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

F Frederick Adigun 13 min read · Aug 21, 2025

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.

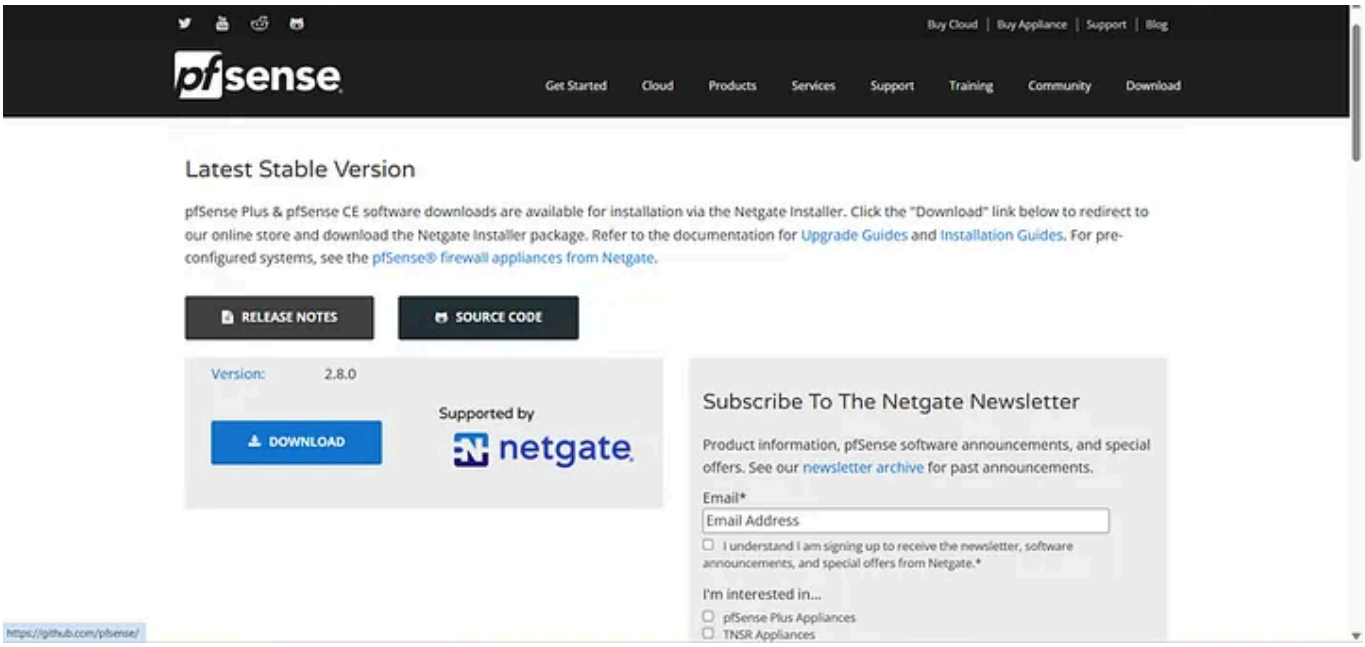

Fig. 1

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).

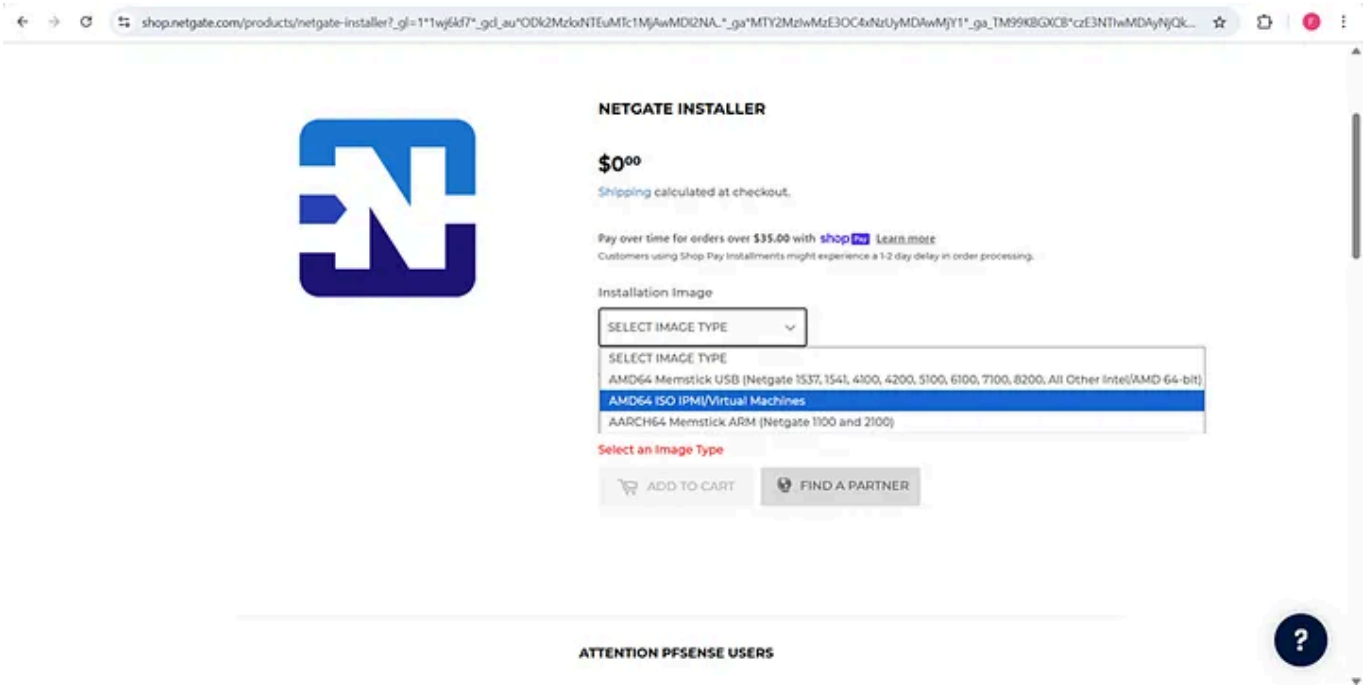

Fig. 2

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

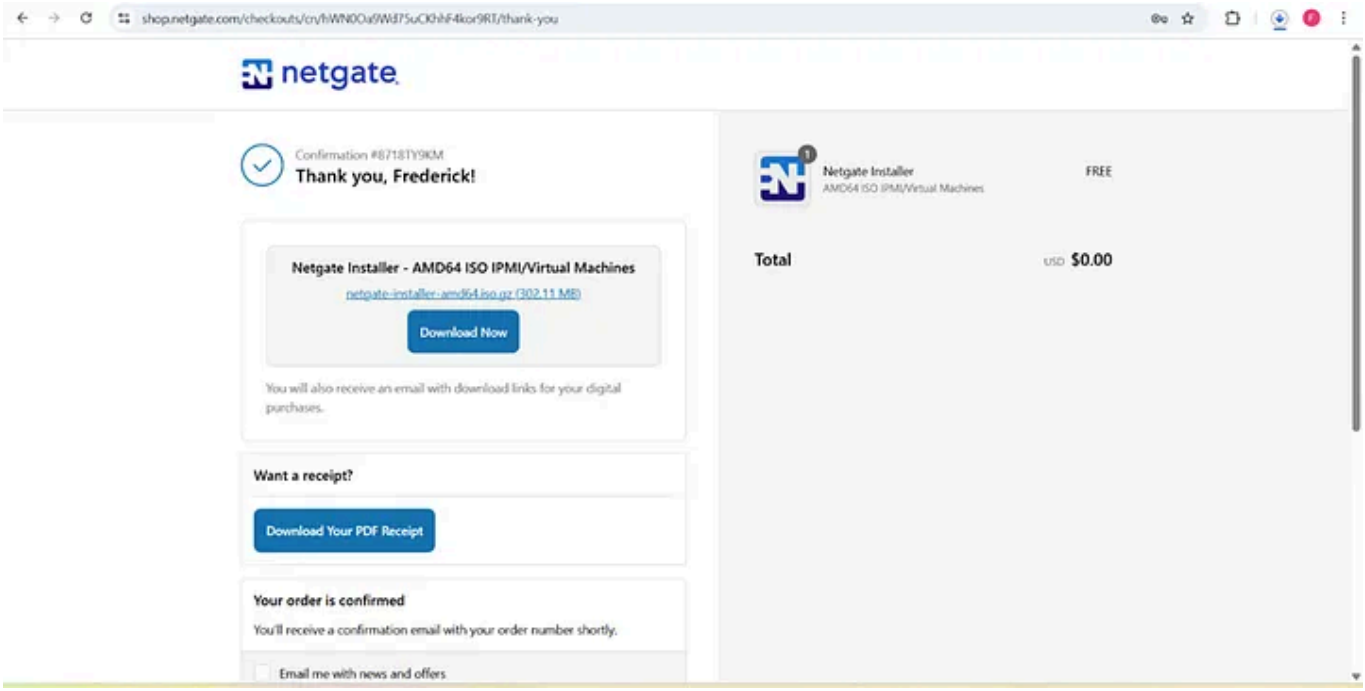

Fig. 3

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

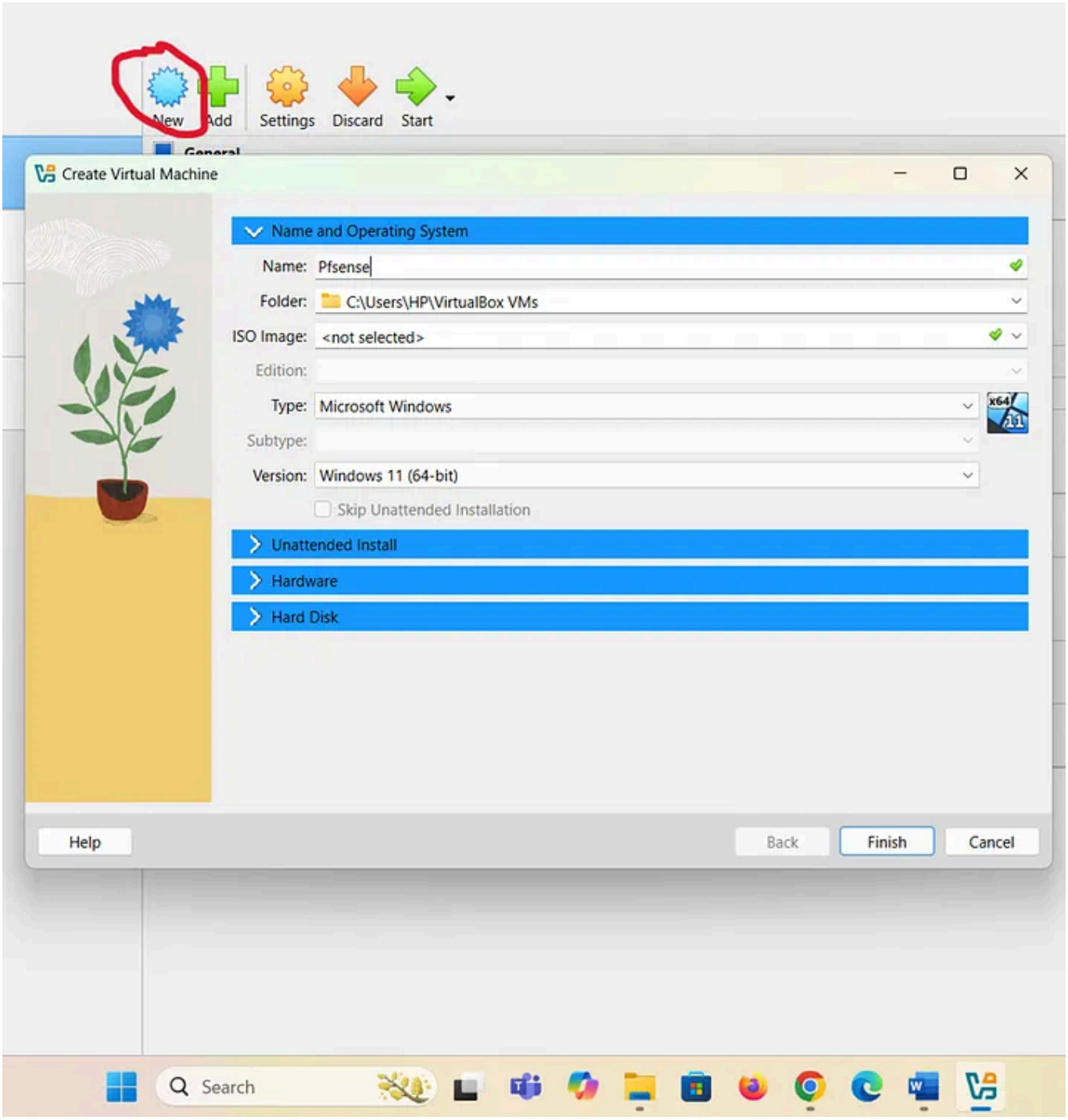

Fig. 4

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).

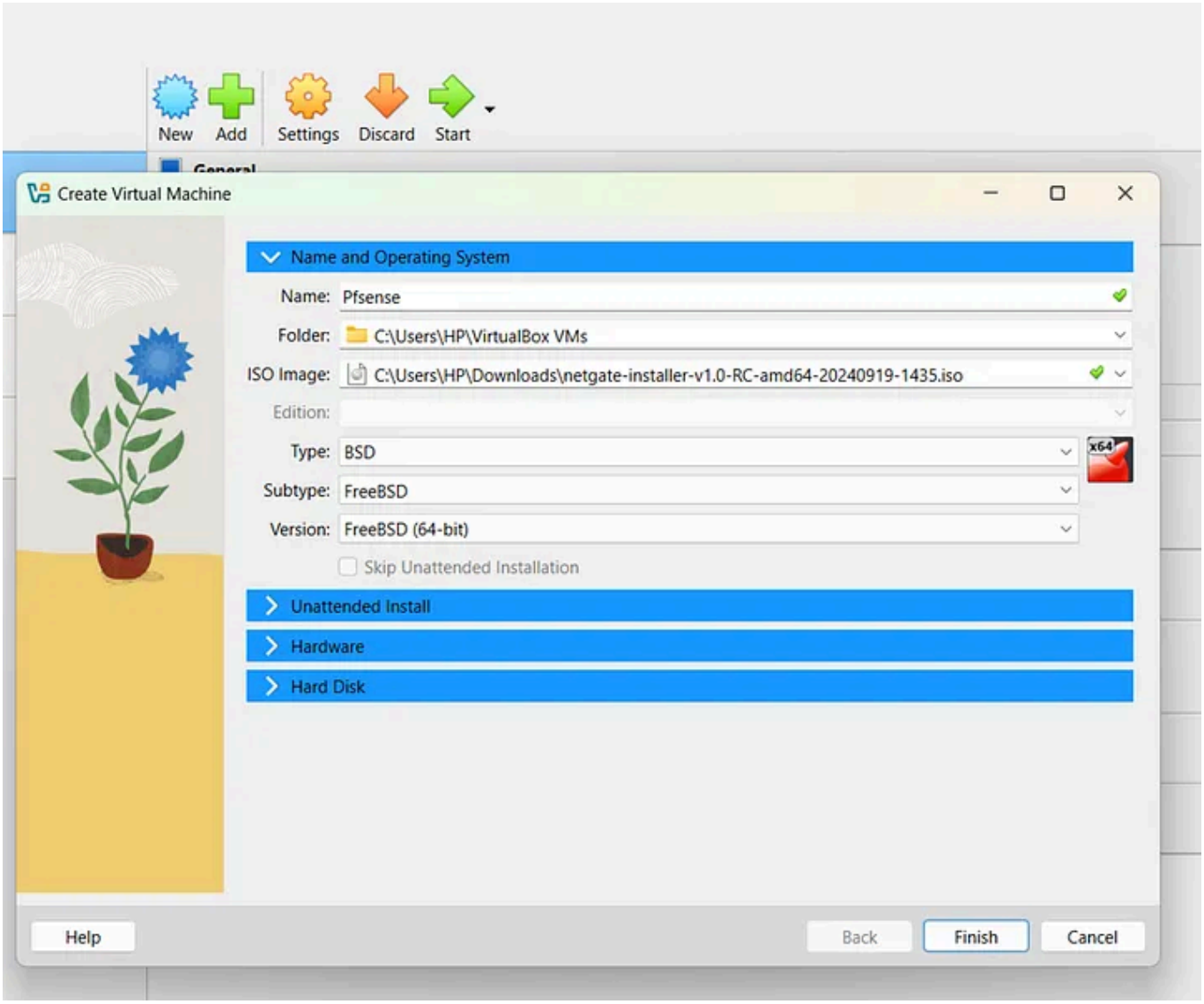

Fig. 5

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

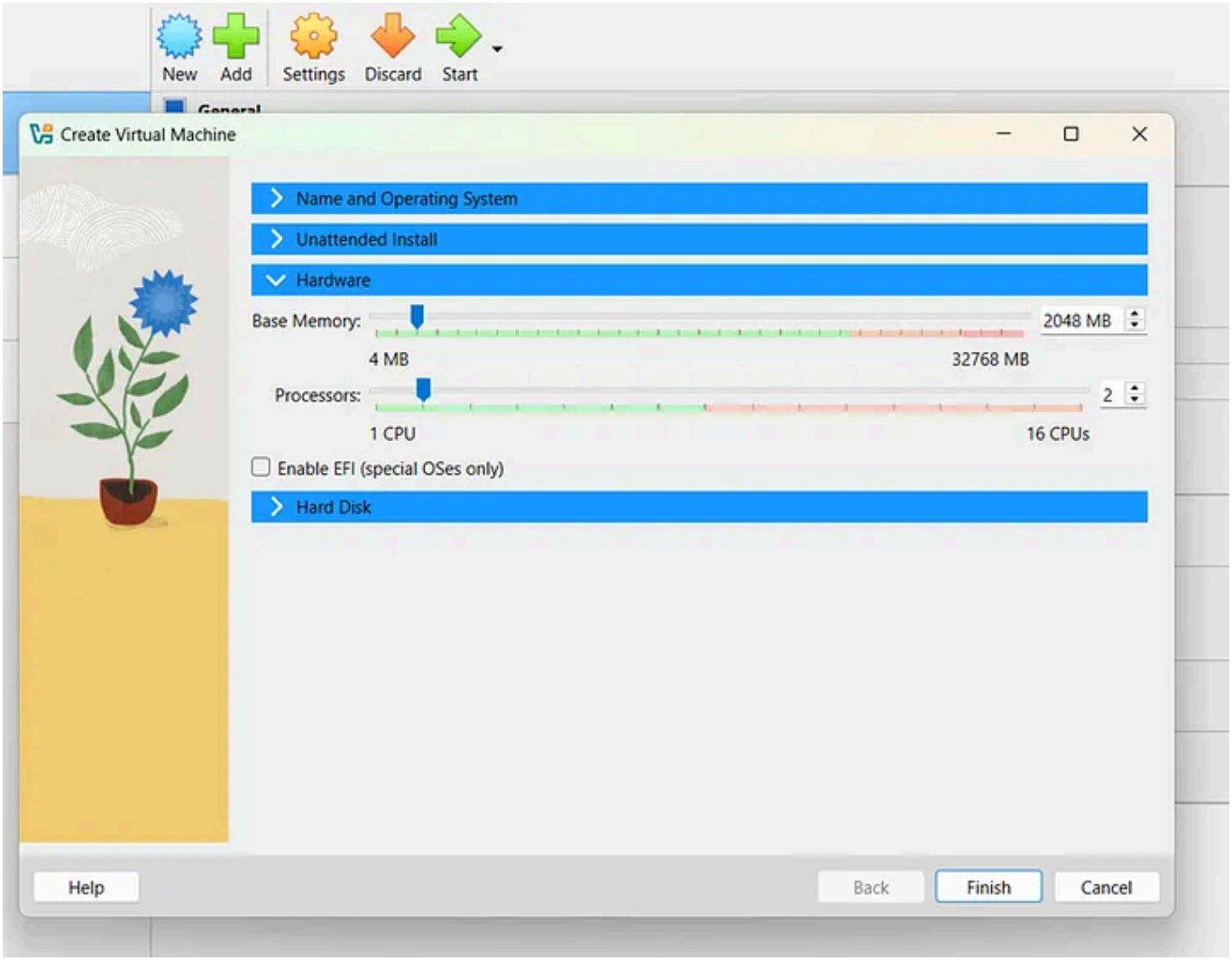

Fig. 6

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).

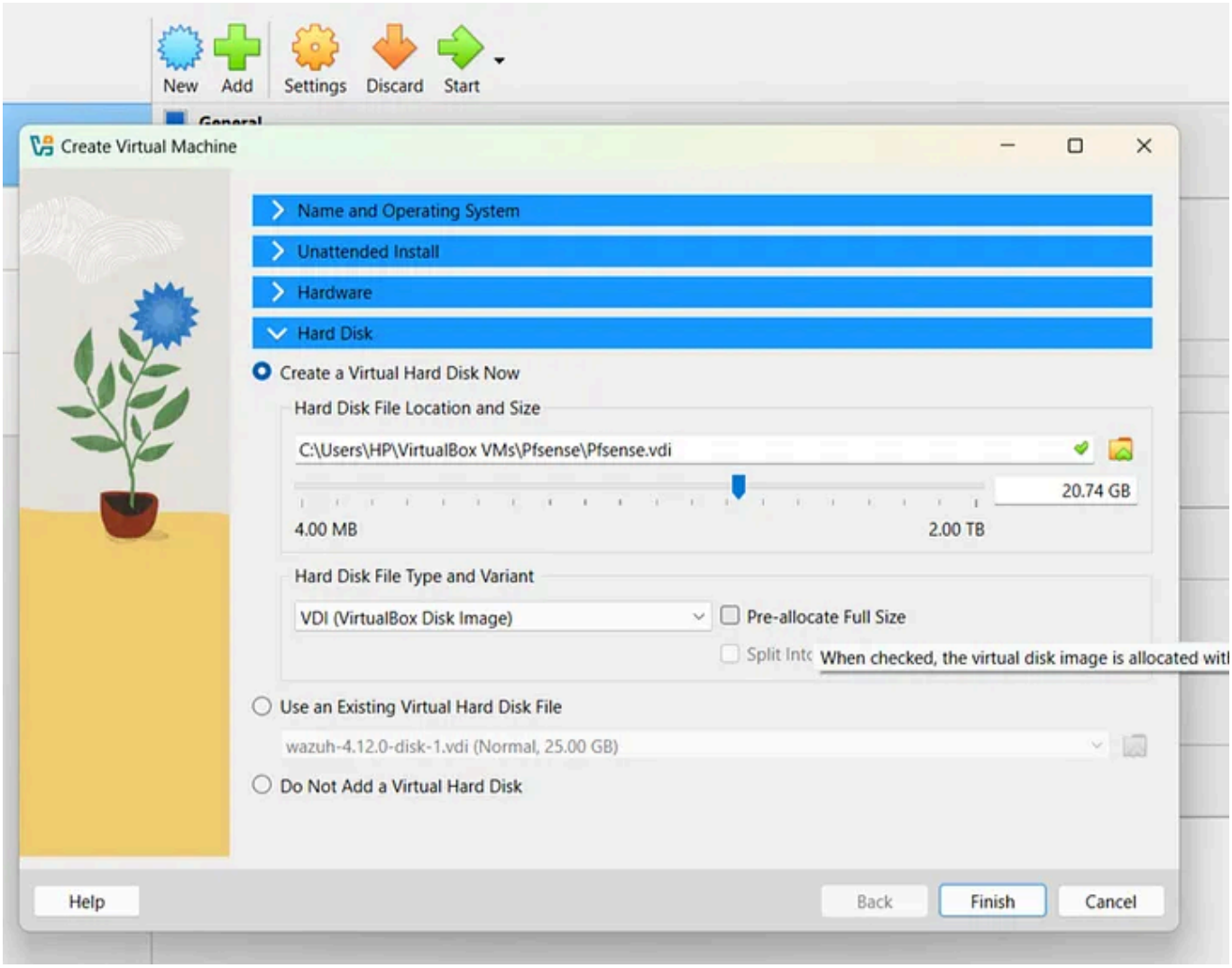

Fig. 7

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.

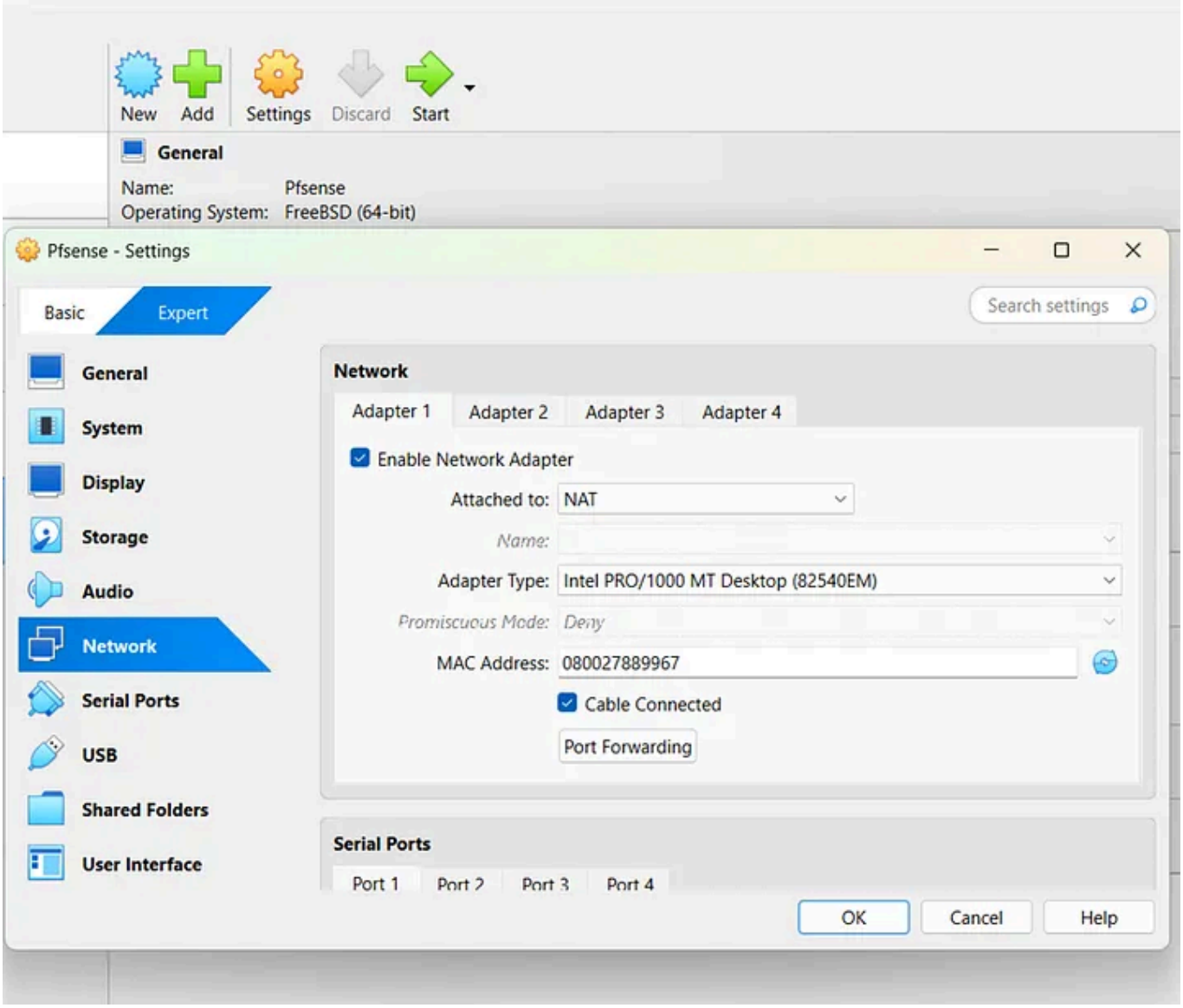
New
Add
Settings
Discard
Start
General
Name: Pfsense
Operating System: FreeBSD (64-bit)
Pfsense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to: NAT
Name:
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 080027889967
Cable Connected
Port Forwarding
Serial Ports
Port 1
Port 2
Port 3
Port 4
OK
Cancel
Help

Fig. 8

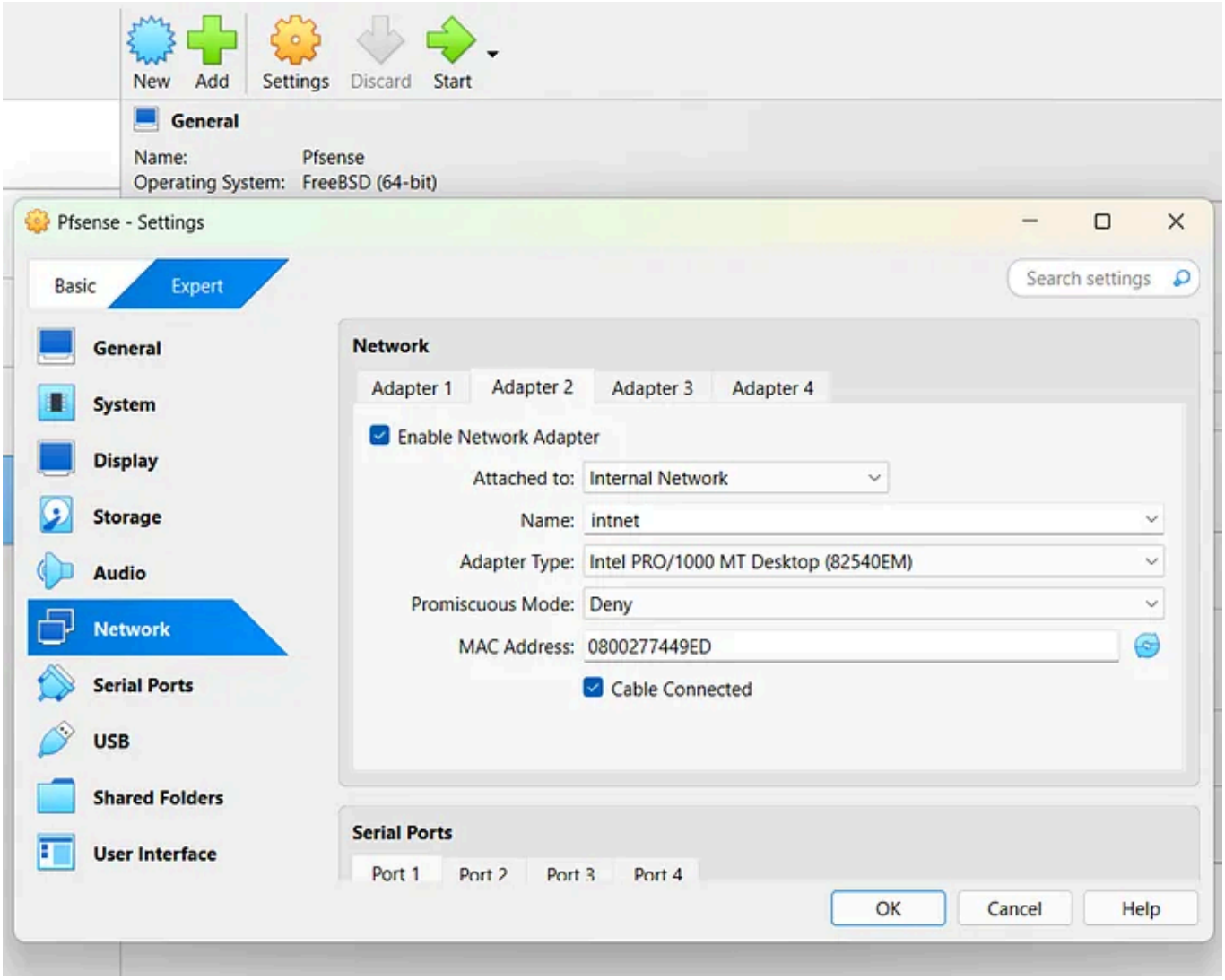

Fig. 9

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).

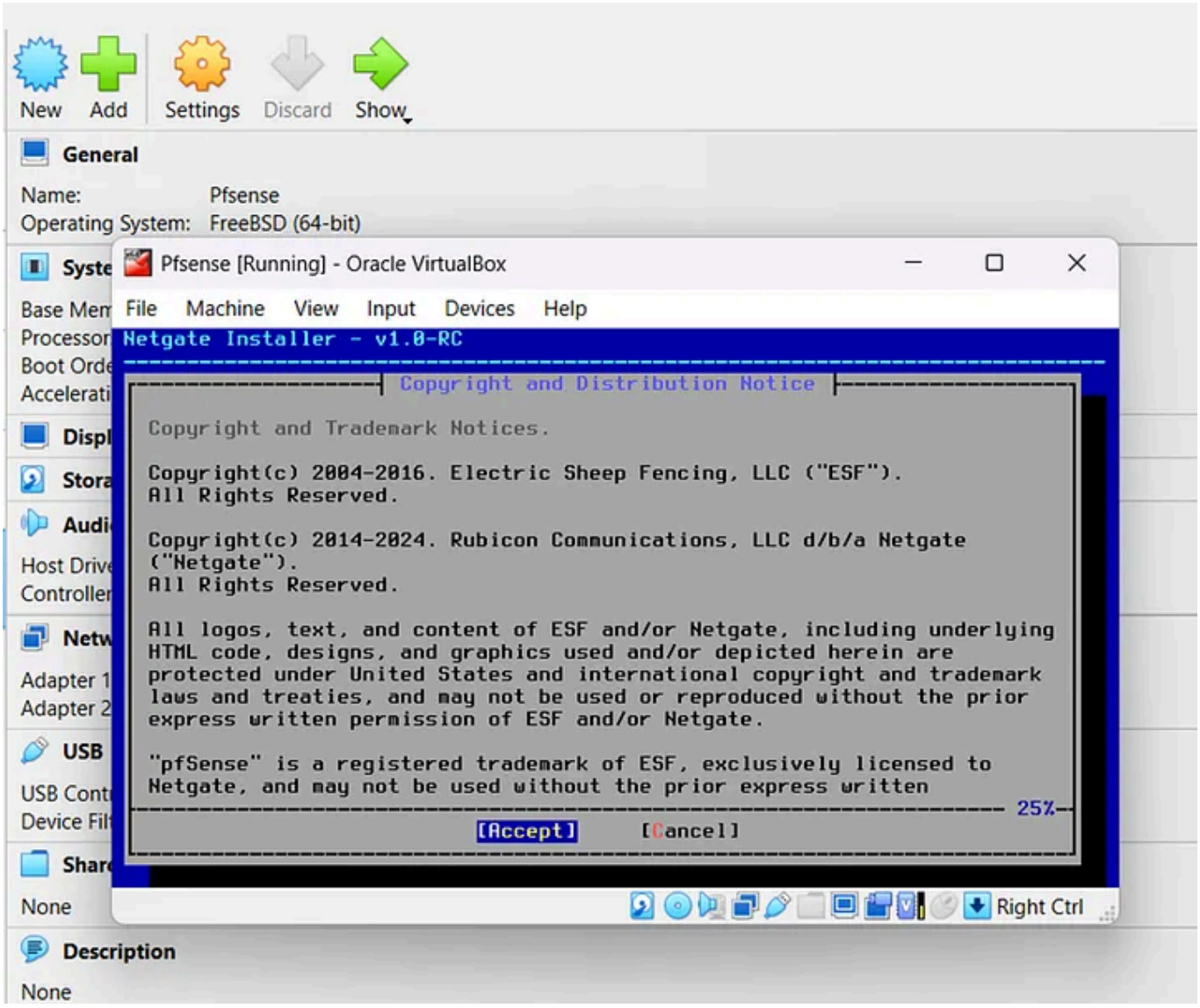

Fig. 10

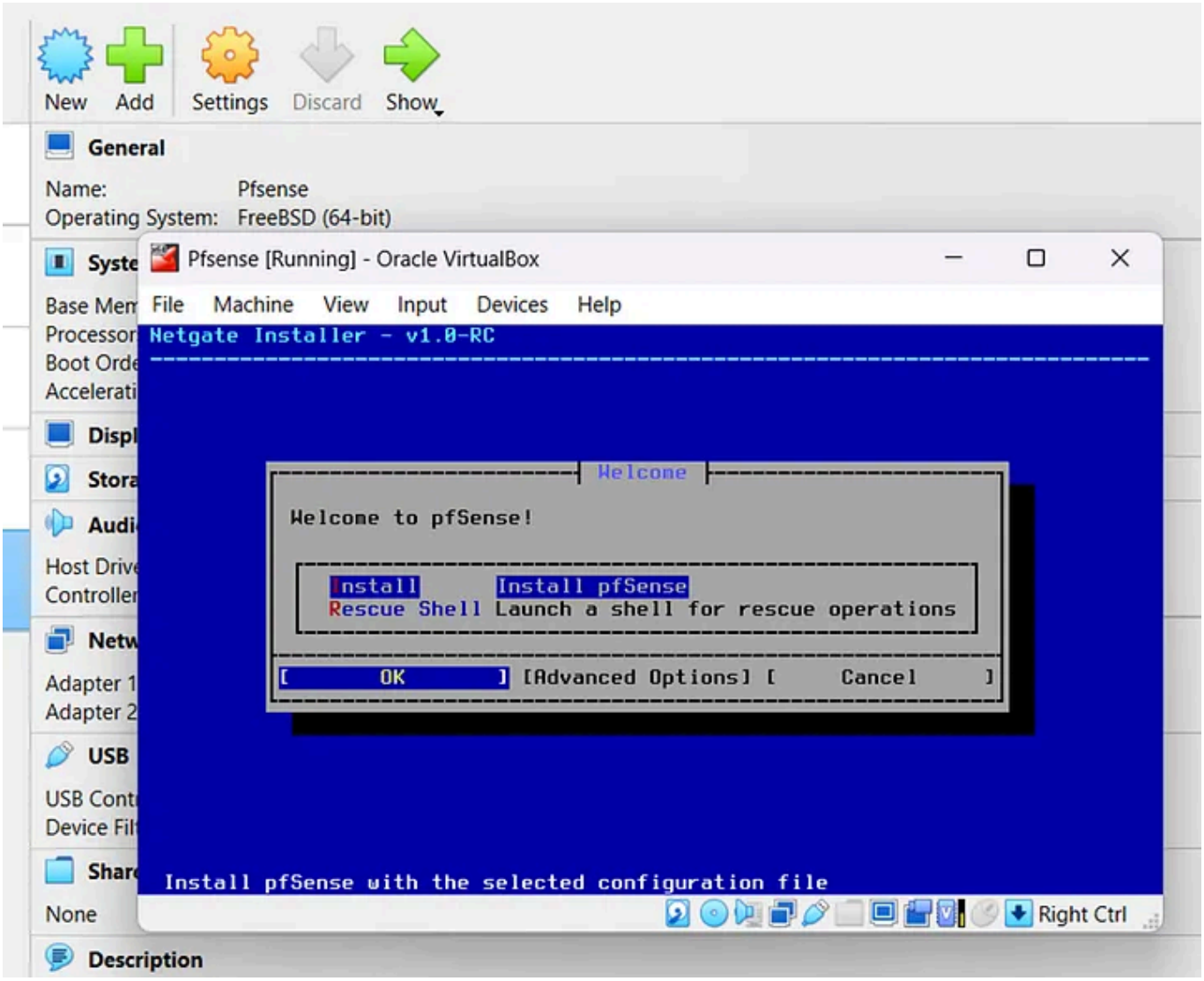

Fig. 11

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

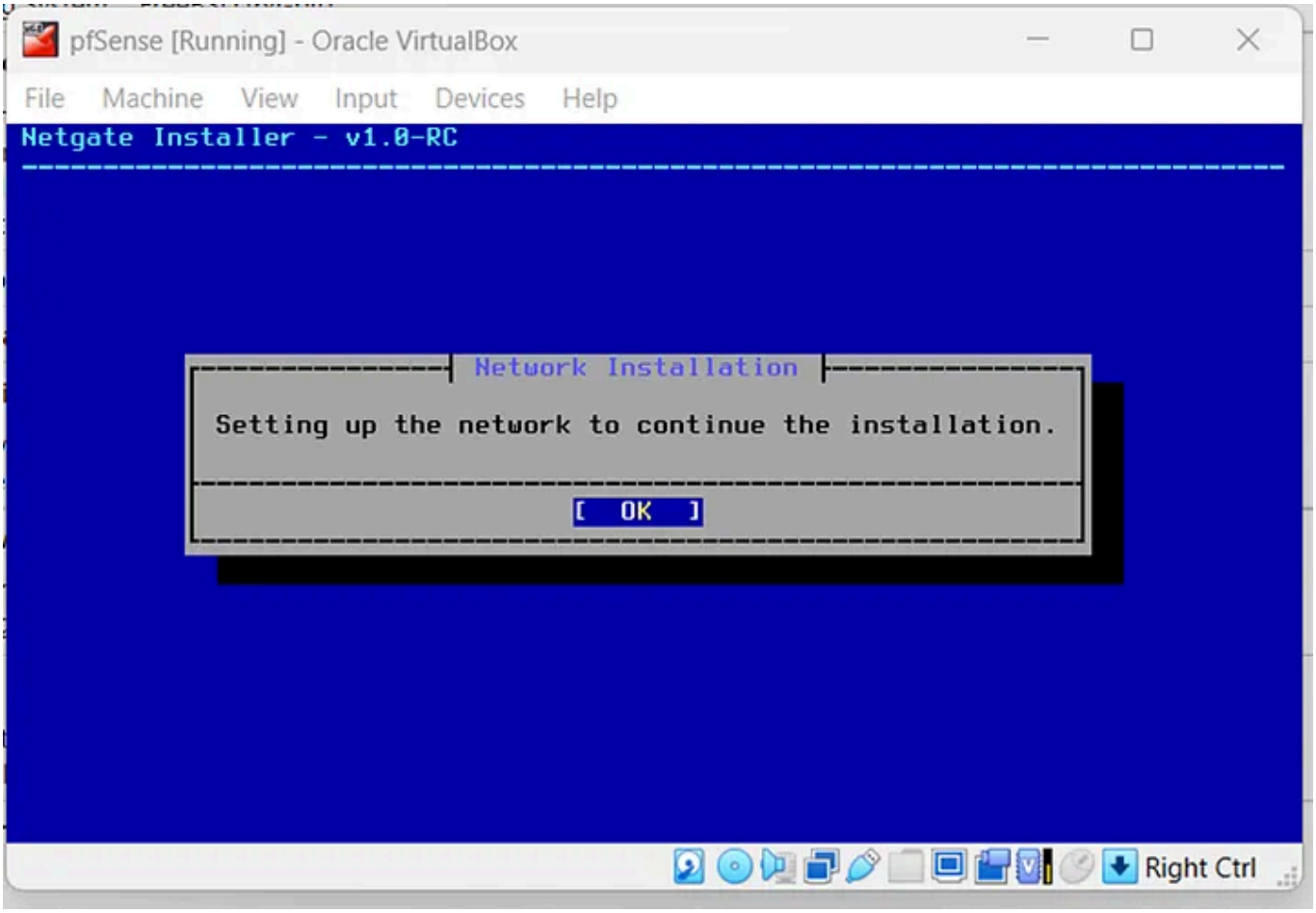

Fig. 12

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).

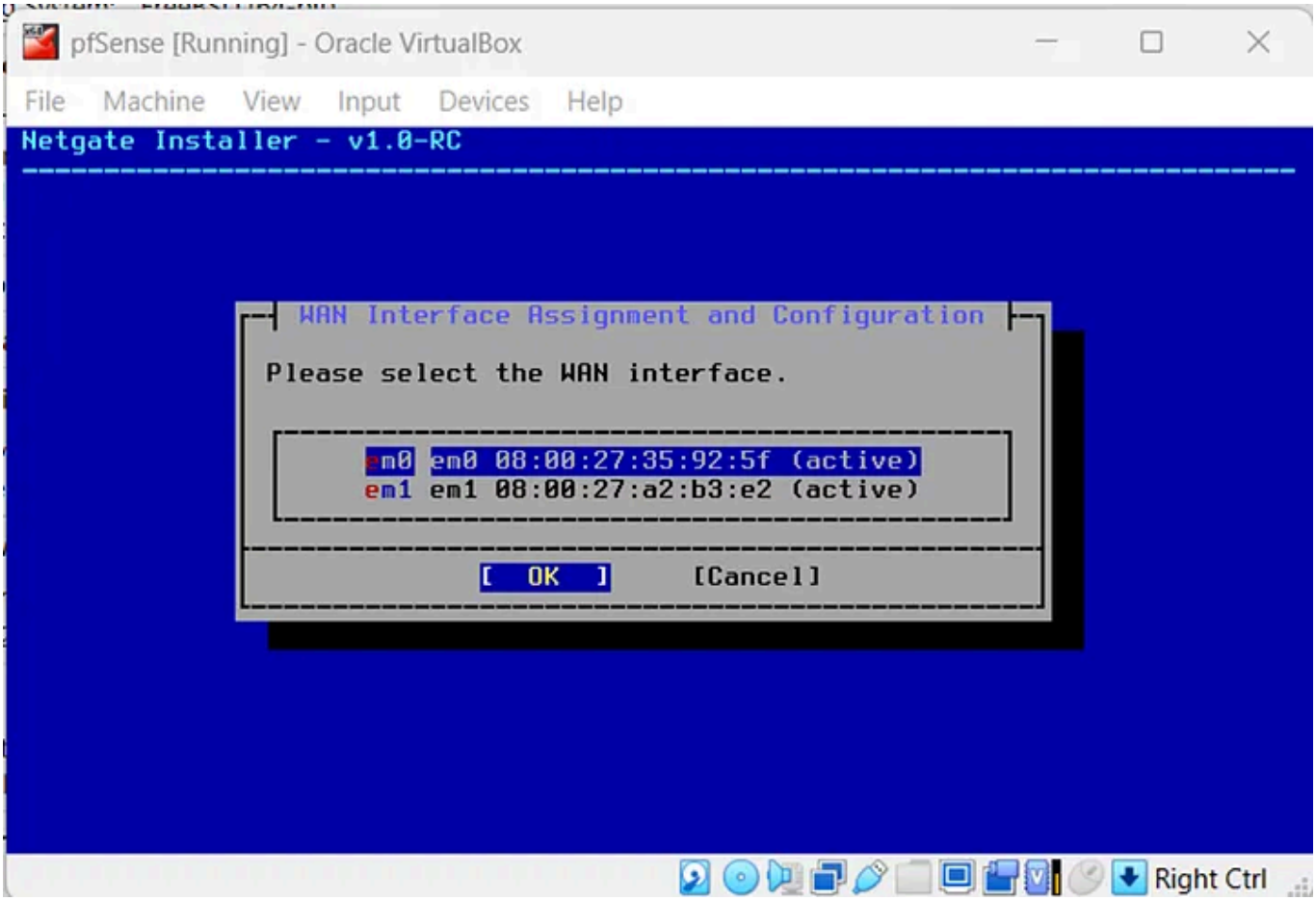

Fig. 13

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

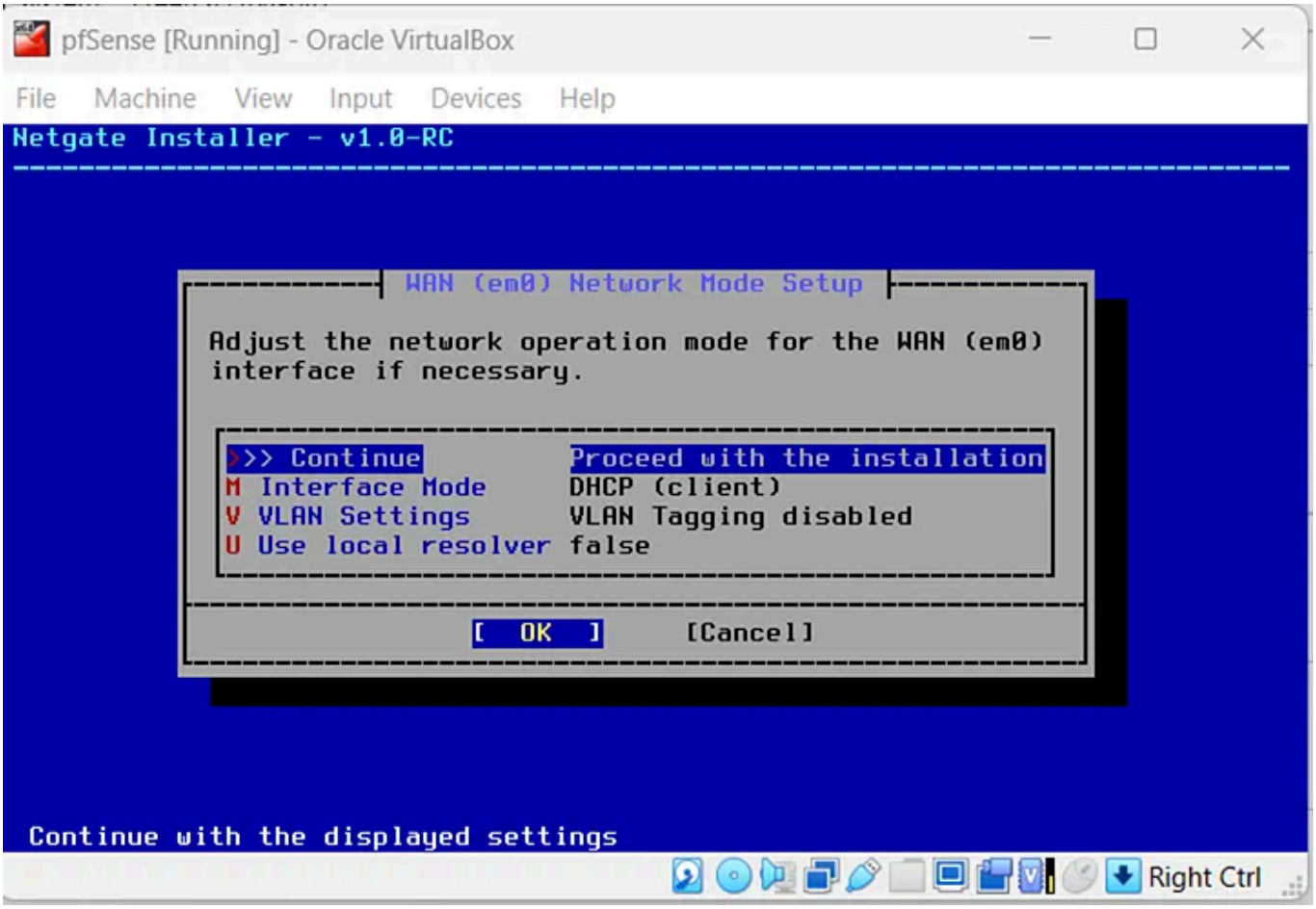

Fig. 14

Next, select the LAN (Fig. 15).

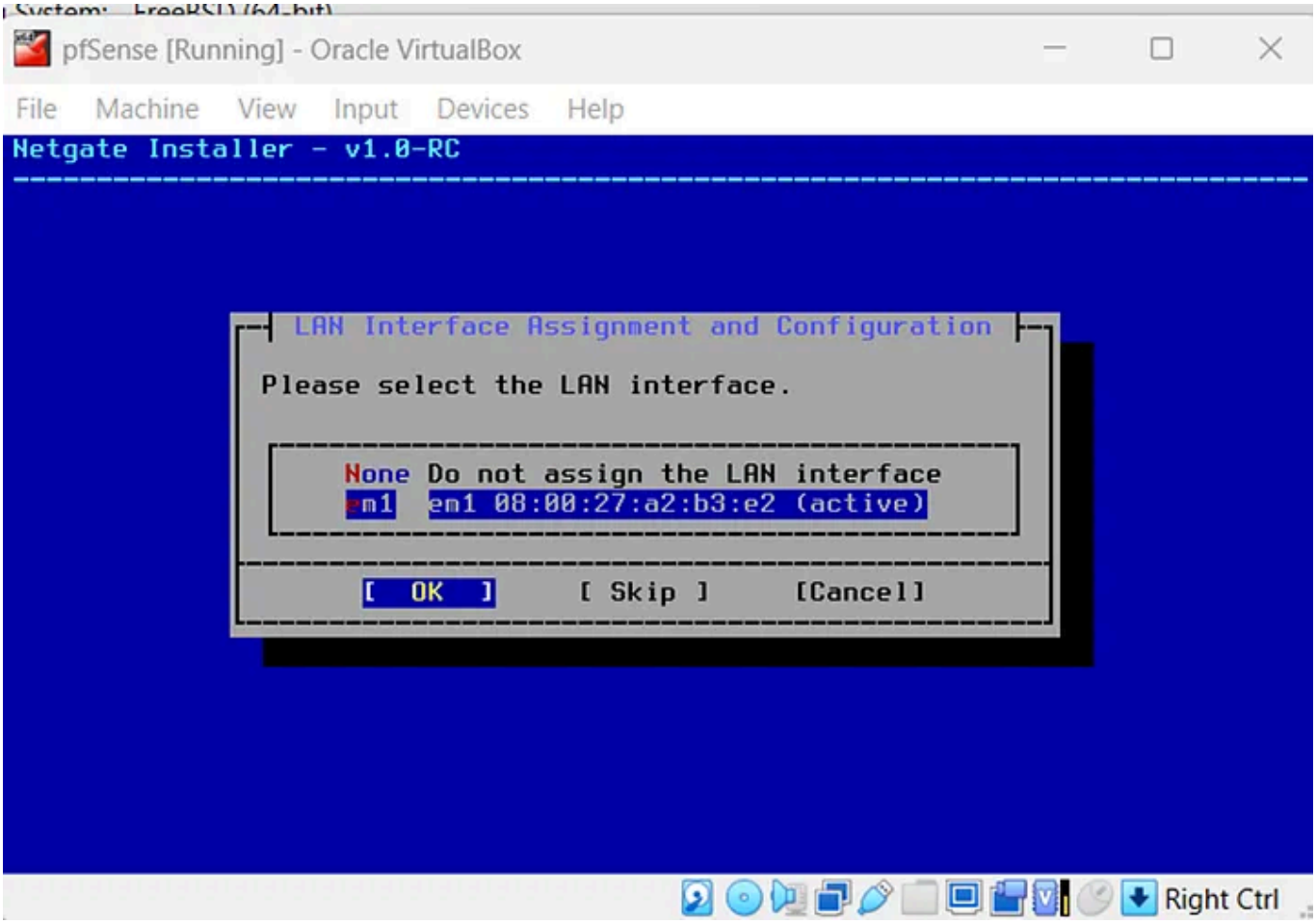

Fig. 15

Proceed with installation (Fig. 16).

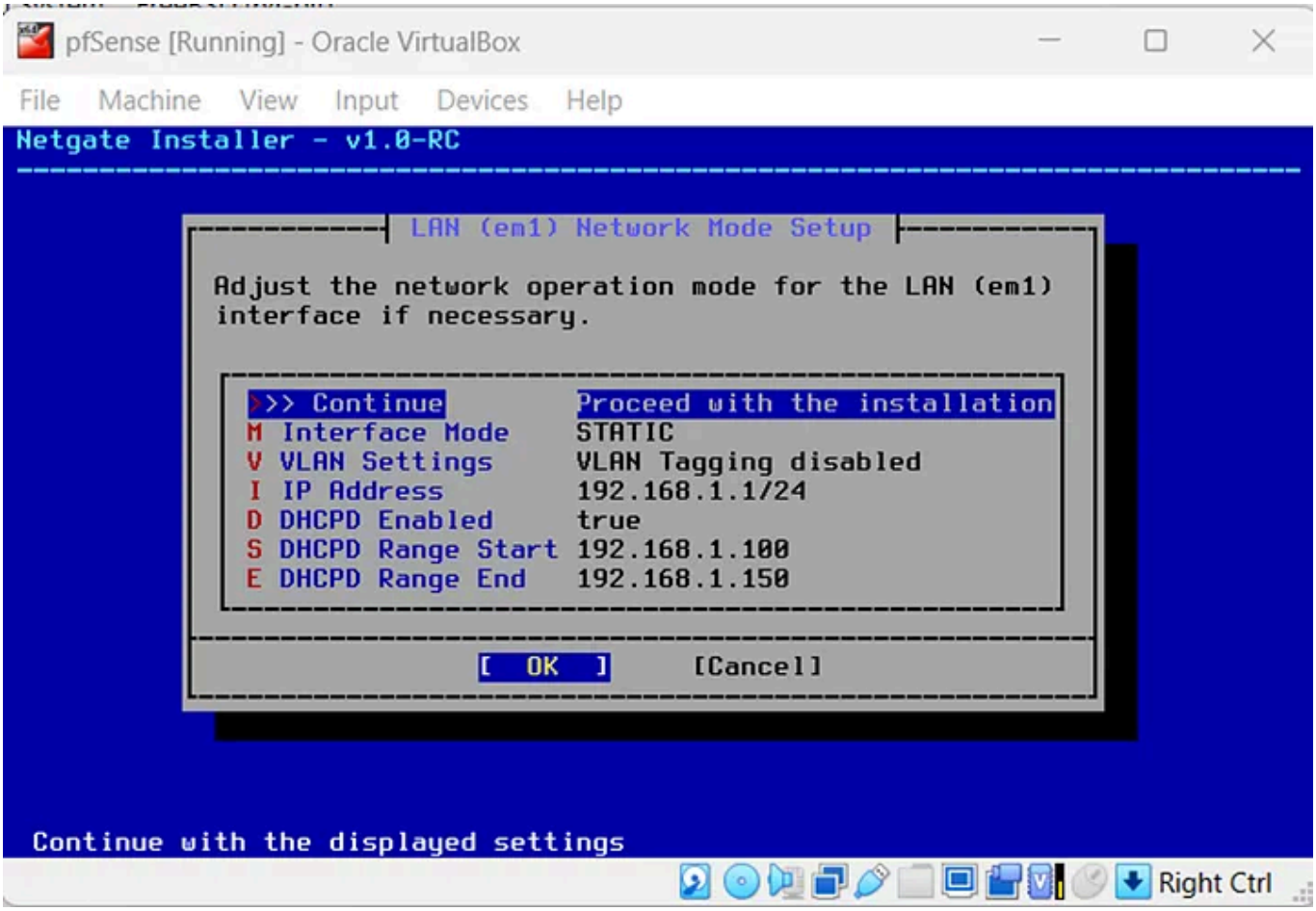

Fig. 16

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

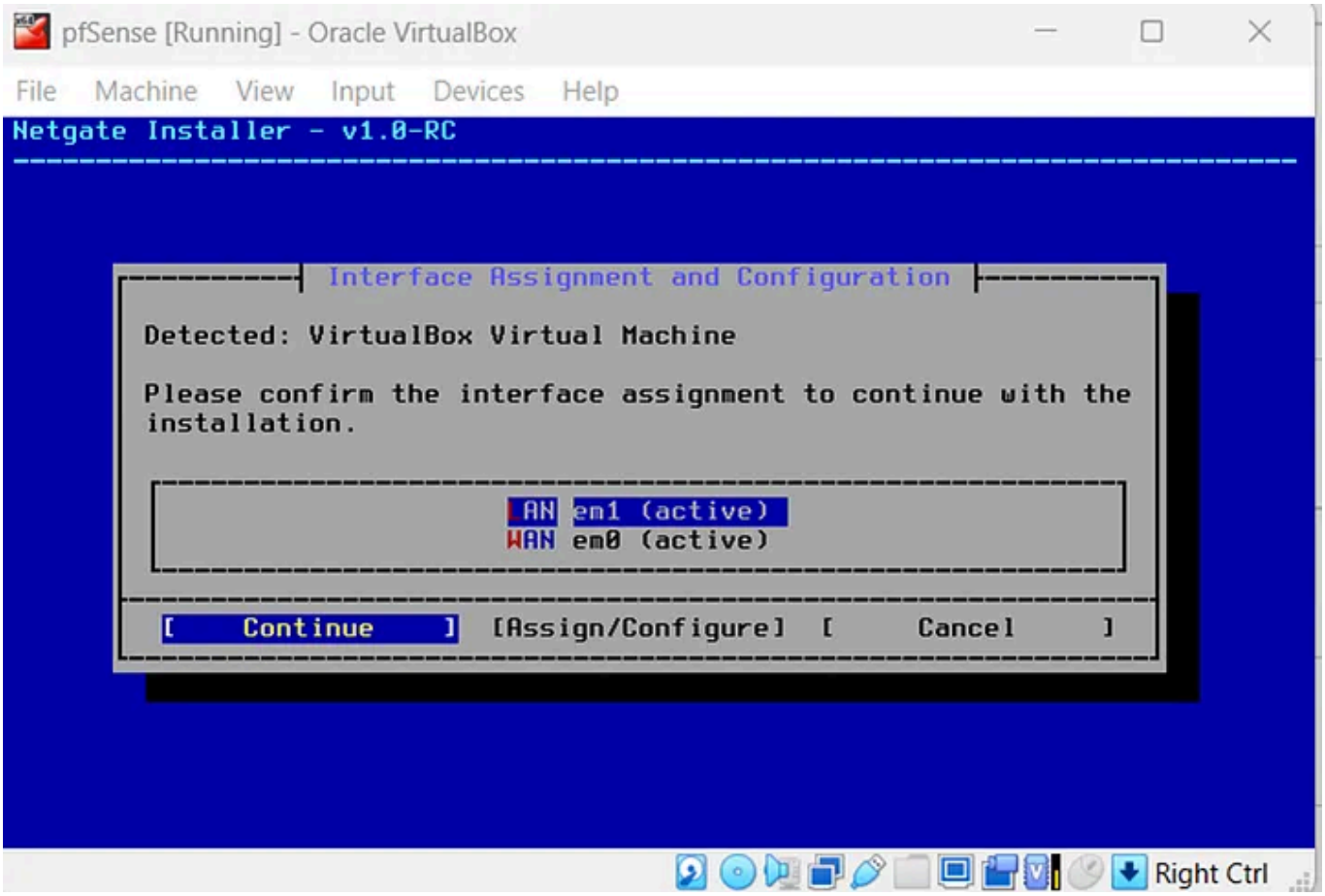

Fig. 17

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.

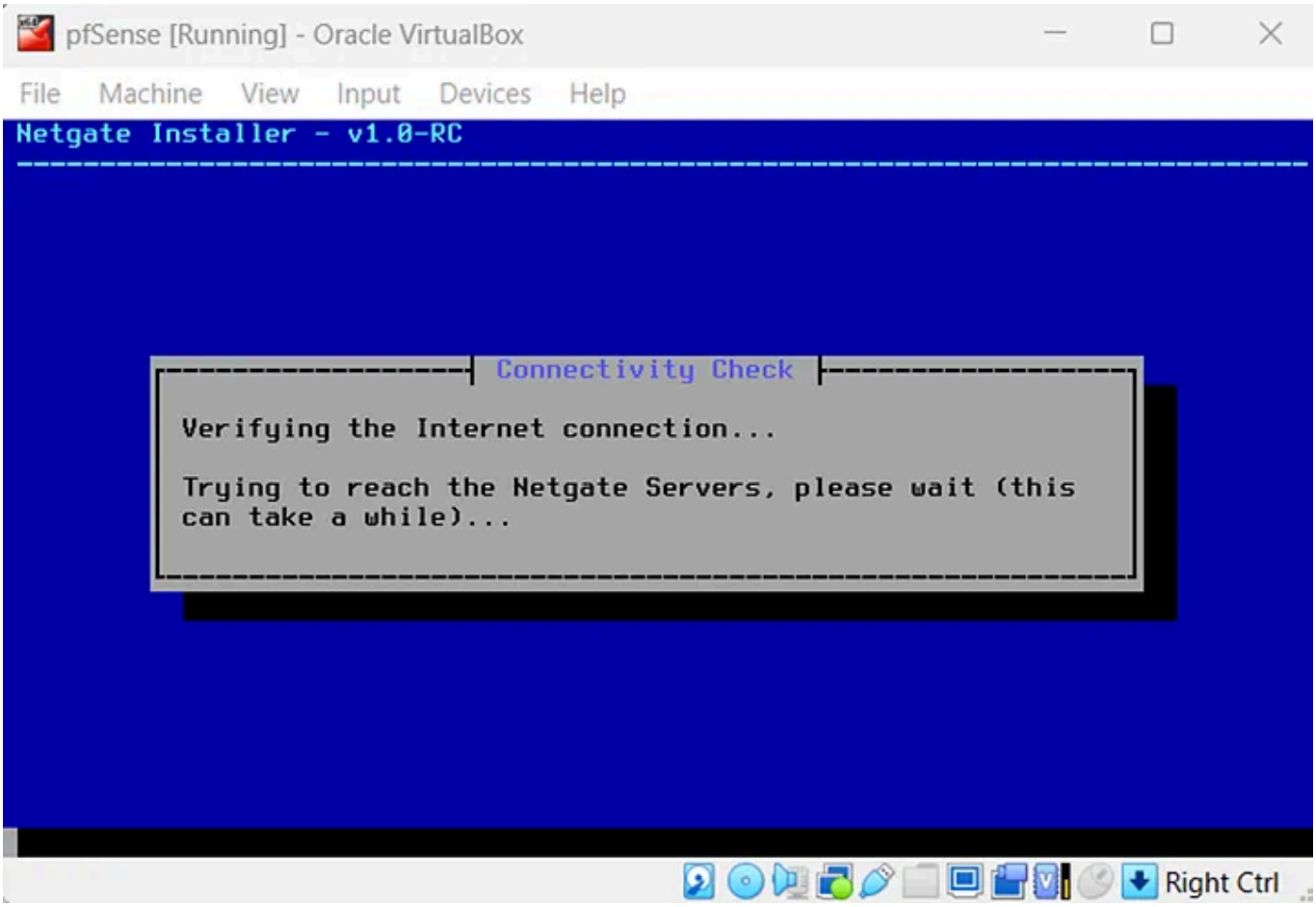
pfSense [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Netgate Installer - v1.0-RC
Connectivity Check
Verifying the Internet connection...
Trying to reach the Netgate Servers, please wait (this can take a while)...
Right Ctrl

Fig. 18

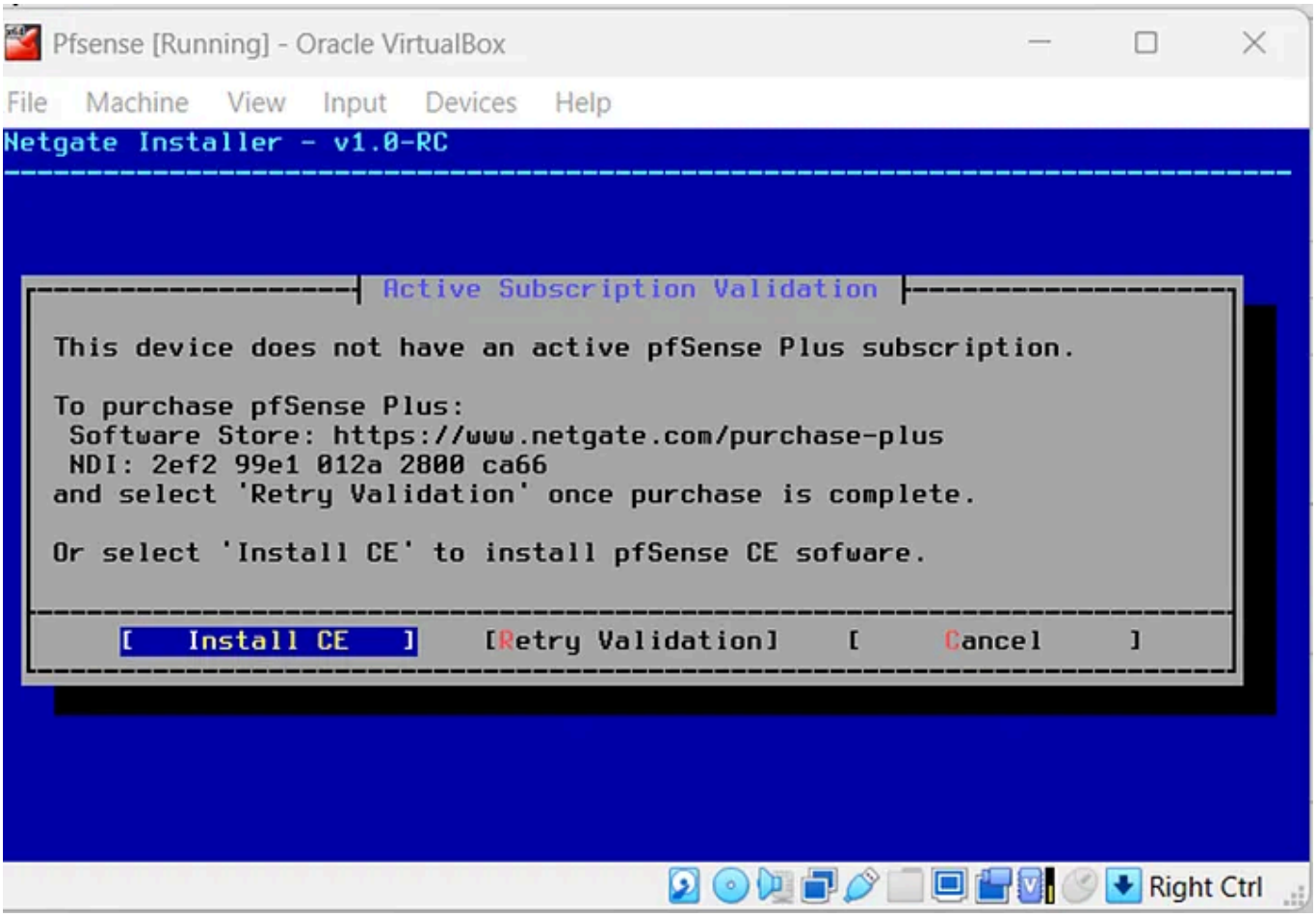

Fig. 19

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

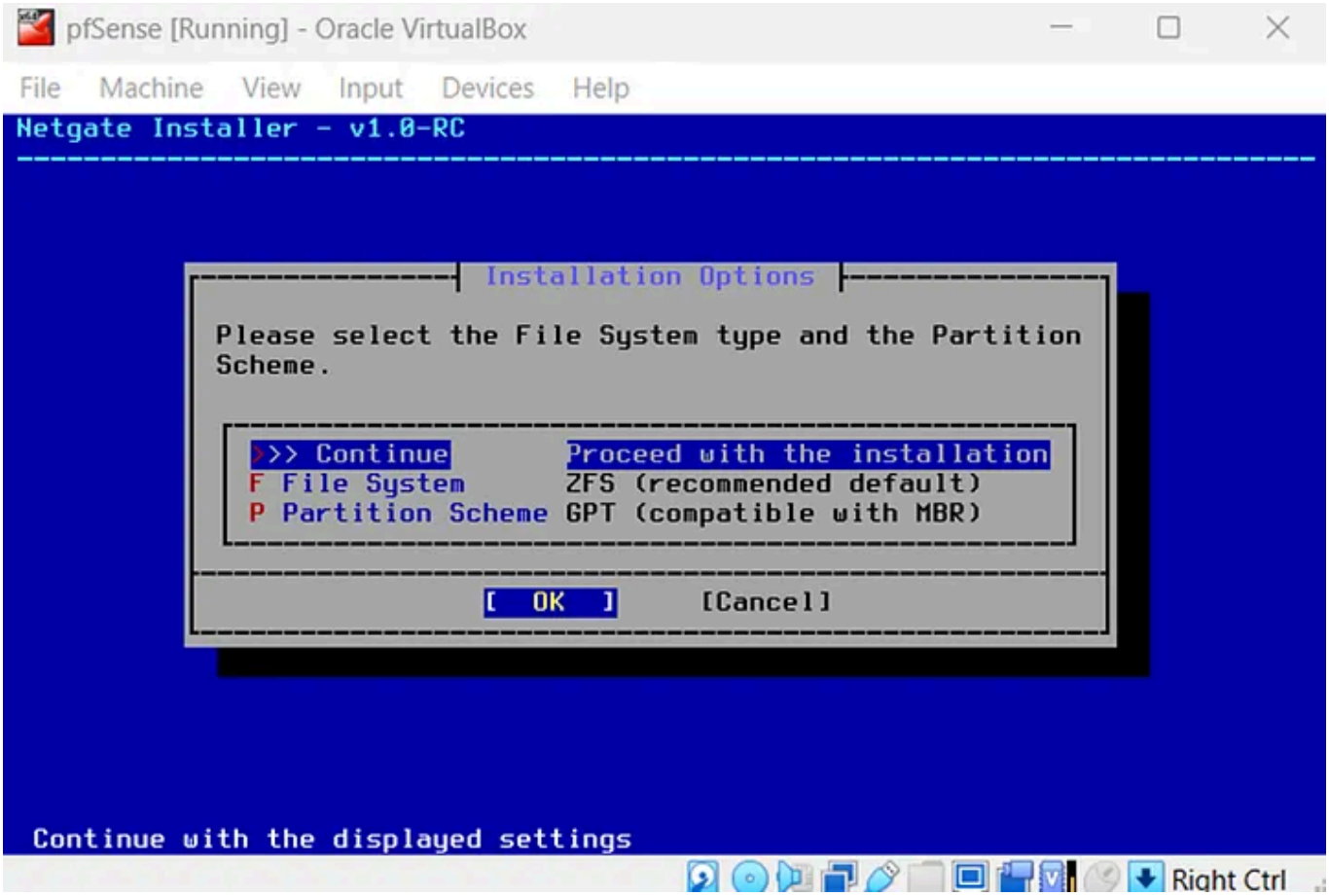

Fig. 20

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

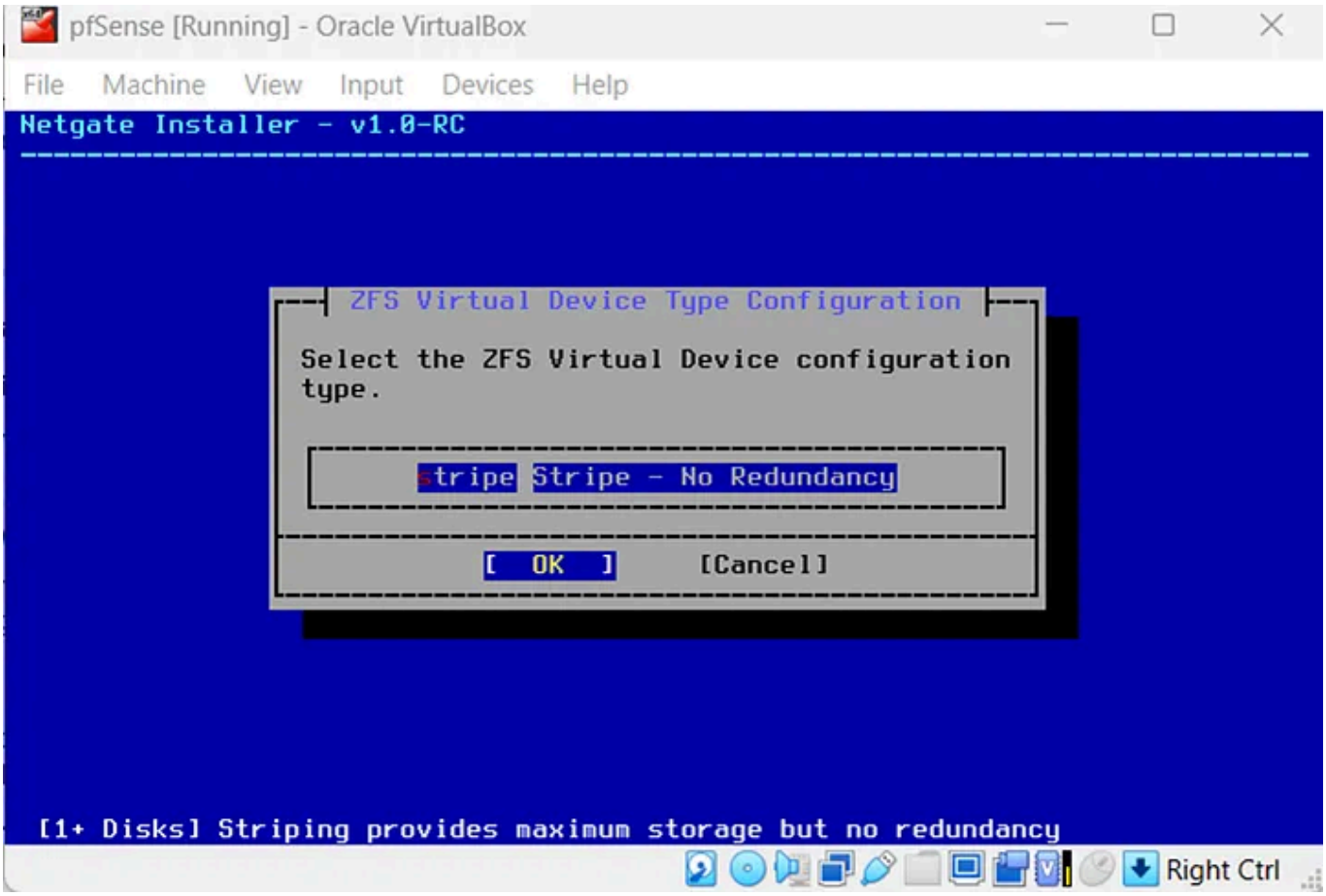

Fig. 21

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

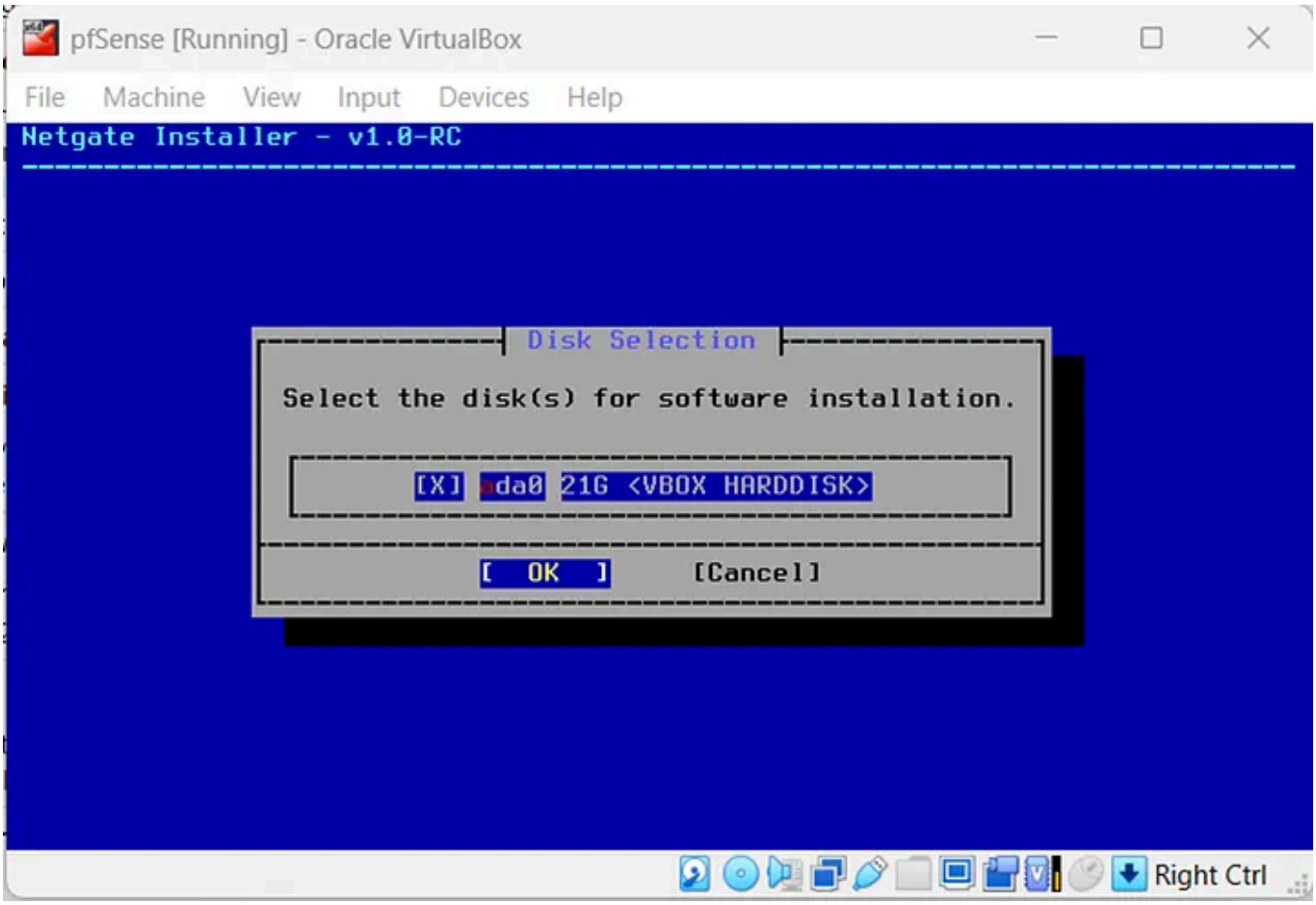

Fig. 22

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

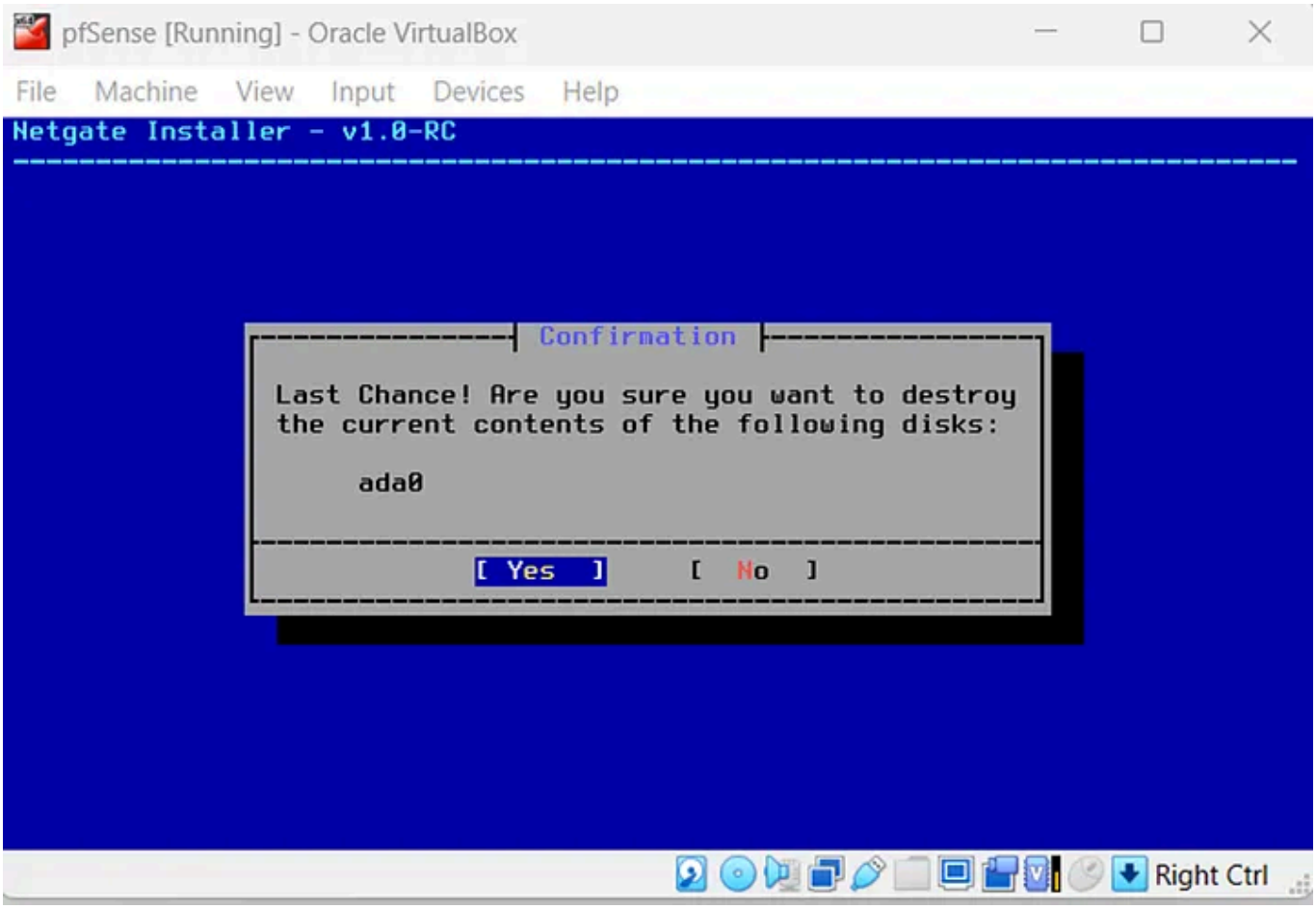

Fig. 23

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).

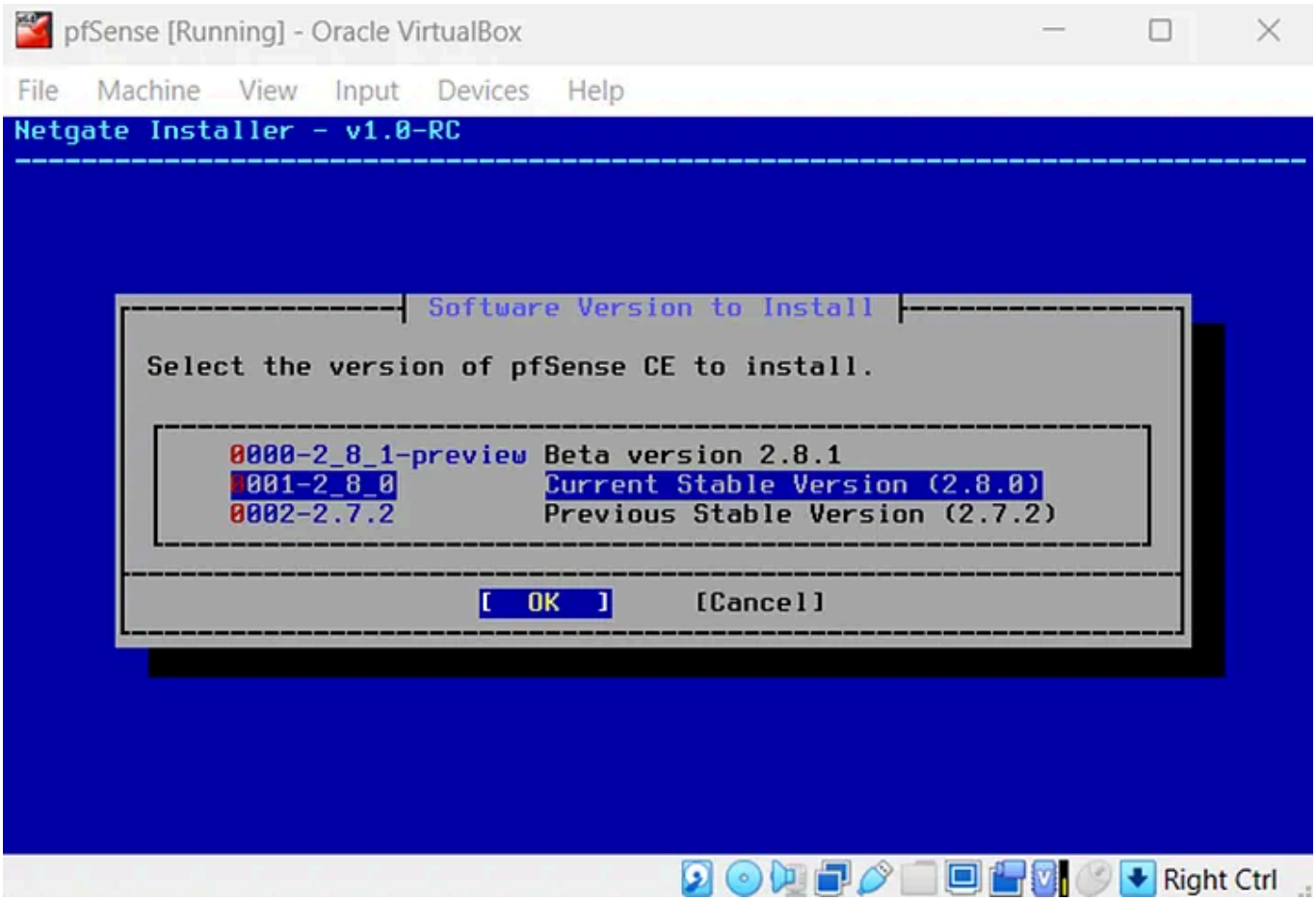

Fig. 24

The installation will then begin (Fig. 25).

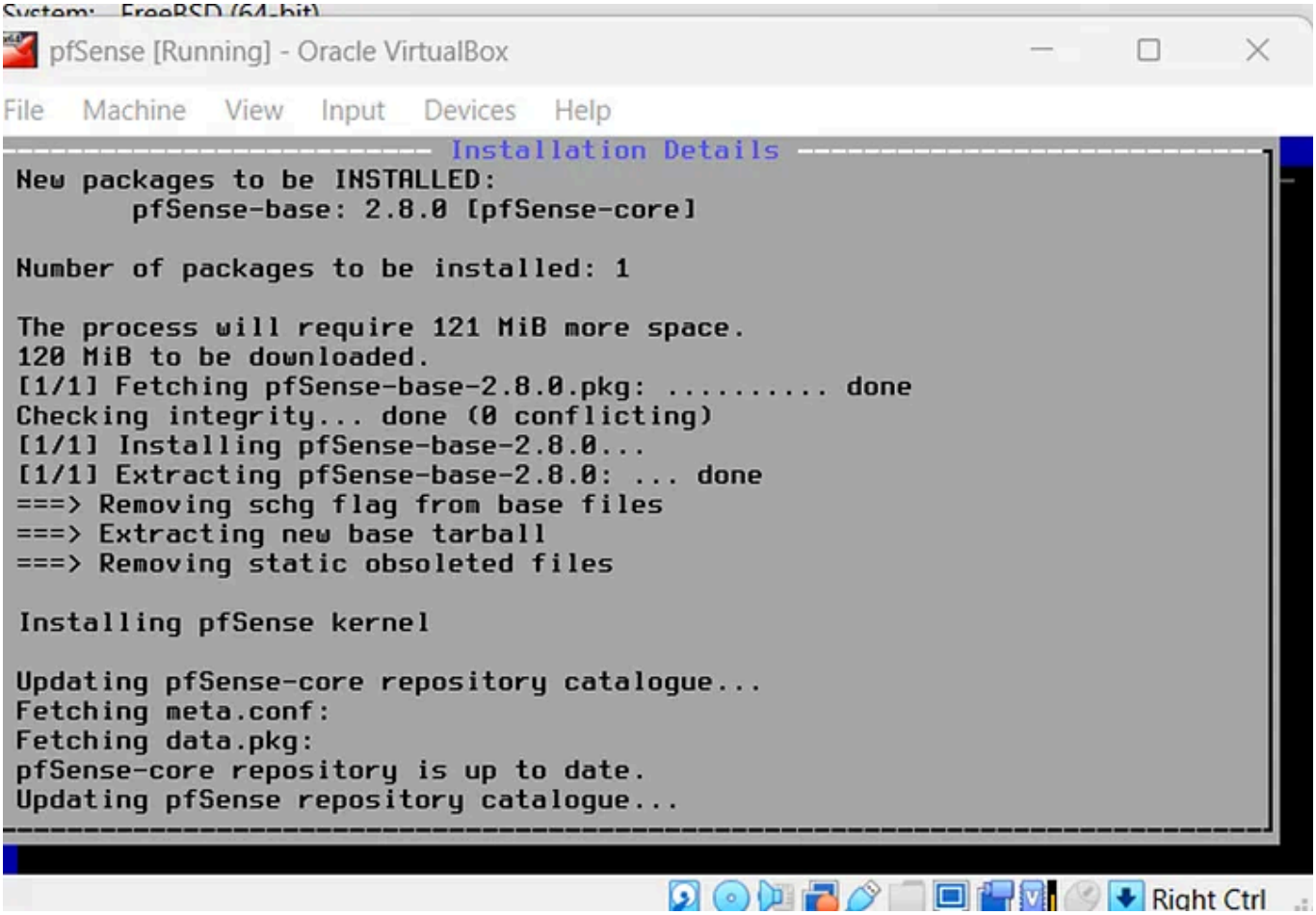

Fig. 25

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)

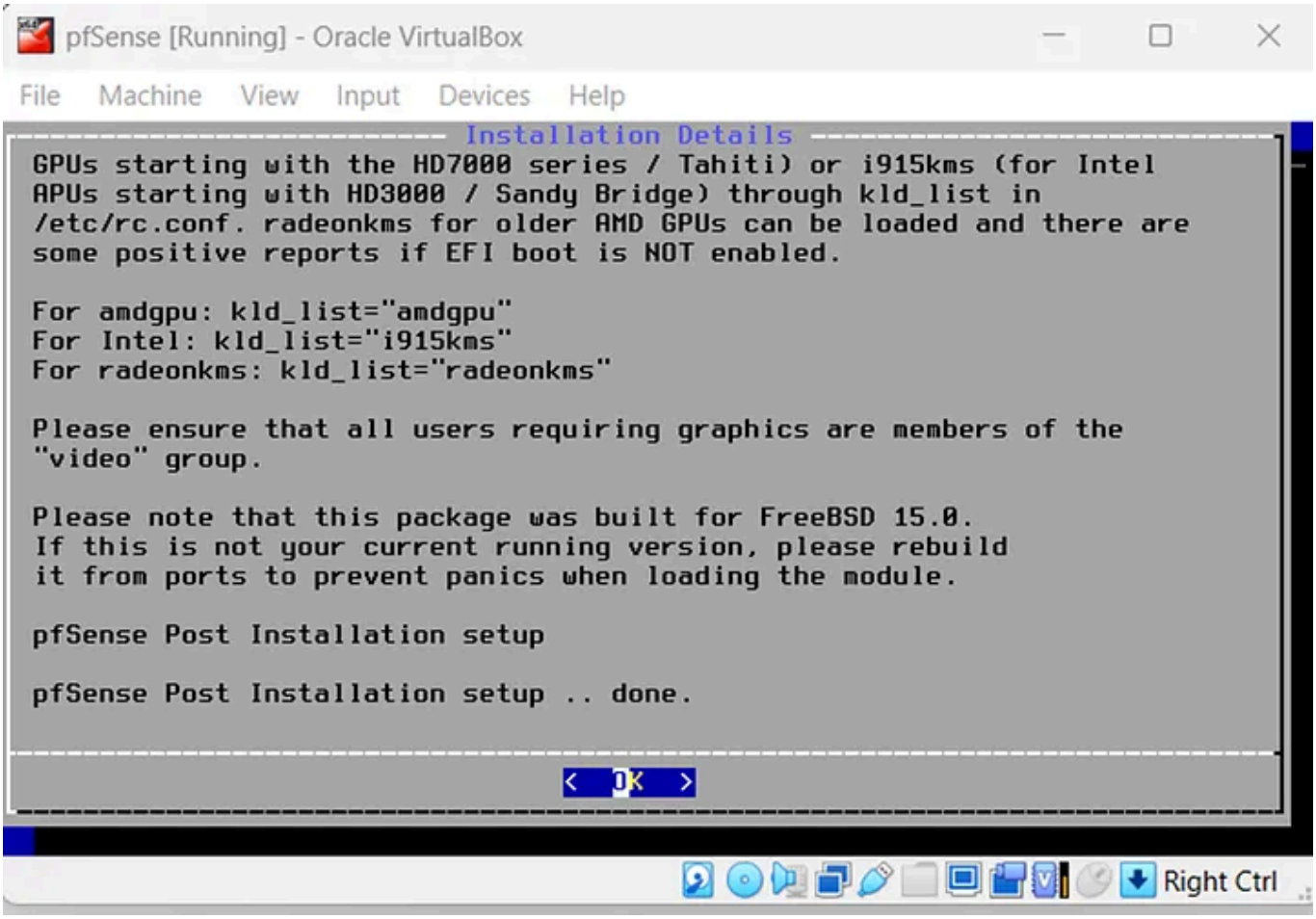

Fig. 26

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

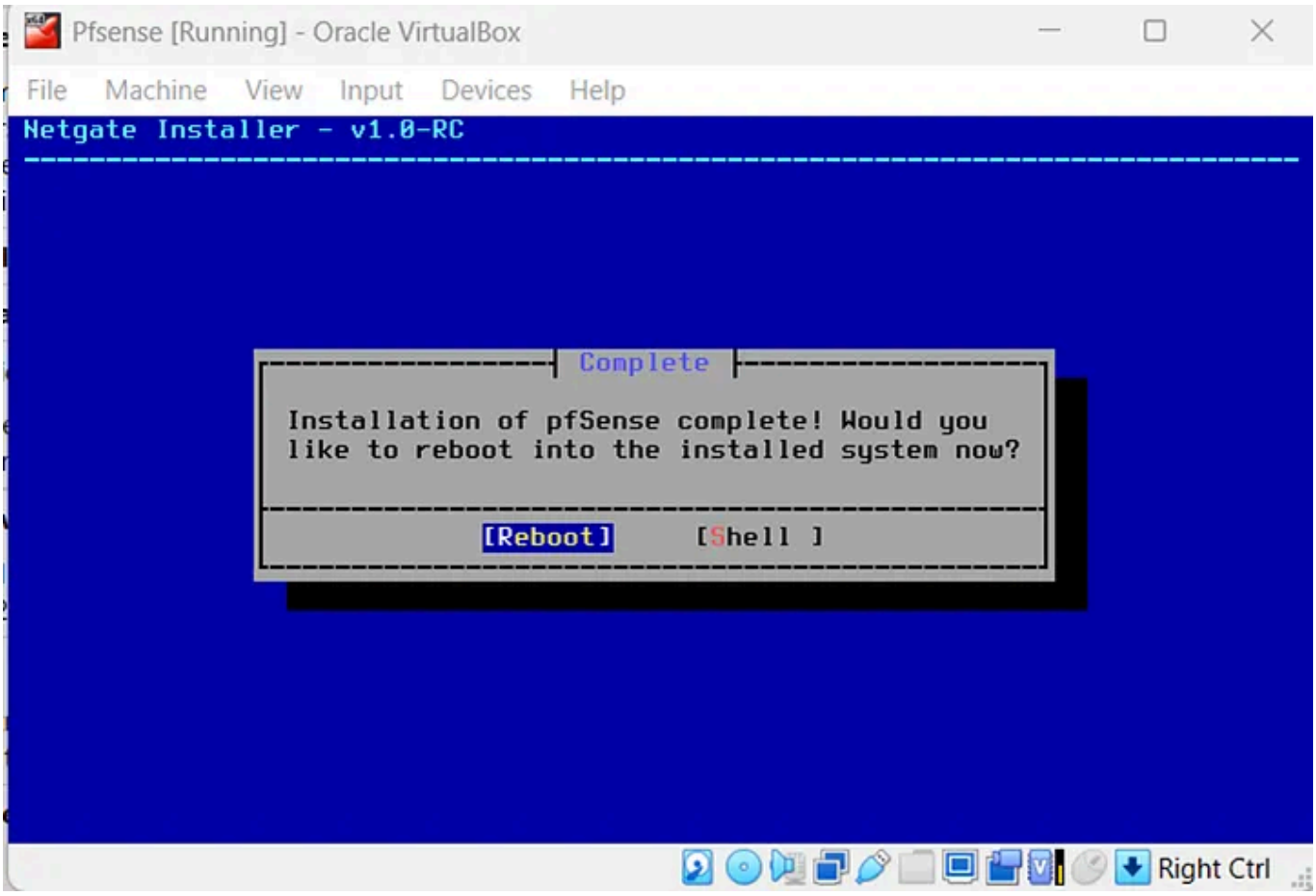

Fig. 27

Power of 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).

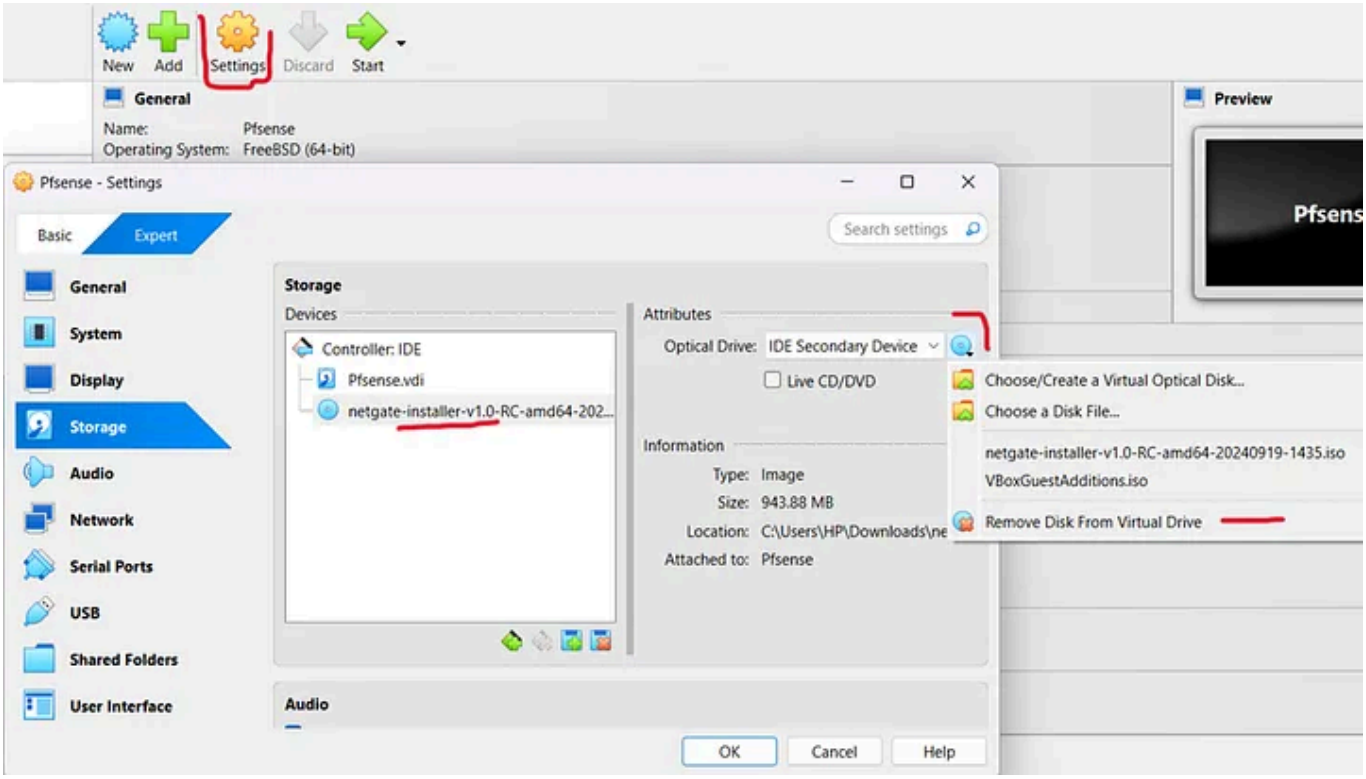

Fig. 28

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).

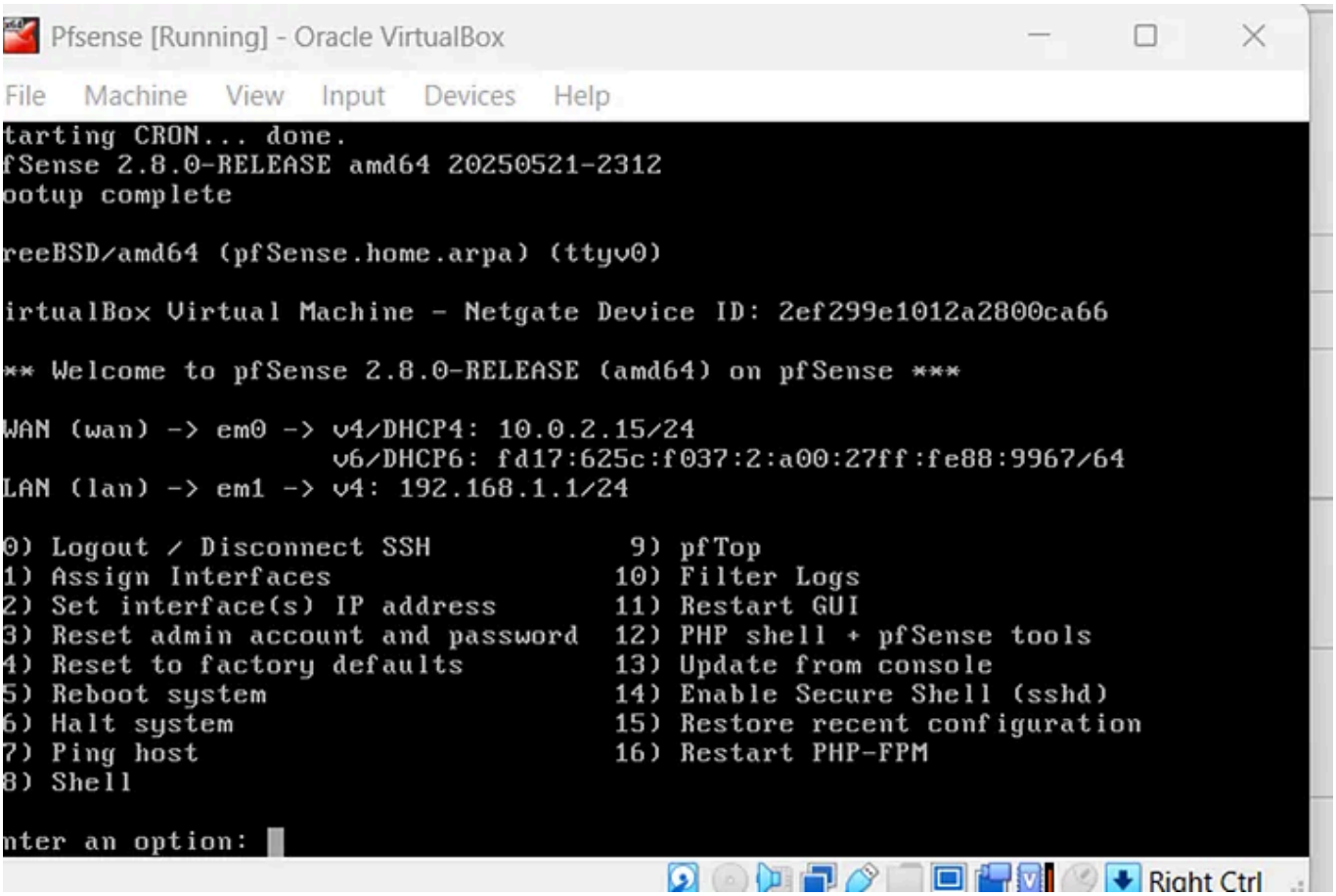

Fig. 29

> *# 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).

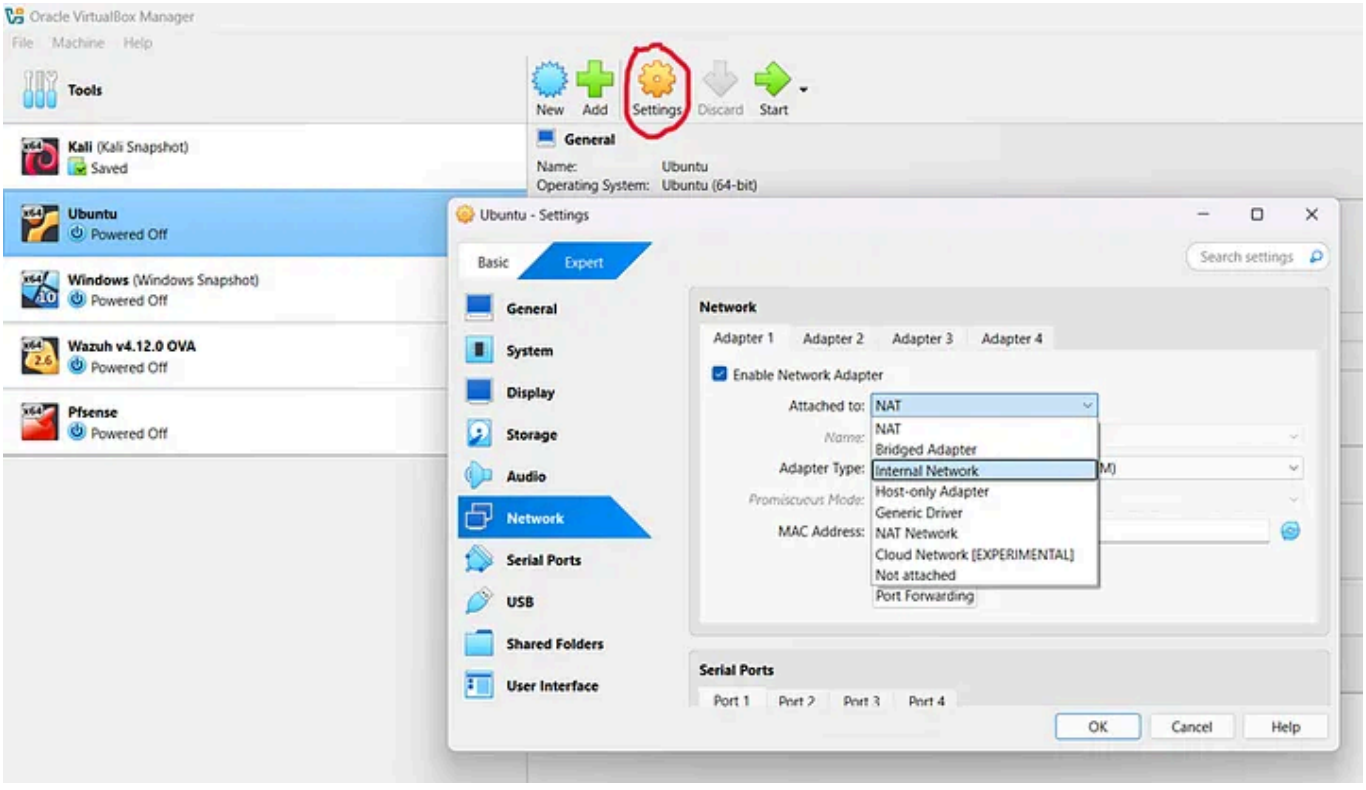

Fig. 30

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).

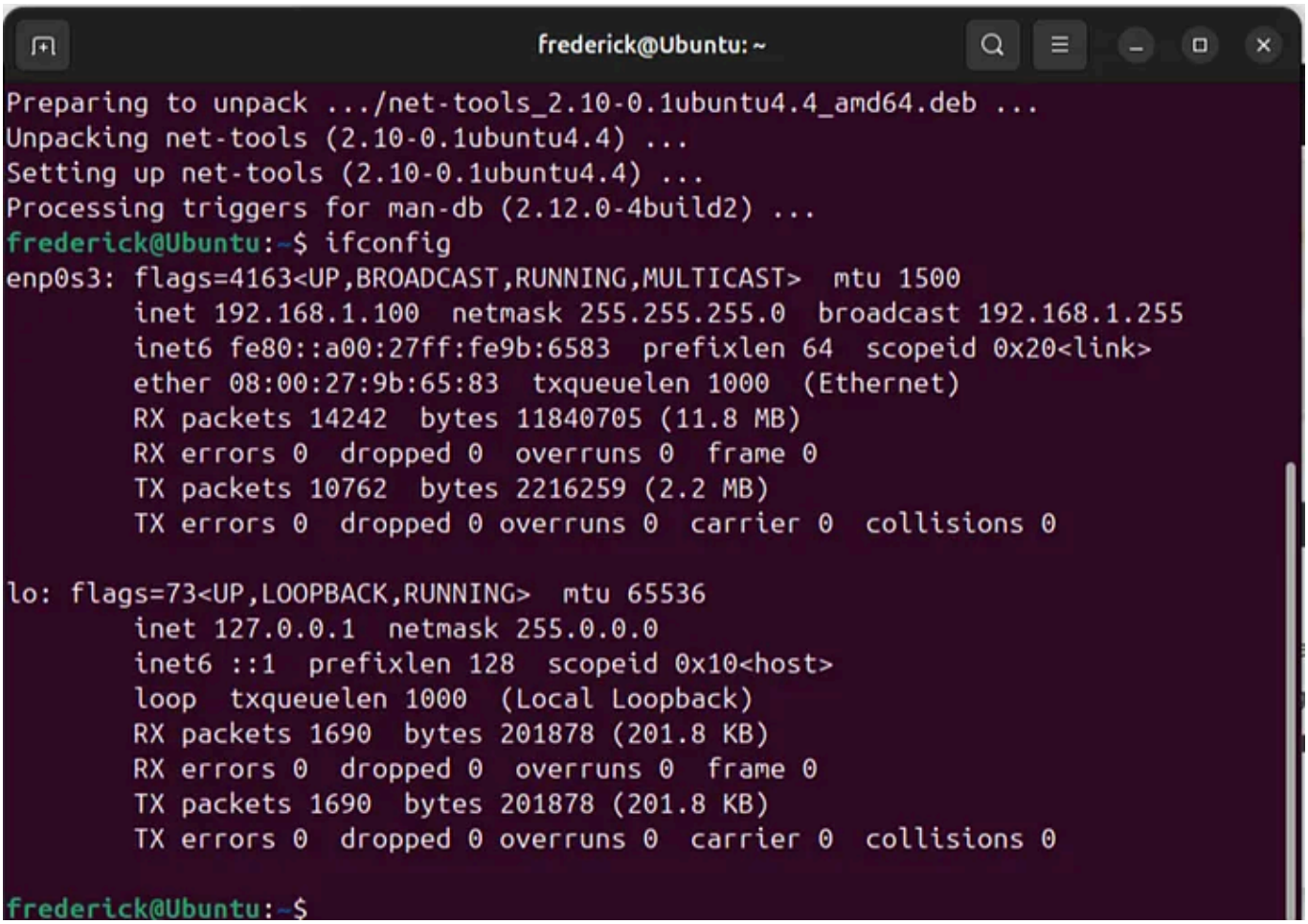

Fig. 31

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).

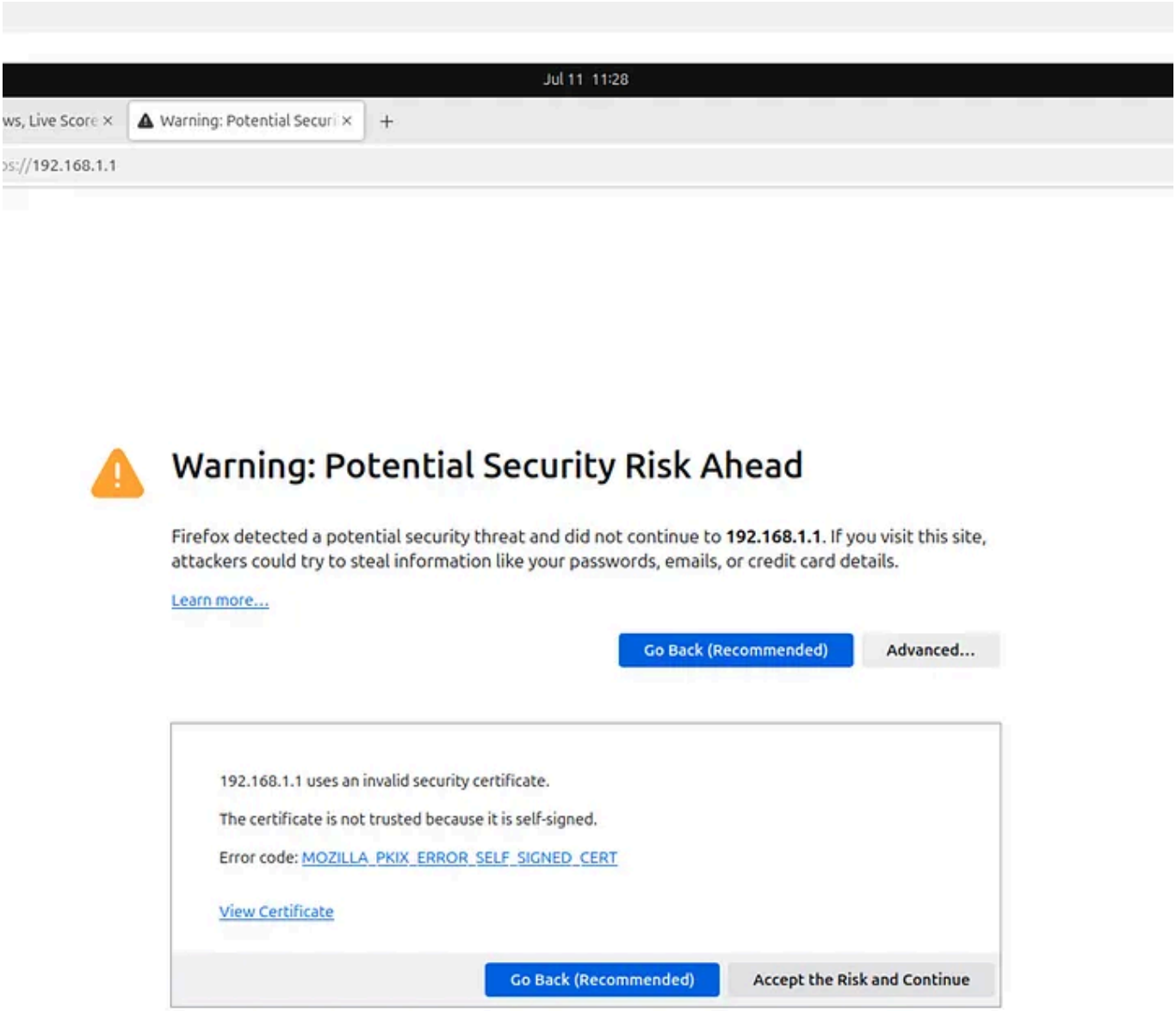

Fig. 32

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).

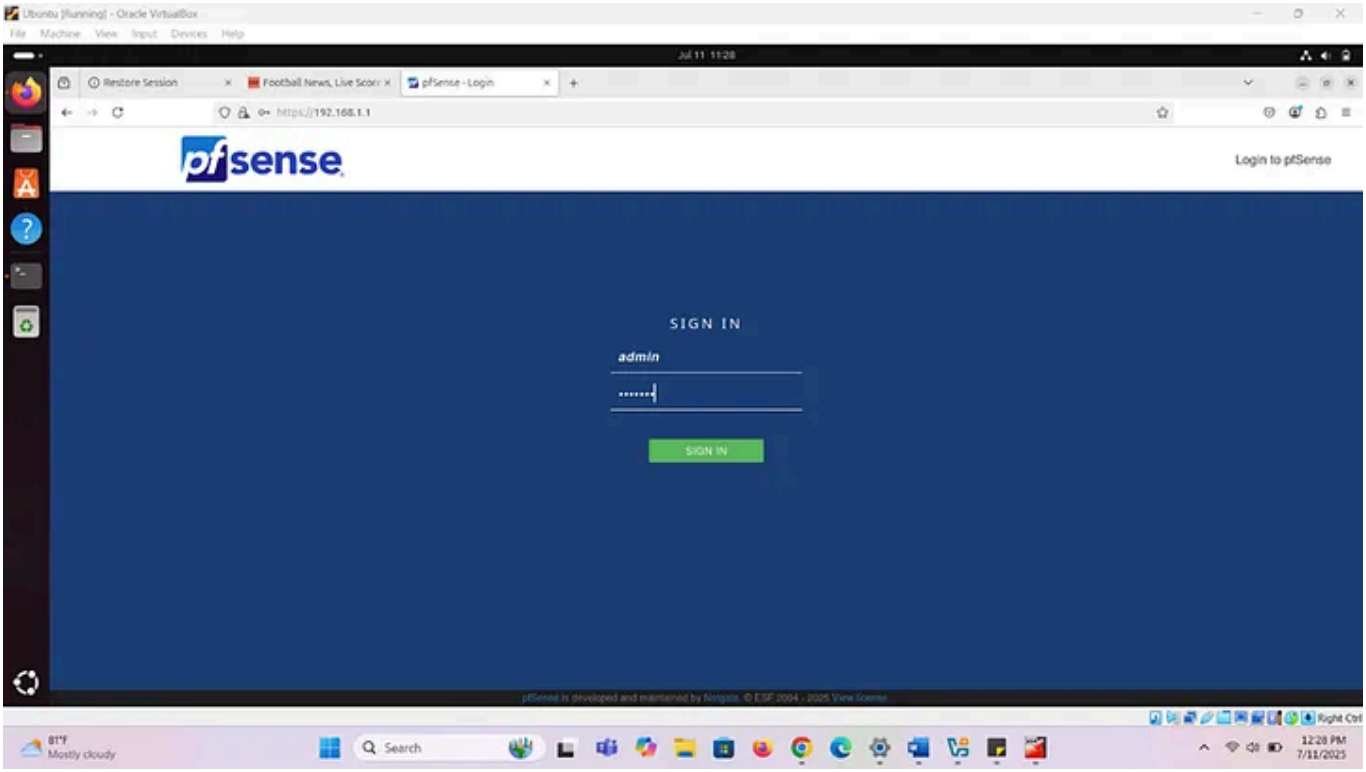

Fig. 33

The homepage loads (Fig. 34).

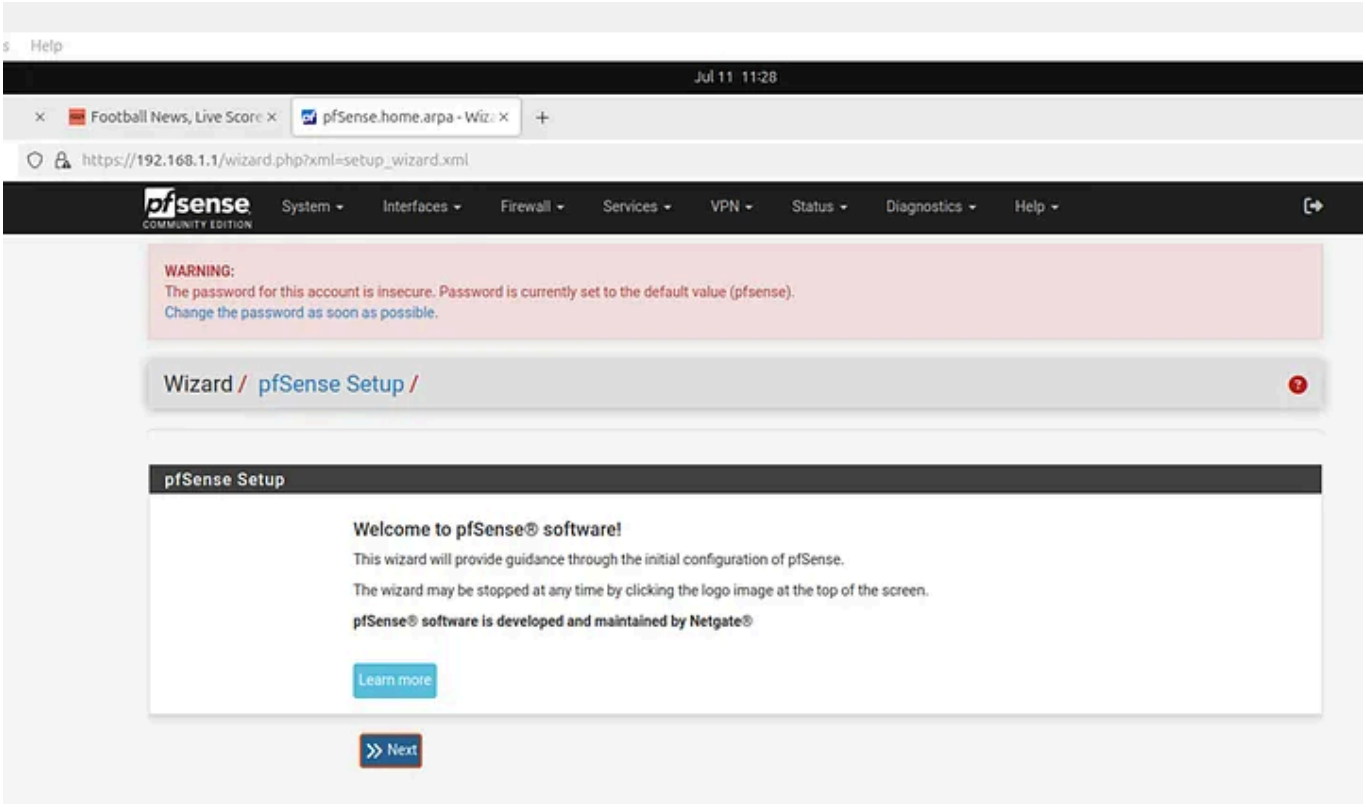

Fig. 34

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).

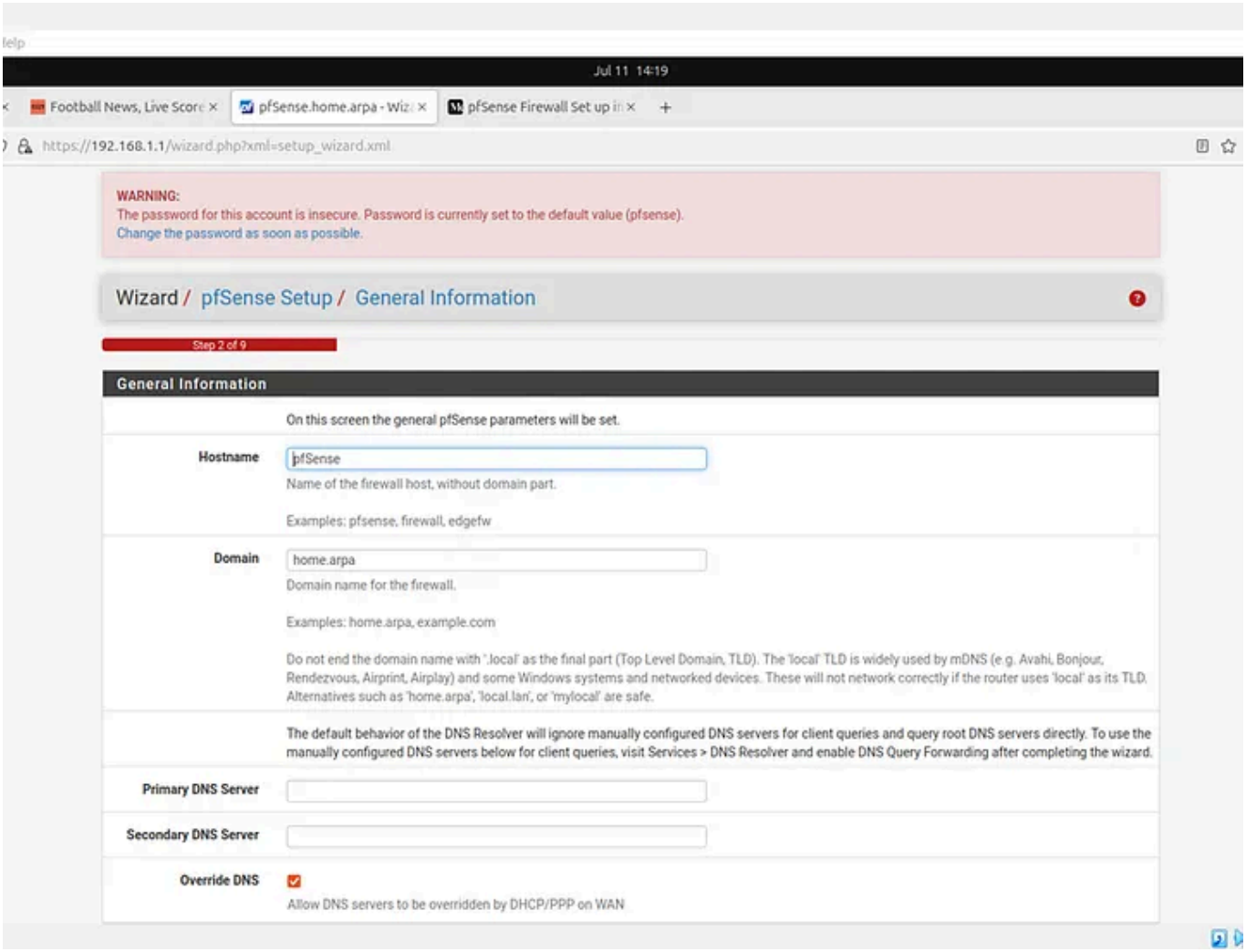

Fig. 35

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

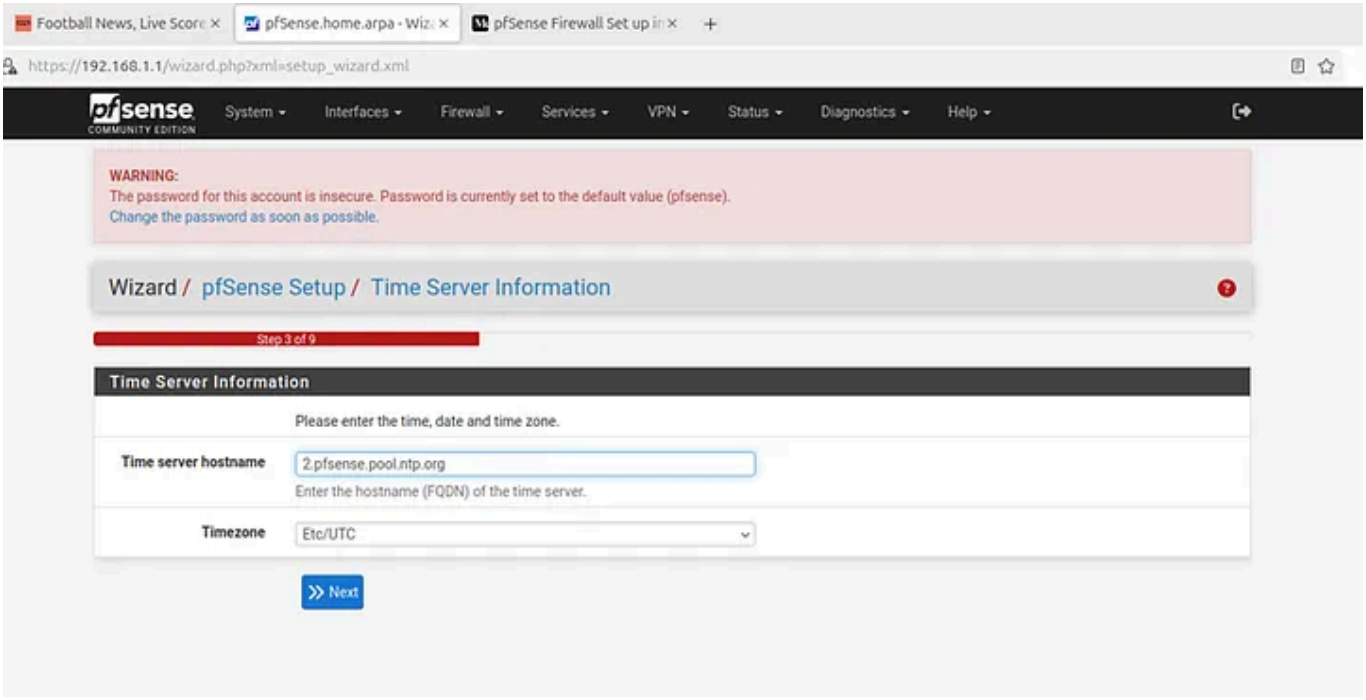

Fig. 36

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

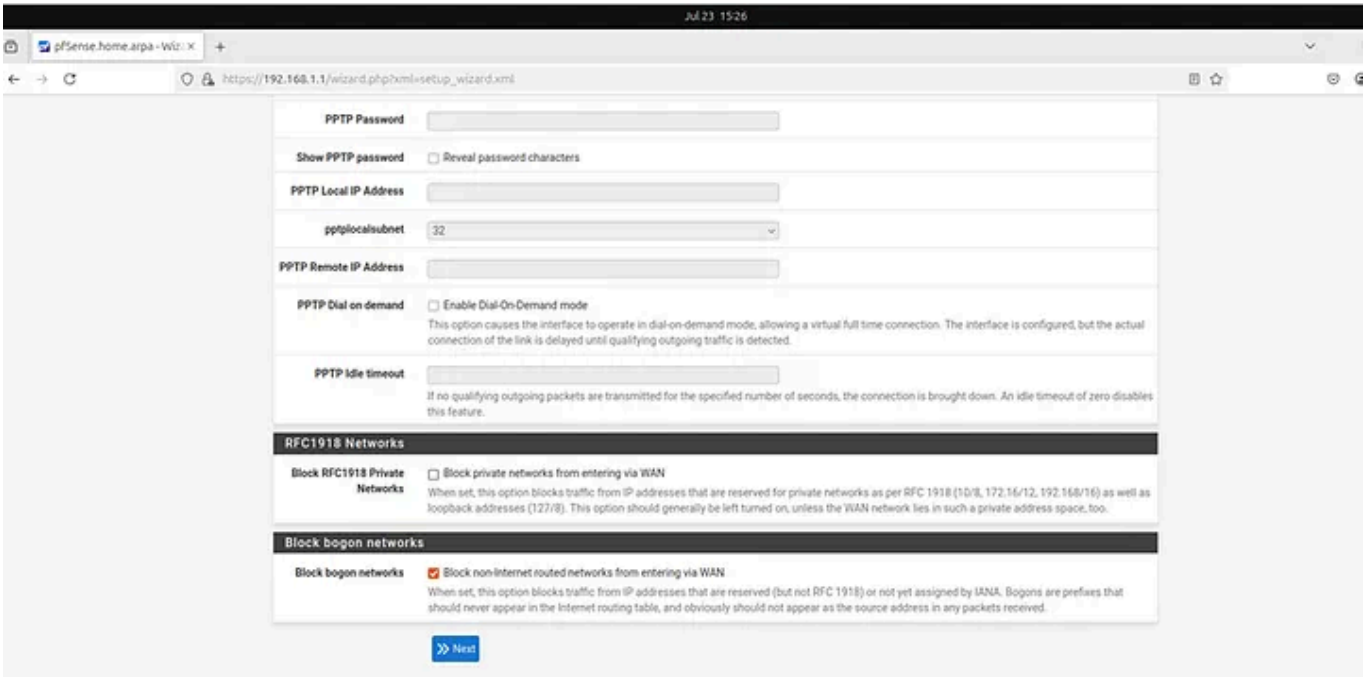

Fig. 37

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

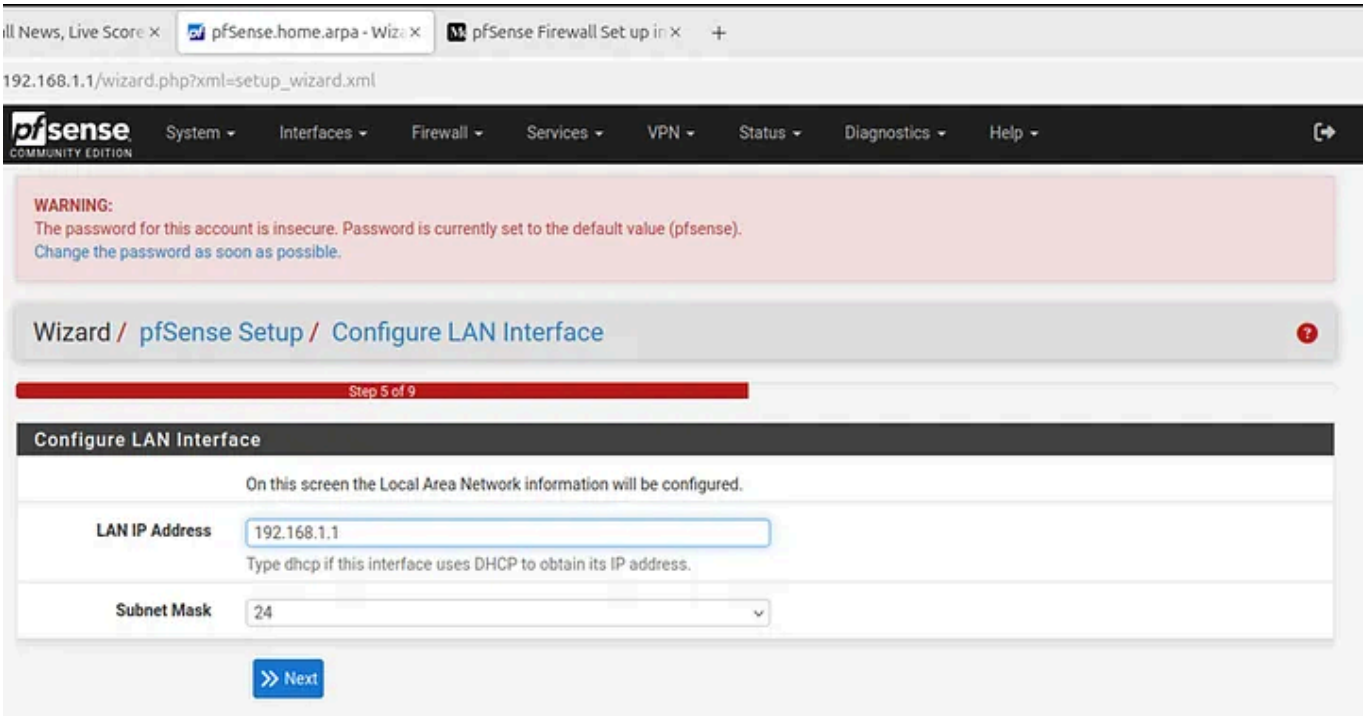

Fig. 38

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

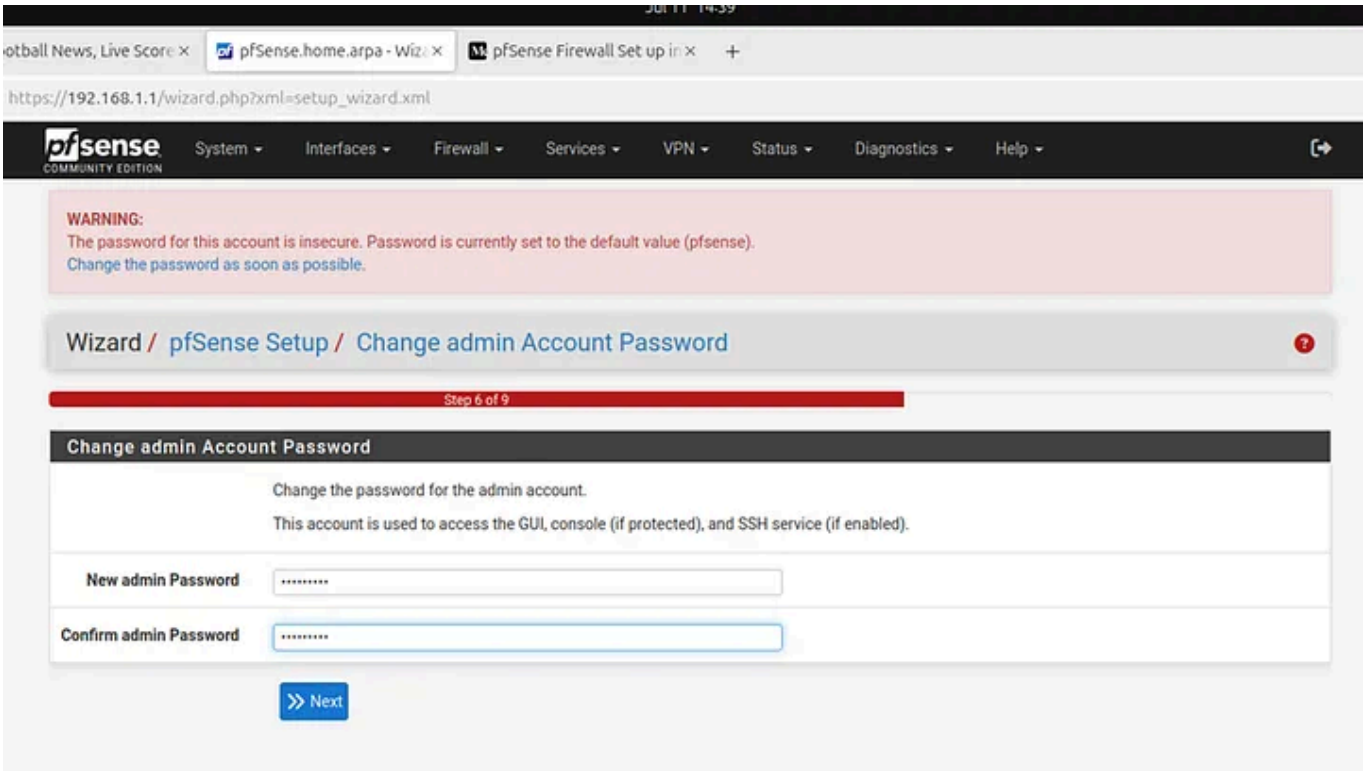

Fig. 39

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

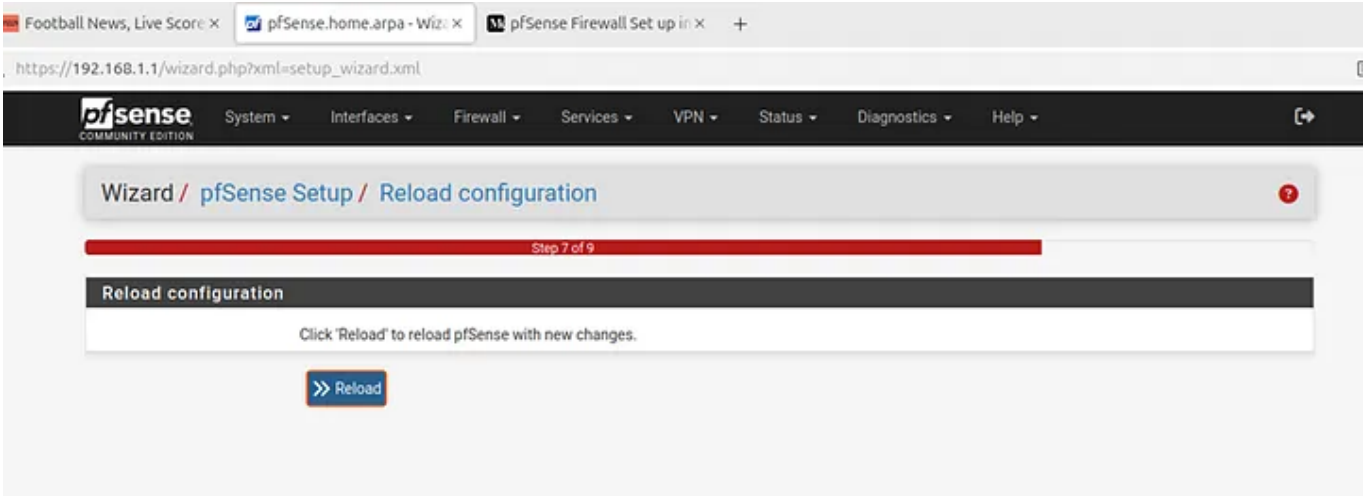

Fig. 40

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

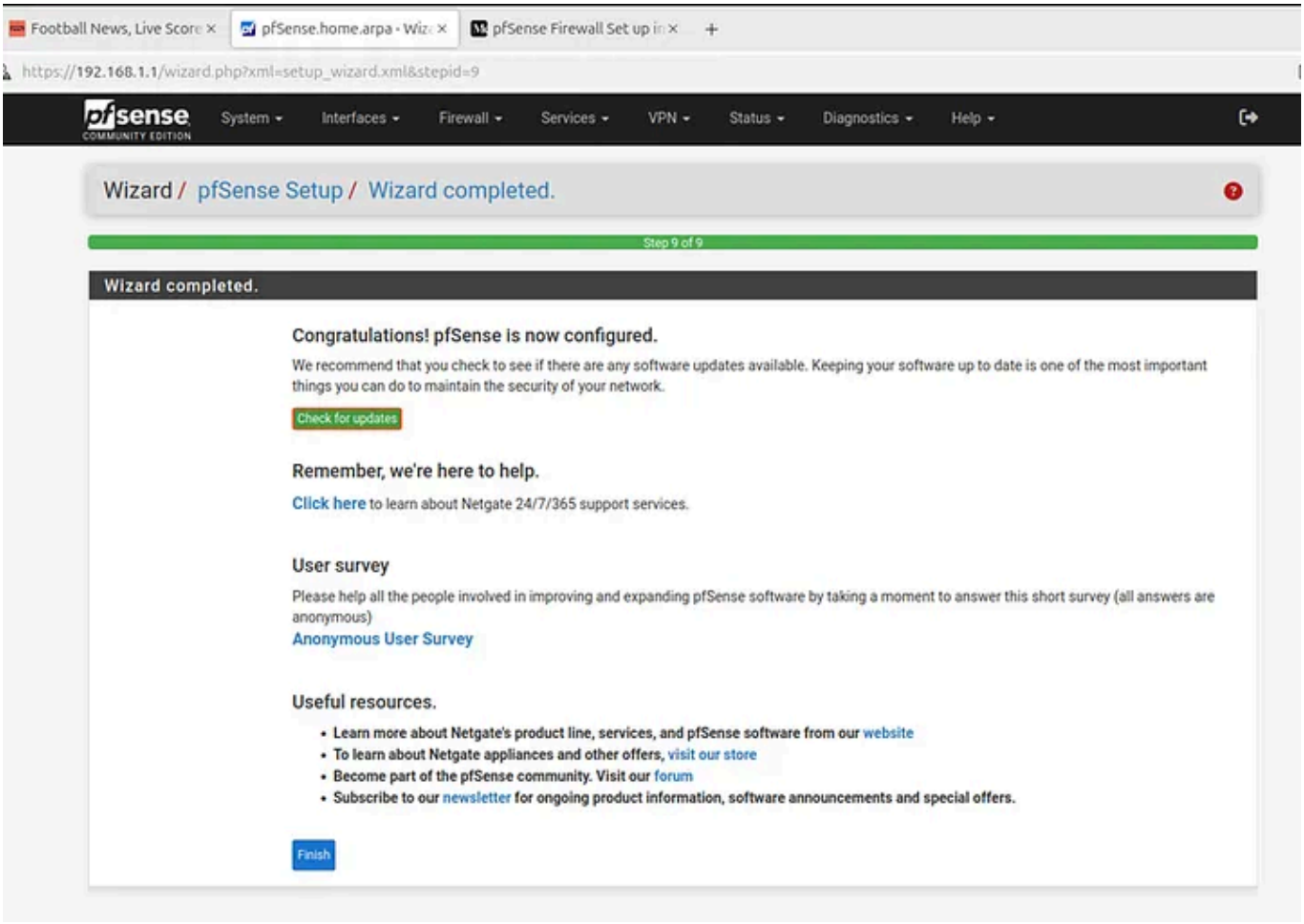

Fig. 41

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

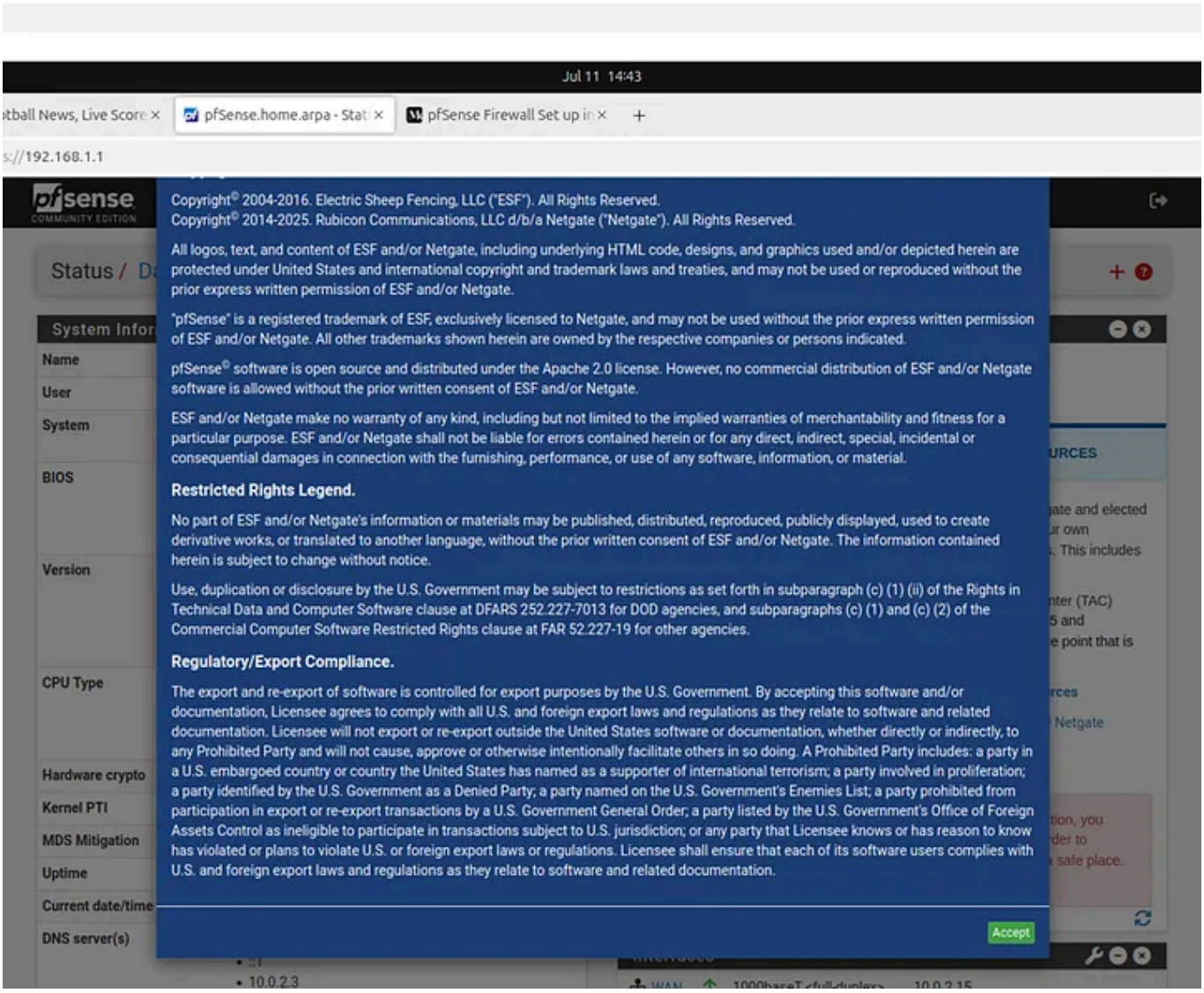

Fig. 42

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

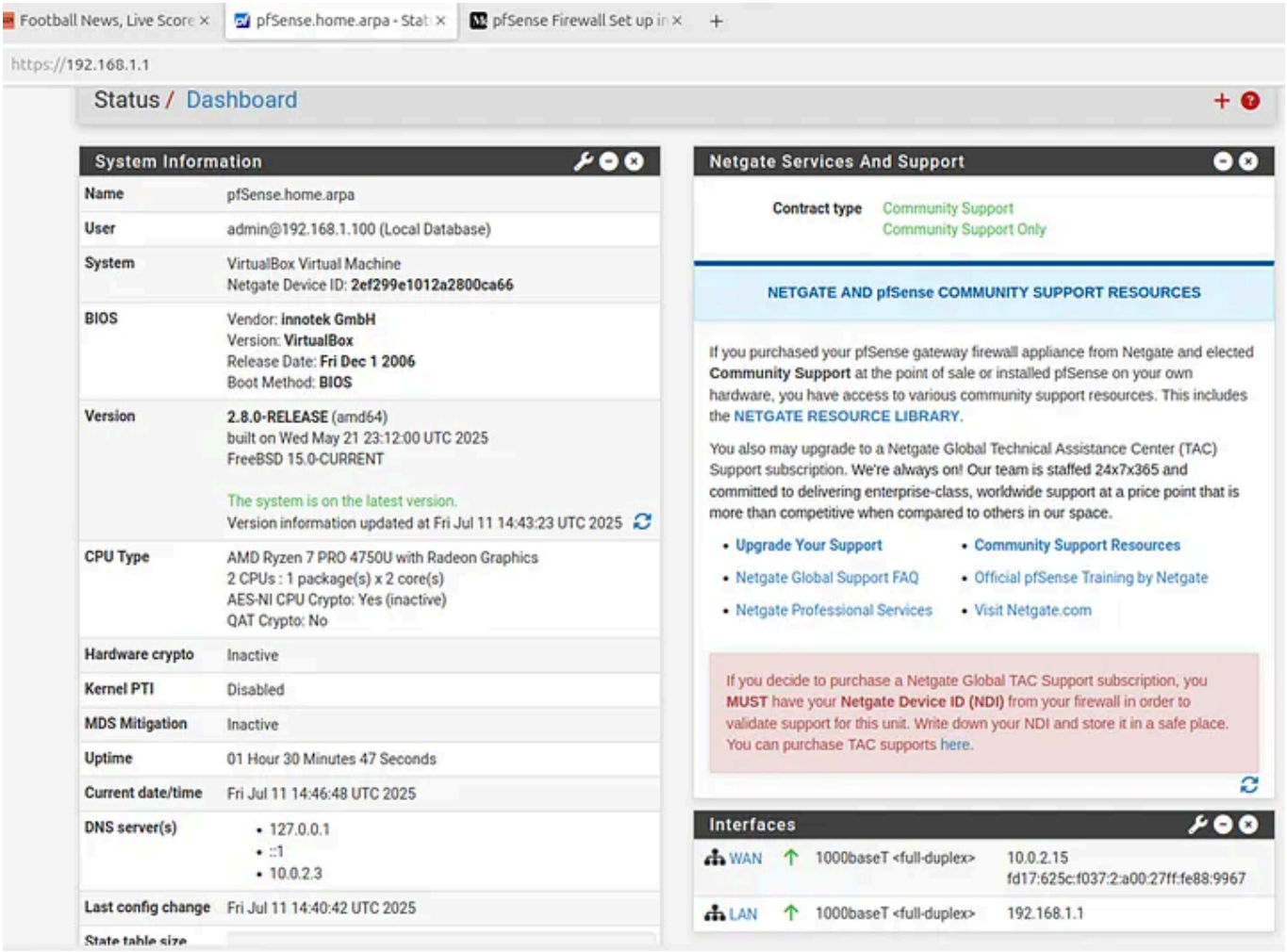

Fig. 43

> *# 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.

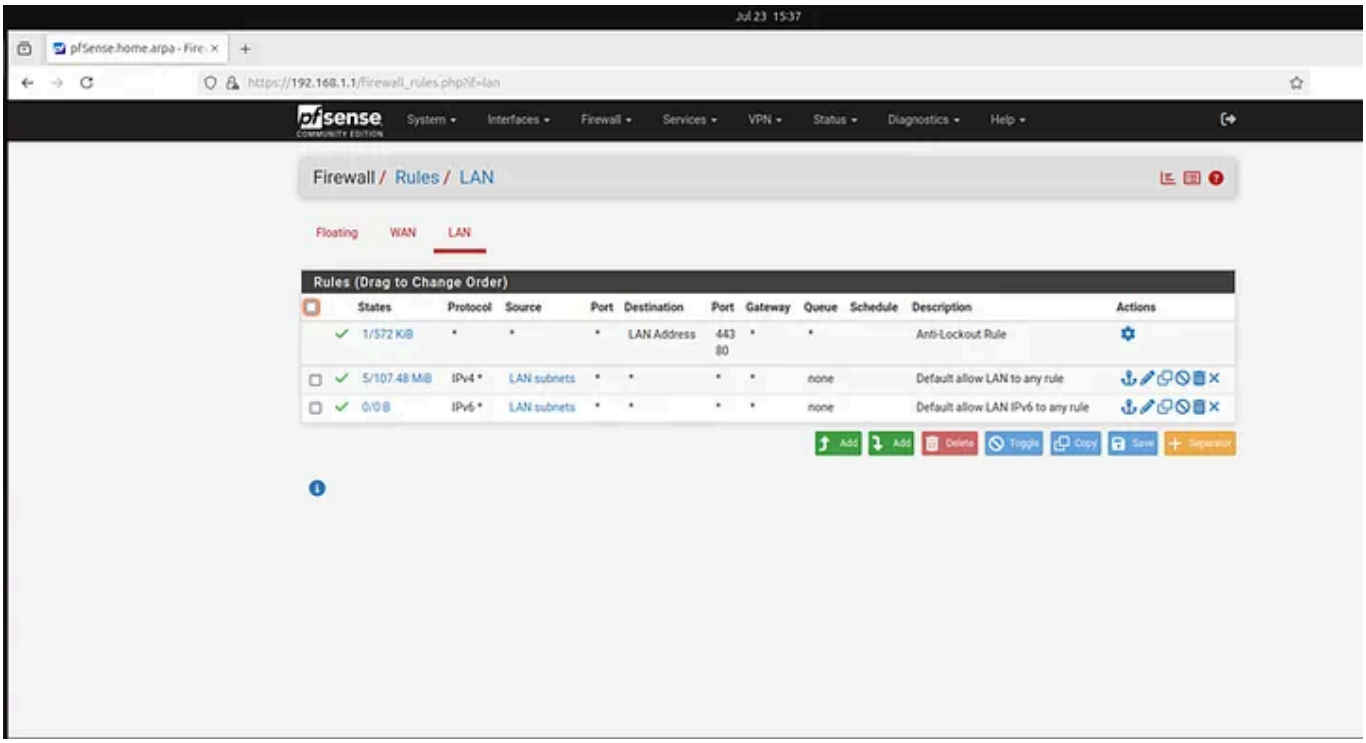

Fig. 44

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).

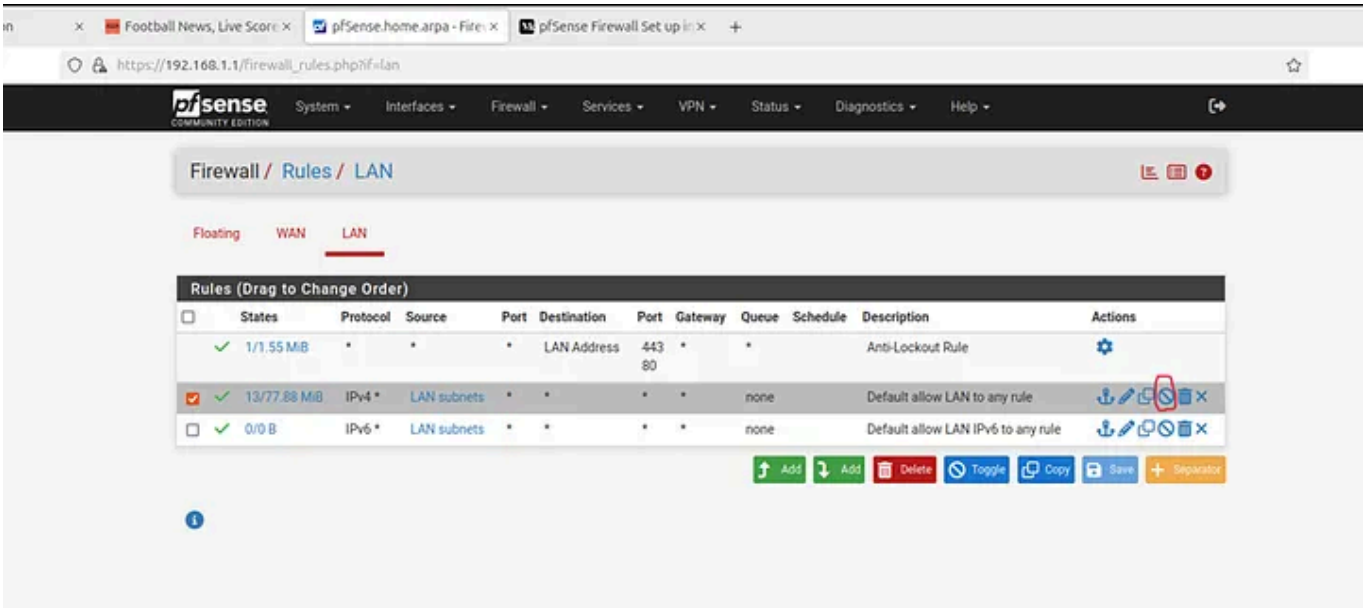

Fig. 45

Next, apply changes (Fig. 46).

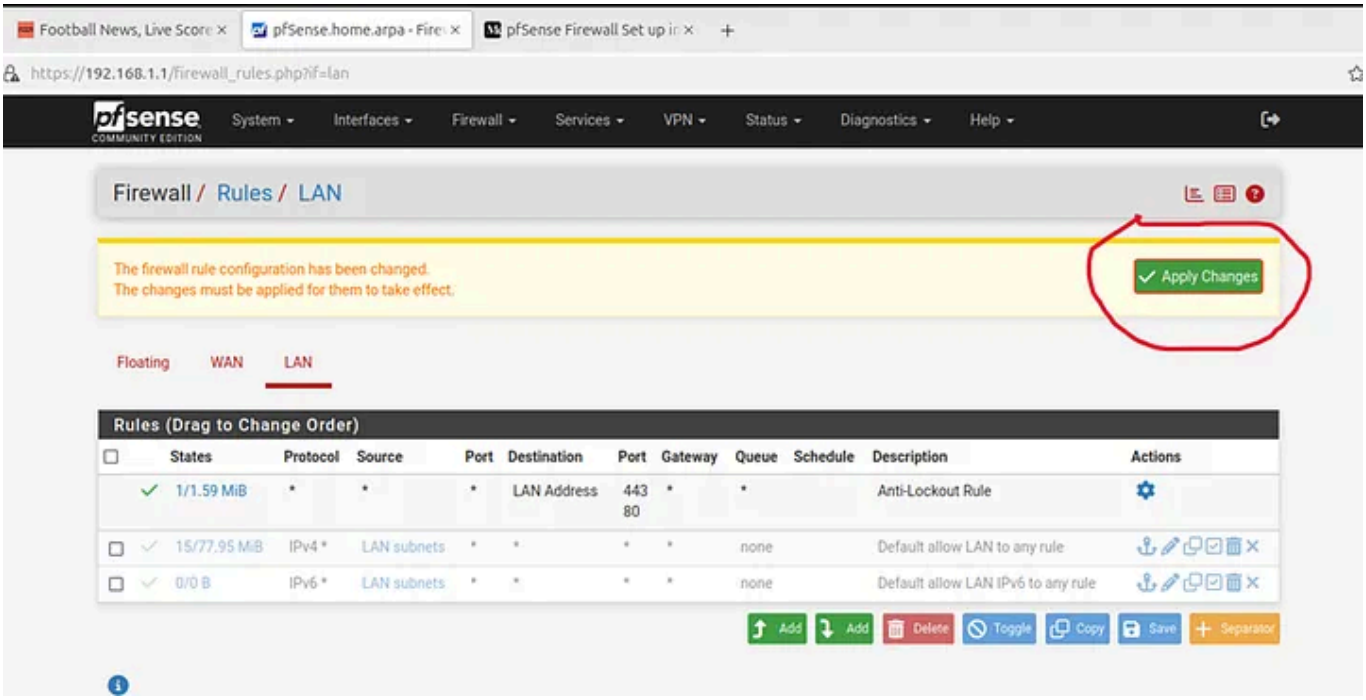

Fig. 46

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

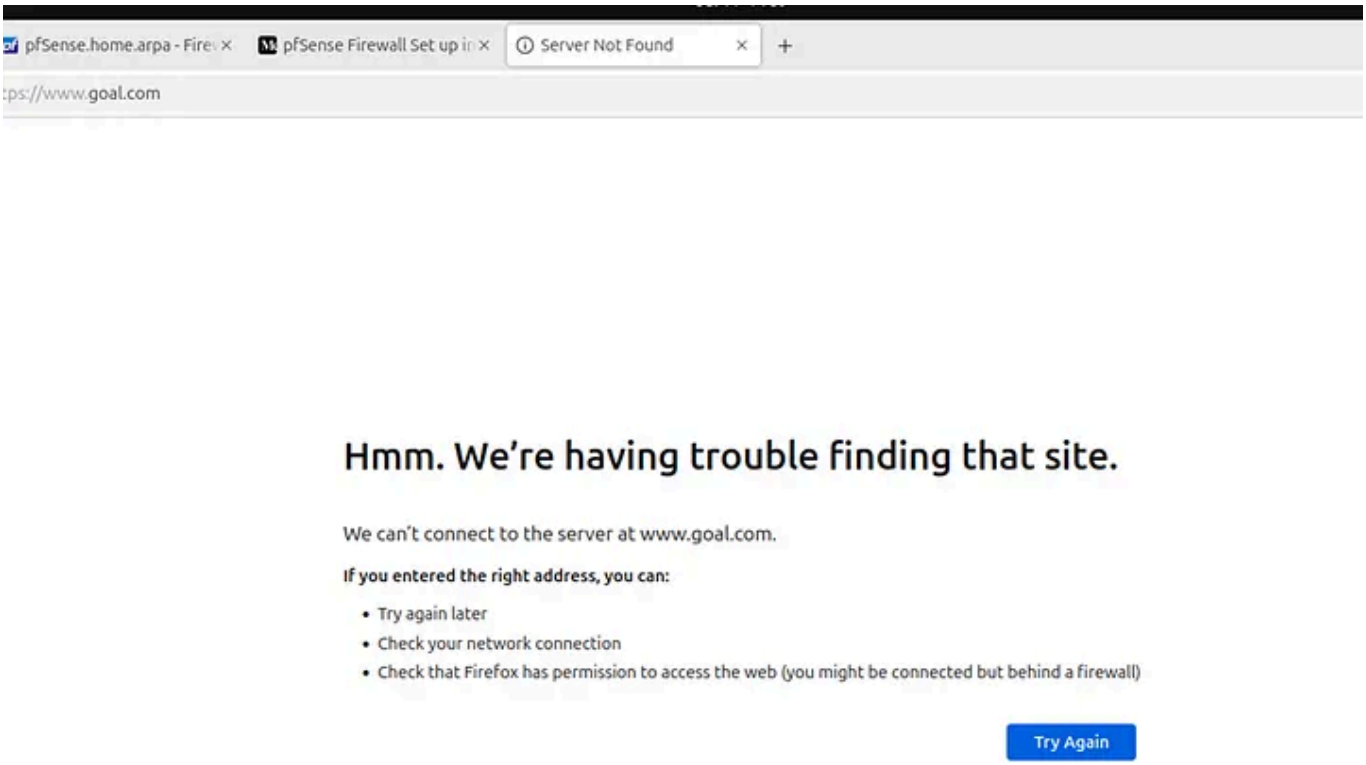

Fig. 47

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.

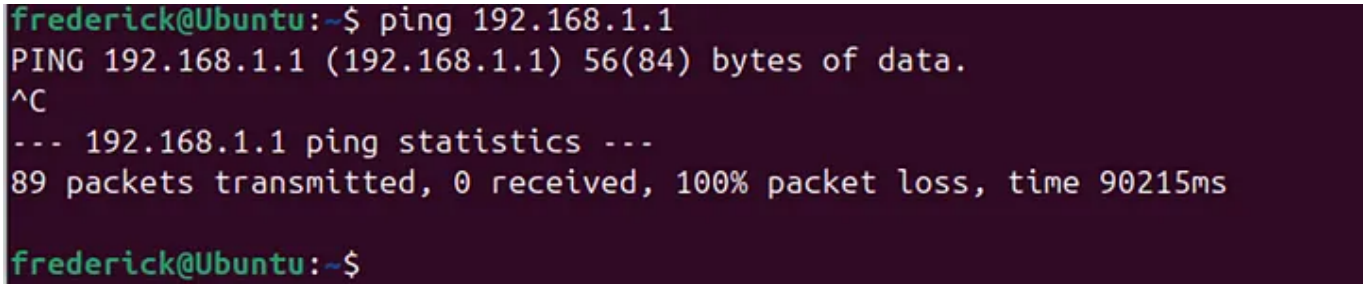

Fig. 48

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.

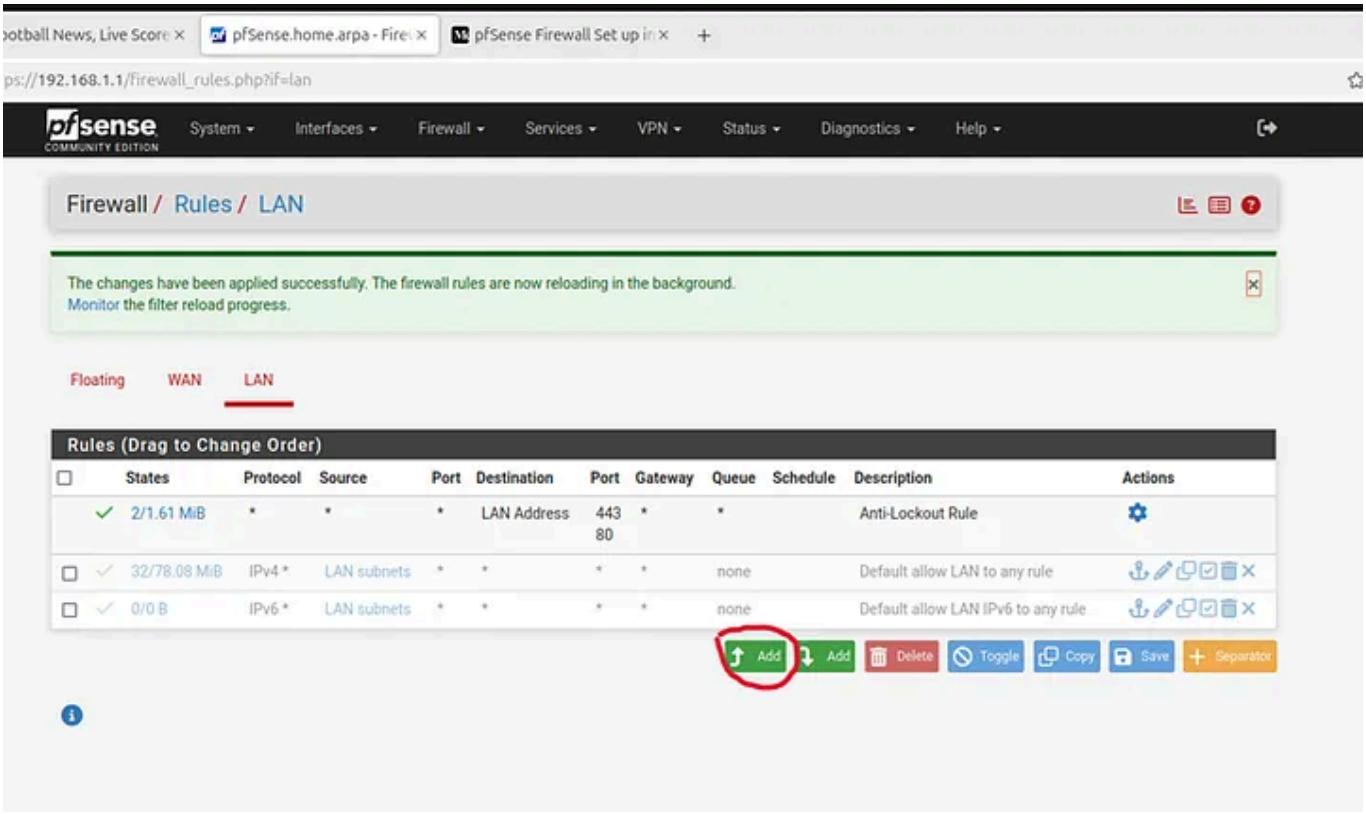

Fig. 49

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).

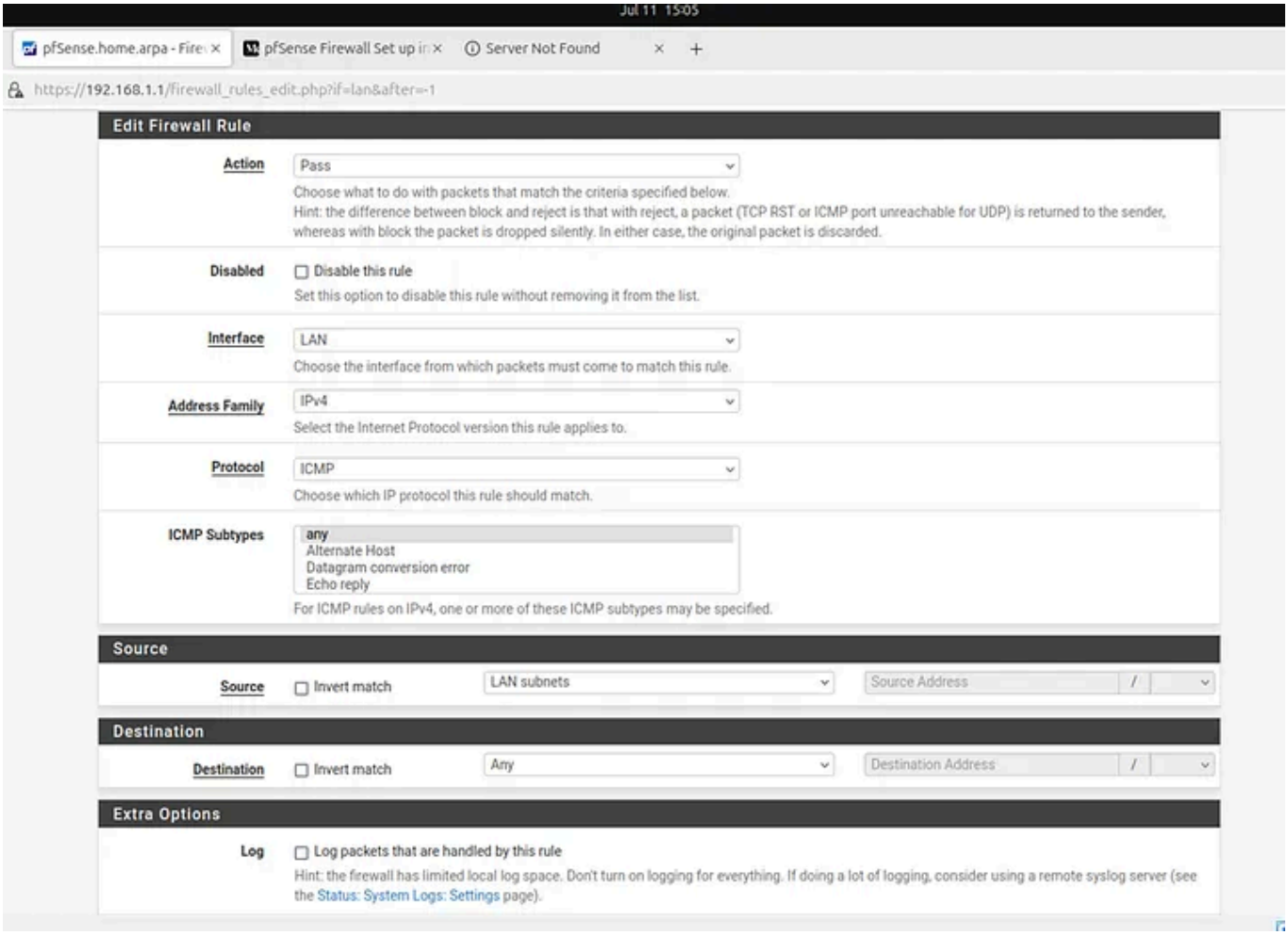

Fig. 50

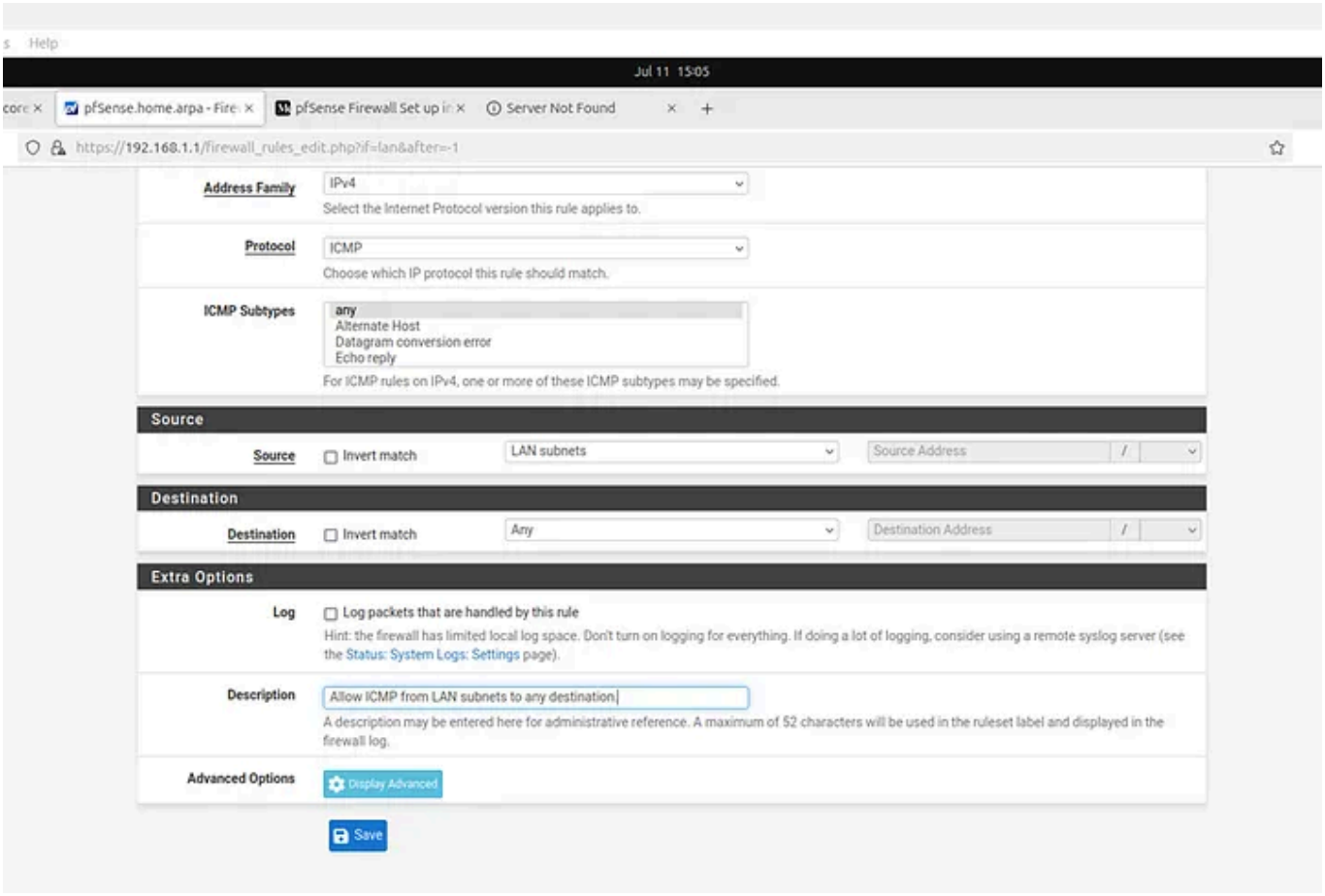

Fig. 51

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).

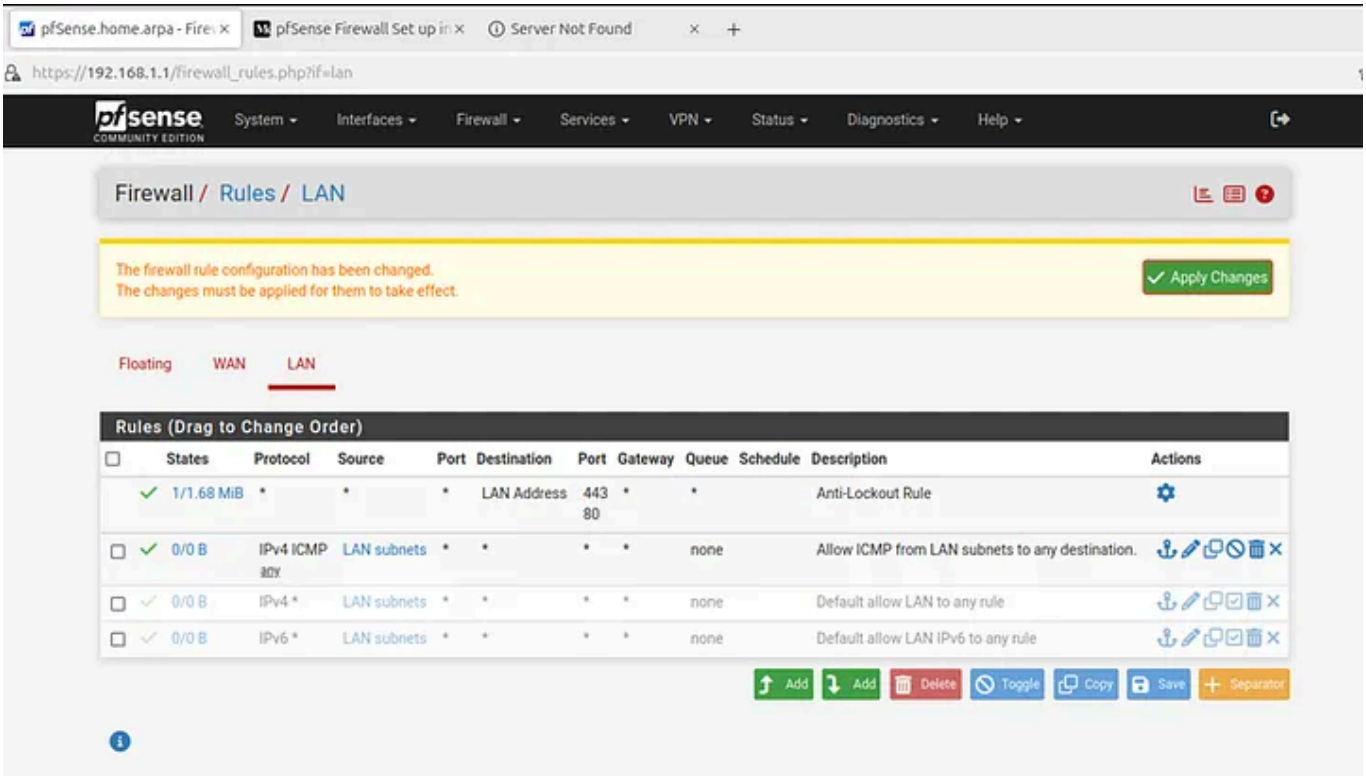

Fig. 52

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

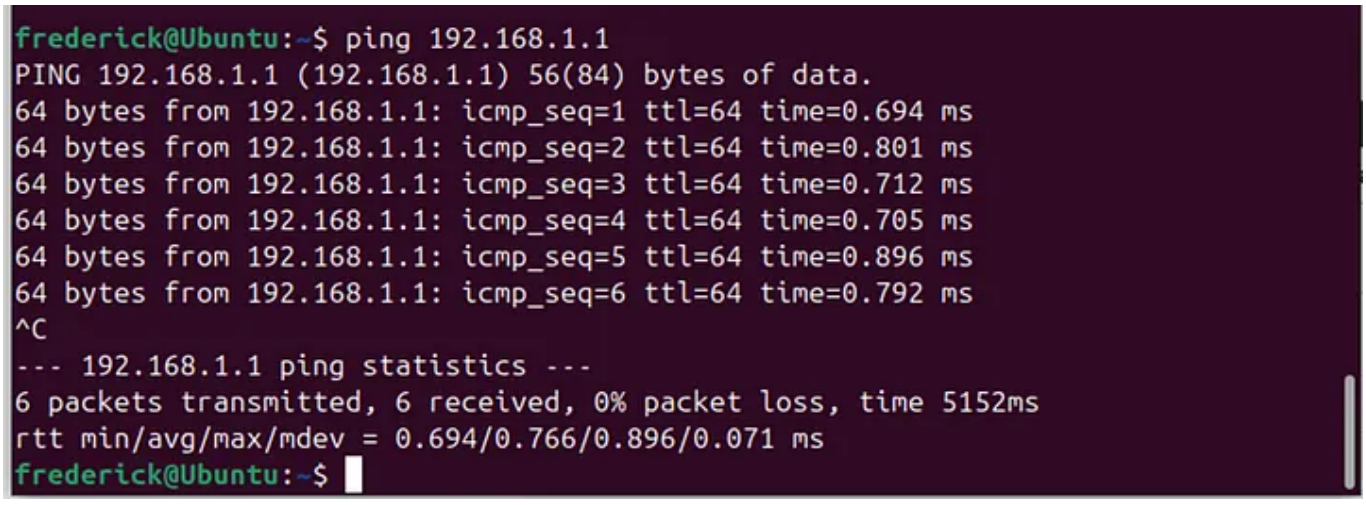

Fig. 53

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).

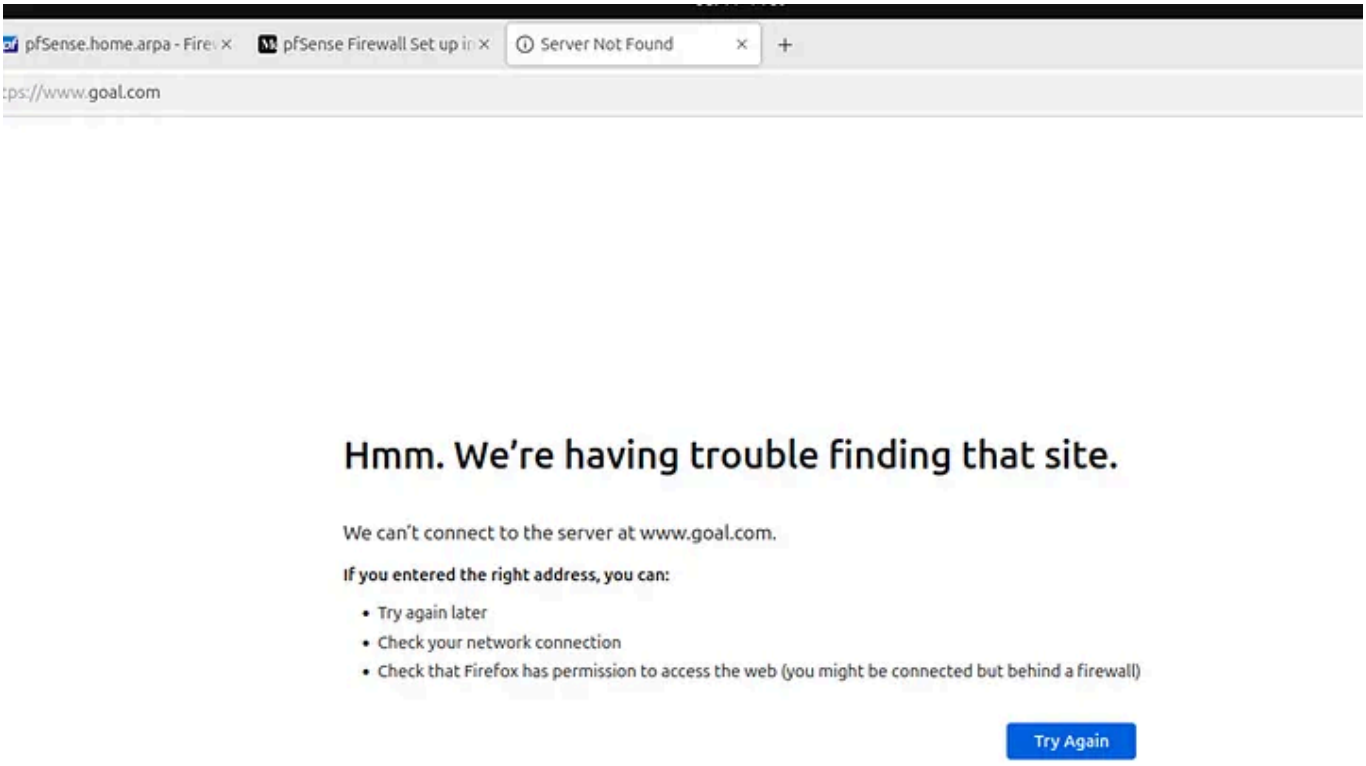

Fig. 54

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).

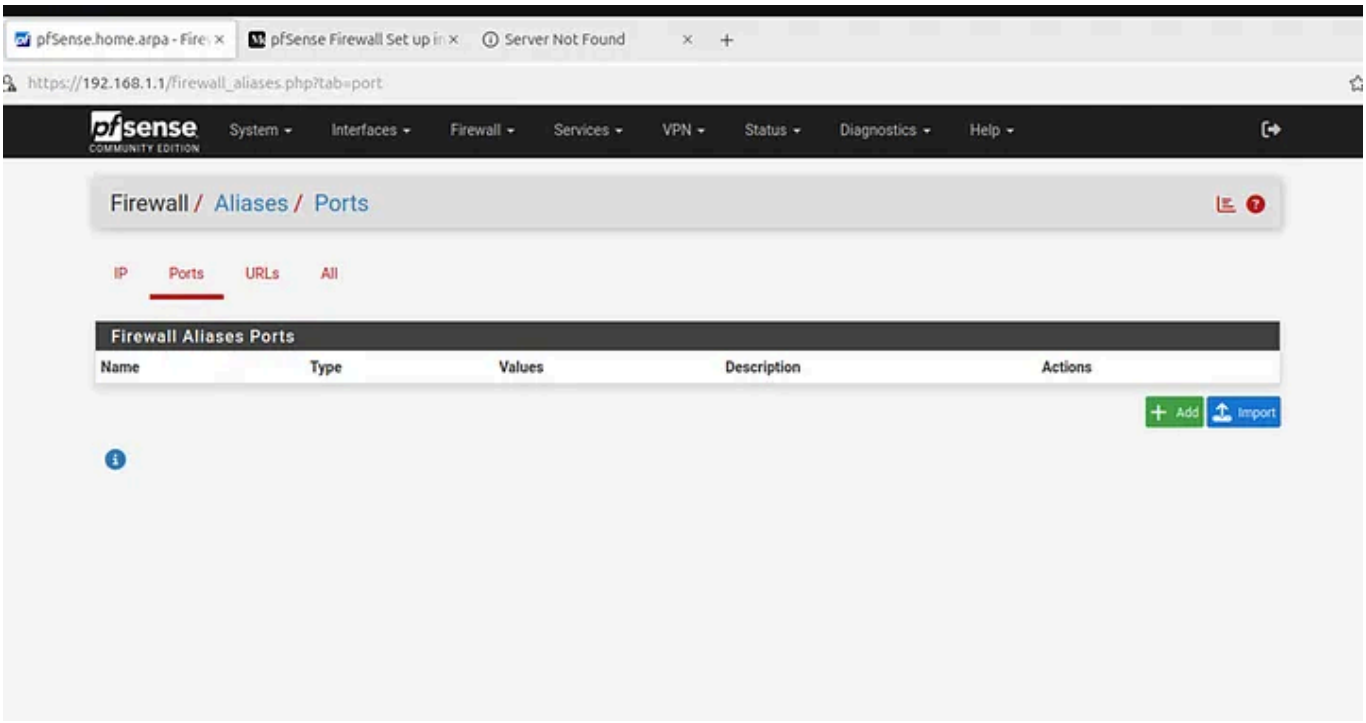

Fig. 55

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

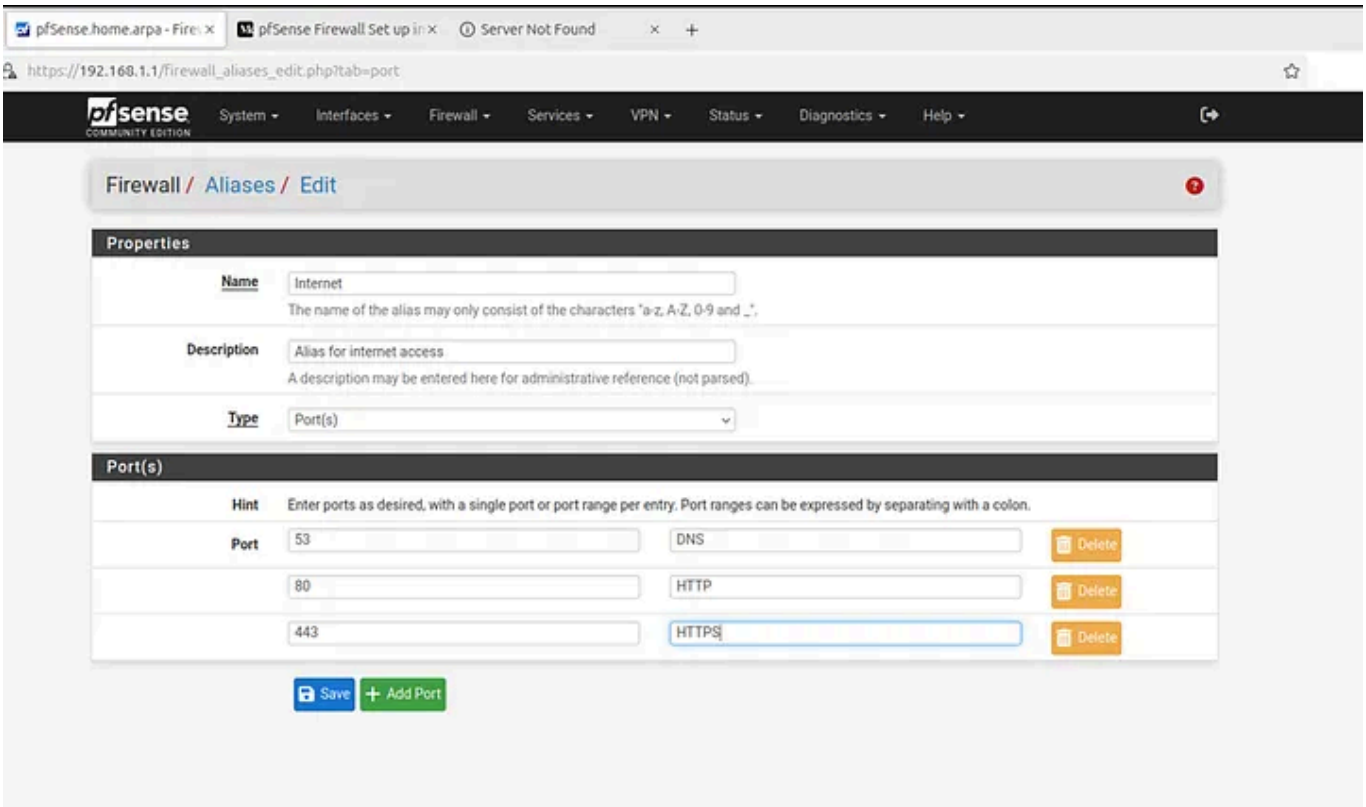

Fig. 56

Save and apply the changes (Fig. 57).

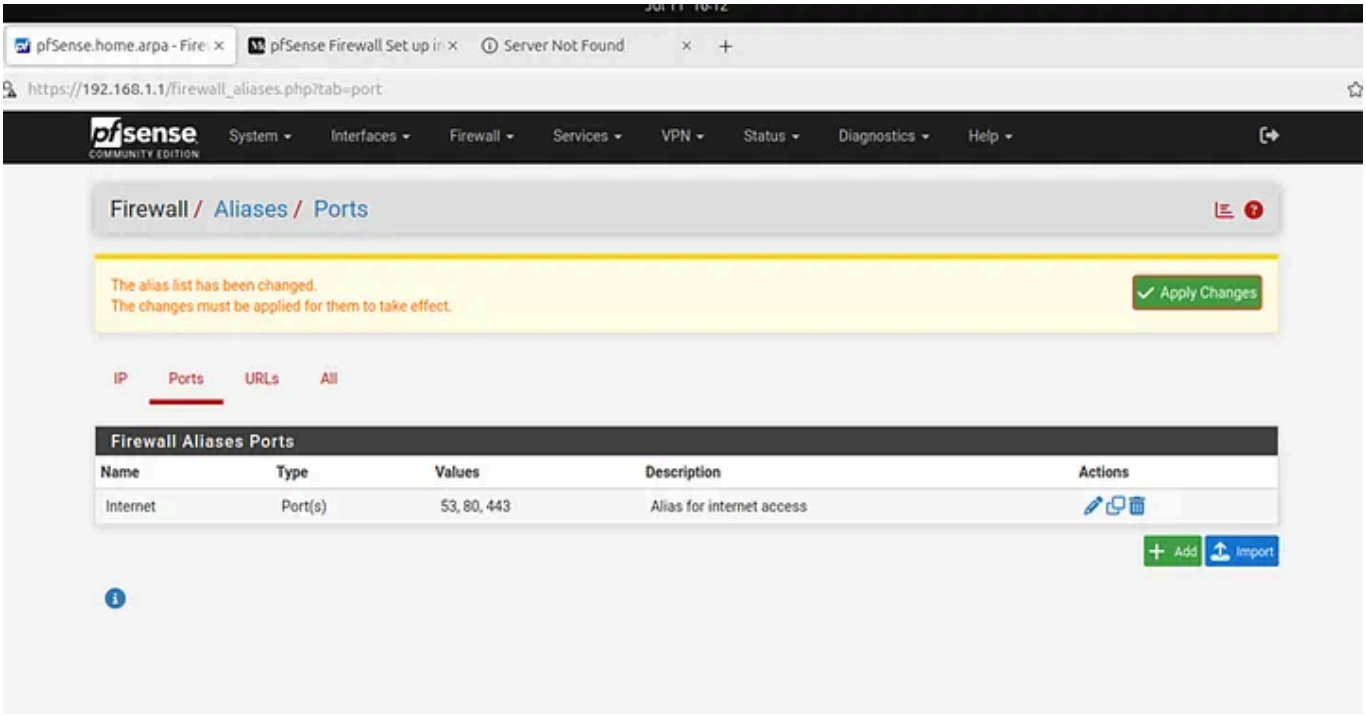

Fig. 57

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

Then click Add (the upward facing green arrow).

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

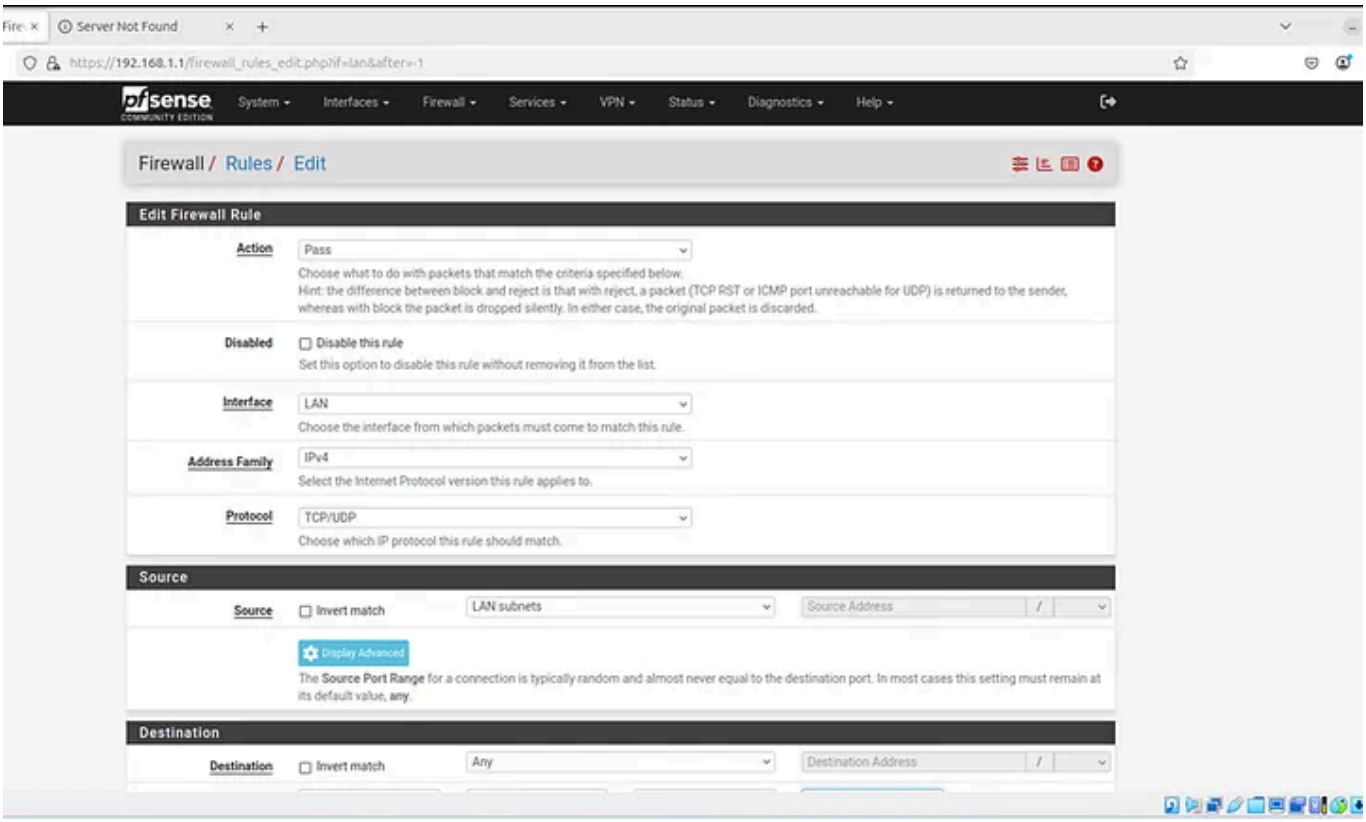

Fig. 58

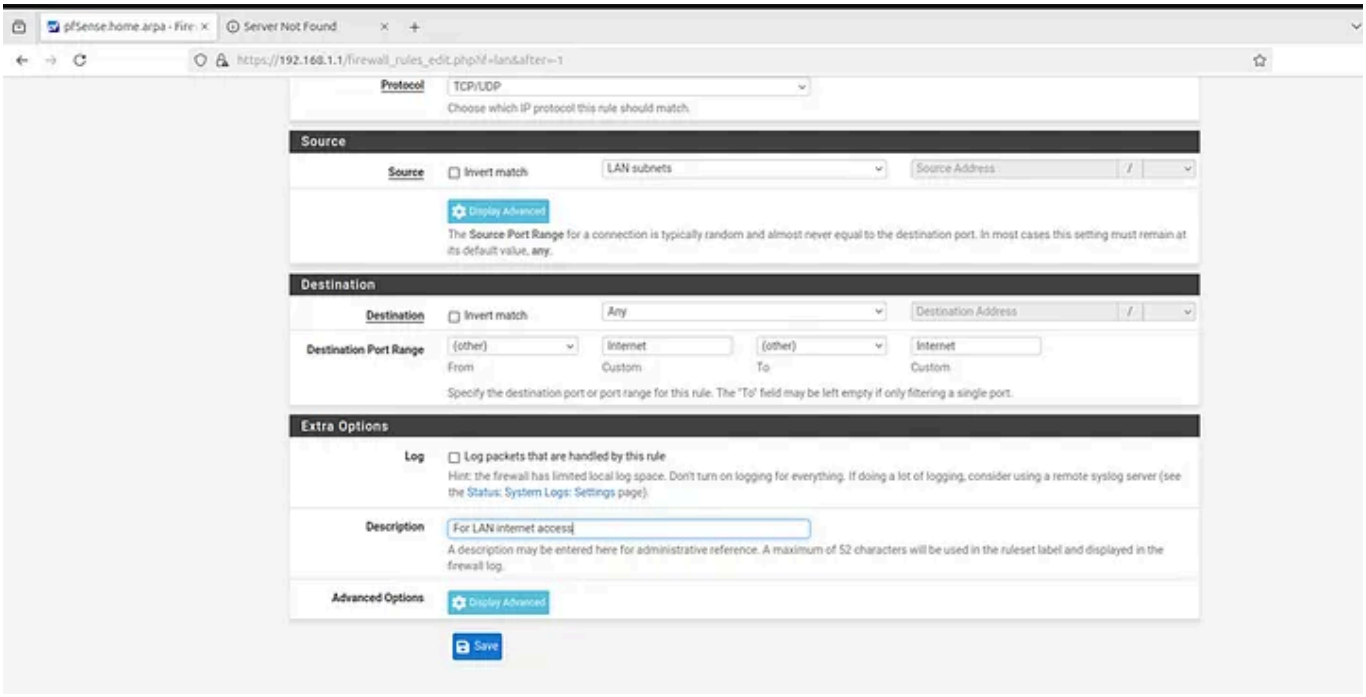

Fig. 59

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).

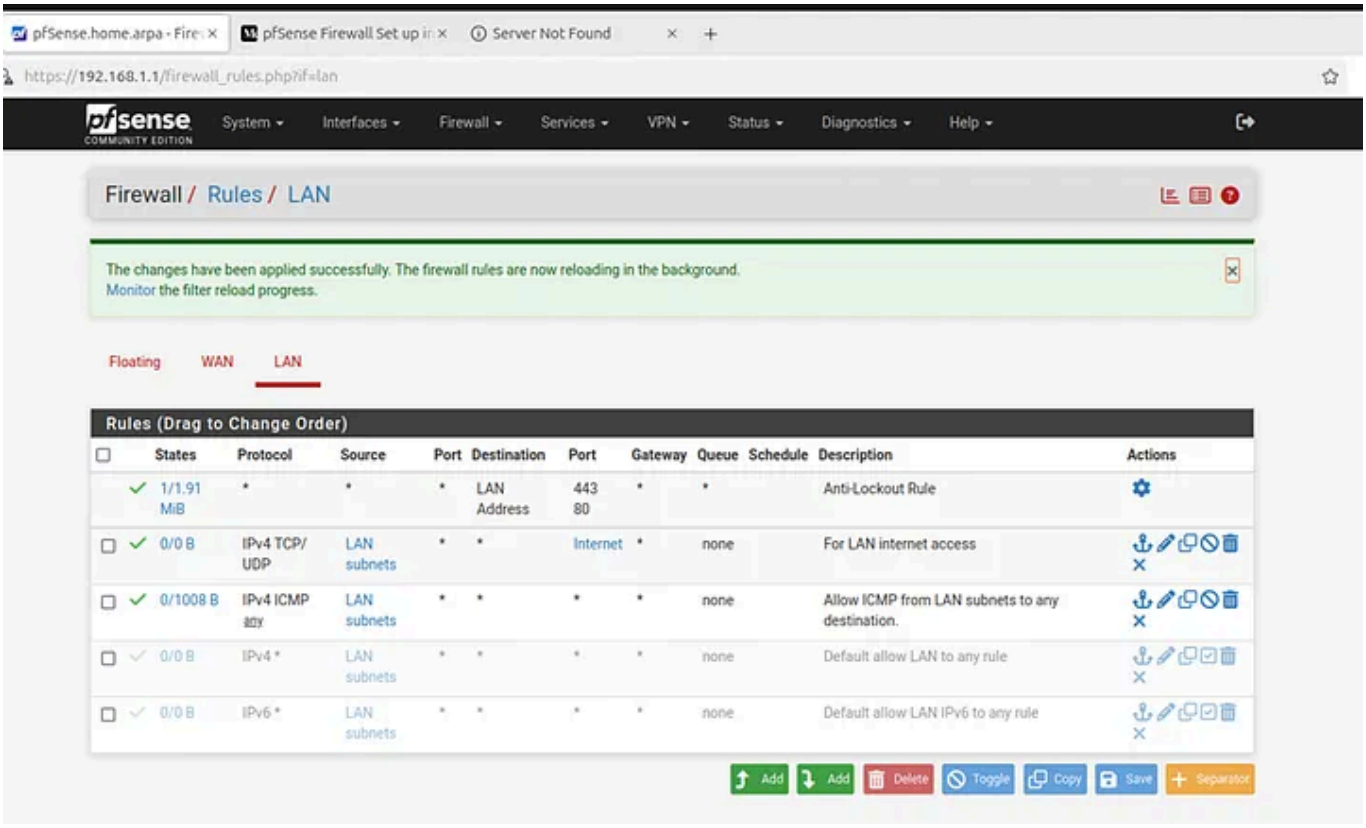

Fig. 60

Internet connection is now possible (Fig. 61).

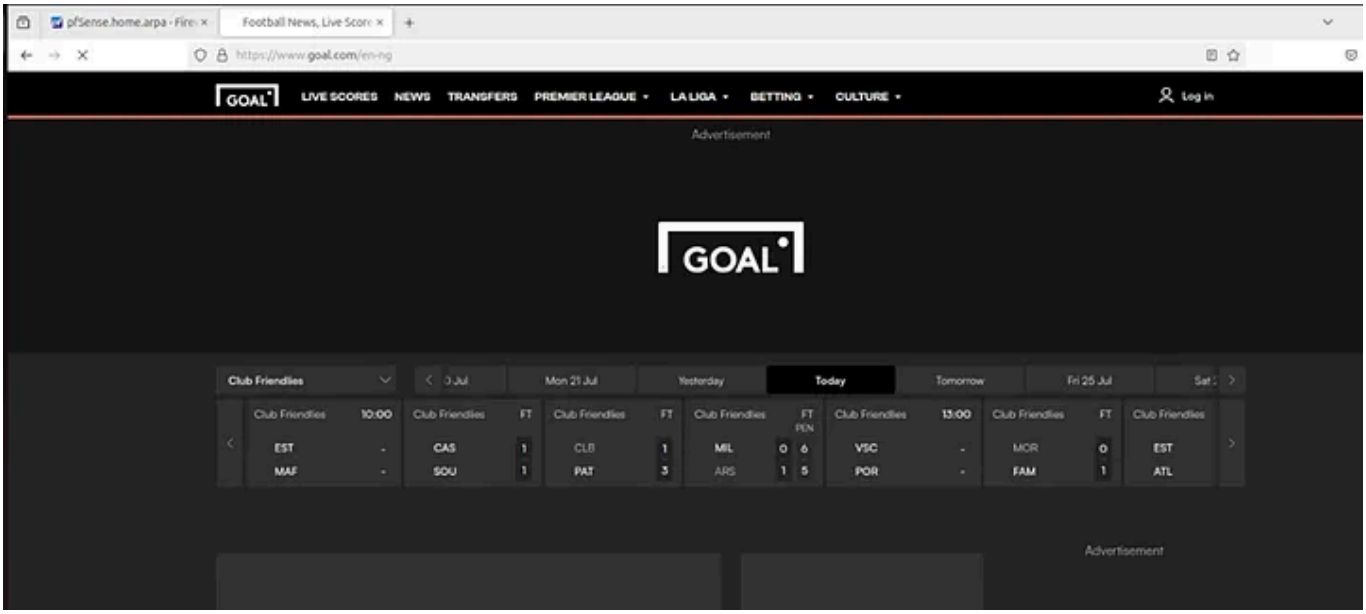

Fig. 61

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

Tchau!

Cybersecurity Homelab Pfsense Firewall Open Source

F

Written by Frederick Adigun

3 followers · 2 following

Edit profile

No responses yet

F Frederick Adigun

What are your thoughts?

More from Frederick Adigun