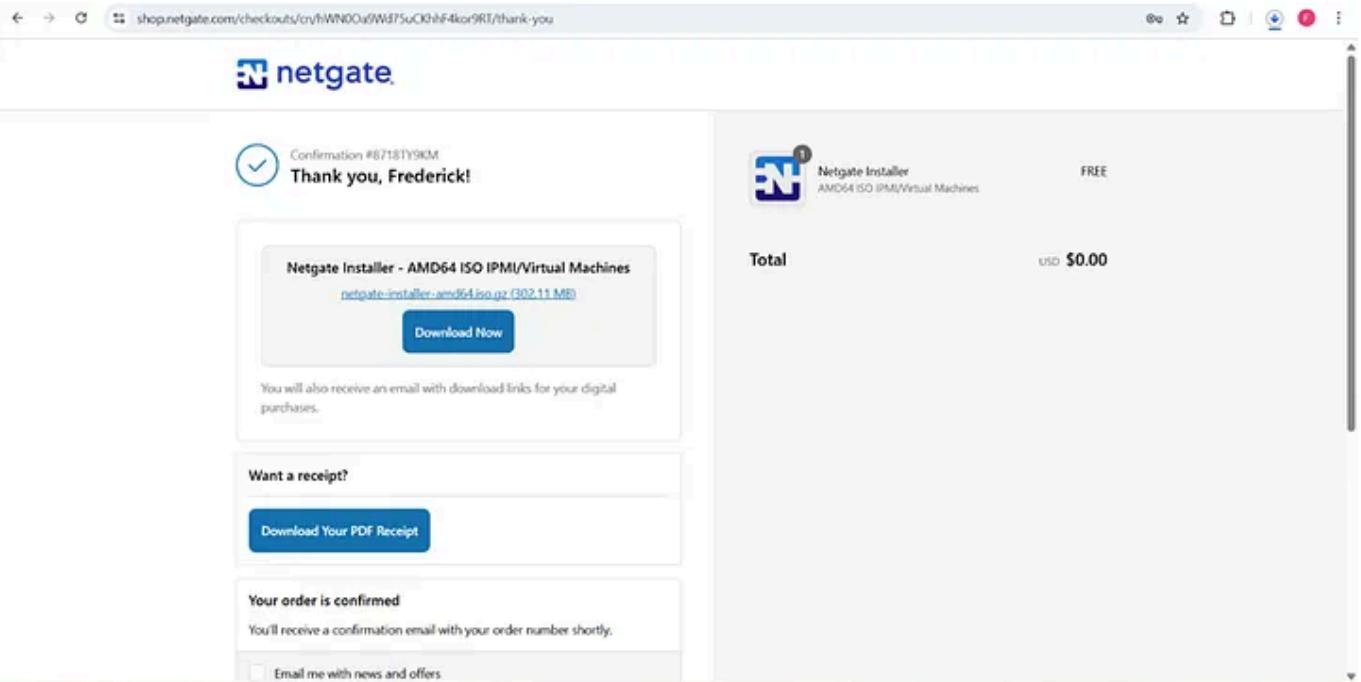


Fig. 3

Now that the download is complete, open VirtualBox and click **New** to create a new virtual machine (Fig. 4).

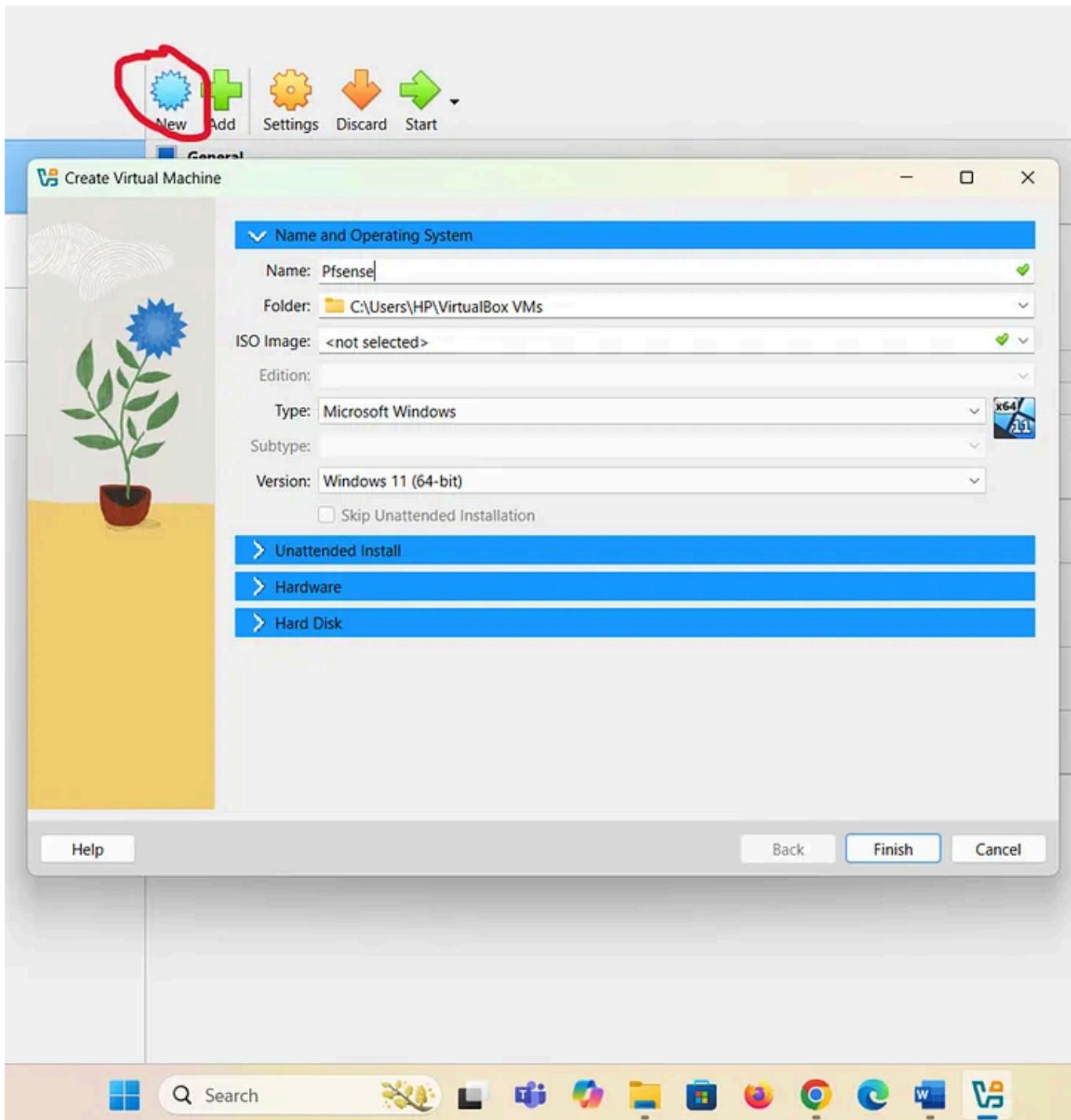


Fig. 4

Name it **pfSense**. Select the ISO image you just downloaded for pfSense — you need to first extract it because it is a compressed file. Without extracting, I will not find the ISO image in the download folder. You can use either WinZip or 7-Zip to extract the file.

Now that the ISO image has been extracted, select it. Set the type to BSD and version to FreeBSD 64-bit (Fig. 5).

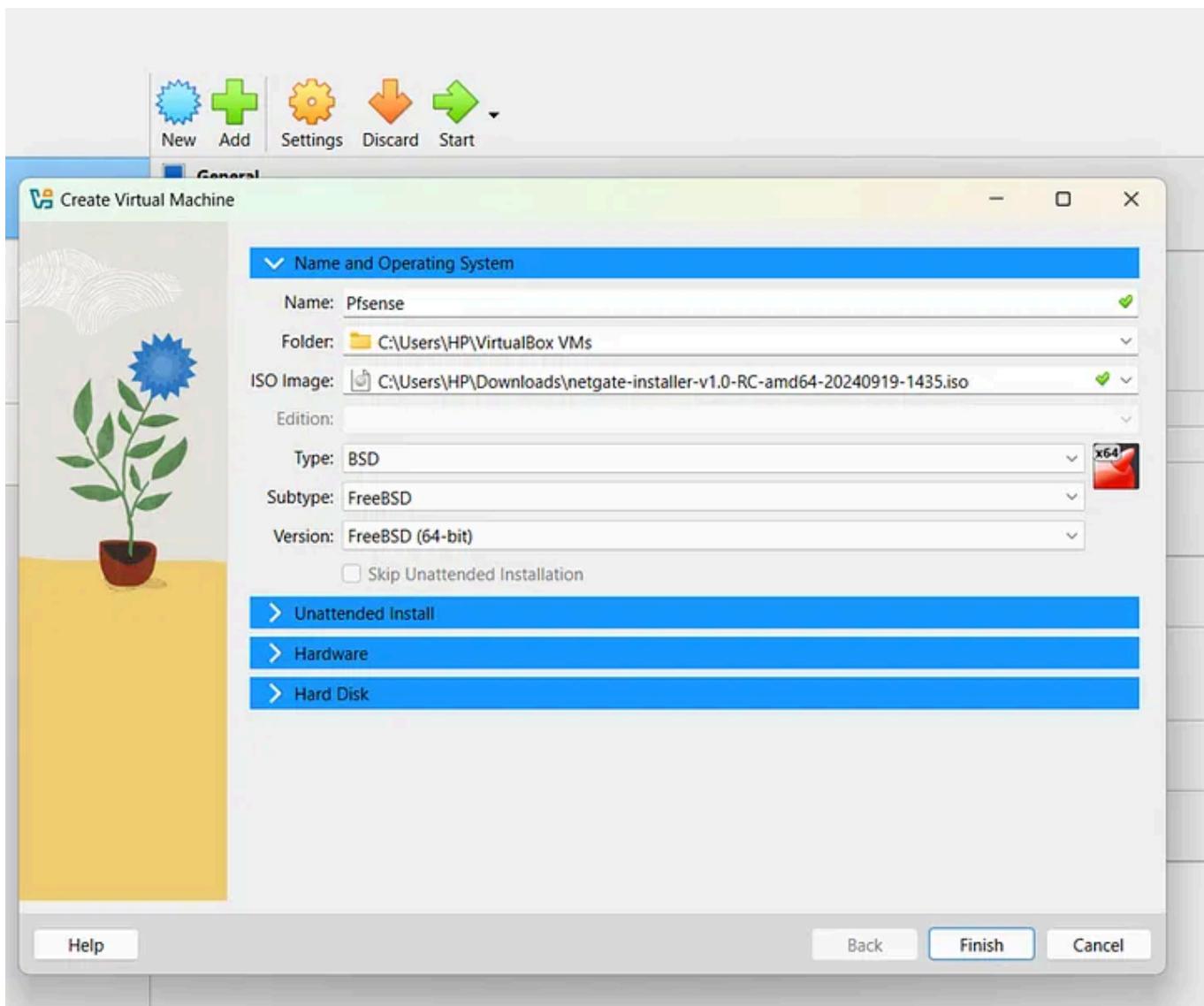


Fig. 5

Allocate at least 1 GB of RAM; 2 GB is recommended for better performance (Fig. 6).

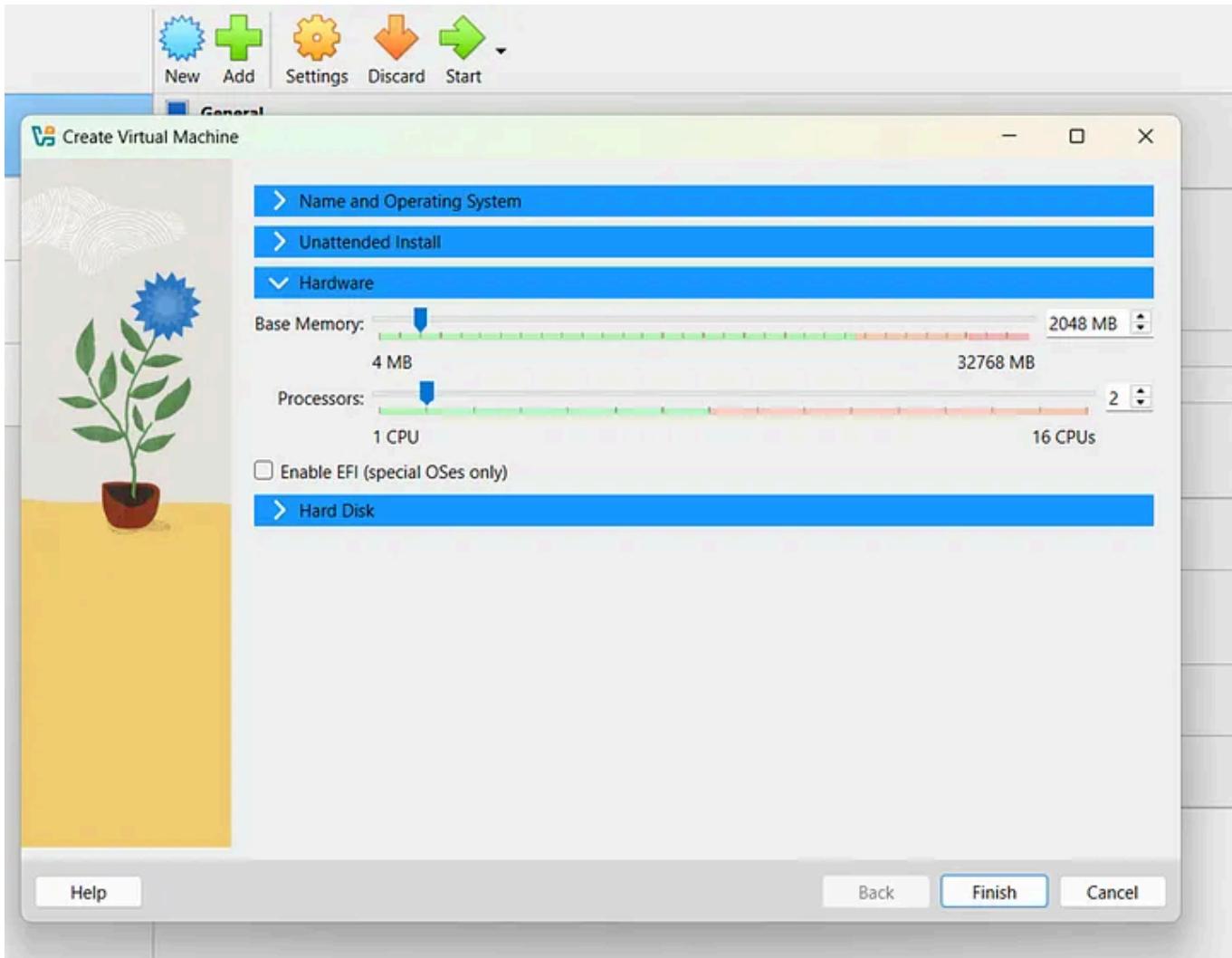


Fig. 6

Next, create a virtual hard disk. 20 GB should be enough for testing. For the hard disk type and variant, choose VDI. Click **Finish**, and your VM is ready (Fig. 7).

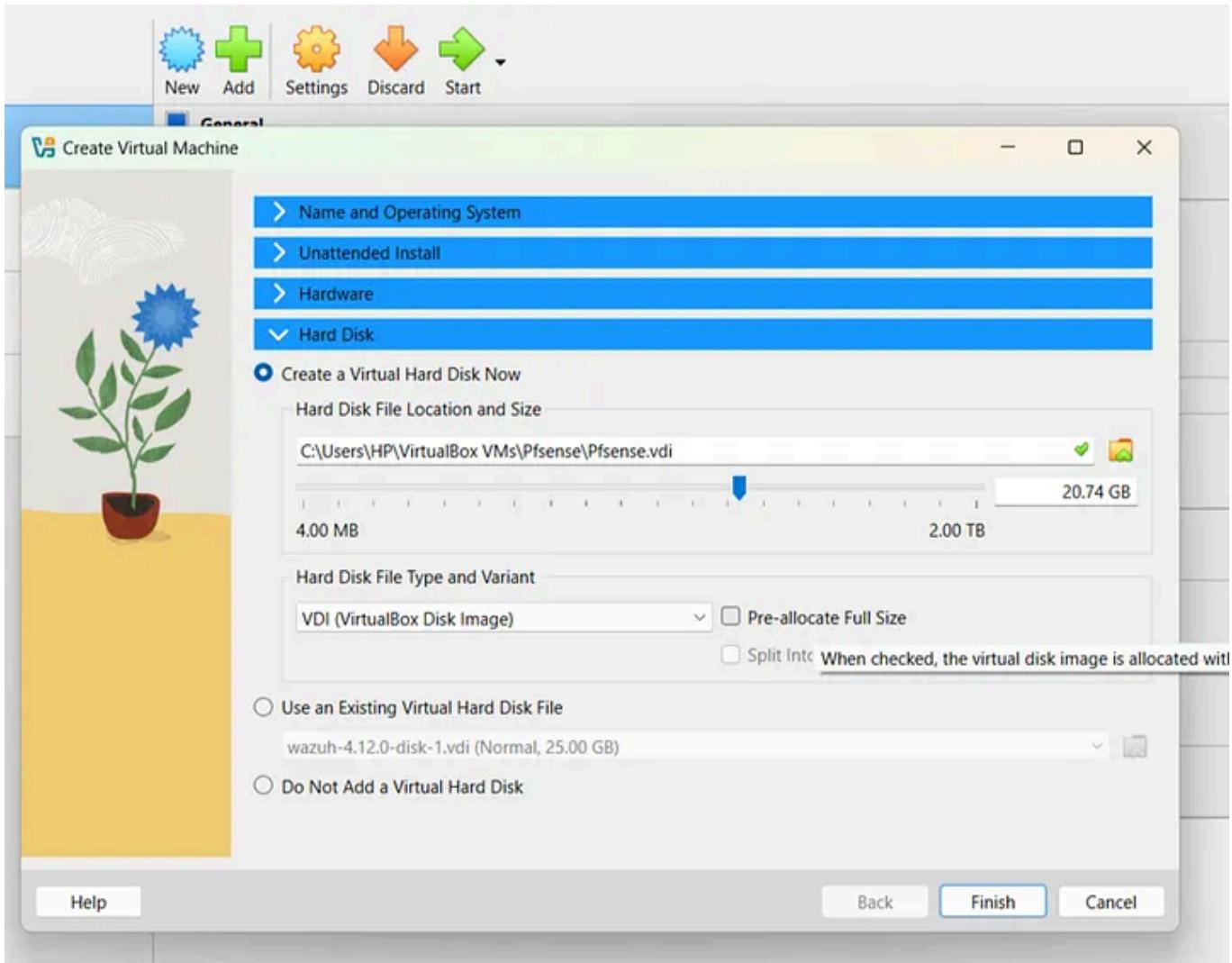


Fig. 7

Before starting the VM, we need to configure networking. Go to **Settings > Network**. We'll need two adapters: **Adapter 1** will be left at NAT for internet access (Fig. 8), and **Adapter 2** will be set to **Internal Network** for LAN simulation (Fig. 9). This setup mimics a real pfSense router with WAN and LAN ports.

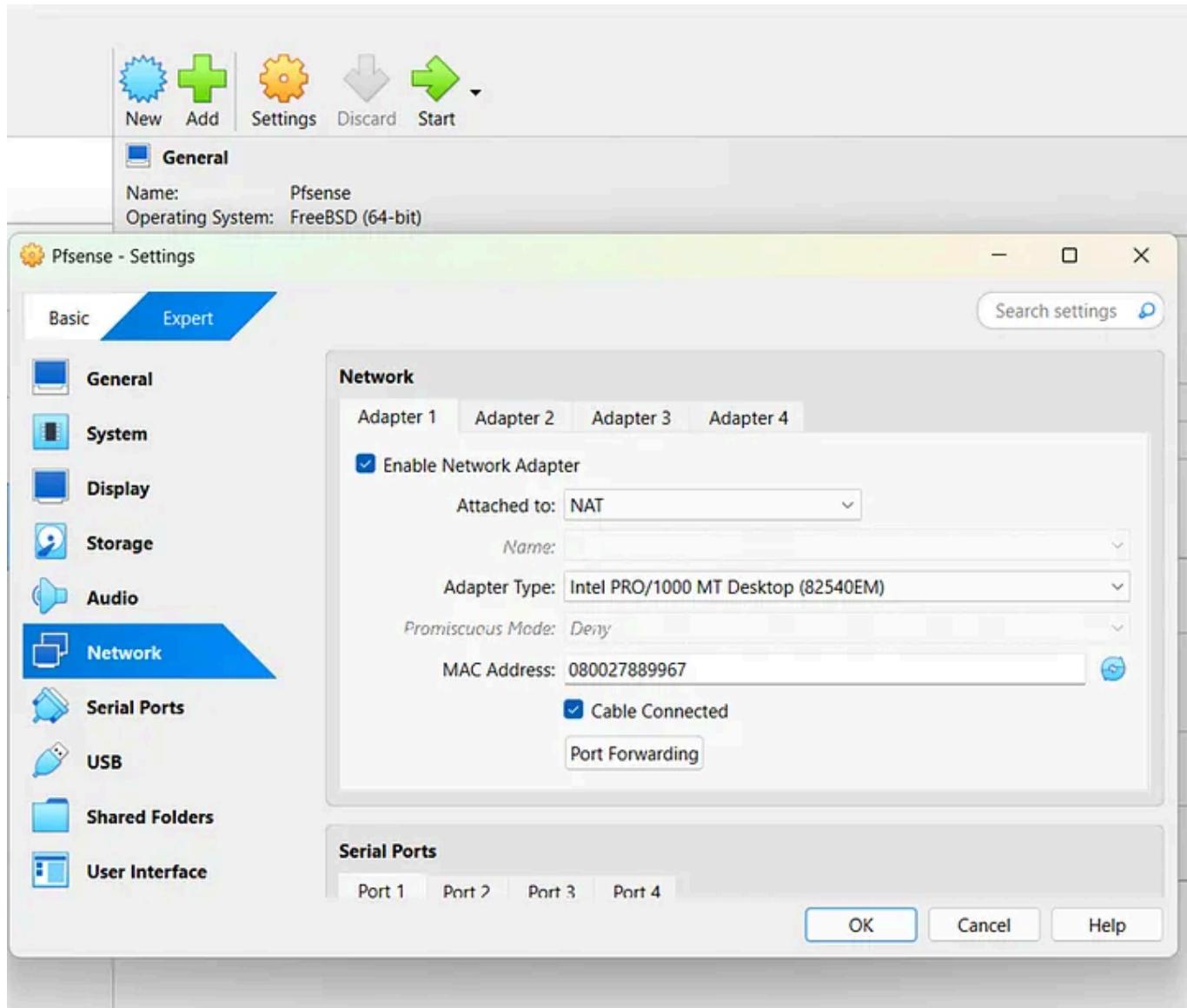


Fig. 8

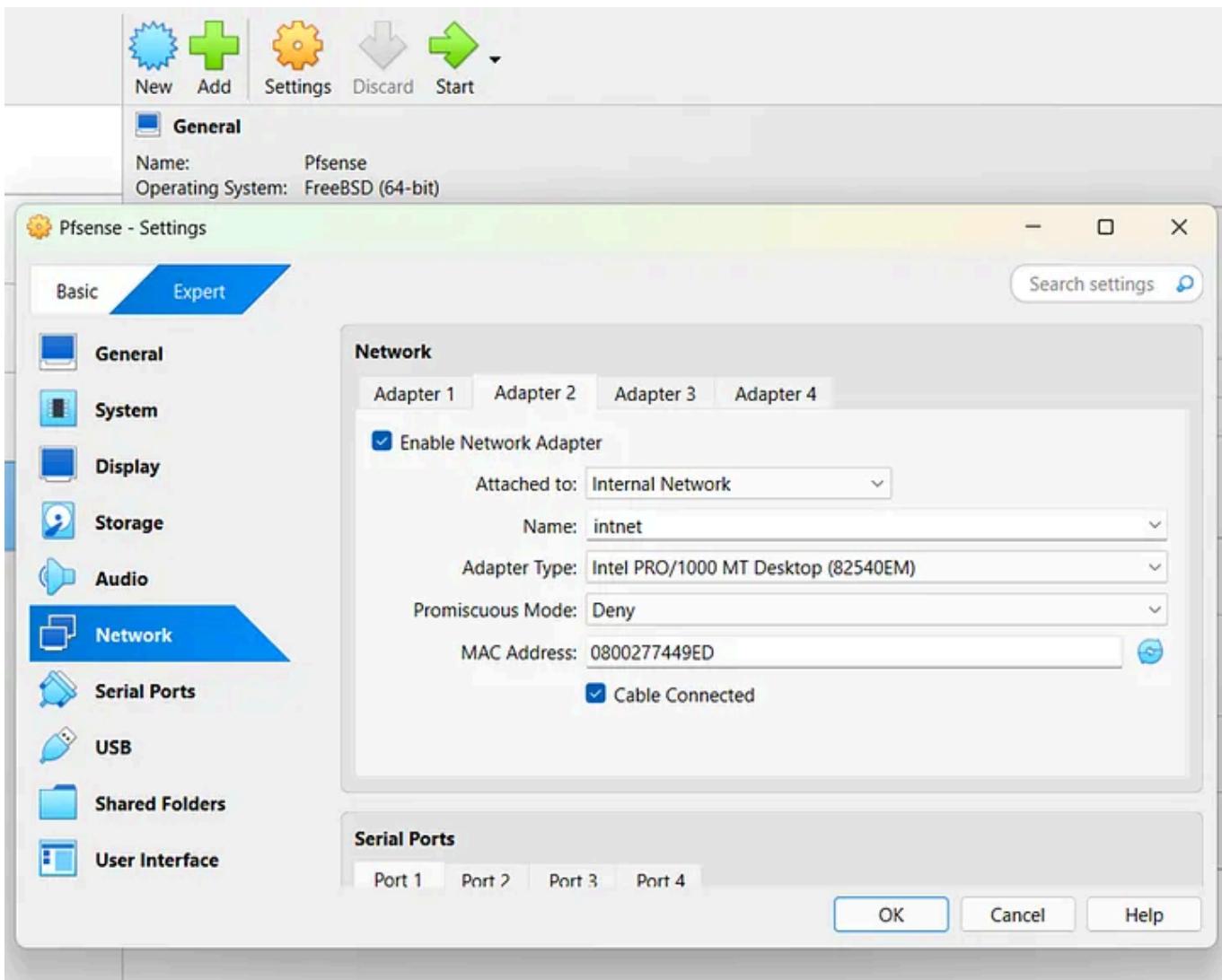


Fig. 9

In VirtualBox, adapters refer to the virtual network interfaces that connect your virtual machines to different types of networks. VirtualBox provides several adapter types, which determine how the VM communicates with the host and external networks. Here's a brief explanation of each:

- **NAT** is for simple internet access and is the default.
- In **Bridged Mode**, the VM acts like a physical machine on the network.
- In **Internal Mode**, there is only VM-to-VM communication.
- In **Host-Only Mode**, the VM is in an isolated network between the host and other virtual machines.

Take note of the MAC address of each adapter as you will require this during the installation process.

Now let us fire up the VM and install pfSense. If you see an error, just reboot your machine and try starting the virtual machine again.

Upon starting up the VM, hold up for the startup process to be completed, then **Accept the Copyright and Trademark Notices** (Fig. 10). Next select **Install pfSense** and follow the installer steps (Fig. 11).

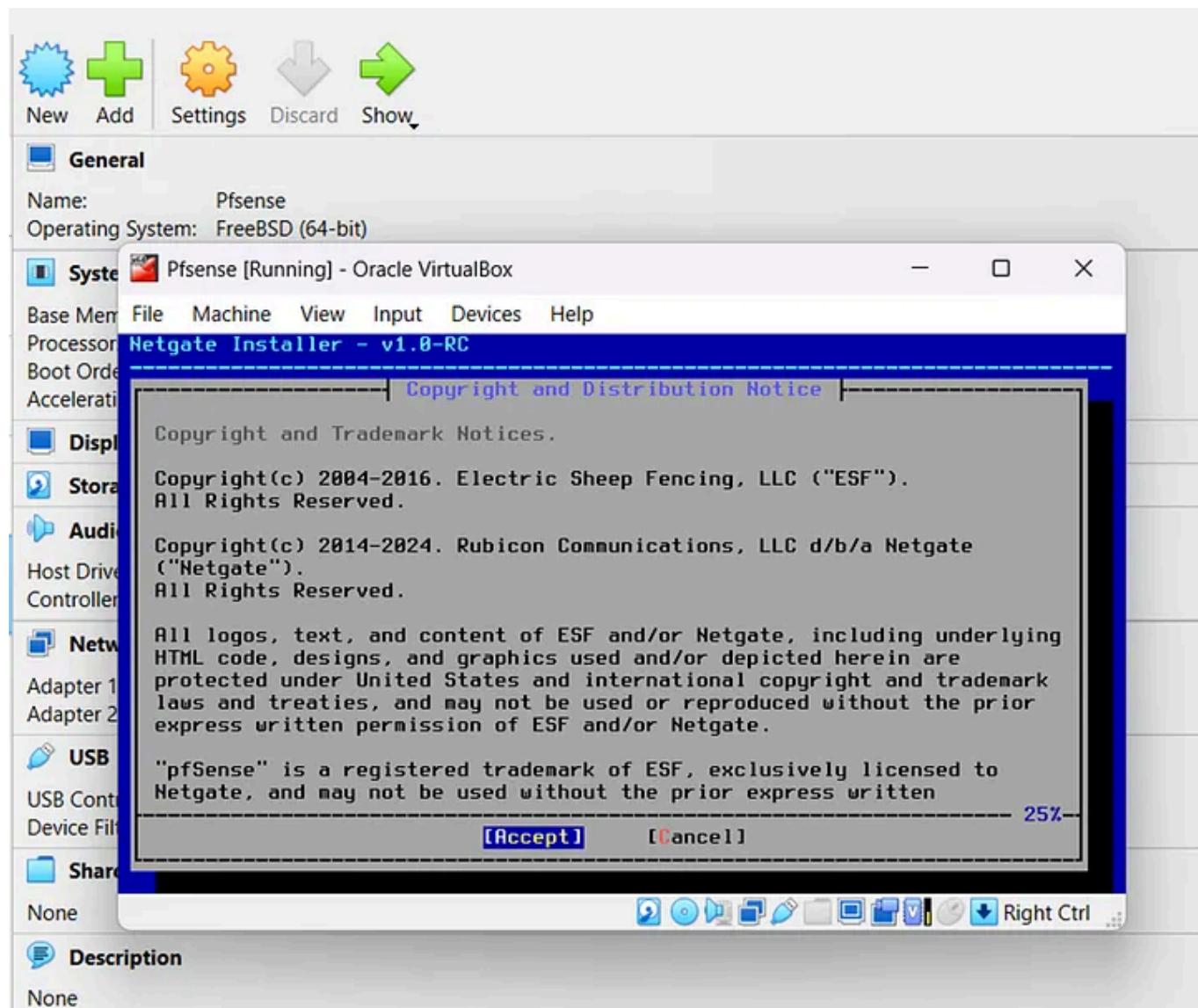


Fig. 10

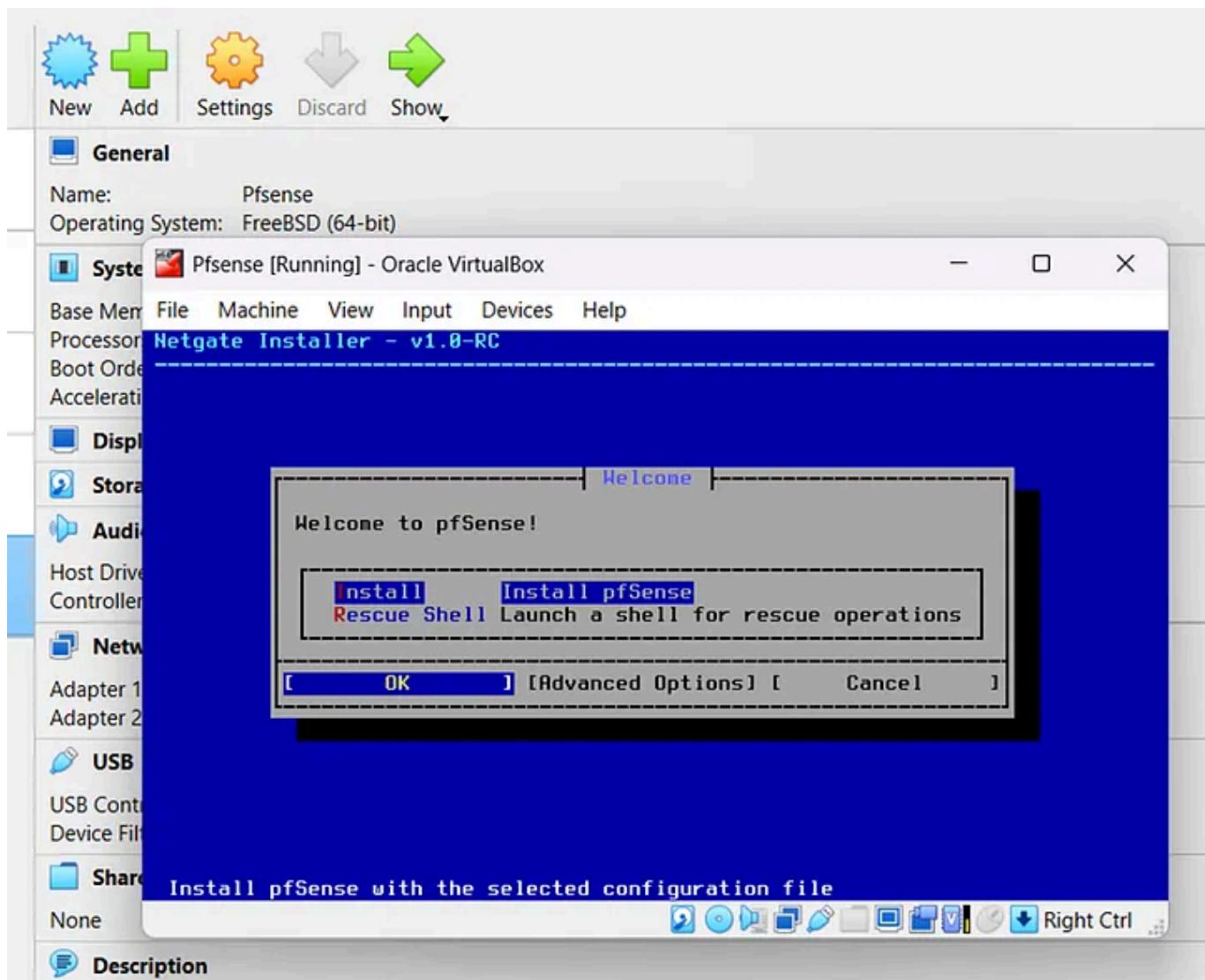


Fig. 11

You then see a prompt about setting up the network, click OK (Fig. 12).

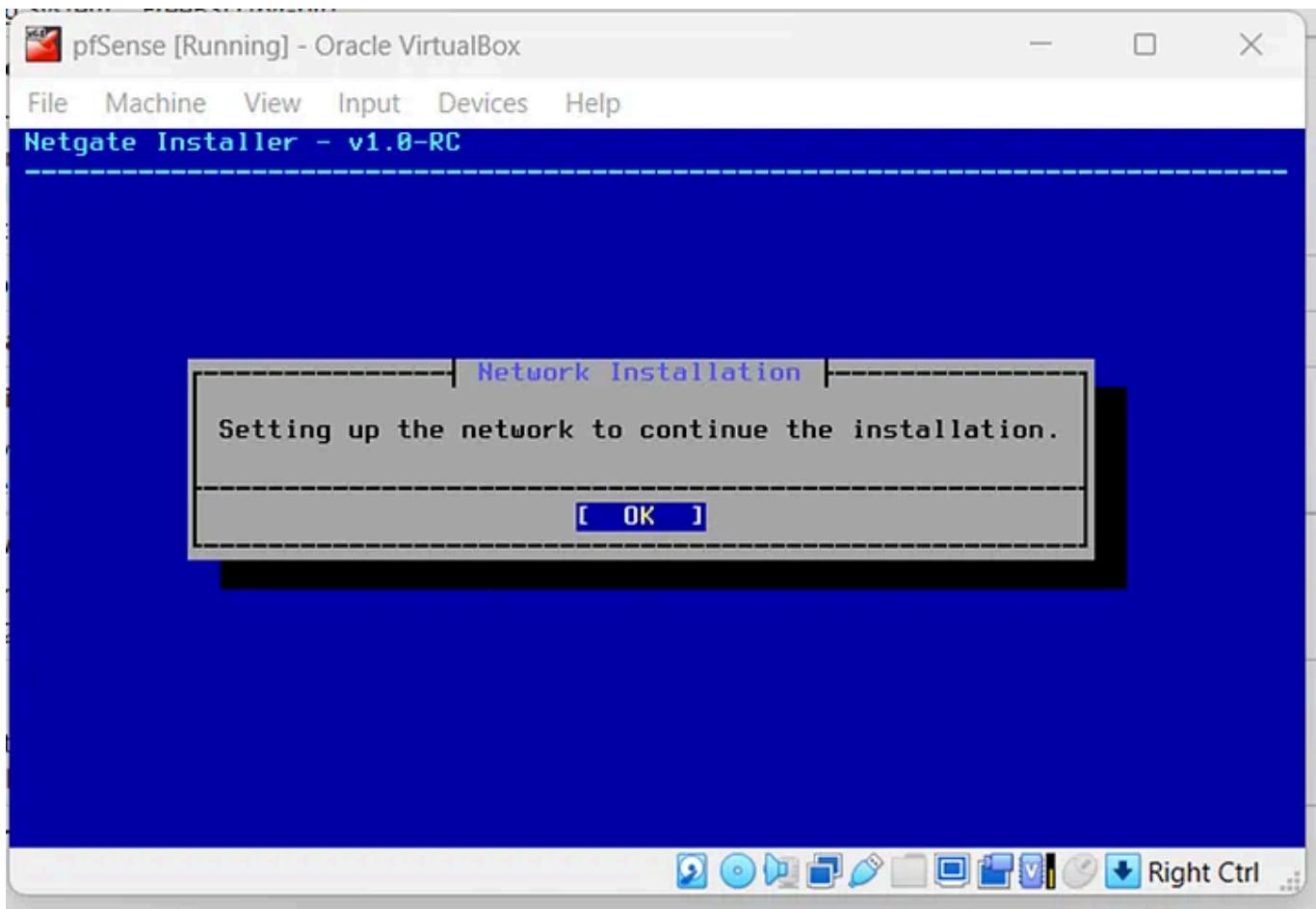


Fig. 12

Next, you are to select the WAN port — you should have taken note of the MAC address. If not, you can check from the **Settings > Network**.

You will be prompted to select the MAC address for the WAN (Fig. 13).

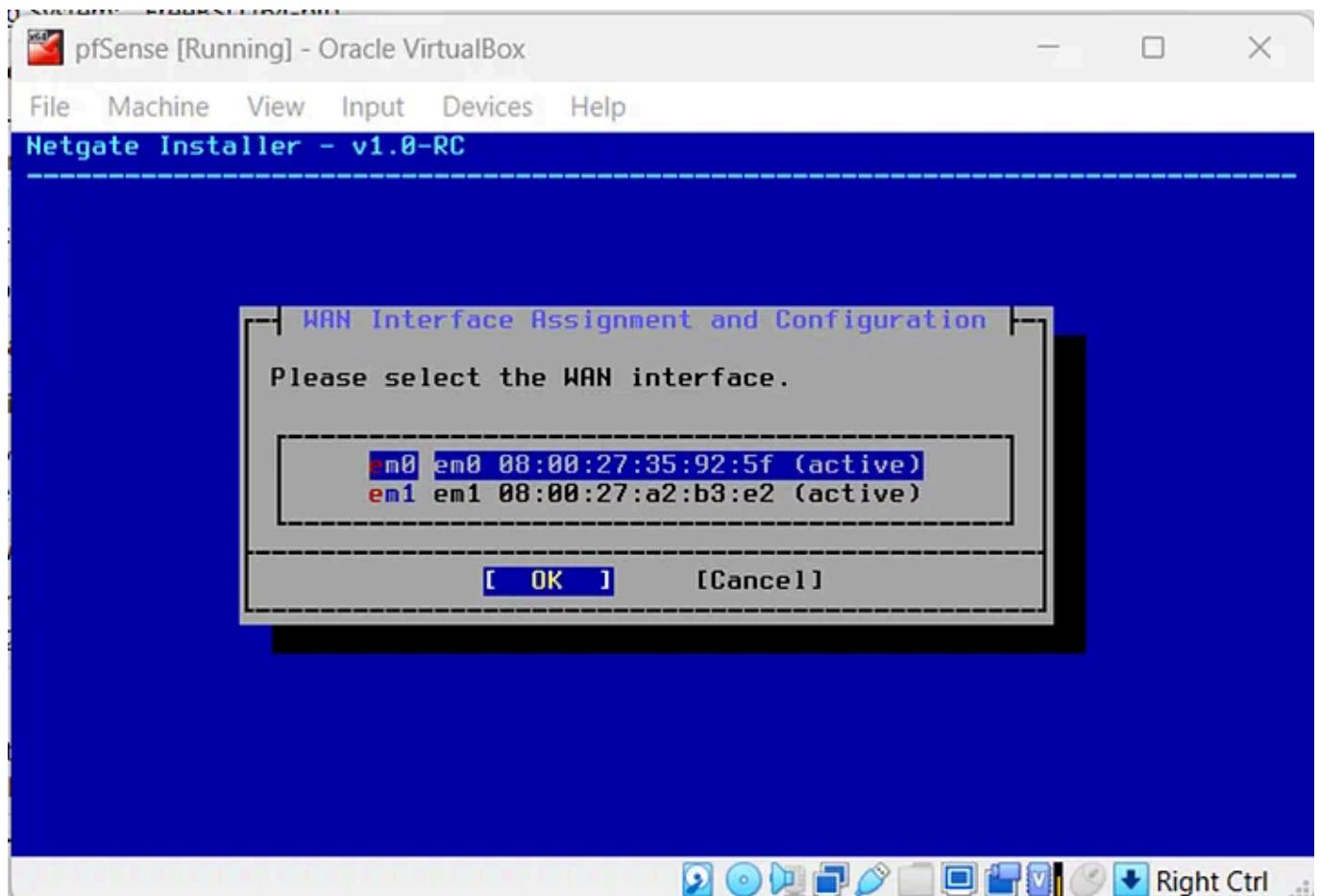


Fig. 13

When asked about the network operation mode for the WAN, click **Continue** (Fig. 14).

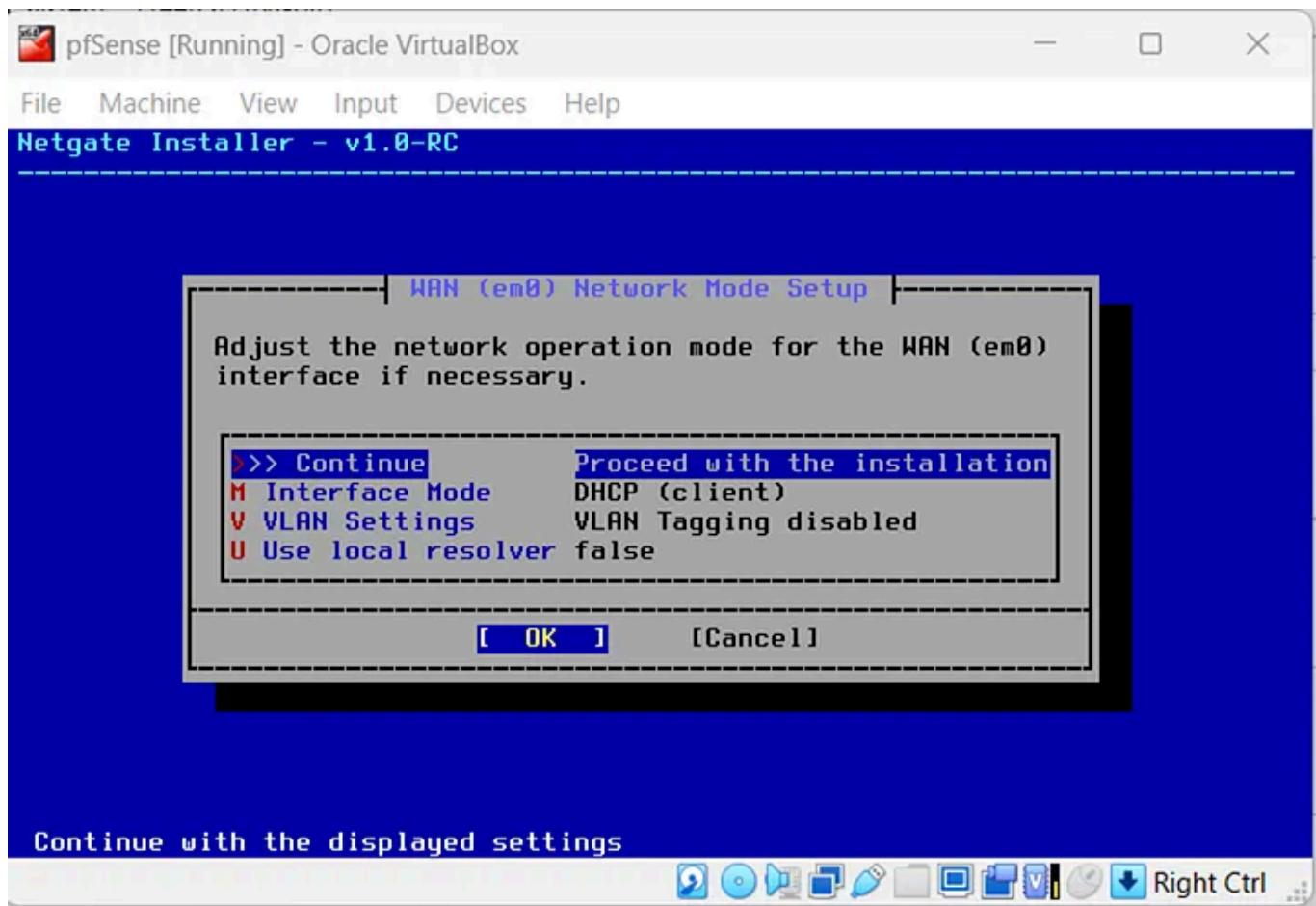


Fig. 14

Next, select the LAN (Fig. 15).

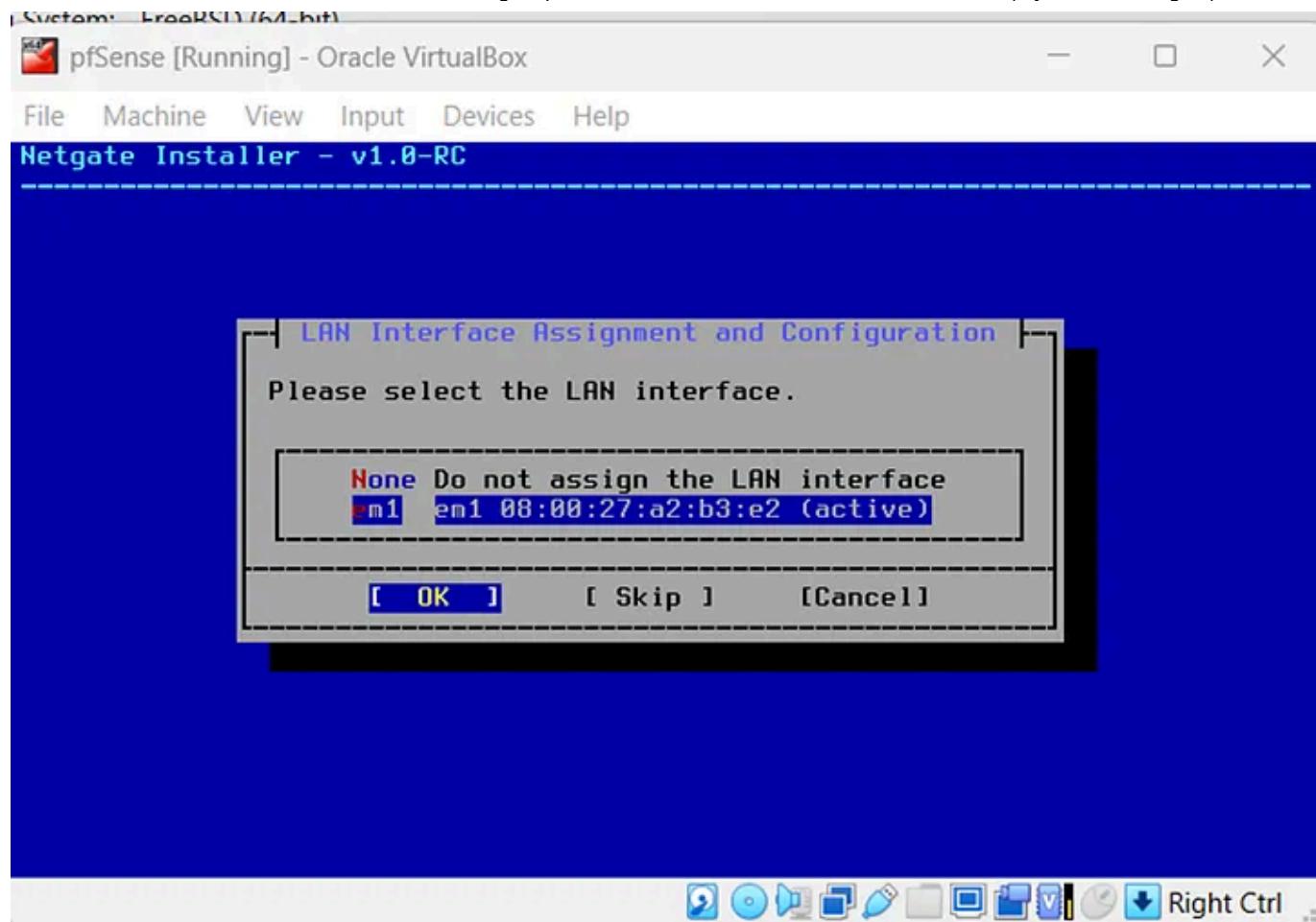


Fig. 15

Proceed with installation (Fig. 16).

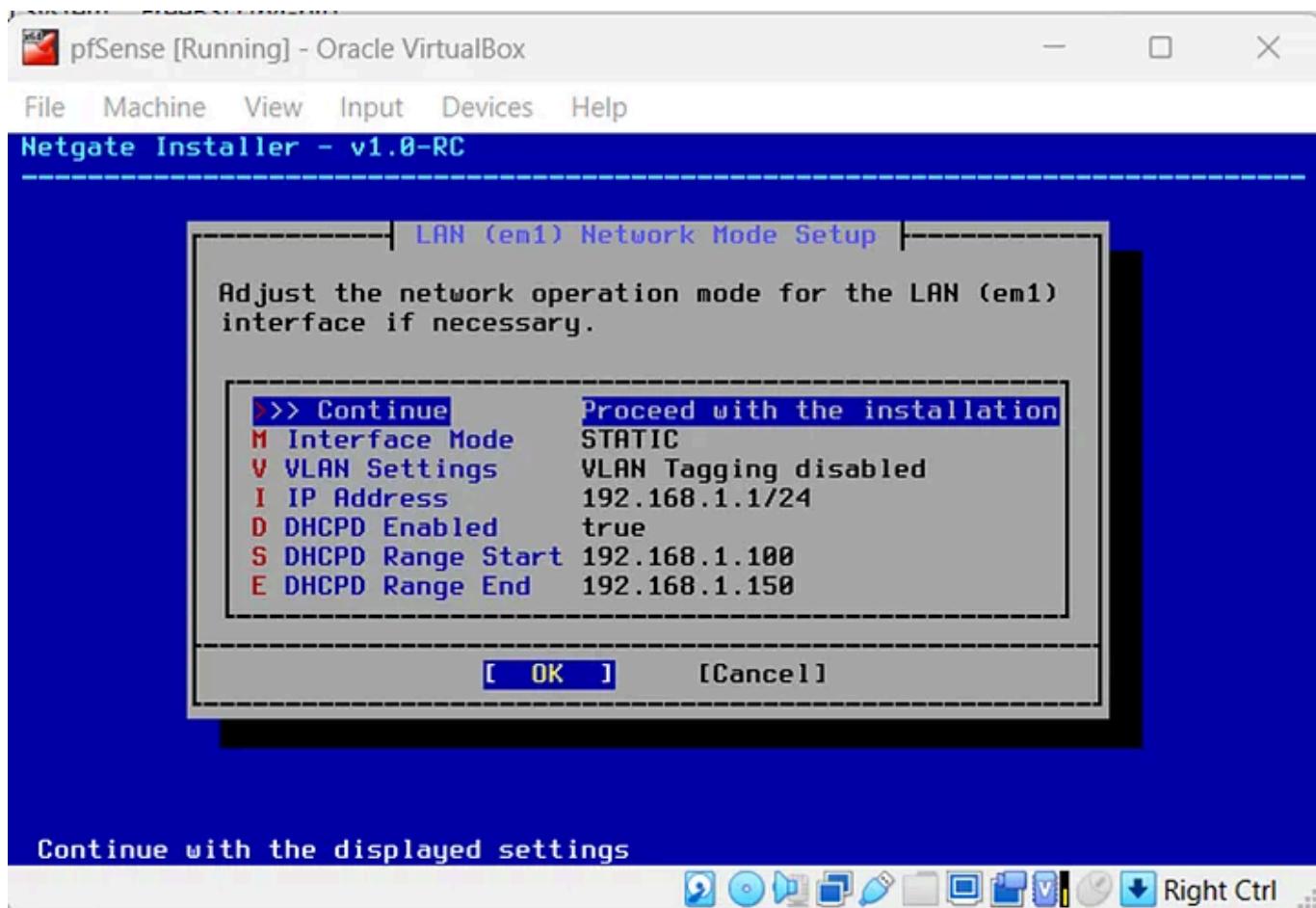


Fig. 16

Then, click **Continue** to confirm the interface assignment.

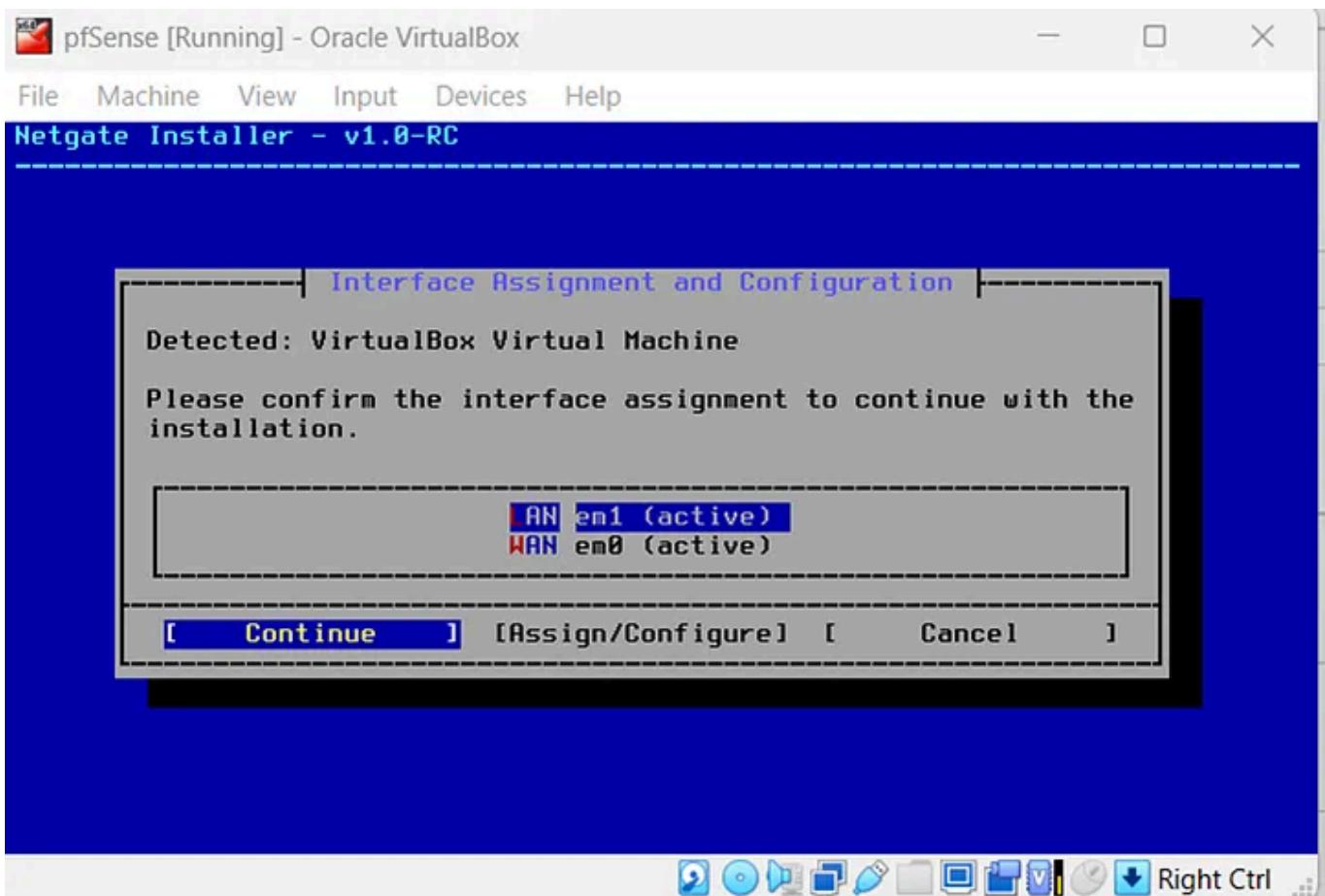


Fig. 17

After that, there is a connectivity check (Fig. 18). You might see a message saying validation failed because the device does not have a valid pfSense Plus subscription. Here, select **Install CE** to use the free Community Edition (Fig. 19), unless you have a pfSense Plus subscription, in which case you can proceed with validation.

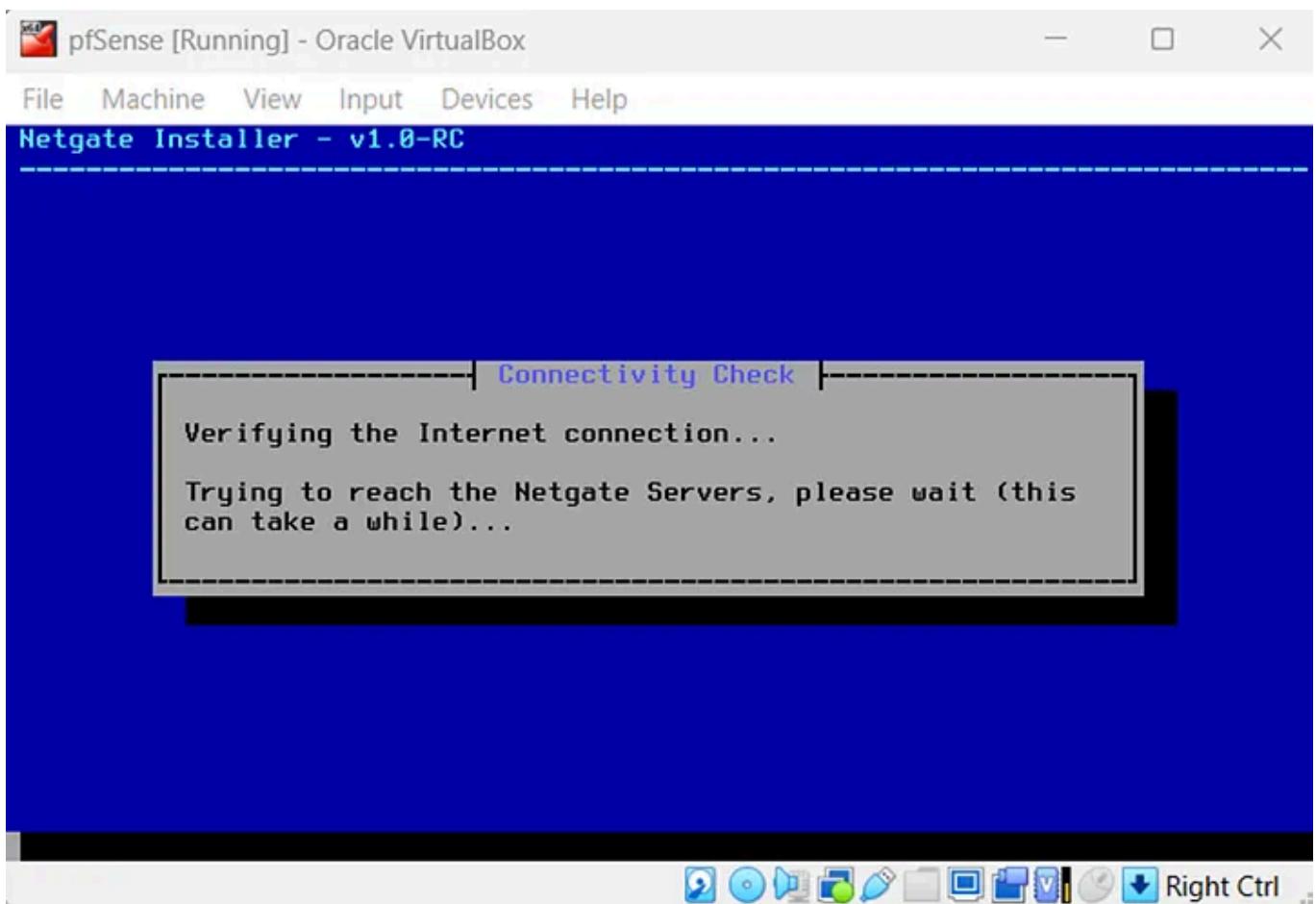


Fig. 18

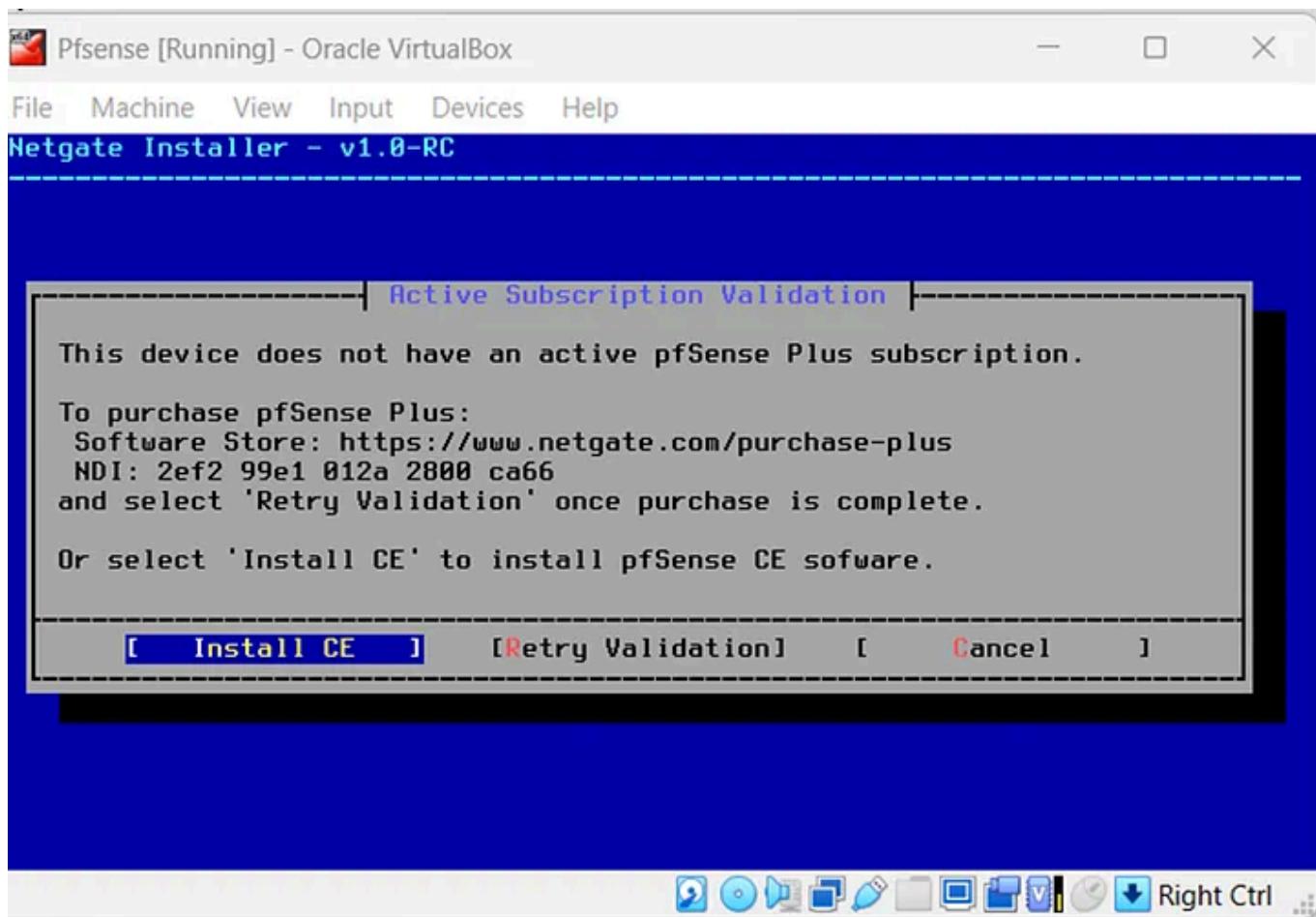


Fig. 19

You will then be prompted to select the file system time and partition scheme. Click **Continue** to proceed with installation (Fig. 20).

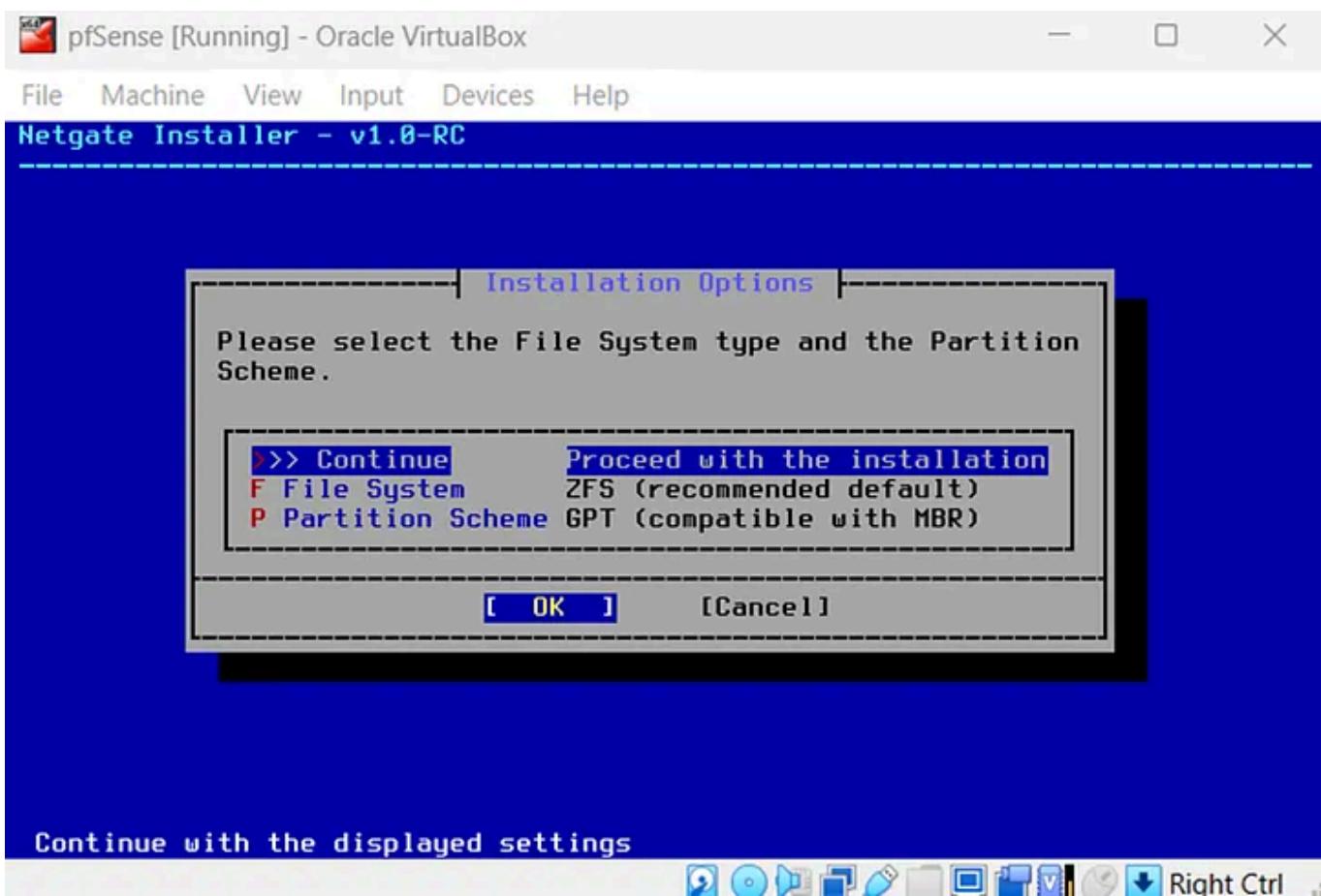


Fig. 20

Next click OK to select the ZFS virtual device configuration type (Fig. 21).

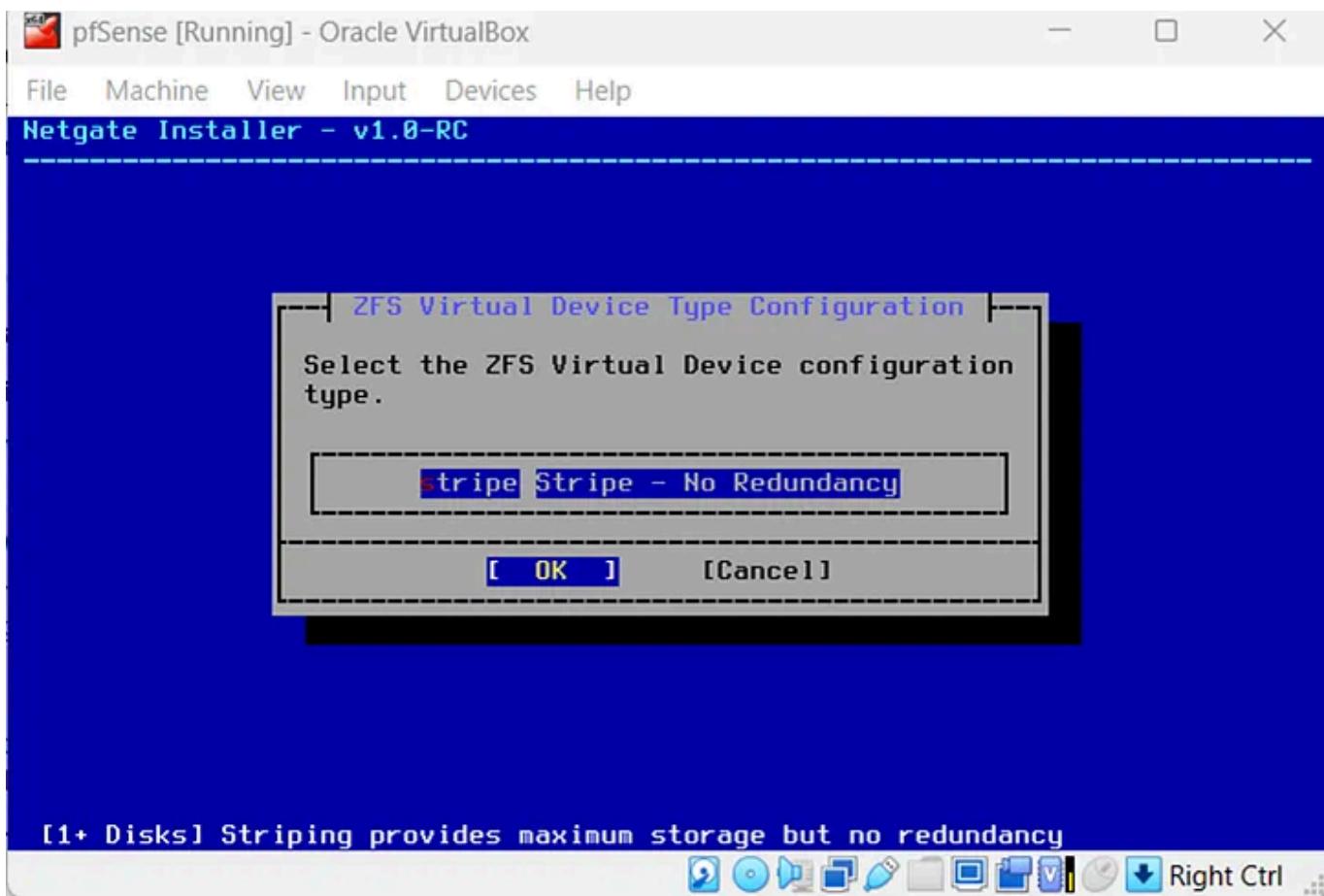


Fig. 21

Then click OK, to select the highlighted disc for software installation (Fig. 22).

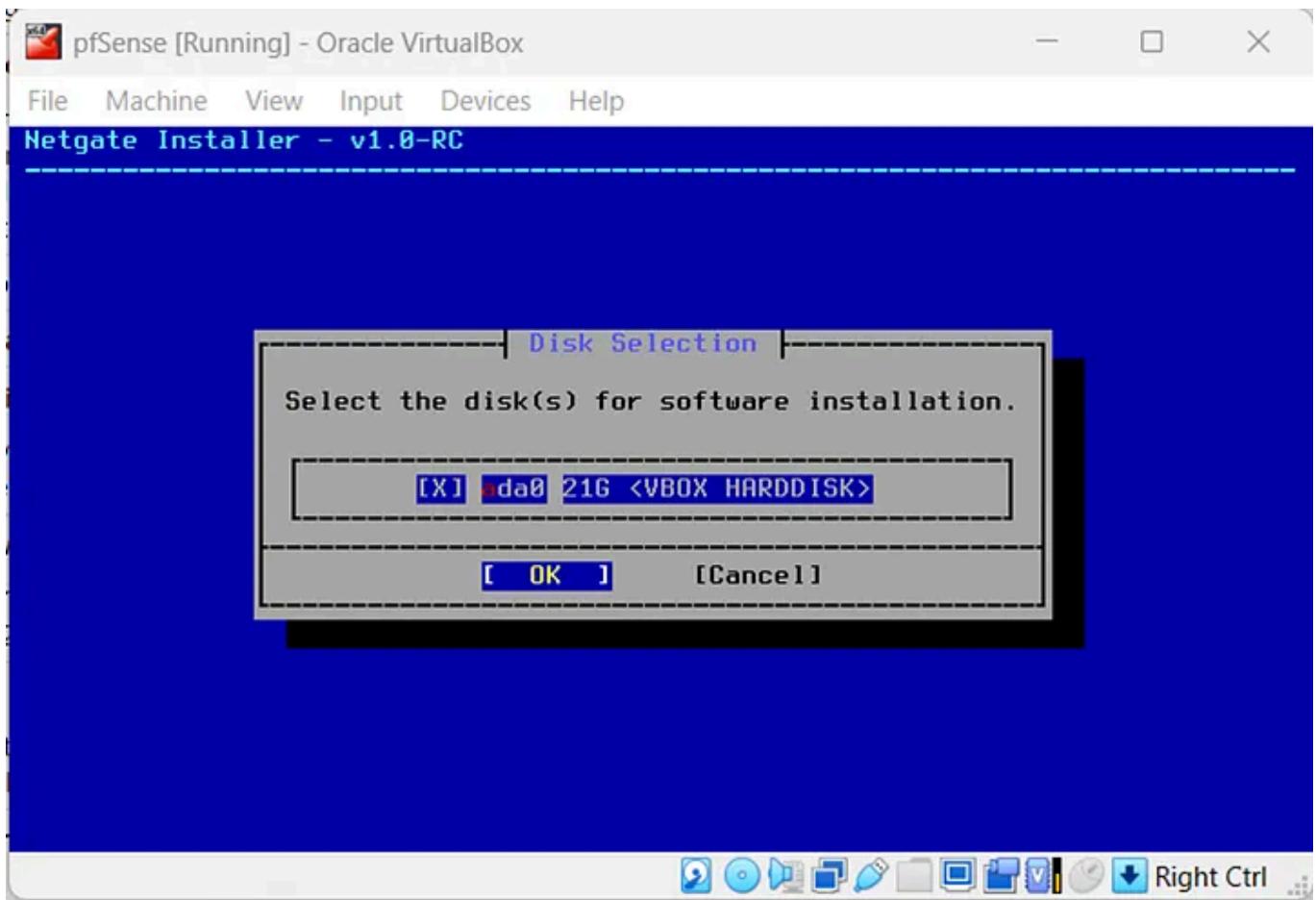


Fig. 22

If you get prompted about destroying the contents of the following disc, click **Yes** (Fig. 23).

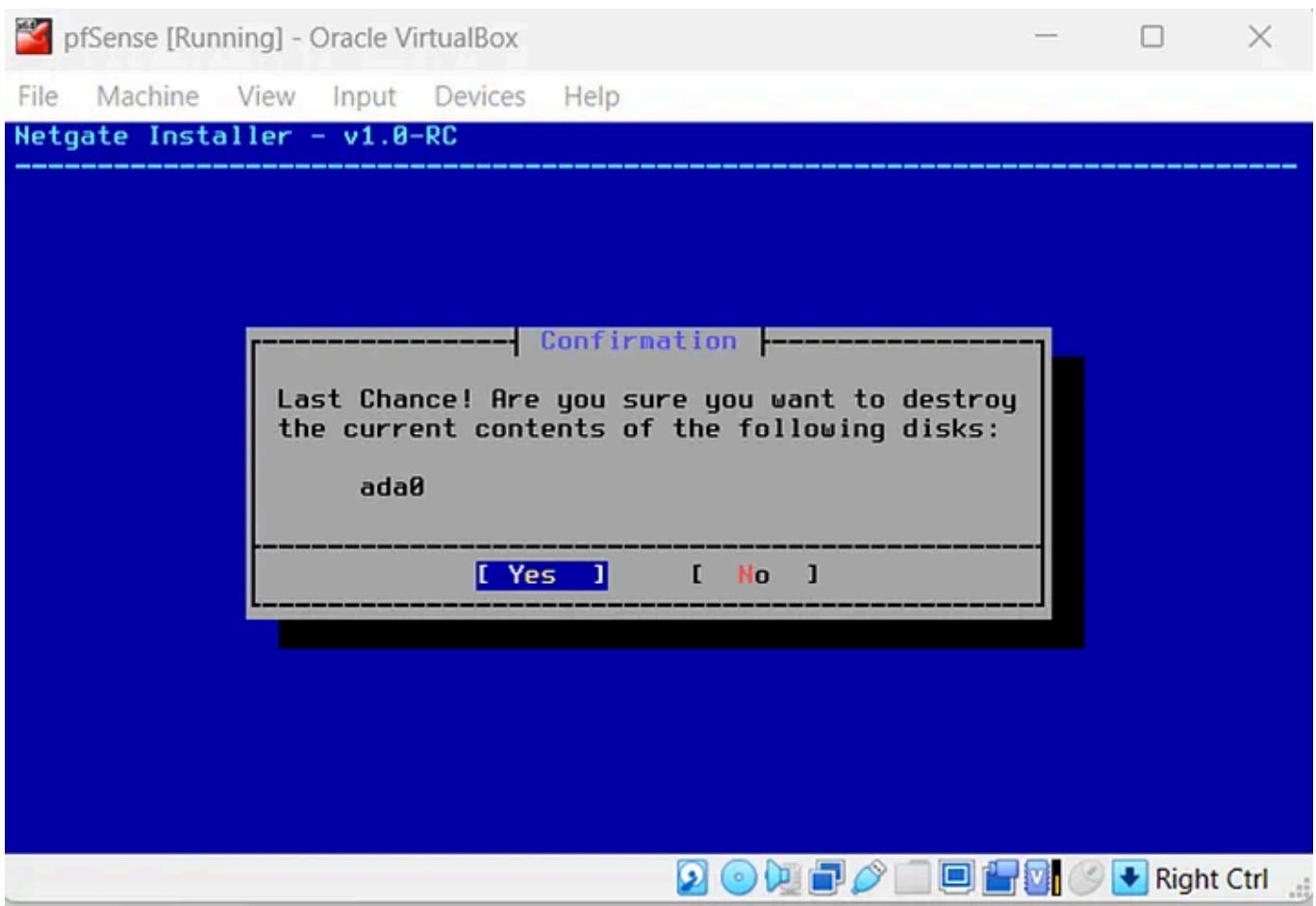


Fig. 23

You will then be asked which version of pfSense to Install.

I will select the **Current Stable Version** at the time of this documentation (Fig. 24).

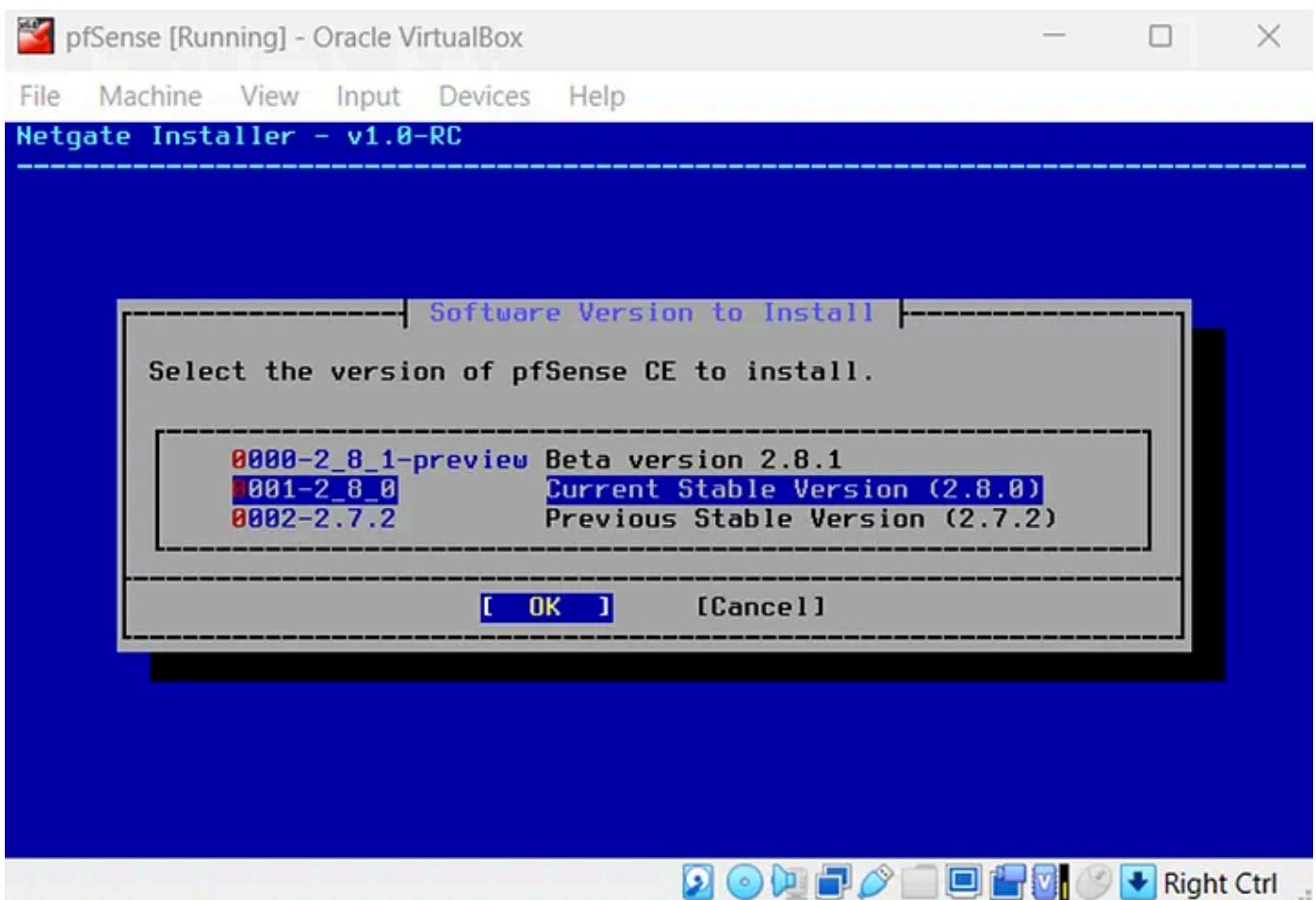


Fig. 24

The installation will then begin (Fig. 25).

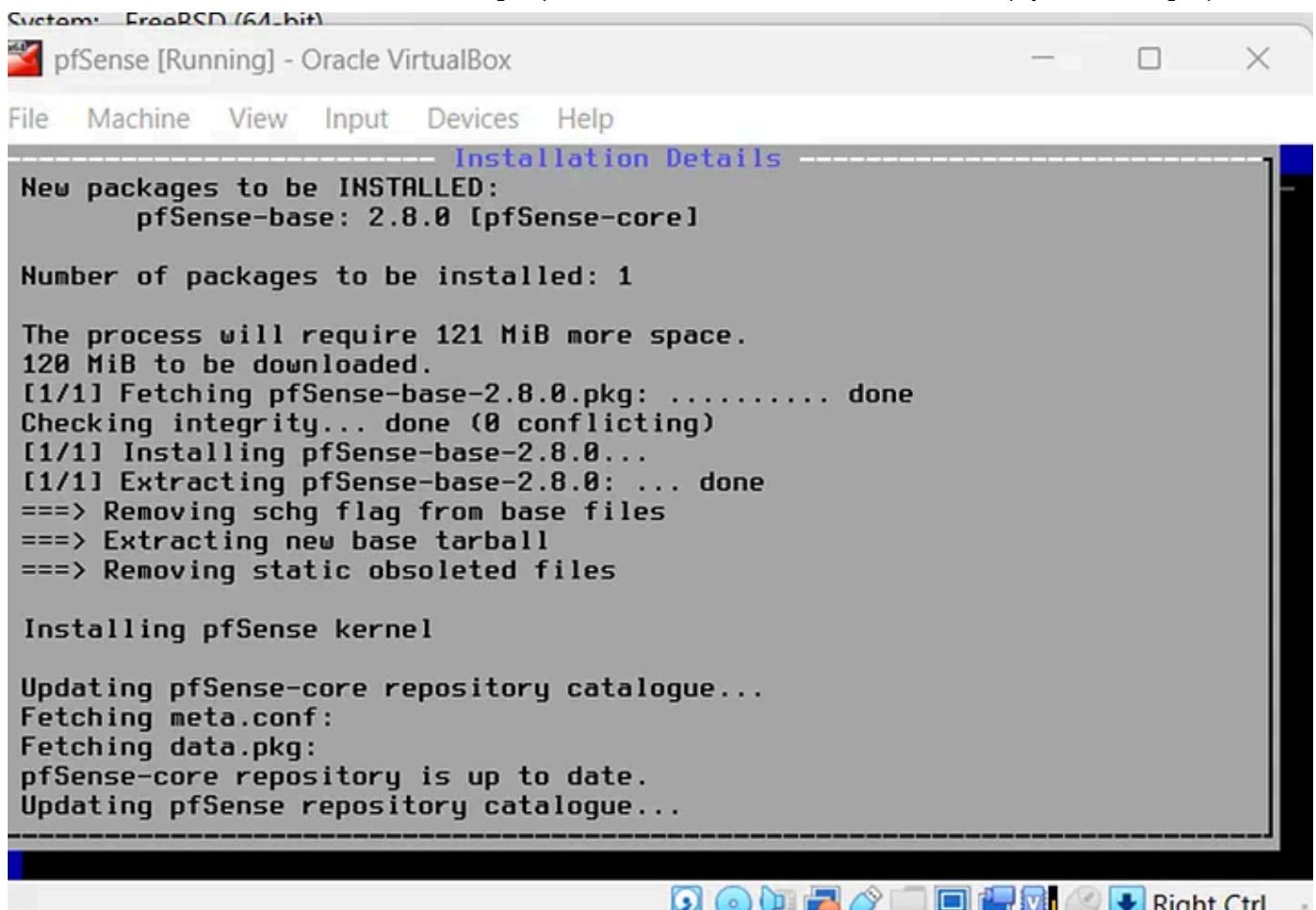


Fig. 25

This will take some time depending on your internet speed.

You will need loads of patience for this.

Once the installation is complete, click **OK** (Fig. 26)

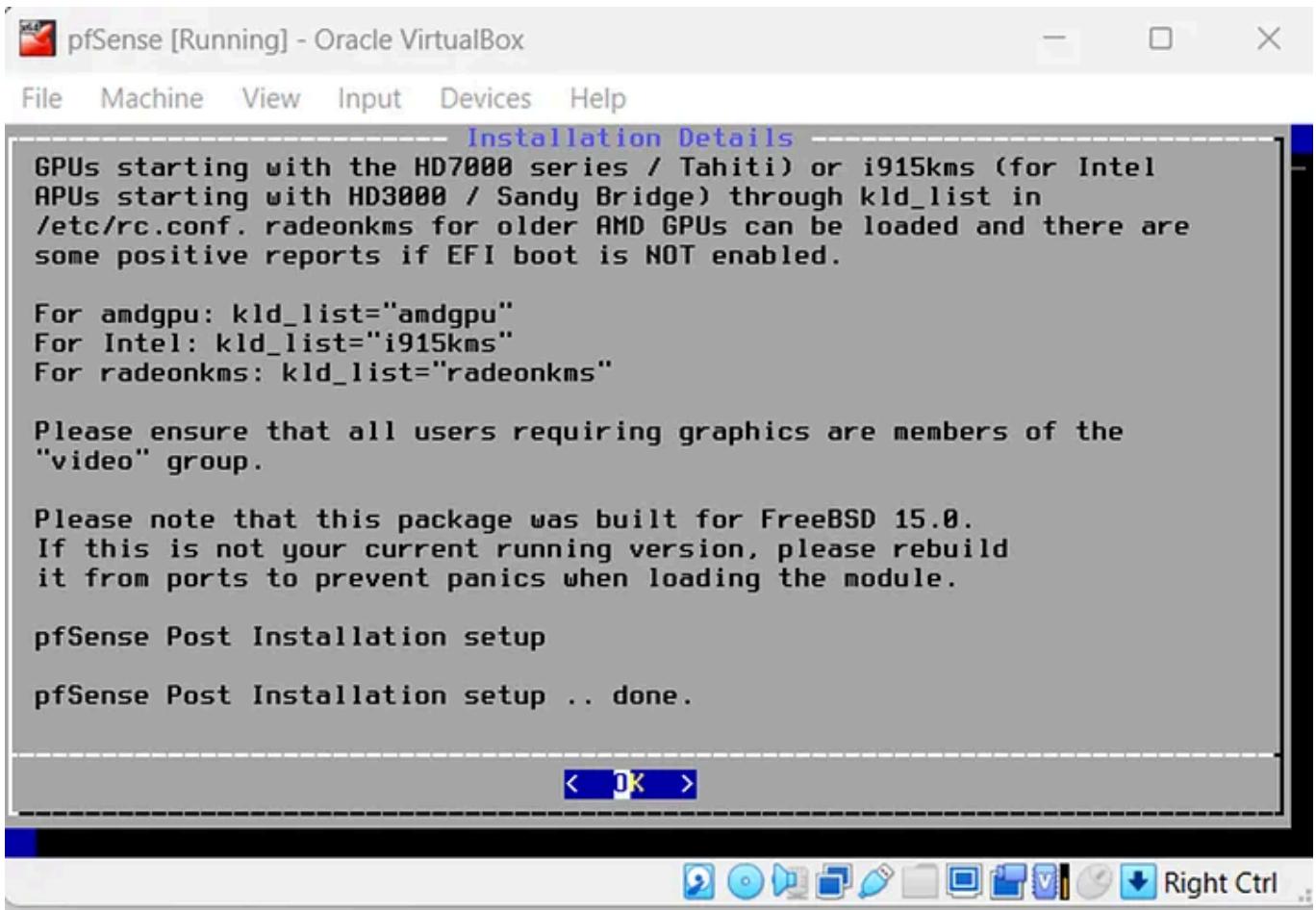


Fig. 26

Then you will be prompted to reboot, click reboot and then power off the pfSense VM (Fig. 27).

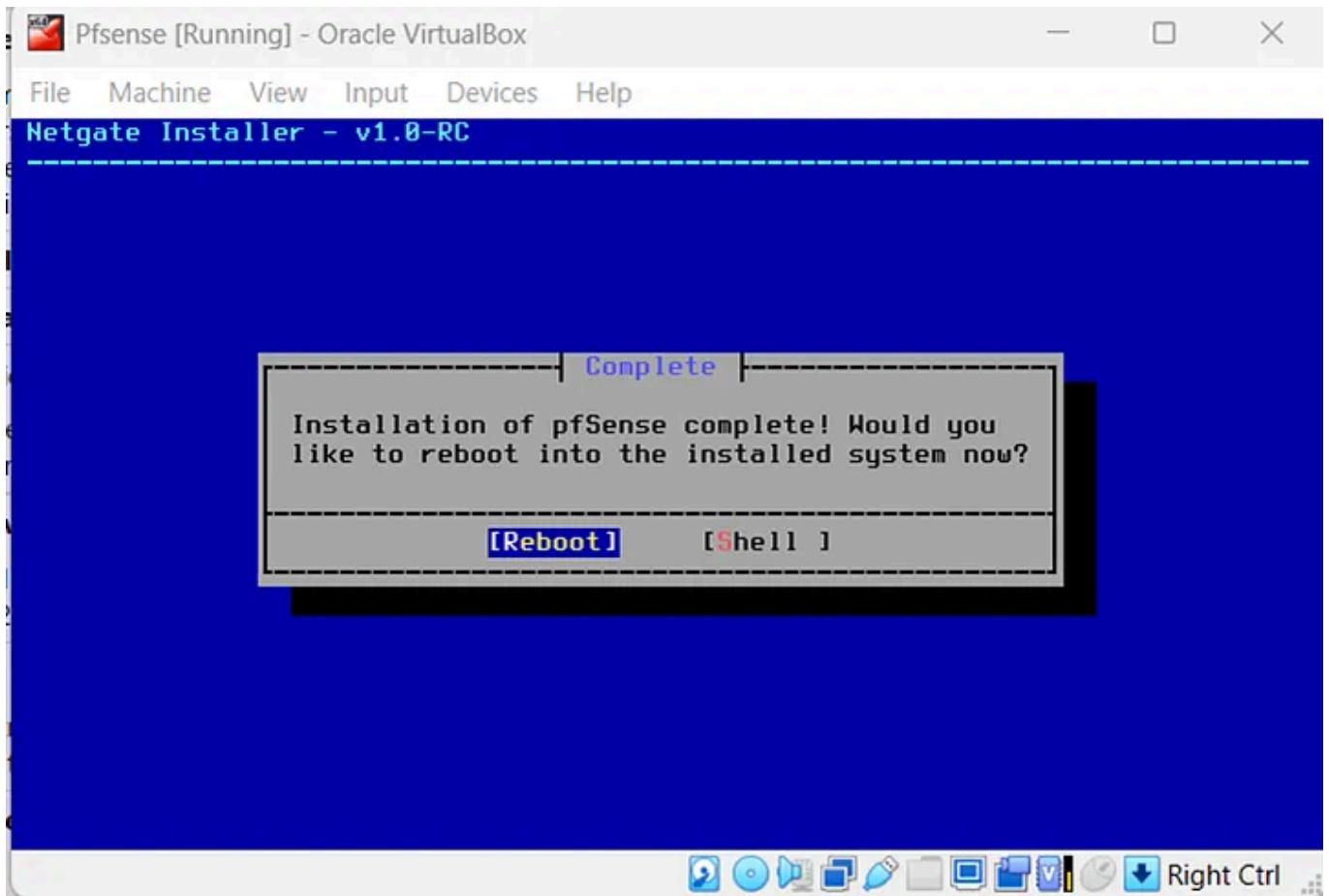


Fig. 27

Power off the VM to remove the ISO from the virtual drive. It is important to remove the ISO after reboot to prevent the VM from booting from the installer again. Go to **Settings > Storage**, select the **netgate-installer** under **Controller: IDE** (Fig. 28).

Under **Attributes**, click the disc icon next to **IDE Secondary Device** and choose **Remove Disk from Virtual Drive**. Click **OK** to save the settings (Fig. 28).

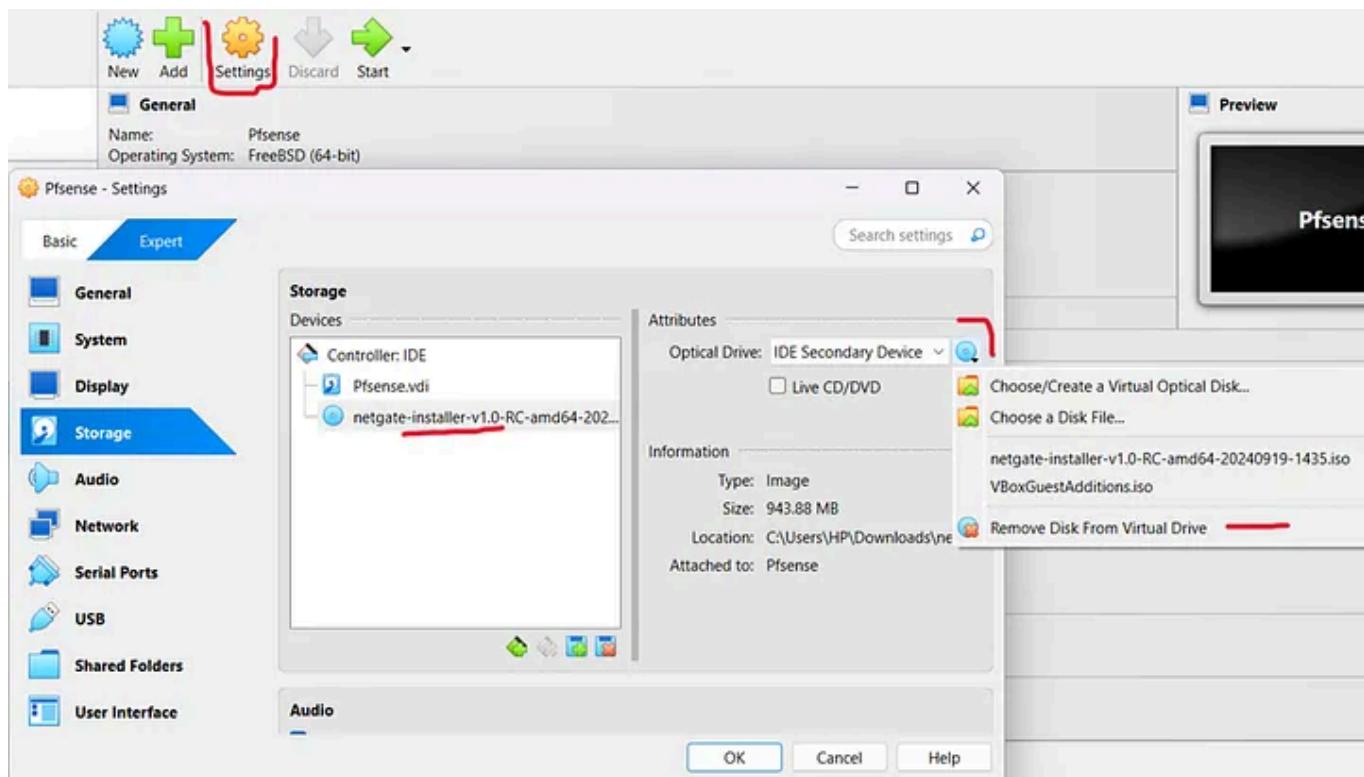


Fig. 28

Now restart the pfSense VM. pfSense will start in console mode, and you'll see the WAN and LAN interfaces. It will assign IPs to both the WAN and LAN (Fig. 29).

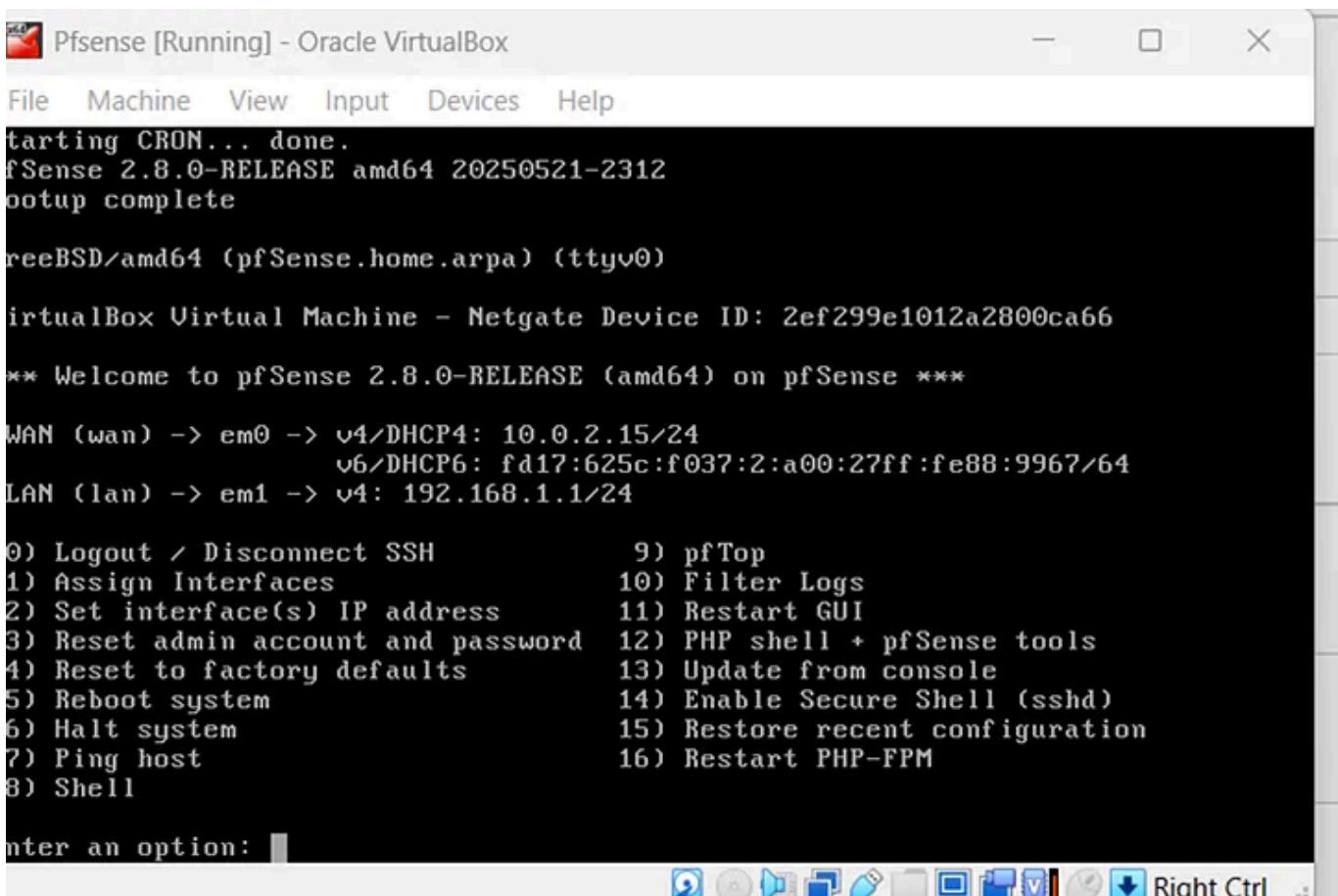


Fig. 29

The world's first website, info.cern.ch, created by Tim Berners-Lee in 1991, is still online. It's a simple page explaining the World Wide Web

Step 2: ACCESSING THE PFSENSE WEB INTERFACE

I can access the pfSense web GUI from another VM by connecting to its LAN IP (default: 192.168.1.1), which serves as the **default gateway**. pfSense acts as both a firewall and router, connecting the LAN (internal network) to the WAN (internet) and directing traffic while enforcing firewall rules and NAT.

The default gateway is the IP pfSense uses to reach external networks. It can be:

- **Static:** manually set for the WAN interface,
- **Dynamic via DHCP:** provided by the upstream router or ISP, or
- **Assigned by PPPoE** or similar connections.

pfSense forwards all traffic for unknown networks to this gateway. Devices within the LAN use pfSense's LAN IP as their gateway, sending internet-bound traffic through pfSense to the WAN gateway.

I will use the Ubuntu virtual machine to access the pfSense GUI.

First, I need to set the adapter to internal for it to pick an IP address from pfSense.

Under settings for the Ubuntu VM, I will proceed to **Network**, then set the adapter to **Internal Network** (Fig. 30).

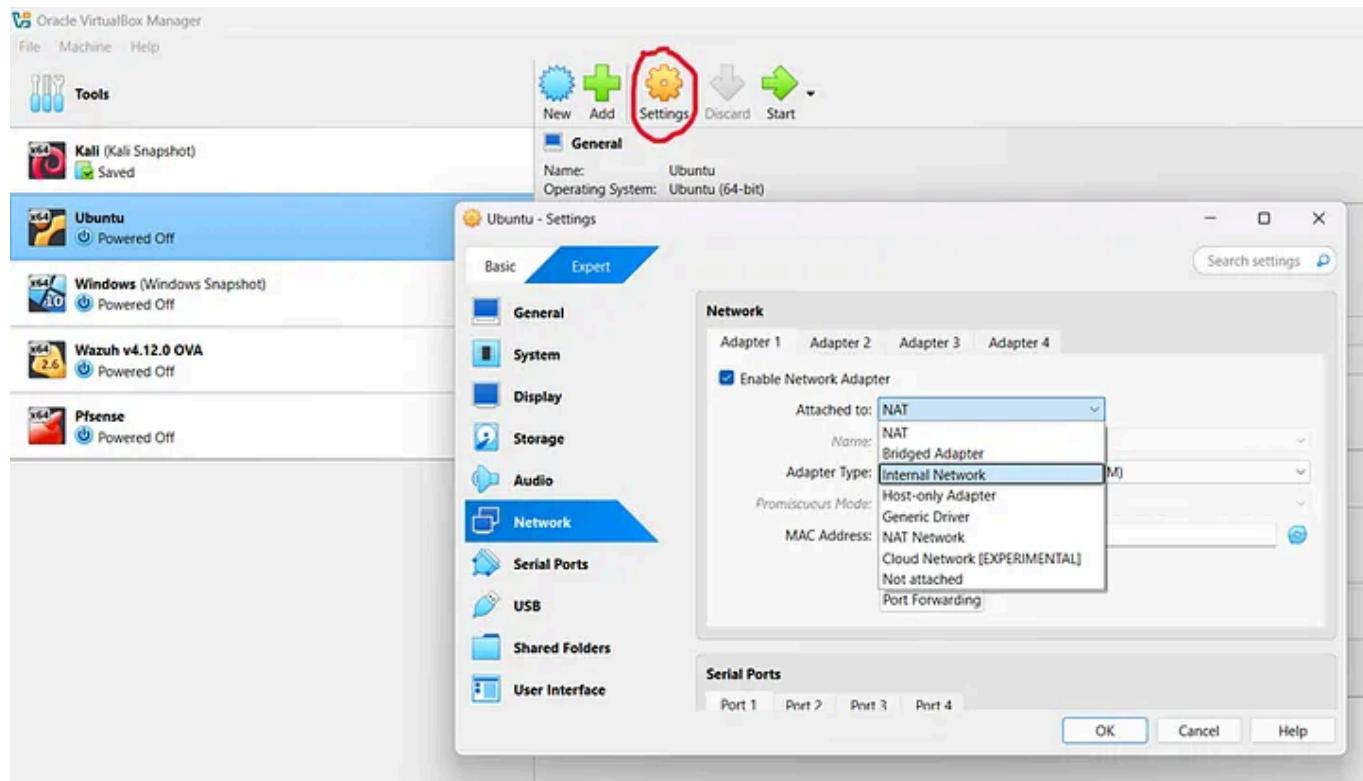


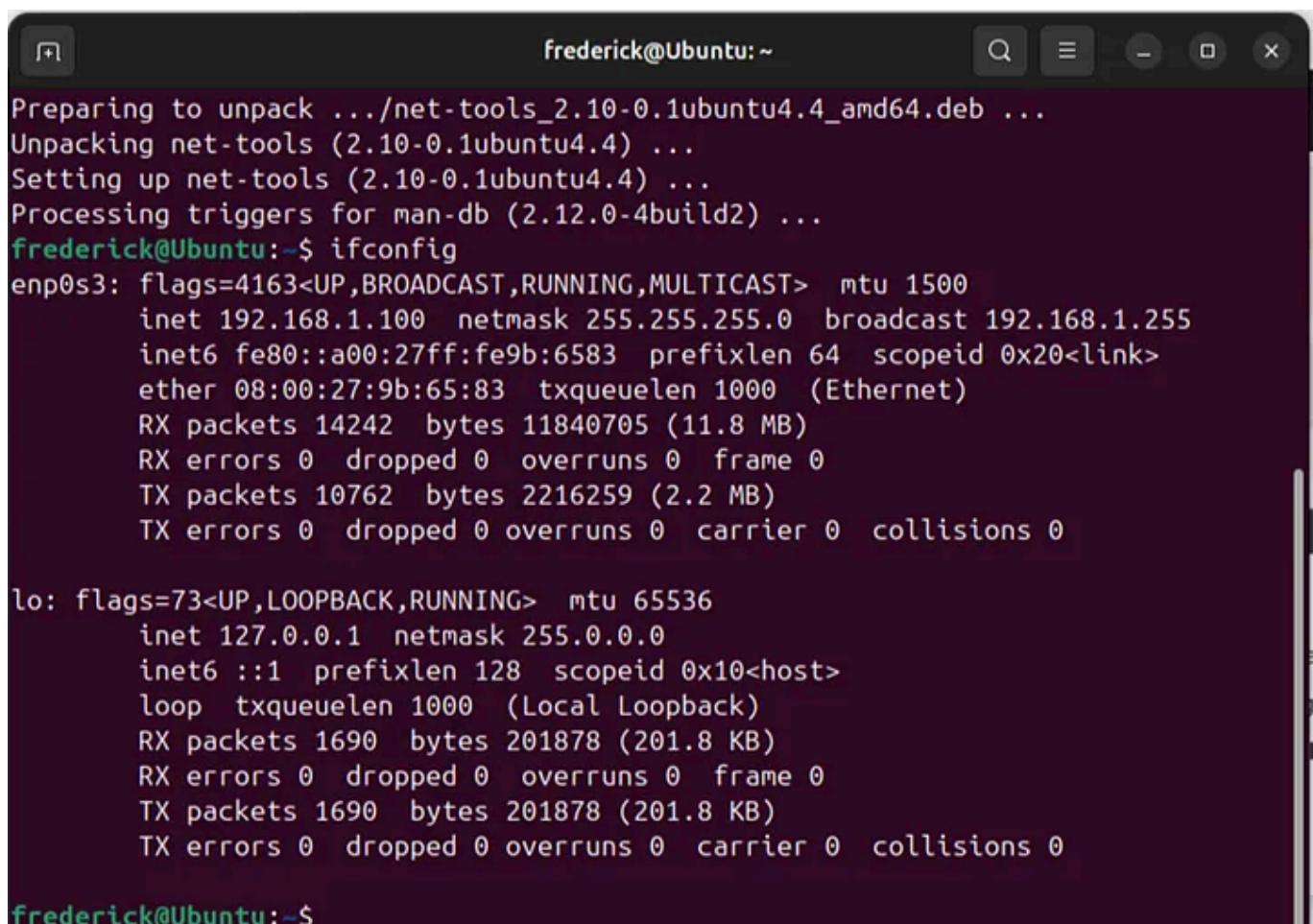
Fig. 30

Remember the LAN interface for pfSense is also in internal mode (Fig. 9).

Now switch on the Ubuntu VM

Check the IP address the Ubuntu VM picked up, open up the terminal and run the `ifconfig` command.

The IP address should be in the 192.168.1.x range. Mine here is 192.168.1.100 (Fig. 31).



```
Preparing to unpack .../net-tools_2.10-0.1ubuntu4.4_amd64.deb ...
Unpacking net-tools (2.10-0.1ubuntu4.4) ...
Setting up net-tools (2.10-0.1ubuntu4.4) ...
Processing triggers for man-db (2.12.0-4build2) ...
frederick@Ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
              inet6 fe80::a00:27ff:fe9b:6583 prefixlen 64 scopeid 0x20<link>
                ether 08:00:27:9b:65:83 txqueuelen 1000 (Ethernet)
                  RX packets 14242 bytes 11840705 (11.8 MB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 10762 bytes 2216259 (2.2 MB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 1690 bytes 201878 (201.8 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 1690 bytes 201878 (201.8 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

frederick@Ubuntu:~$
```

Fig. 31

Now let's check if we can access the internet through pfSense.

Enter the IP address of the pfSense dashboard (in my case, 192.168.1.1) into the browser on the Ubuntu VM. You might see a warning about a potential security risk. Click **Advanced**, then **Accept the Risk and Continue** (Fig. 32).

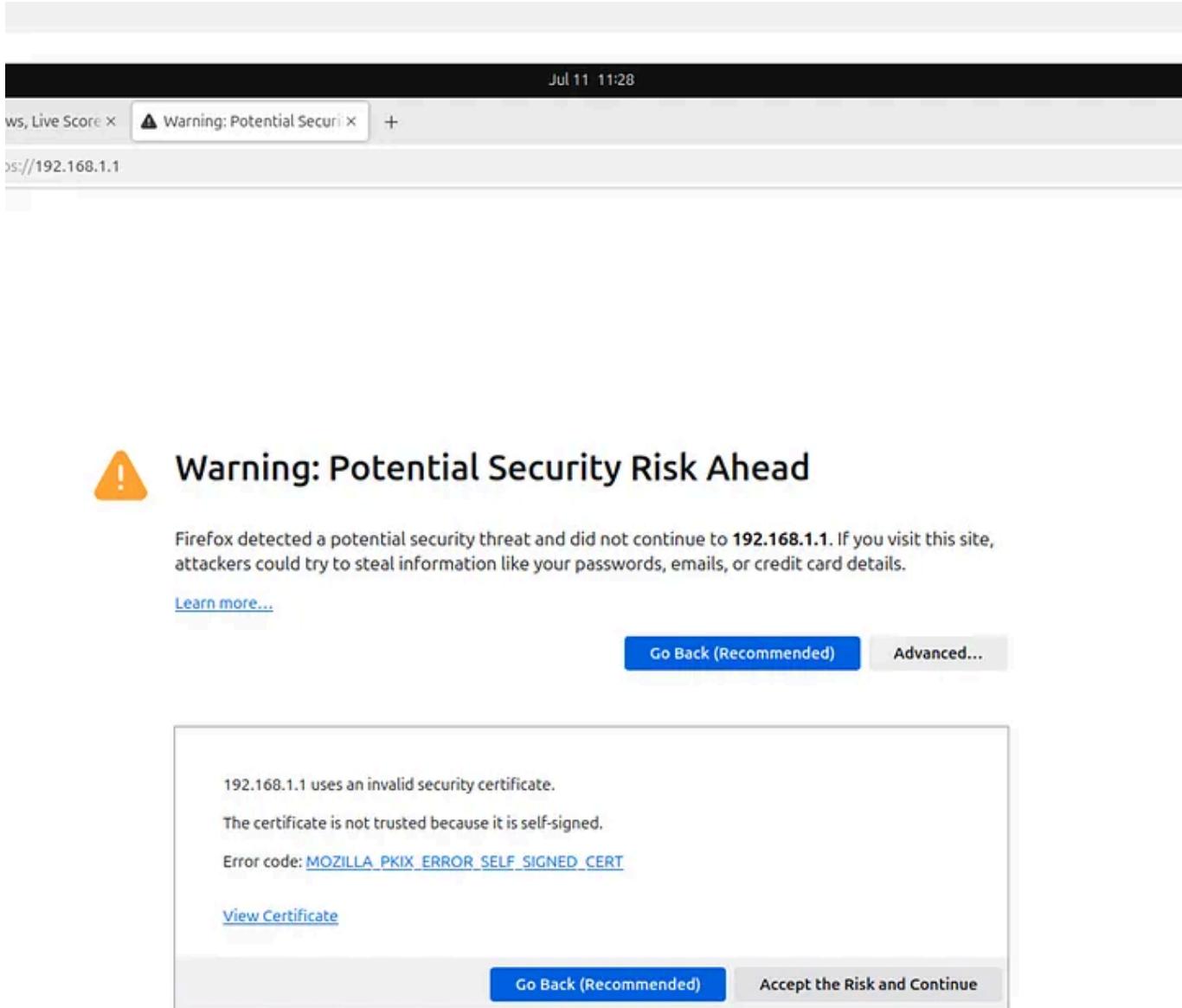


Fig. 32

Next, you will be presented with a login page for pf sense.

To access the dashboard, enter admin as the username and pfsense as the password (in lowercase) (Fig. 33).

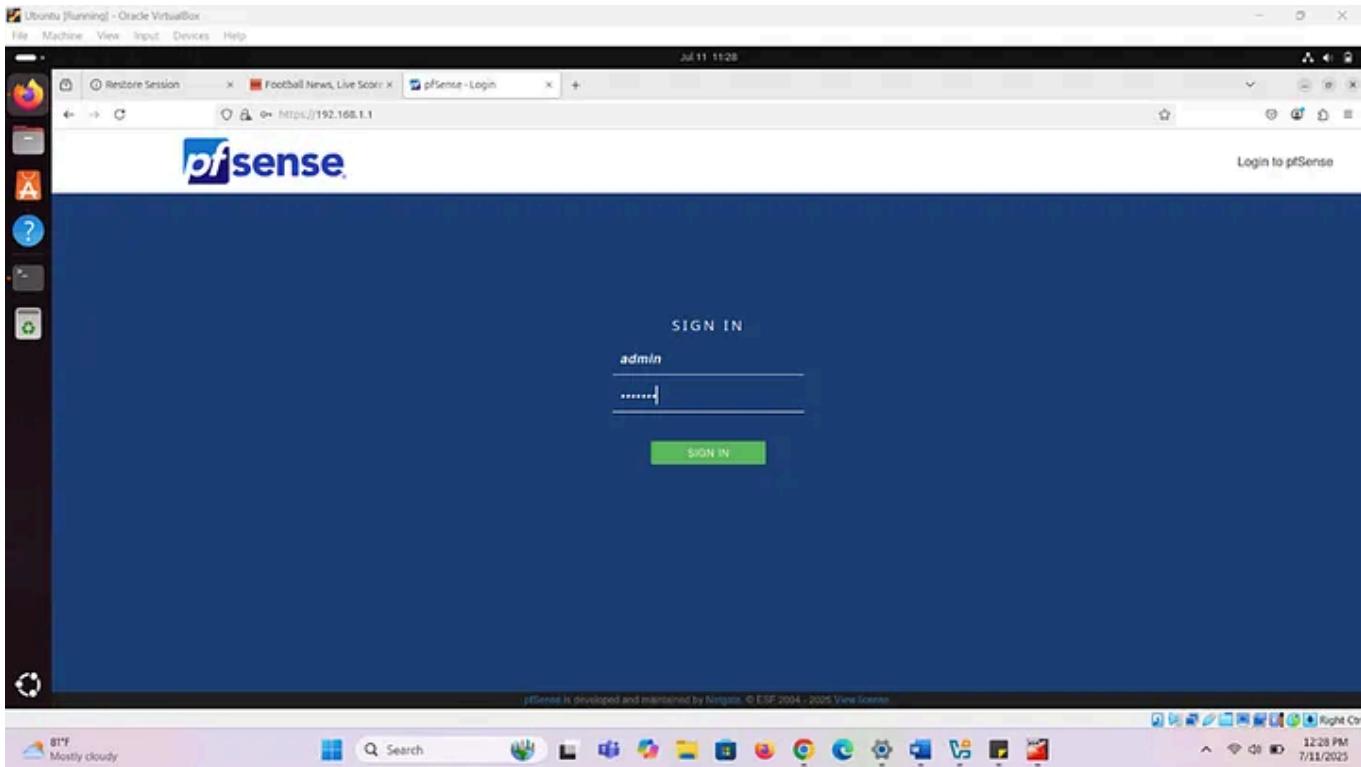


Fig. 33

The homepage loads (Fig. 34).

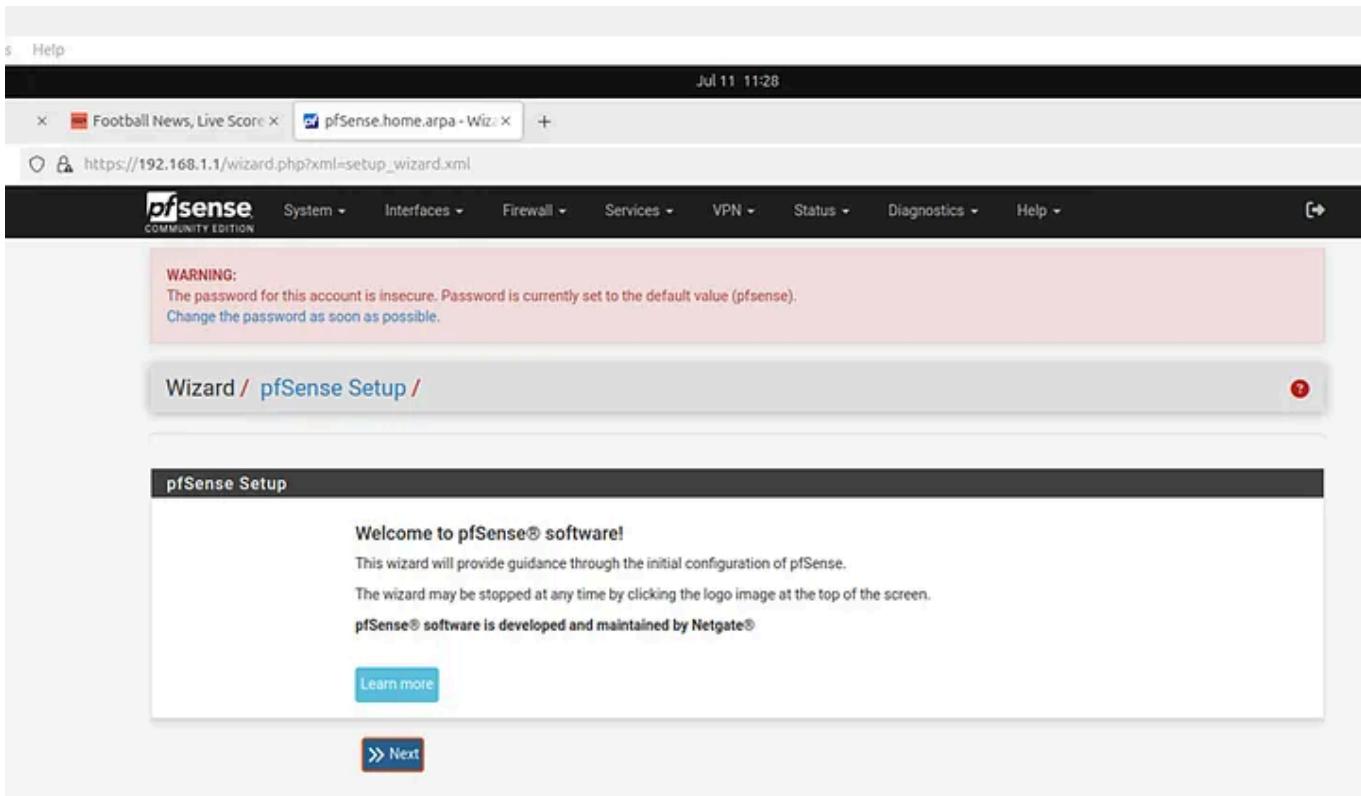


Fig. 34

Click on **Next** to go through the initial setup wizard to configure timezone, interfaces, admin password, and more (Fig 34).

On the General information page, leave the configuration as it is, then click **Next** (Fig. 35).

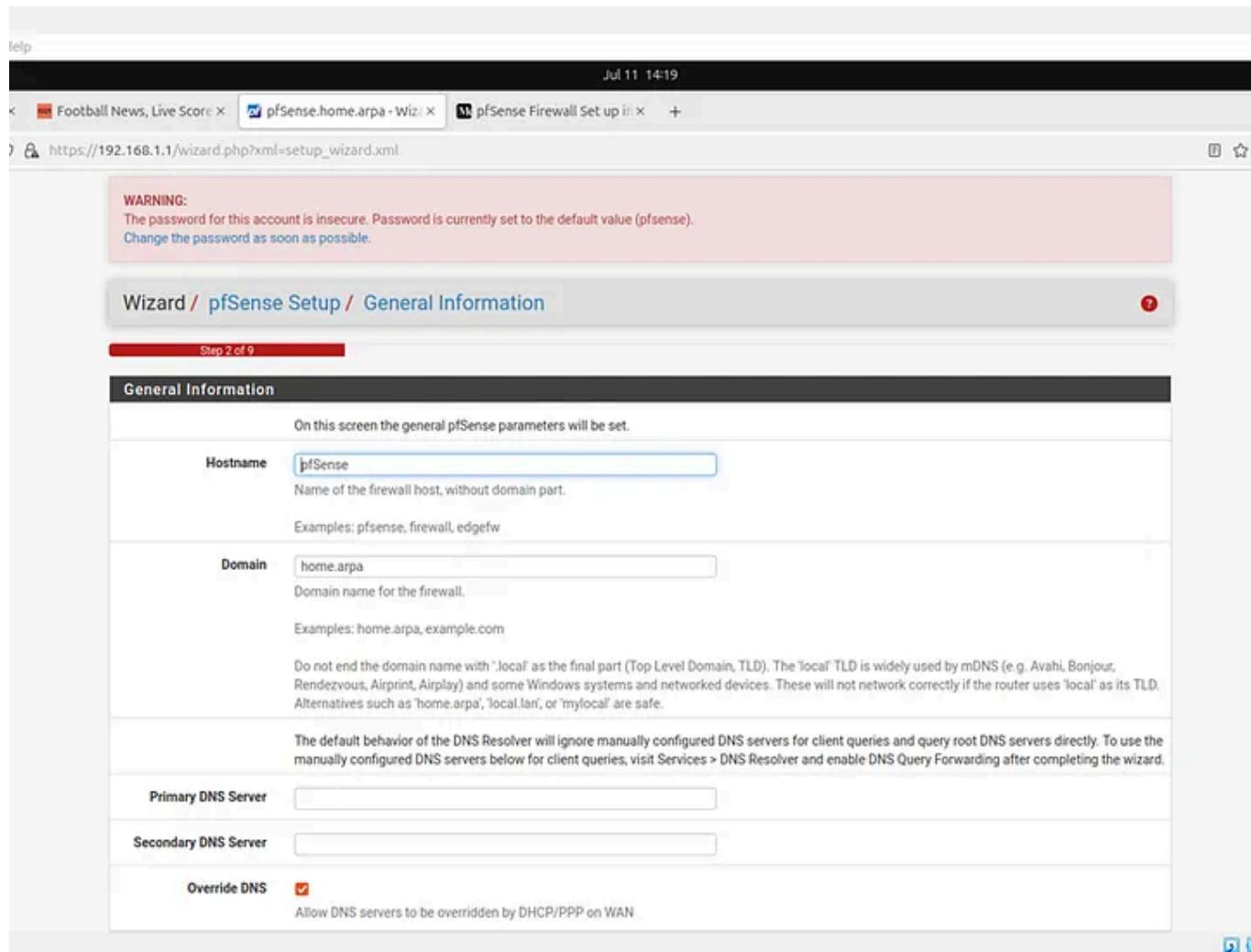


Fig. 35

Leave the configuration on the Time Server Information page and click **Next** (Fig. 36).

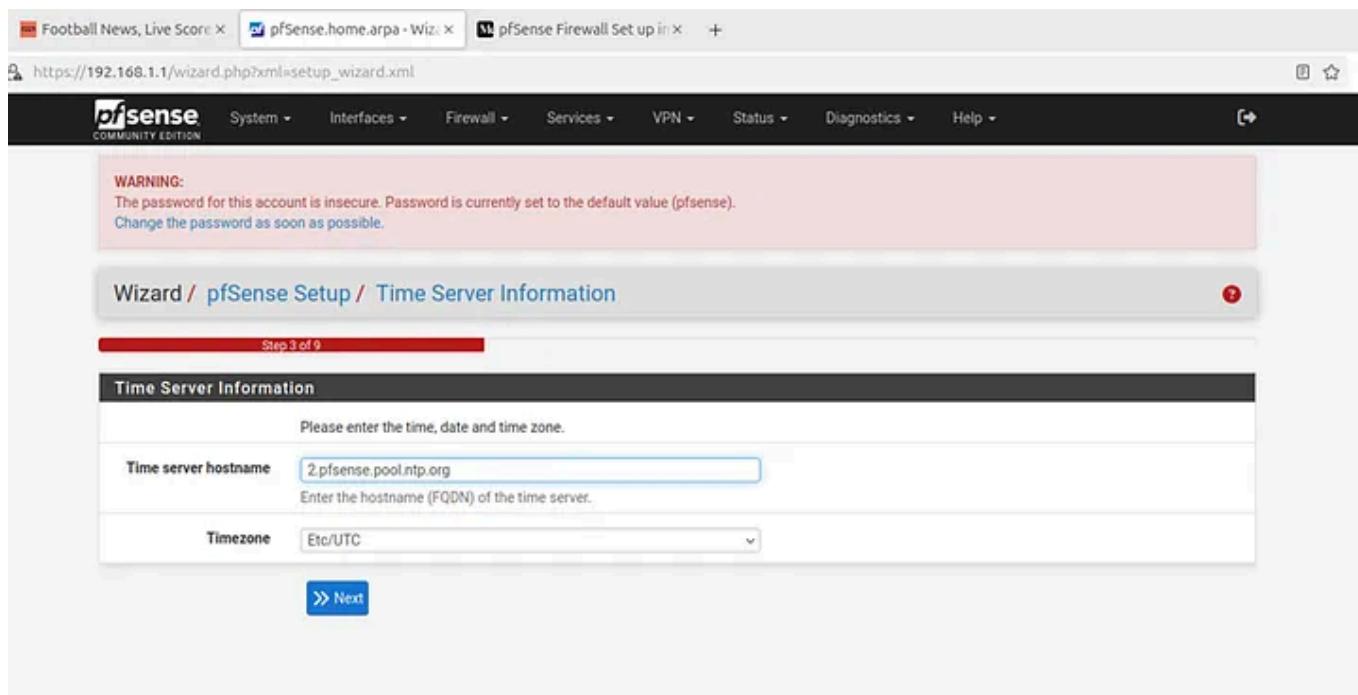


Fig. 36

On the next page, uncheck the box for **Block RFC1918 Private Networks** (Fig. 37).

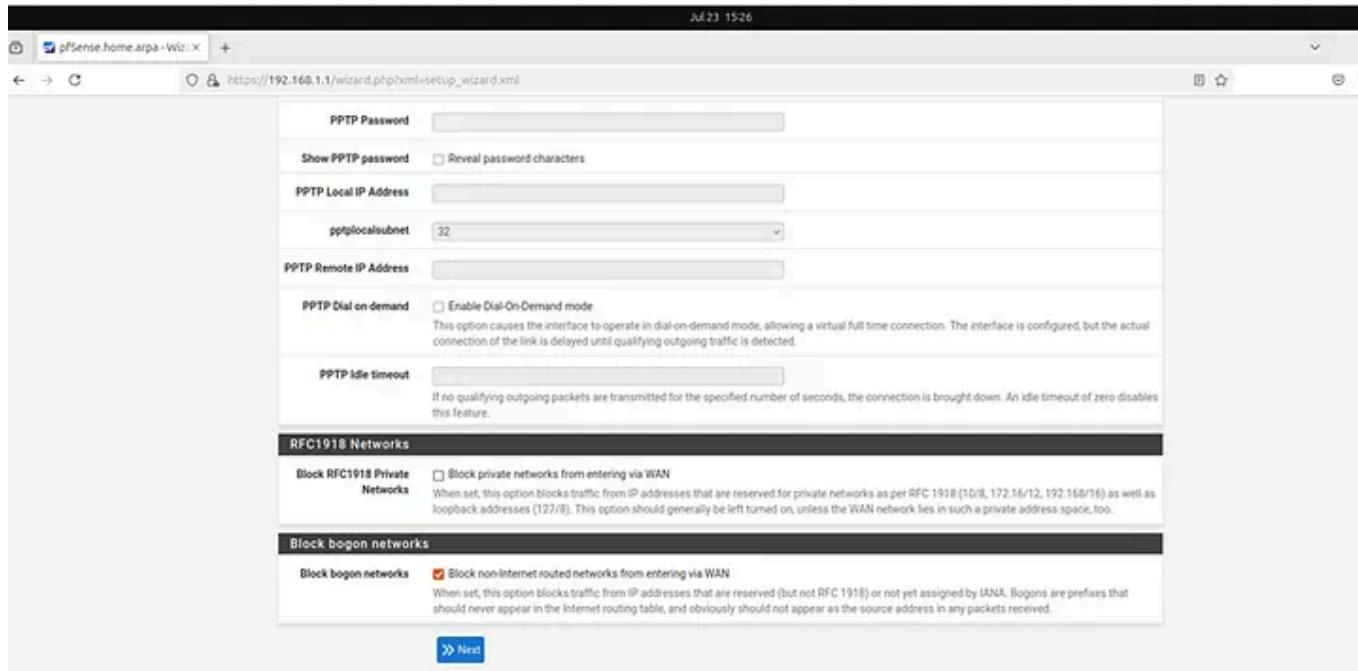


Fig. 37

Leave the page for the LAN configuration unaltered and click **Next** (Fig. 38).

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

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

LAN IP Address: 192.168.1.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

Fig. 38

Choose a new, secure password and click **Next** (Fig. 39).

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Wizard / pfSense Setup / Change admin Account Password

Step 6 of 9

Change admin Account Password

Change the password for the admin account.
This account is used to access the GUI, console (if protected), and SSH service (if enabled).

New admin Password:
Confirm admin Password:

>> Next

Fig. 39

Next, click Reload to reload pfSense with new changes (Fig. 40)

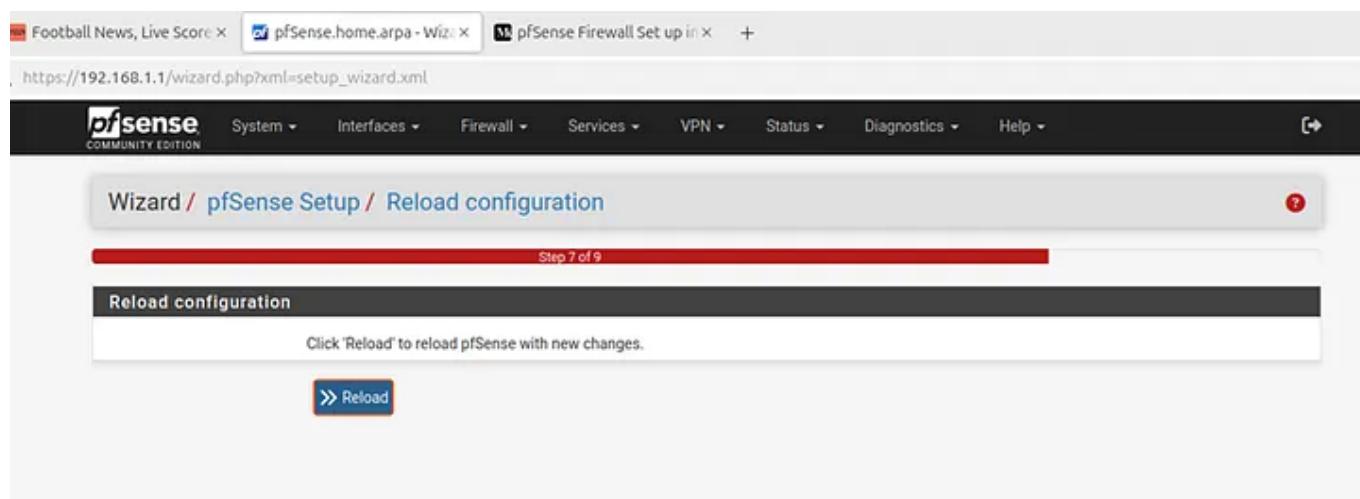


Fig. 40

Click Finish and accept the terms presented on the next page (Fig. 41).

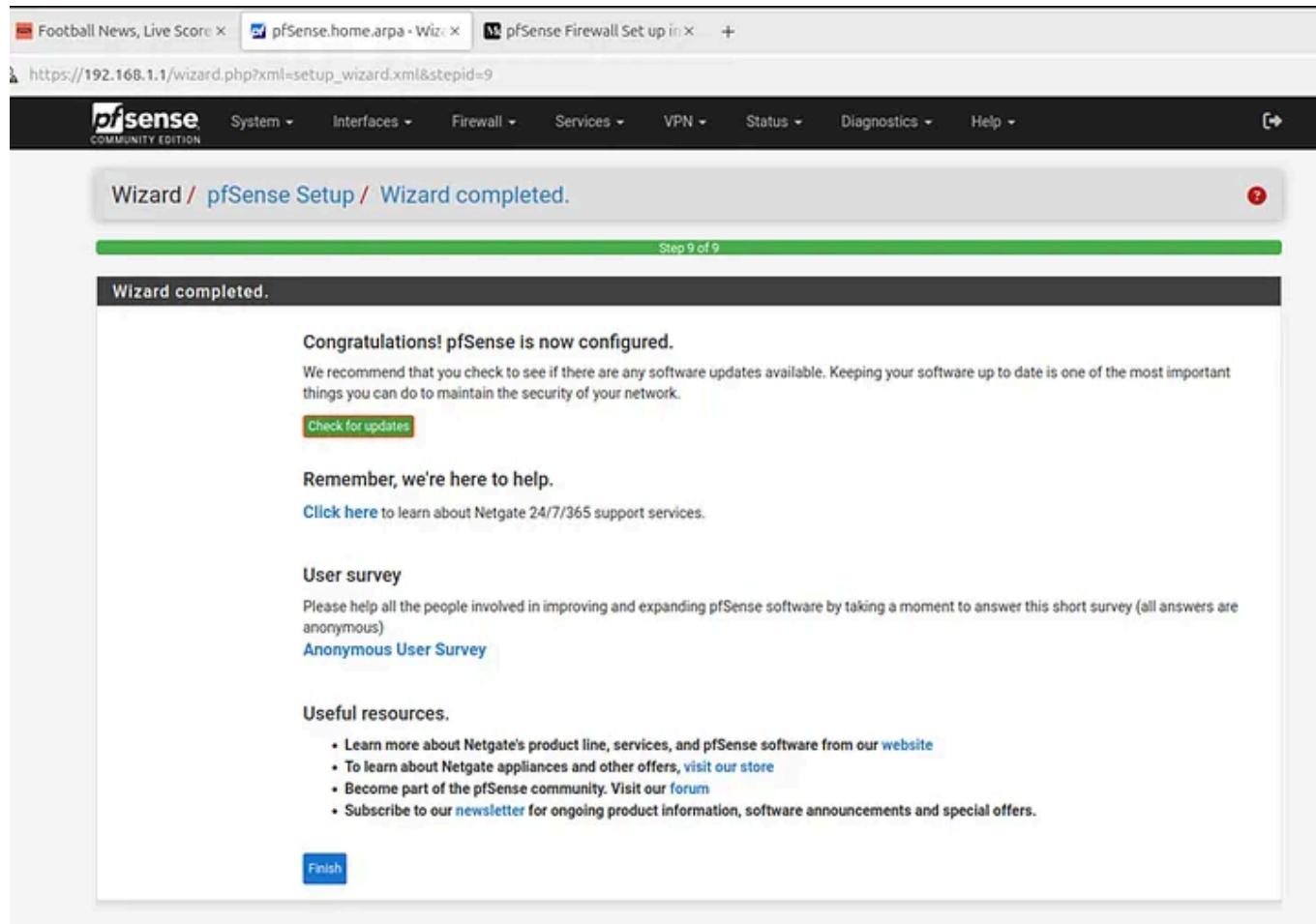


Fig. 41

Accept the terms presented on that page (Fig. 42).

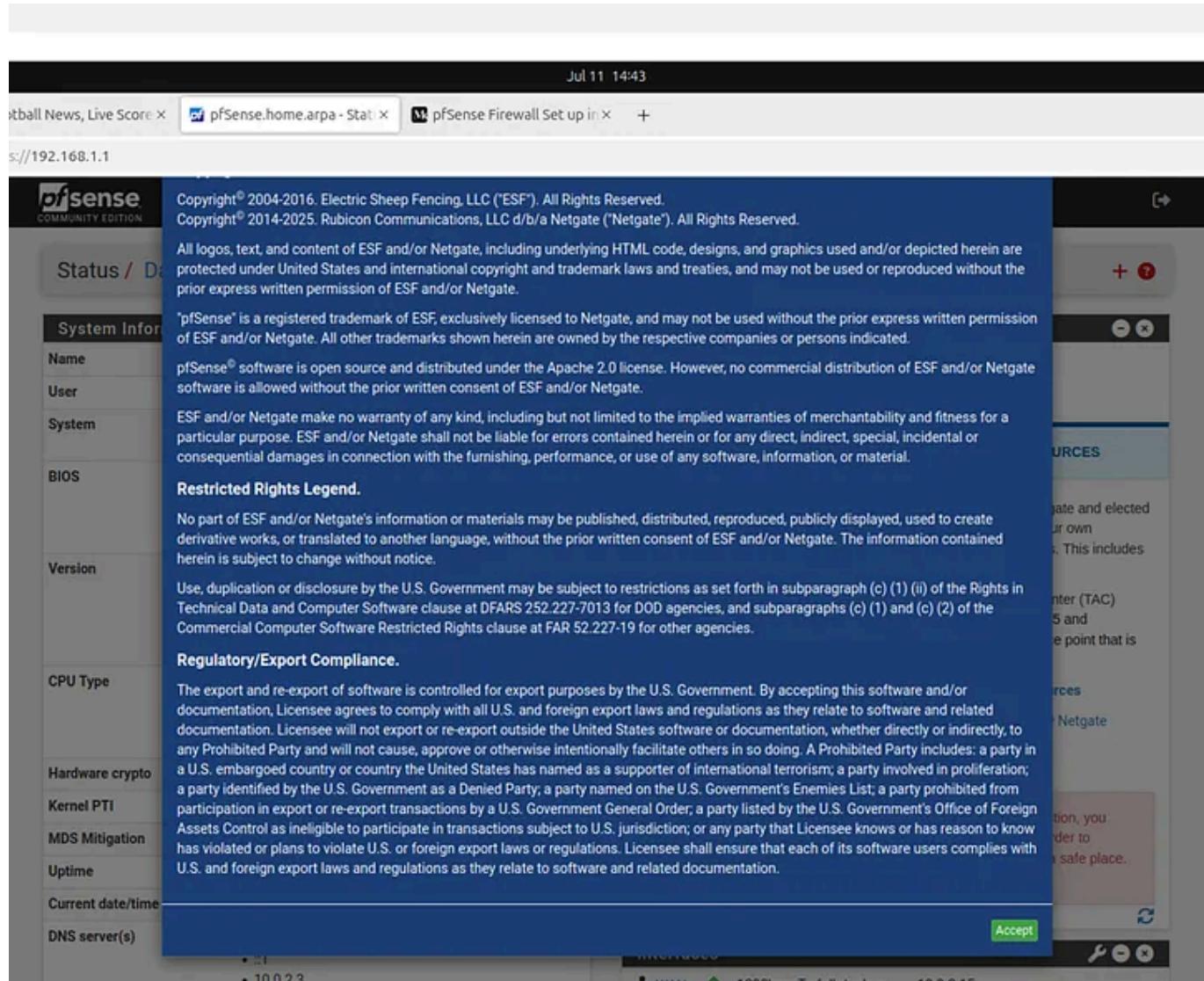


Fig. 42

You can now access your dashboard (Fig. 43).

The screenshot shows the pfSense Status / Dashboard interface. On the left, there's a 'System Information' table with details like Name (pfSense.home.arpa), User (admin@192.168.1.100), System (VirtualBox Virtual Machine, Netgate Device ID: 2ef299e1012a2800ca66), BIOS (Vendor: Innotek GmbH, Version: VirtualBox, Release Date: Fri Dec 1 2006, Boot Method: BIOS), Version (2.8.0-RELEASE (amd64), built on Wed May 21 23:12:00 UTC 2025, FreeBSD 15.0-CURRENT), CPU Type (AMD Ryzen 7 PRO 4750U with Radeon Graphics, 2 CPUs: 1 package(s) x 2 core(s), AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No), Hardware crypto (Inactive), Kernel PTI (Disabled), MDS Mitigation (Inactive), Uptime (01 Hour 30 Minutes 47 Seconds), Current date/time (Fri Jul 11 14:46:48 UTC 2025), DNS server(s) (127.0.0.1, ::1, 10.0.2.3), Last config change (Fri Jul 11 14:40:42 UTC 2025), and State table size (1024). On the right, there's a 'Netgate Services And Support' section with 'Community Support' and 'Community Support Only' options, and a 'NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES' section with links to upgrade support, community resources, Netgate Global Support FAQ, official pfSense training, and professional services. Below that is a note about purchasing TAC support. At the bottom, there's an 'Interfaces' section showing WAN (1000baseT <full-duplex>, IP: 10.0.2.15, MAC: fd:17:62:5c:f0:37) and LAN (1000baseT <full-duplex>, IP: 192.168.1.1, MAC: fe:88:99:67).

Fig. 43

The Leaning Tower of Pisa in Italy was never meant to lean. Construction began in 1173, but the foundation sank into soft ground on one side, causing the iconic tilt that has fascinated visitors for centuries.

Step 3: CONFIGURING FIREWALL RULES IN PFSENSE

To access firewall rules in pfSense, click on Firewall from the top menu, then select Rules, and choose the LAN tab. pfSense comes with three default rules on the LAN interface (Fig. 44).

The first is the **anti-lockout rule**, which ensures you can still reach the web interface on the LAN IP even if you misconfigure other rules by allowing

HTTP (port 80) and HTTPS (port 443) connections to the LAN address from any source.

The second rule is the **default allow LAN to any (IPv4)** rule, which permits all IPv4 traffic originating from LAN subnets to reach any destination using any port or protocol. This grants devices on the LAN unrestricted outbound access to the internet or other networks.

The third rule is the **default allow LAN to any (IPv6)** rule, functioning similarly to the IPv4 rule but for IPv6 traffic.

These defaults are useful for initial setup but should be reviewed and customized in a production or security-focused environment.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/572 KiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
✗ 5/107.48 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✗ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Fig. 44

Now, you should disable the 2 rules granting unfettered outbound access. To do this, click on each rule, then click on the prohibition sign (🚫) at the far

right under the Action (Fig. 45).

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 1/1.55 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/> 13/77.88 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Buttons at the bottom: Add, Add, Delete, Toggle, Copy, Save, Separator.

Fig. 45

Next, apply changes (Fig. 46).

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 1/1.59 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/> 15/77.95 MiB	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	

Buttons at the bottom: Add, Add, Delete, Toggle, Copy, Save, Separator.

Fig. 46

After disabling these two rules, any network connections from the Ubuntu VM will fail (Fig. 47).

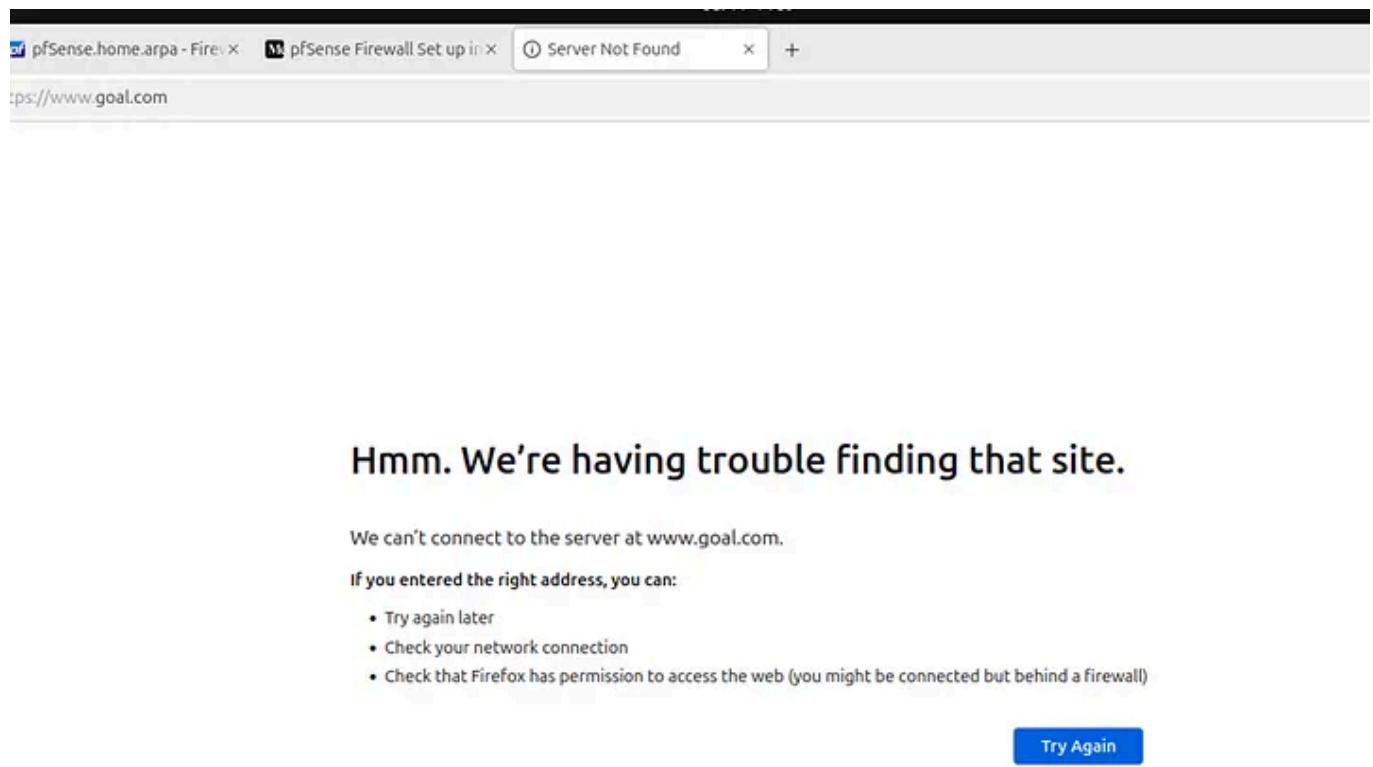


Fig. 47

Adding Custom Firewall Rules

This can be done in two ways:

- Adding individual rules
- Adding rules as a group

Adding Individual Rules

A useful rule to add is one that allows outbound ICMP traffic, enabling devices within the LAN subnet to ping both themselves and external devices.

Ping is currently not going through.

```
frederick@Ubuntu:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
^C
--- 192.168.1.1 ping statistics ---
89 packets transmitted, 0 received, 100% packet loss, time 90215ms

frederick@Ubuntu:~$
```

Fig. 48

To add the ICMP rule, click the green upward arrow (Fig. 49). This ensures the rule is placed at the top of the list, giving it priority over others.

The screenshot shows the pfSense Firewall Rules LAN interface. The URL in the address bar is `ps://192.168.1.1/firewall_rules.php?f=lan`. The LAN tab is selected. A message at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, there is a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/1.61 MiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
✓ 32/78.08 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom of the table, there is a toolbar with several buttons: a green upward arrow labeled "Add" (circled in red), a green downward arrow labeled "Add", a red "Delete" button, a blue "Toggle" button, a blue "Copy" button, a blue "Save" button, and an orange "Separator" button.

Fig. 49

Clicking the green upward arrow opens the configuration page, where you can set up the rule. Configure the rule as shown in the image below (Fig. 50, 51).

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' dropdown is set to 'Pass'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'LAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'ICMP'. Under 'ICMP Subtypes', 'any' is selected. Below it, a note says 'For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.' The 'Source' section shows 'Source' and 'Invert match' options, with 'LAN subnets' selected. The 'Destination' section shows 'Destination' and 'Invert match' options, with 'Any' selected. The 'Extra Options' section has a 'Log' checkbox which is unchecked. A note below it says 'Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).'

Fig. 50

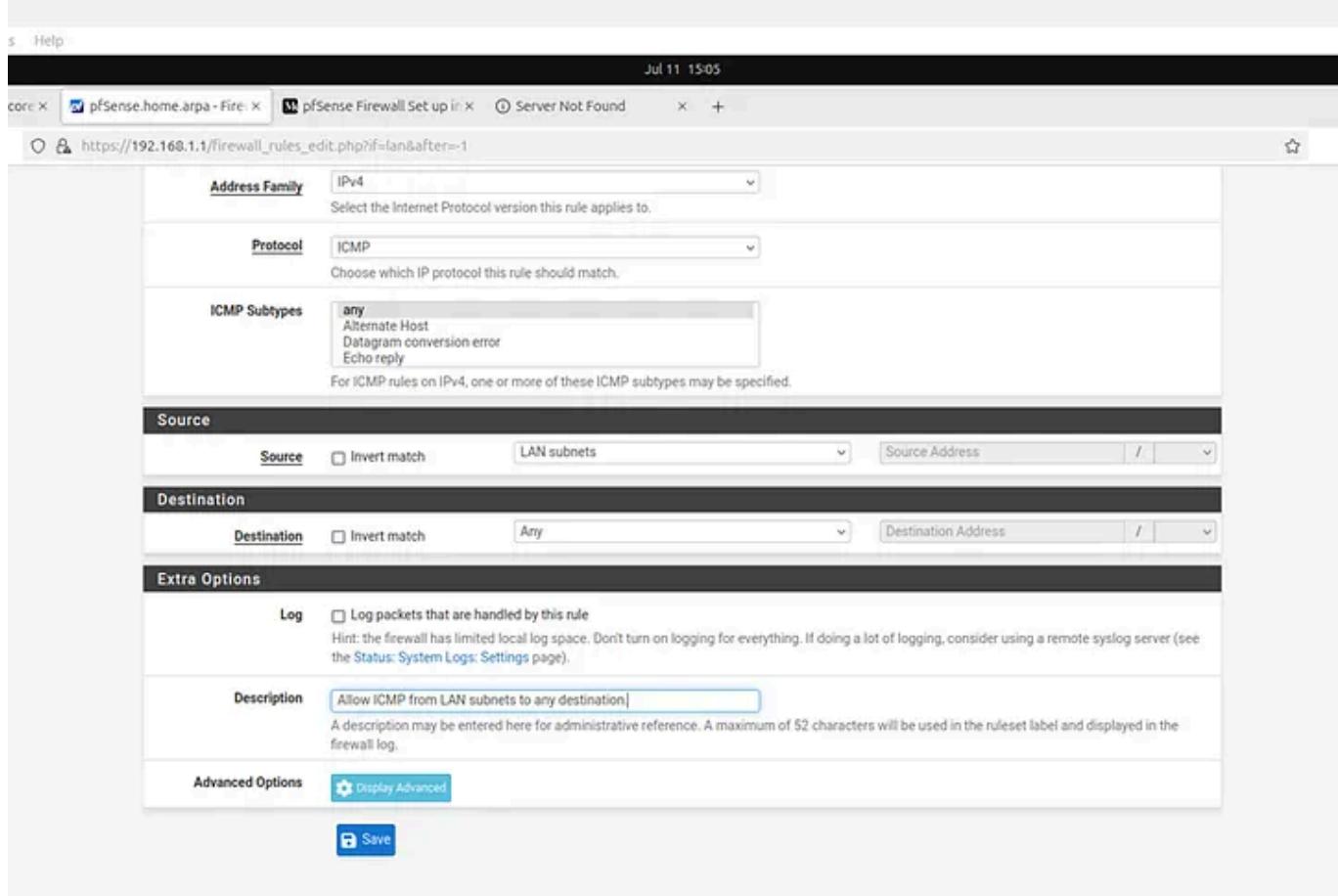


Fig. 51

This pfSense firewall rule allows ICMP (e.g., ping) traffic from LAN devices to any destination. The **Action** is set to **Pass**, meaning matching packets are permitted. The rule applies to the **LAN** interface and only to **IPv4** traffic. The **Protocol** selected is **ICMP**, and **ICMP Subtypes** are set to **any**, allowing all types of ICMP messages (e.g., echo request/reply, unreachable).

The **Source** is set to **LAN subnets**, meaning the rule applies to devices within the local network. The **Destination** is set to **Any**, allowing ICMP packets to reach any external or internal address. Logging is disabled to save space, and the rule is active (not disabled).

In short, this rule enables LAN clients to perform network diagnostics like ping or traceroute without restrictions on ICMP type or destination.

Apply the changes (Fig. 52).

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/1.68 MiB *	*	*	*	LAN Address 80	443 *	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP any	LAN subnets	*	*	*	*	none		Allow ICMP from LAN subnets to any destination.	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Fig. 52

Attempting to ping the default gateway now is now successful (Fig. 53).

```
frederick@Ubuntu:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.694 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.801 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.712 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.705 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.896 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.792 ms
^C
--- 192.168.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5152ms
rtt min/avg/max/mdev = 0.694/0.766/0.896/0.071 ms
frederick@Ubuntu:~$
```

Fig. 53

Adding rules as a group

Beyond ICMP traffic, we also need internet connectivity for devices on the LAN.

At this stage, attempting to visit a website will fail (Fig. 54).

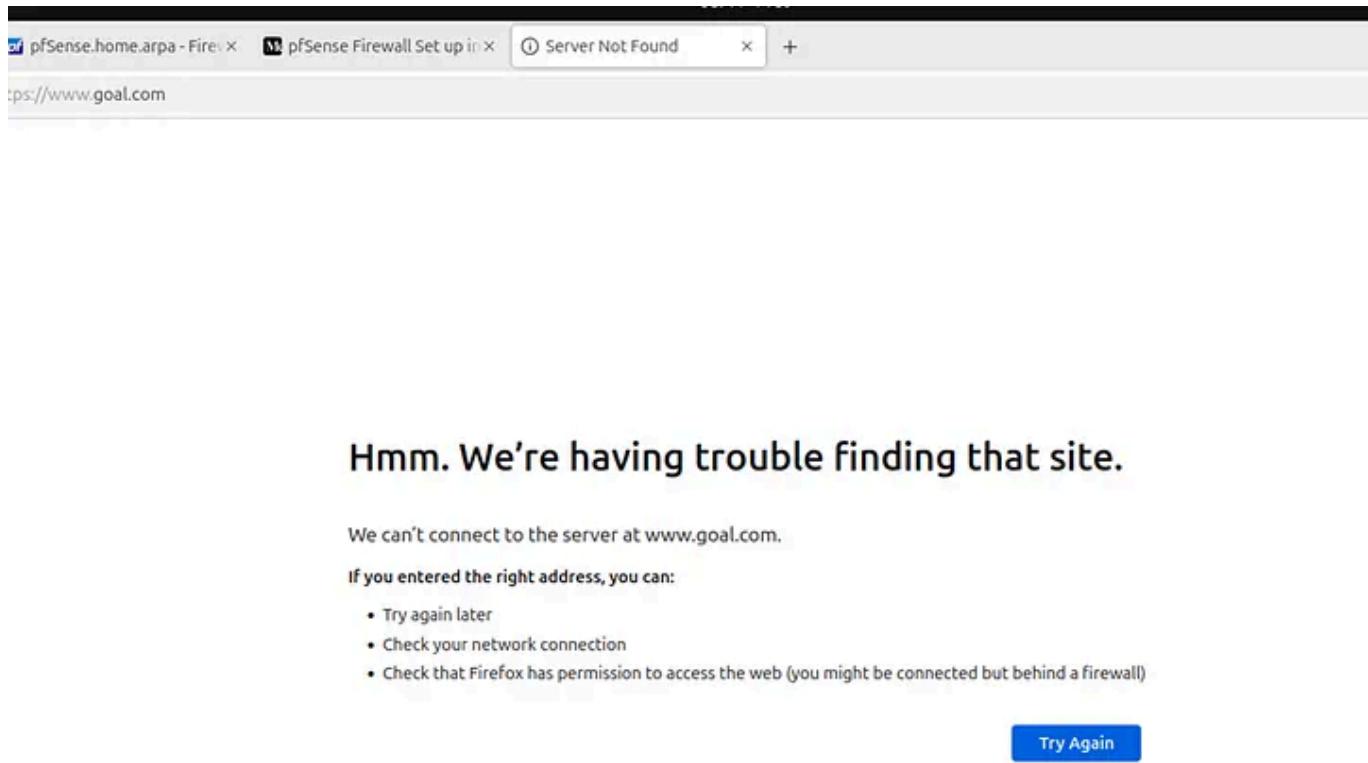


Fig. 54

Key ports need to be open to achieve internet connectivity: 53 (DNS), 80 (HTTP), and 443 (HTTPS). This can be added together as a group. First, we need to create an alias.

Click on **firewall > Aliases > Ports**.

Next, click **Add** (Fig. 55).

Name	Type	Values	Description	Actions
Internet	Port(s)	53, 80, 443	Alias for internet access	Edit Delete

Fig. 55

You can configure as desired, but I am configuring mine as shown below (Fig. 56).

Port	Protocol	Action
53	DNS	Delete
80	HTTP	Delete
443	HTTPS	Delete

Fig. 56

Save and apply the changes (Fig. 57).

The screenshot shows the pfSense Firewall Aliases Ports configuration page. At the top, there is a message: "The alias list has been changed. The changes must be applied for them to take effect." Below this is a green "Apply Changes" button with a checkmark. The main table has four columns: Name, Type, Values, and Description. A single row is present with the name "Internet", type "Port(s)", values "53, 80, 443", and description "Alias for internet access". The "Actions" column contains edit, copy, and delete icons. At the bottom of the table are "Add" and "Import" buttons. The URL in the browser is https://192.168.1.1/firewall_aliases.php?tab=port.

Name	Type	Values	Description	Actions
Internet	Port(s)	53, 80, 443	Alias for internet access	

Fig. 57

Next, navigate to **Firewall > Rules > LAN**.

Then click Add (the upward facing green arrow).

Configure the rule as follows (Fig. 58, 59):

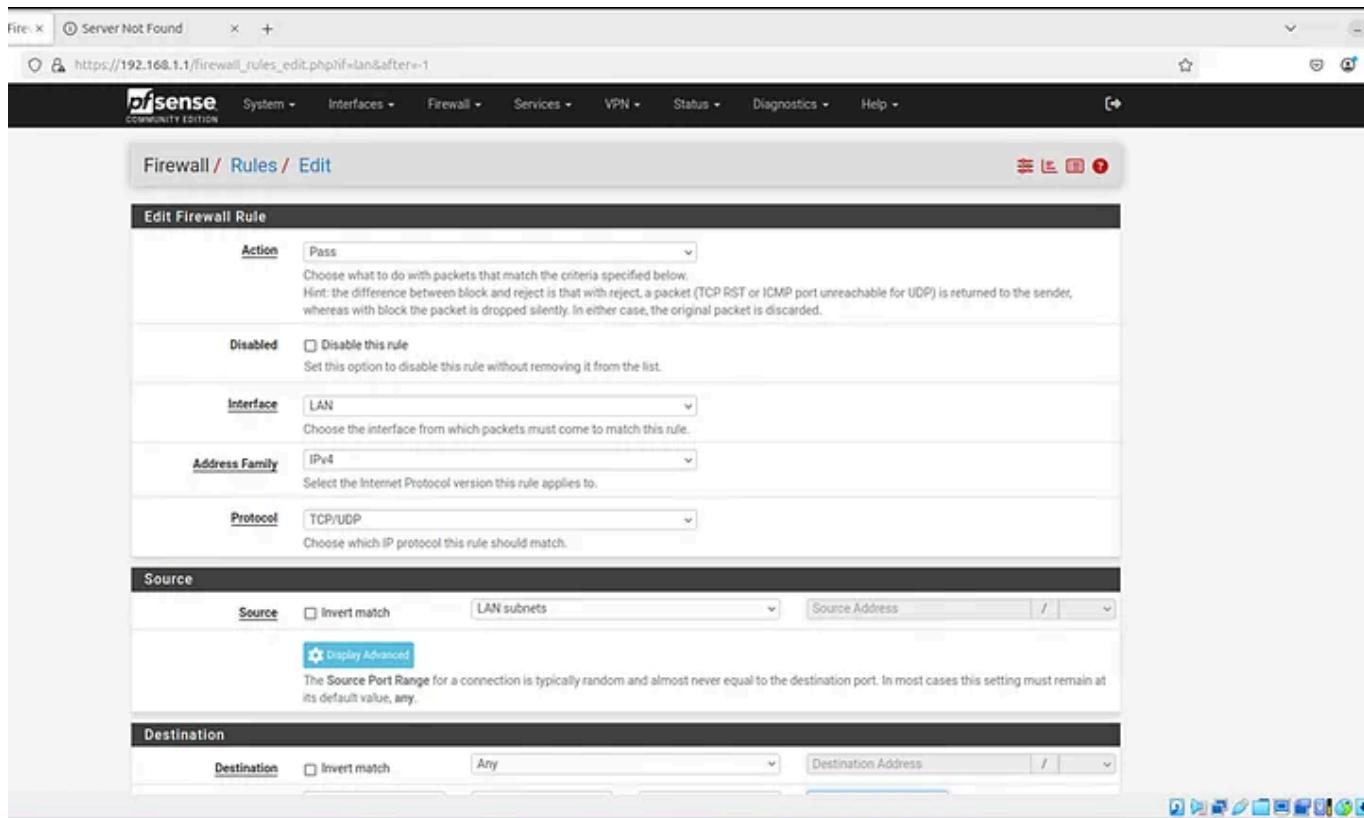


Fig. 58

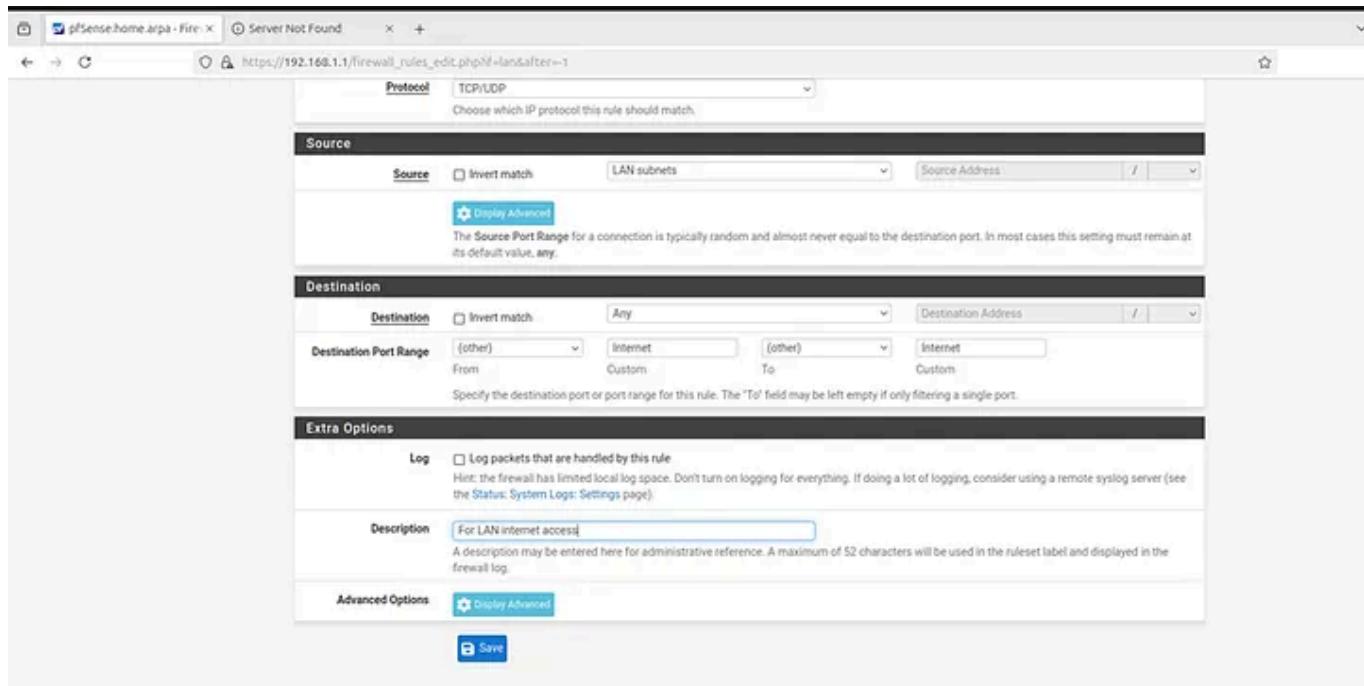


Fig. 59

This pfSense firewall rule is configured to allow LAN devices to access the internet:

- **Action:** Pass, meaning matching traffic is allowed.
- **Disabled:** Not checked, so the rule is active.
- **Interface:** LAN, meaning it applies to traffic coming from the LAN.
- **Address Family:** IPv4, restricting the rule to IPv4 traffic.
- **Protocol:** TCP/UDP, covering most common internet traffic types (like HTTP, HTTPS, DNS, etc.).
- **Source:** LAN subnets, allowing any device within the local network.
- **Destination:** any, with a custom label “Internet” which is the alias that I created earlier, allowing traffic to any destination IP.
- **Destination Port Range:** Left blank (interpreted as any), meaning no restriction on the ports being accessed.
- **Log:** Not enabled, so packets matching this rule won’t be logged.
- **Description:** “For LAN internet access” for administrative clarity.

In summary, this rule enables unrestricted outbound IPv4 TCP/UDP connections from LAN clients to the internet, which is essential for basic connectivity like web browsing and software updates.

Then save and apply (Fig. 60).

The screenshot shows the pfSense Firewall Rules configuration interface. At the top, there are tabs for Floating, WAN, and LAN, with LAN selected. Below the tabs is a table titled "Rules (Drag to Change Order)". The table lists five rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/1.91 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0.8	IPv4 TCP/UDP	LAN subnets	*	*	Internet	*	none		For LAN internet access	
<input type="checkbox"/>	0/100.8 B	IPv4 ICMP	any	*	*	*	*	none		Allow ICMP from LAN subnets to any destination.	
<input type="checkbox"/>	0/0.8	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0.8	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom of the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator. A message at the top of the page says: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." There is also a small red error icon in the top right corner.

Fig. 60

Internet connection is now possible (Fig. 61).

The screenshot shows a web browser window with the URL <https://www.goal.com/en-rg>. The page displays a dark-themed news feed for football. At the top, there is a navigation bar with links for LIVE SCORES, NEWS, TRANSFERS, PREMIER LEAGUE, LA LIGA, BETTING, and CULTURE. On the right side, there is a "Log In" button. The main content area features a large "GOAL" logo. Below the logo, there is a table showing football fixtures for Club Friendlies on Sunday, July 21, 2024. The table includes columns for Club Friendlies, Kick-off time, and results. The fixtures listed are:

Club Friendlies	Kick-off	Result	Club Friendlies	Kick-off	Result	Club Friendlies	Kick-off	Result												
EST	10:00	-	CAS	FT	1	CLB	FT	1	MIL	FT PEN	0-6	VSC	13:00	-	MOR	FT	0	FAM	EST	ATL
MAF	-	-	SOU	FT	1	PAT	FT	3	ARS	FT PEN	1-5	POR	-	-	-	-	-	-		

There are also two "Advertisement" banners on the page.

Fig. 61

You can create additional rules to provide fine-grained control over incoming and outgoing traffic.

Tchau!

Cybersecurity

Homelab

Pfsense

Firewall

Open Source



Written by **Frederick Adigun**

3 followers · 2 following

Edit profile

No responses yet



...



Frederick Adigun

What are your thoughts?

More from **Frederick Adigun**