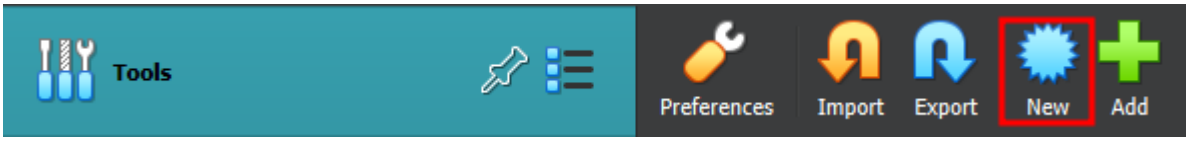
pfSense Setup and Configuration

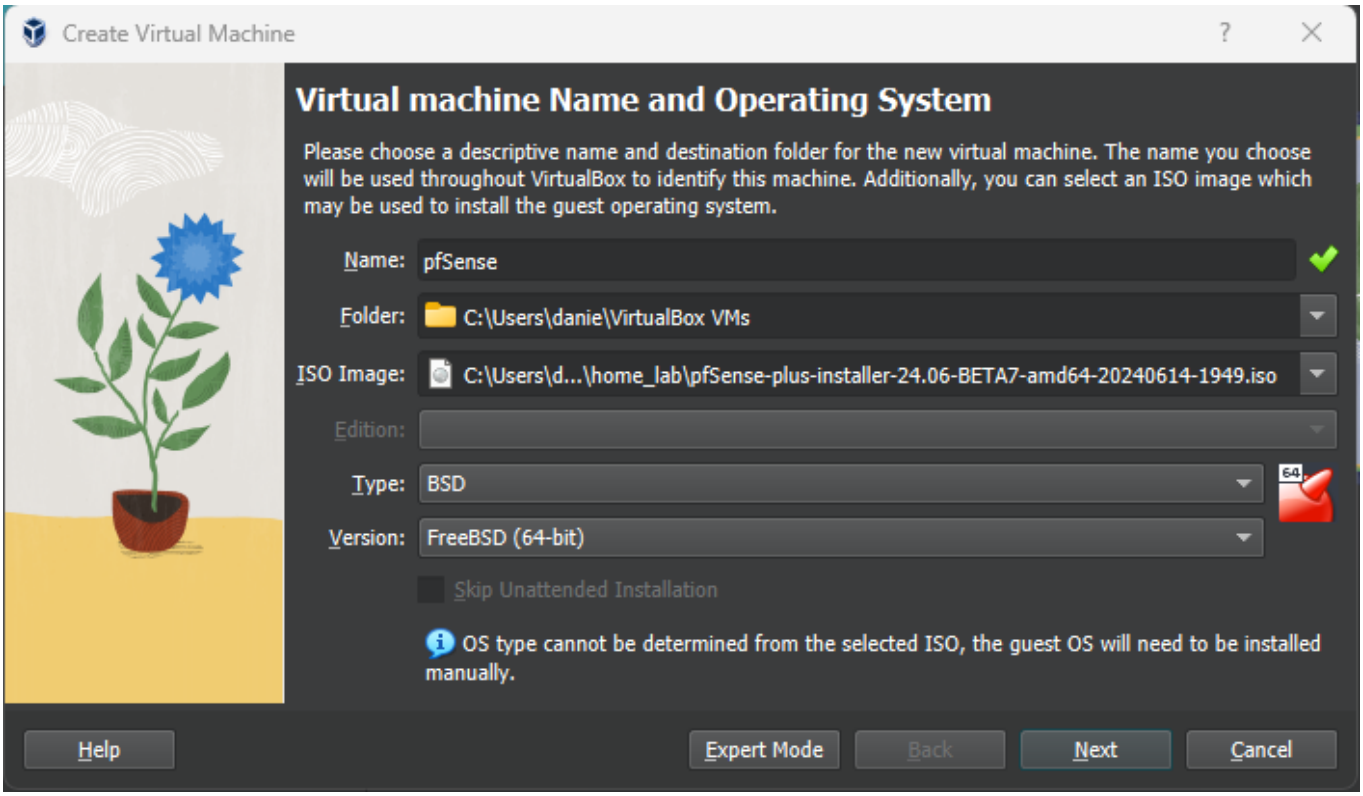
Download: [Download pfSense Intaller]

VM Setup

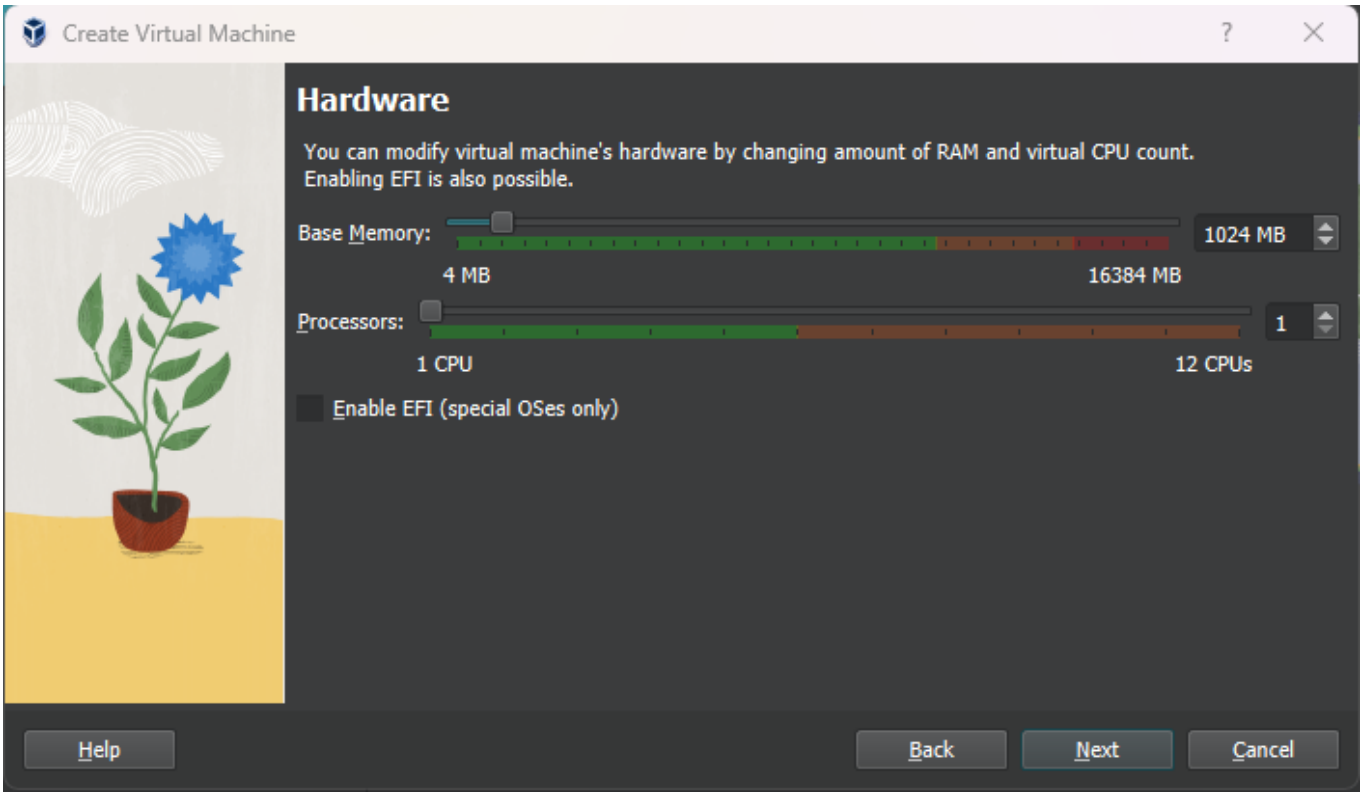
I create a new VM in VirtualBox by clicking on **New**



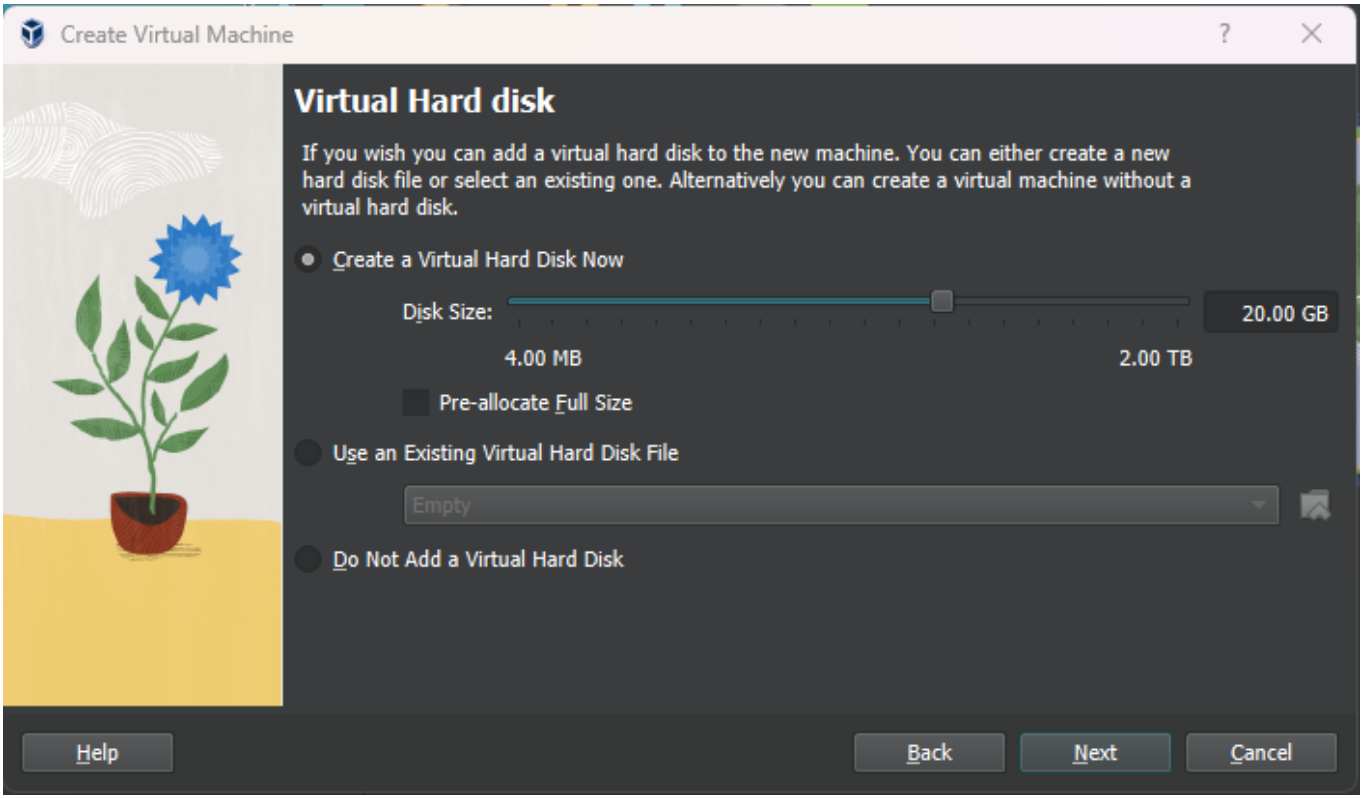
I give it a name, choose where it will be saved and from the **ISO Image** dropdown select others and then the **.iso** image I downloaded. As Type I select **BSD** and as Version I select **FreeBSD(64-bit)** and then I click on **Next**



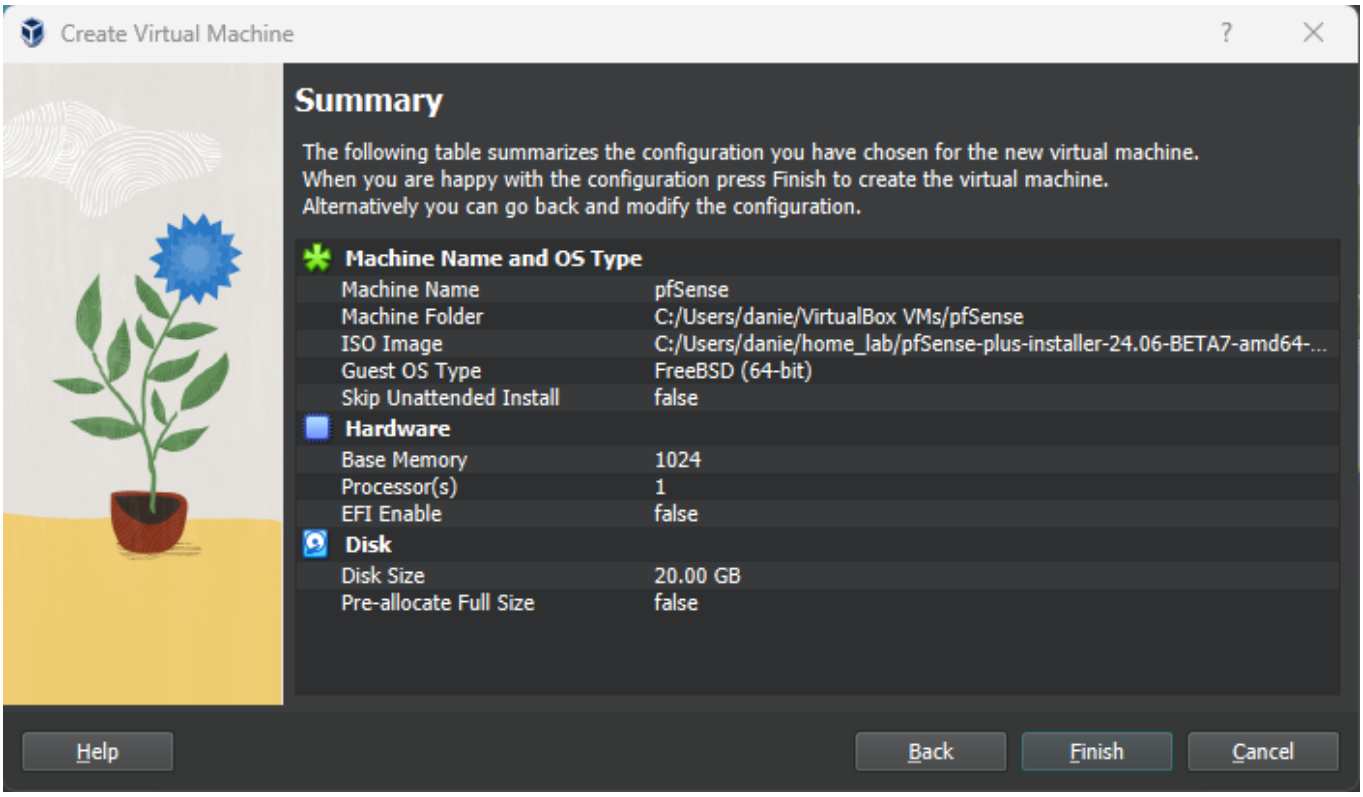
I leave the RAM and CPU setting as default and click on **Next**



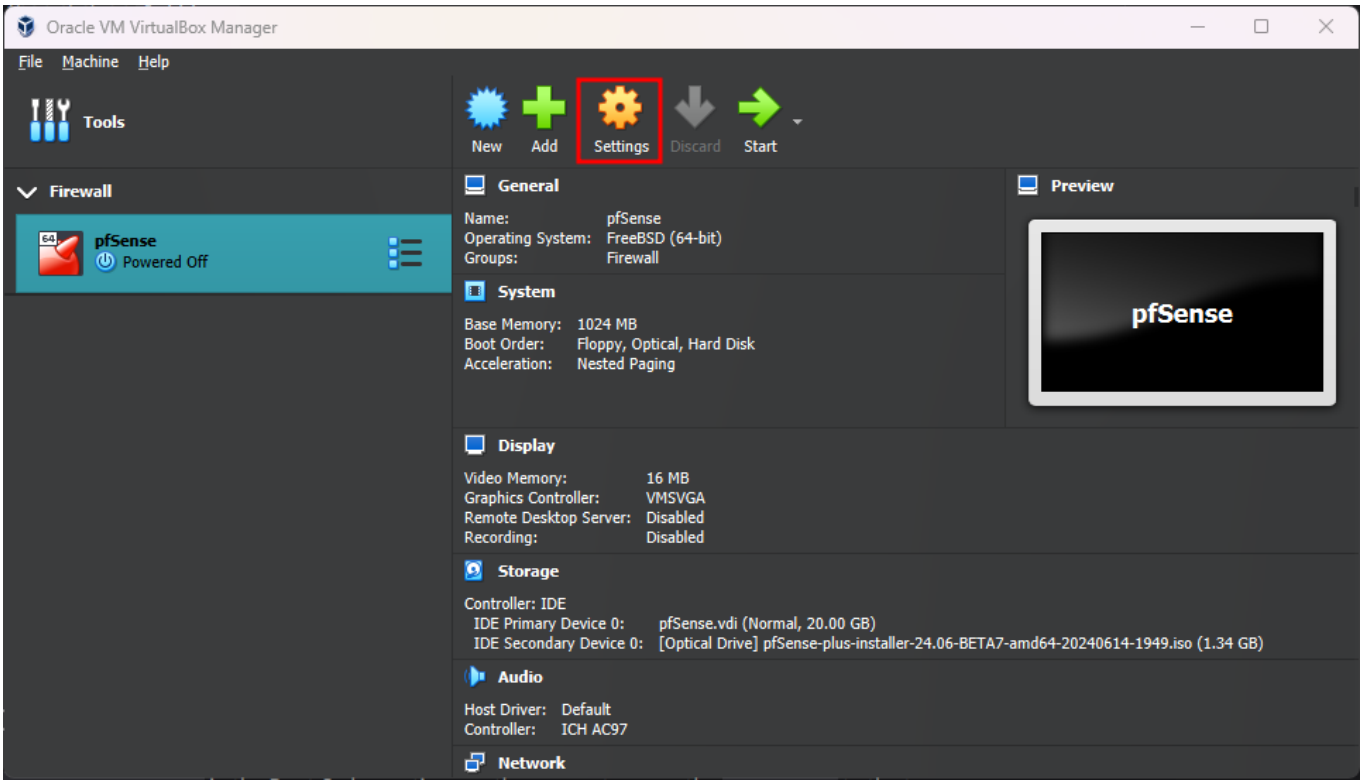
I assign **20GB** of storage space to it



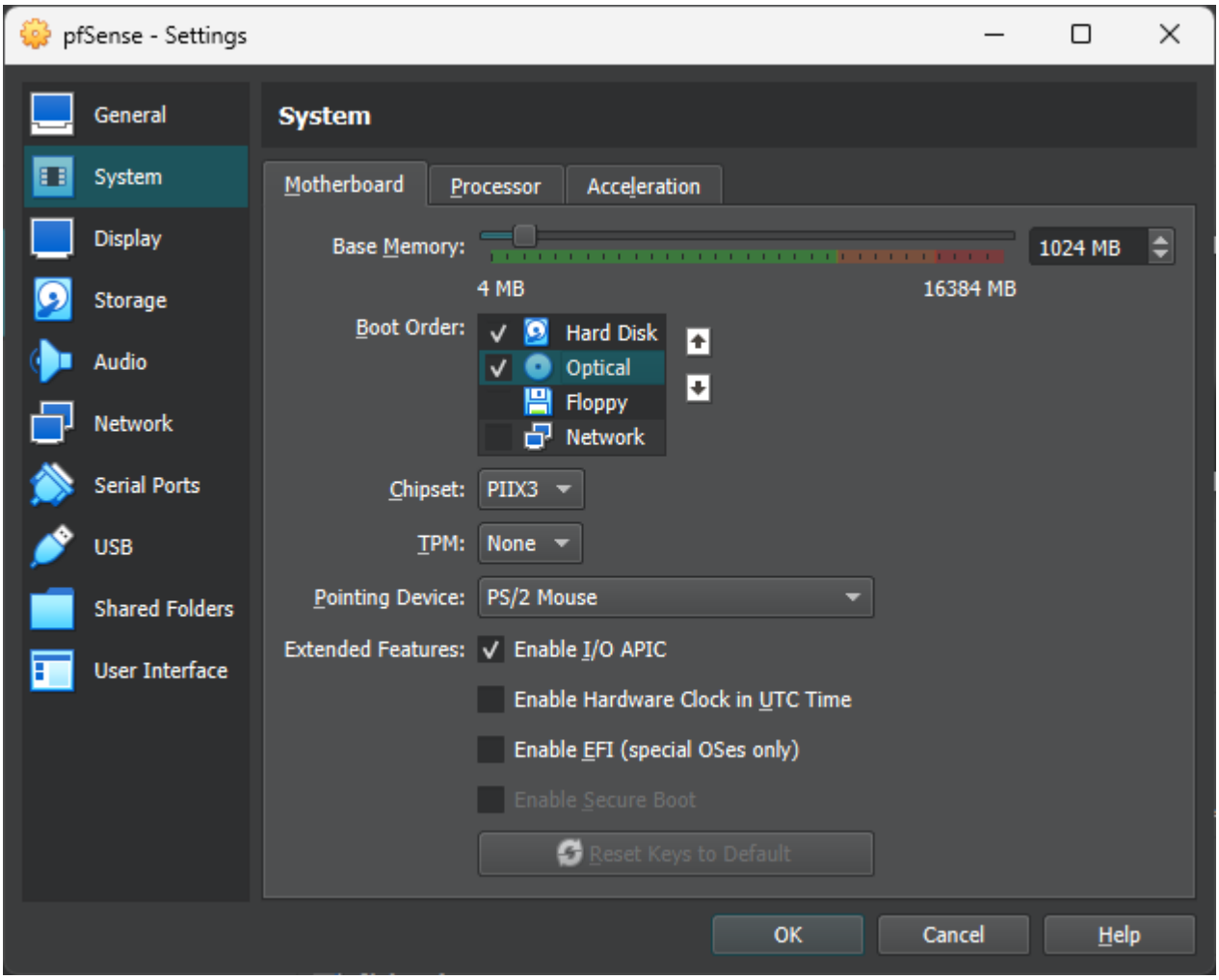
Check if everything is right and then click on **Finish**



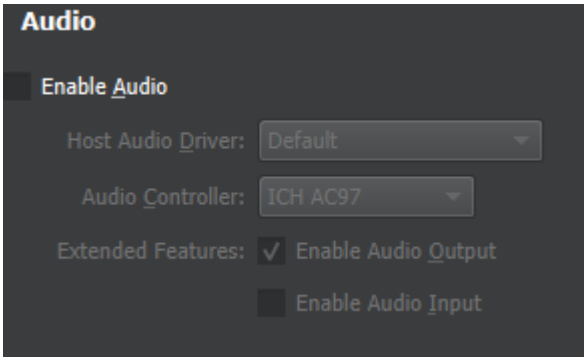
I configure some setting on the machine related to VirtualBox, so I select the pfSense VM and then click on **Settings**

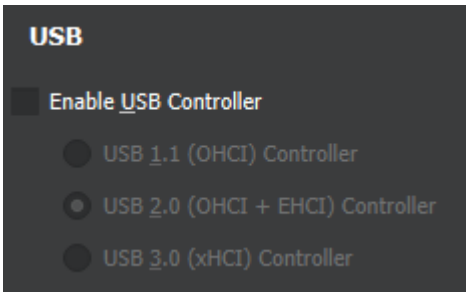


I select **System -> Motherboard** and then change the boot order to have the **Hard Disk** on top, **Optical** and uncheck **Floppy**

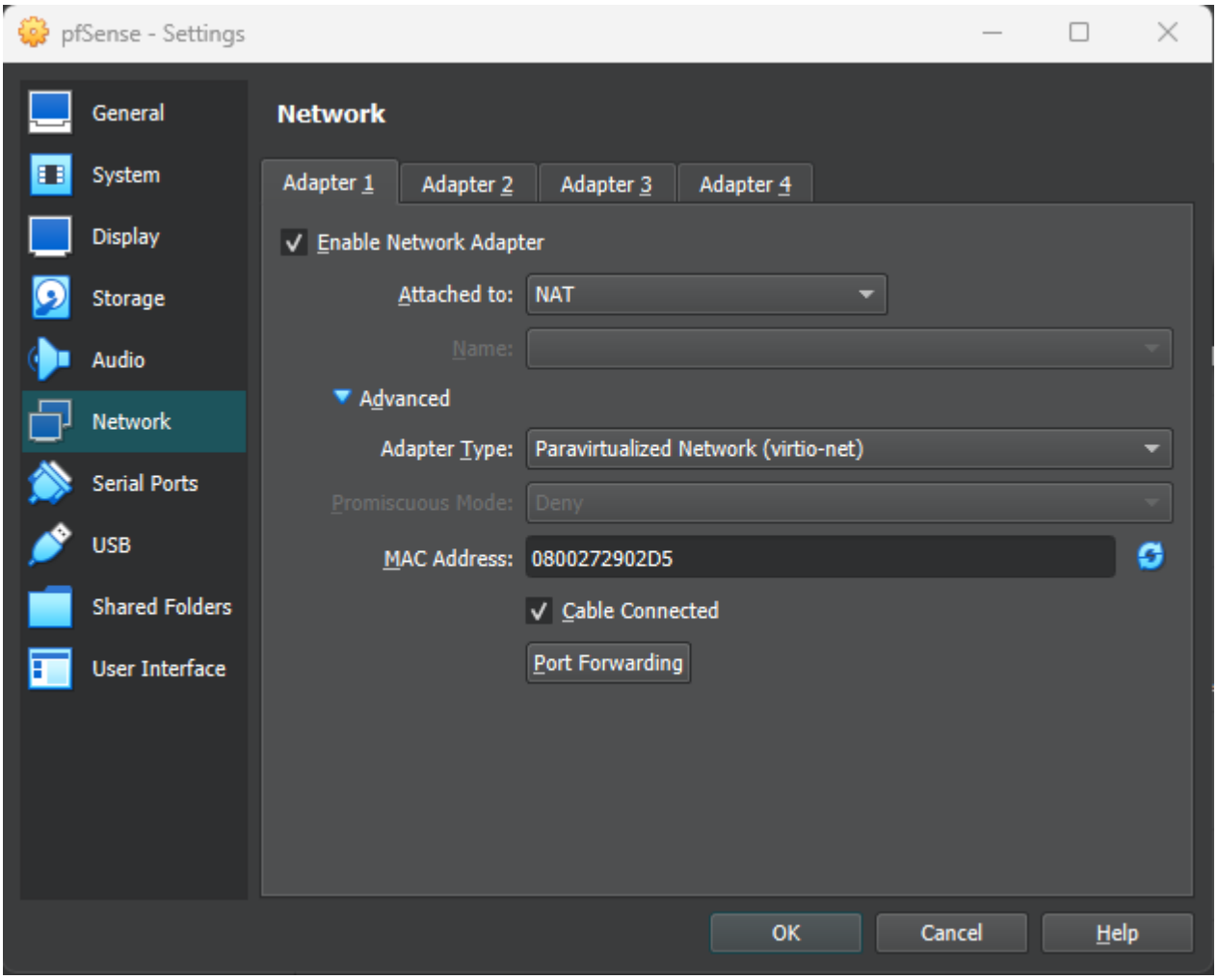


I also disable **Audio** and **USB** since I won't need them

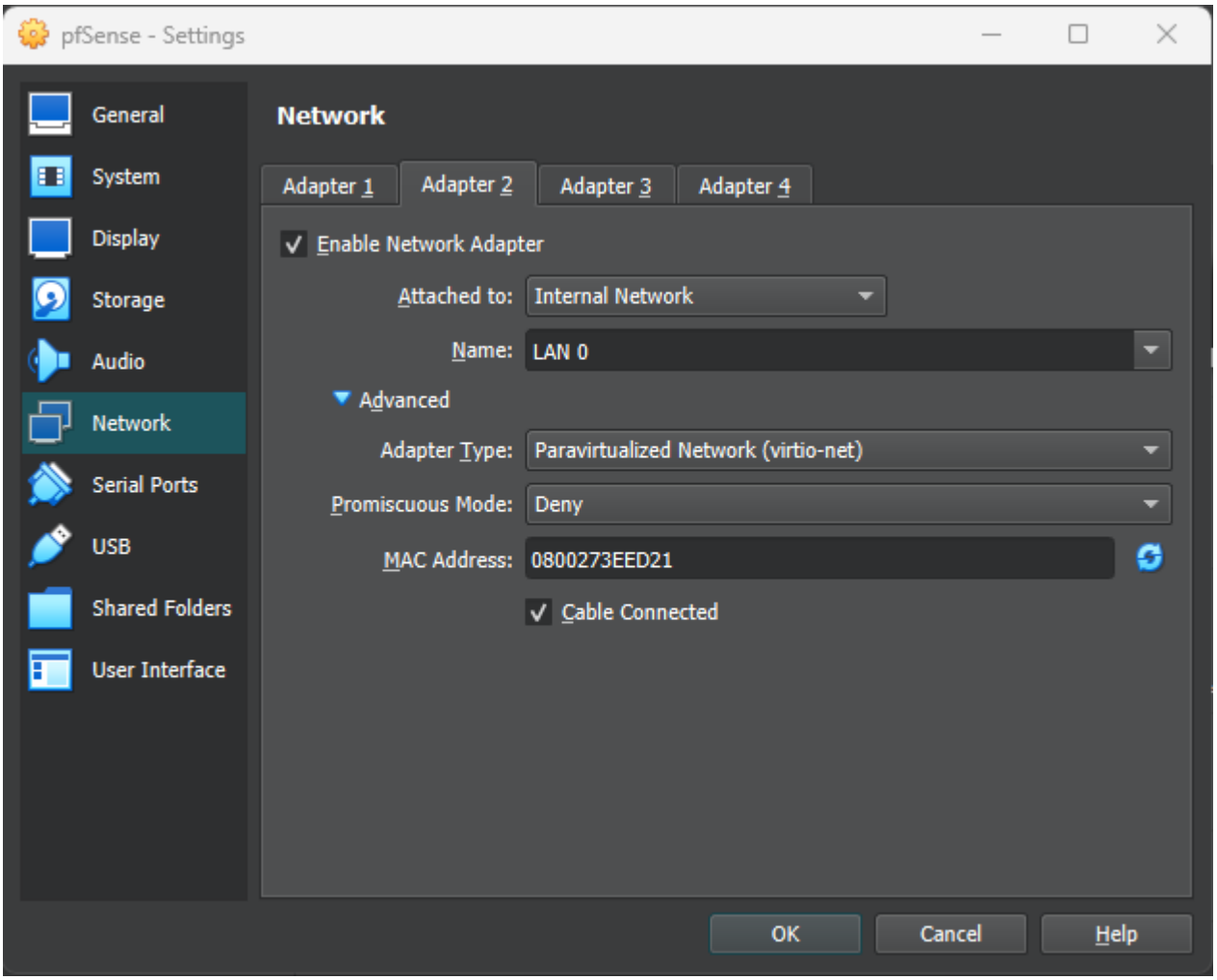




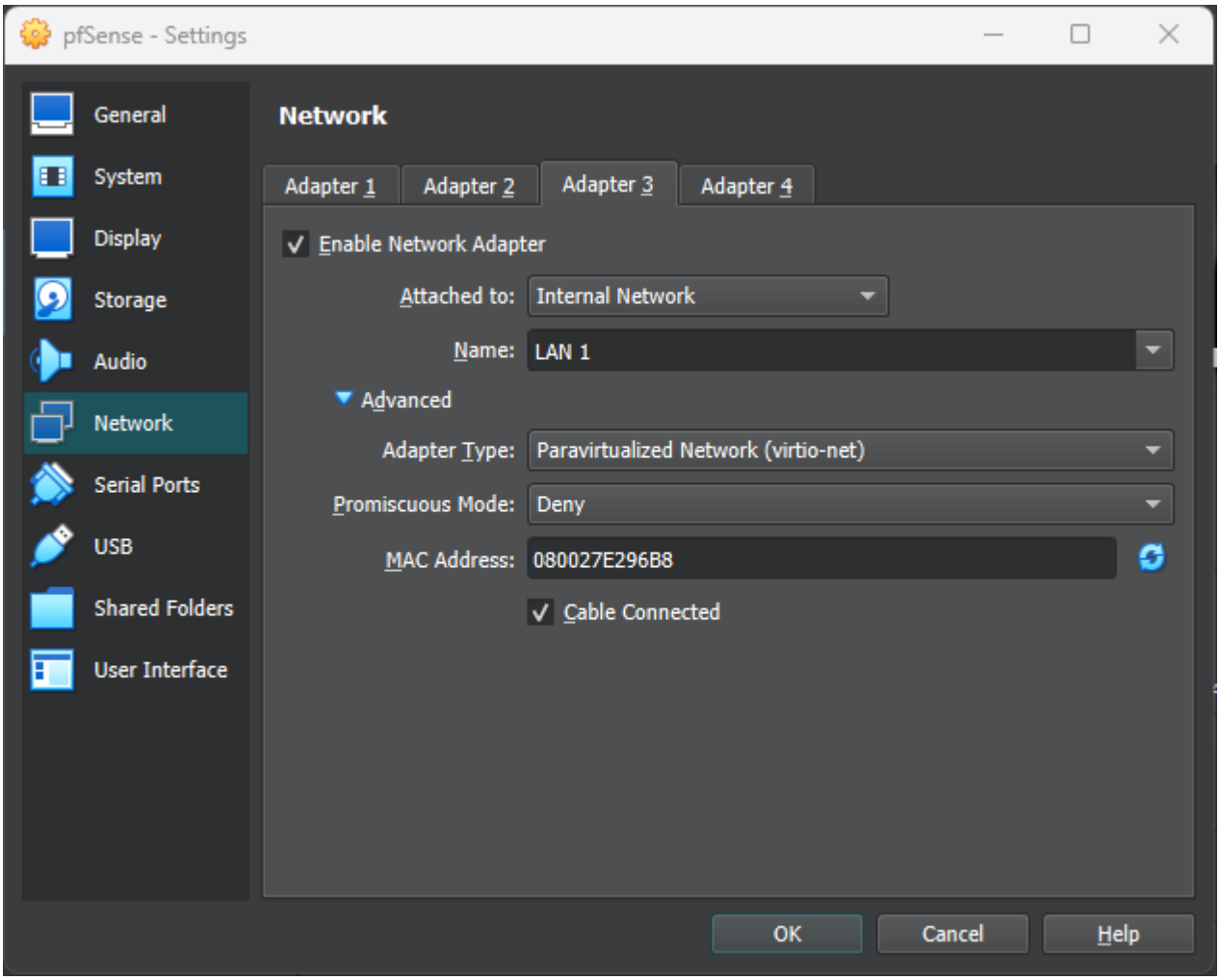
On **Network -> Adapter 1** I select **NAT** and from the **Advanced** section I select **Paravirtualized Network (virtio-net)** as the Adapter Type

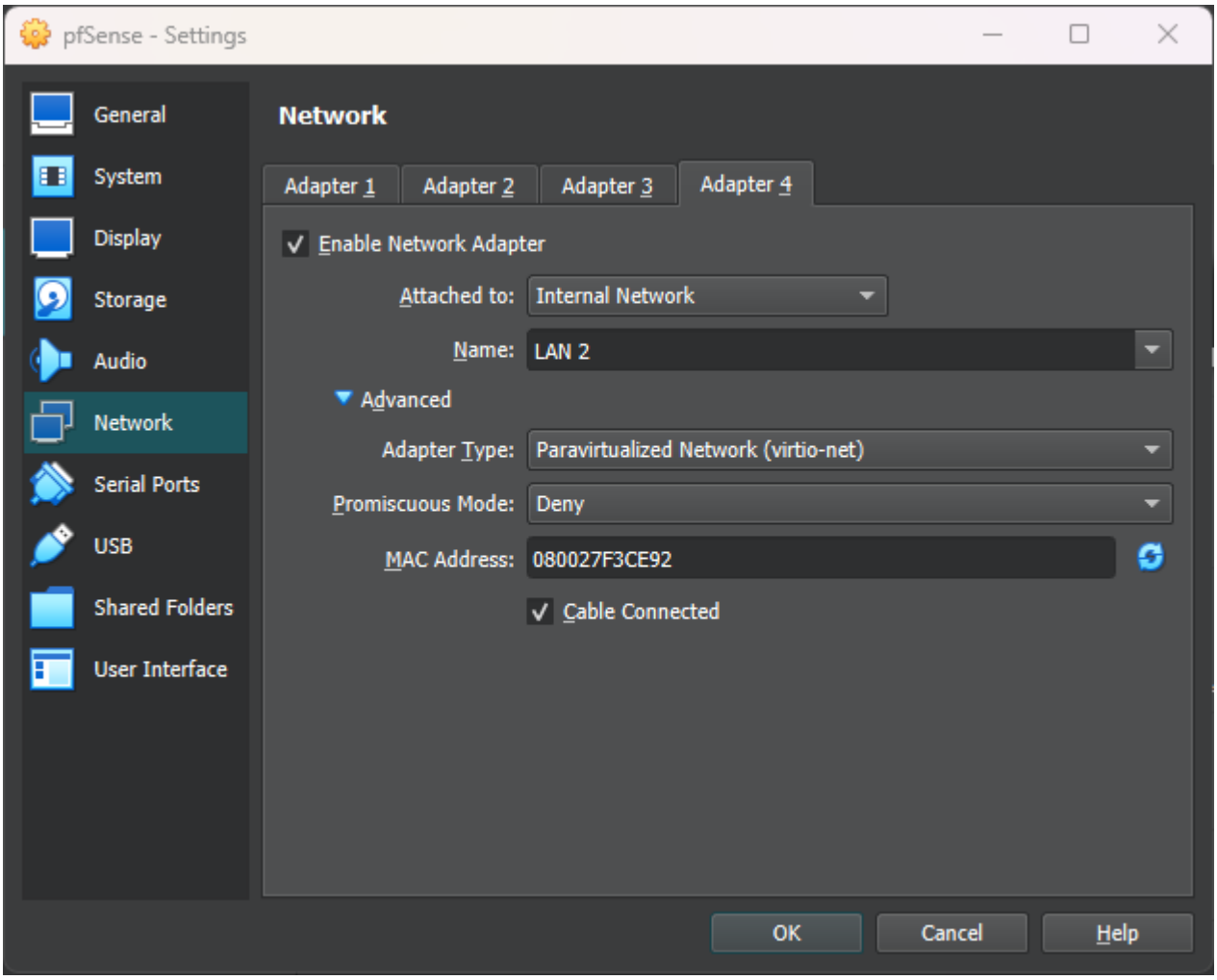


Then I enable the **Adapter 2** and attach it to **Internal Network**. I name it **LAN 0** and, from **Advanced** i select **Paravirtualized Network** (**virtio-net**) as the Adapter Type



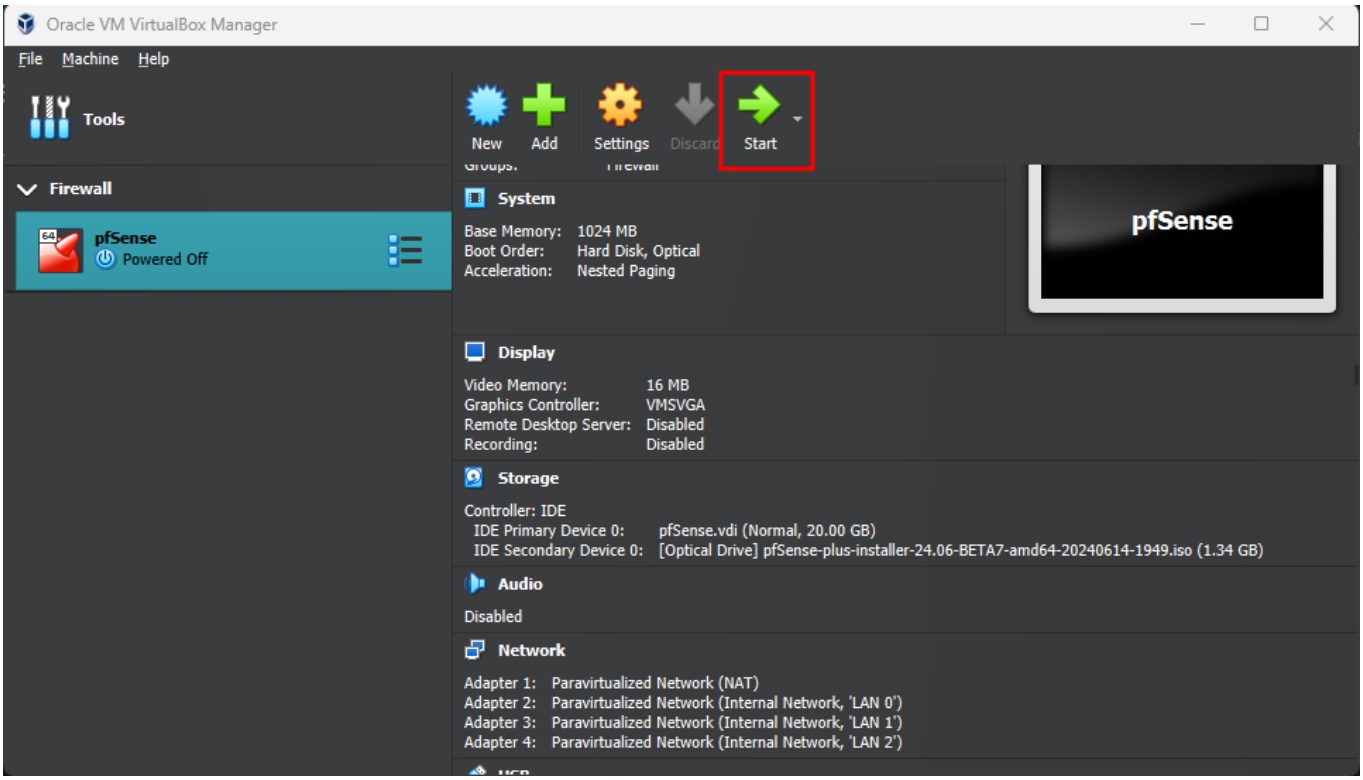
I also do the same on **Adapter 3 and 4** and name them **LAN 1 and LAN 2**


pfSense - 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:
Internal Network
Name:
LAN 1
Advanced
Adapter Type:
Paravirtualized Network (virtio-net)
Promiscuous Mode:
Deny
MAC Address:
080027E296B8
Cable Connected
OK
Cancel
Help

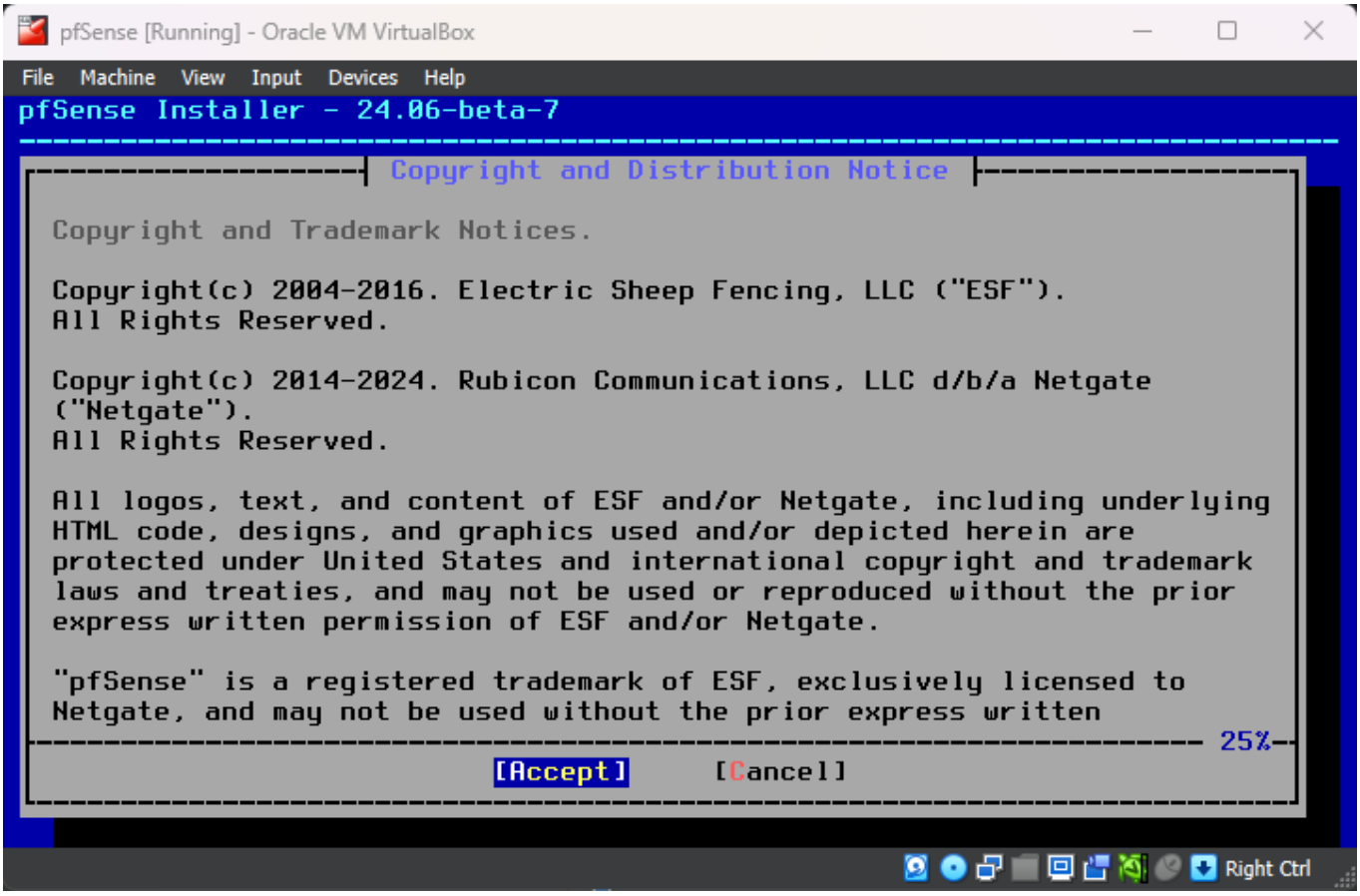


pfSense Installation

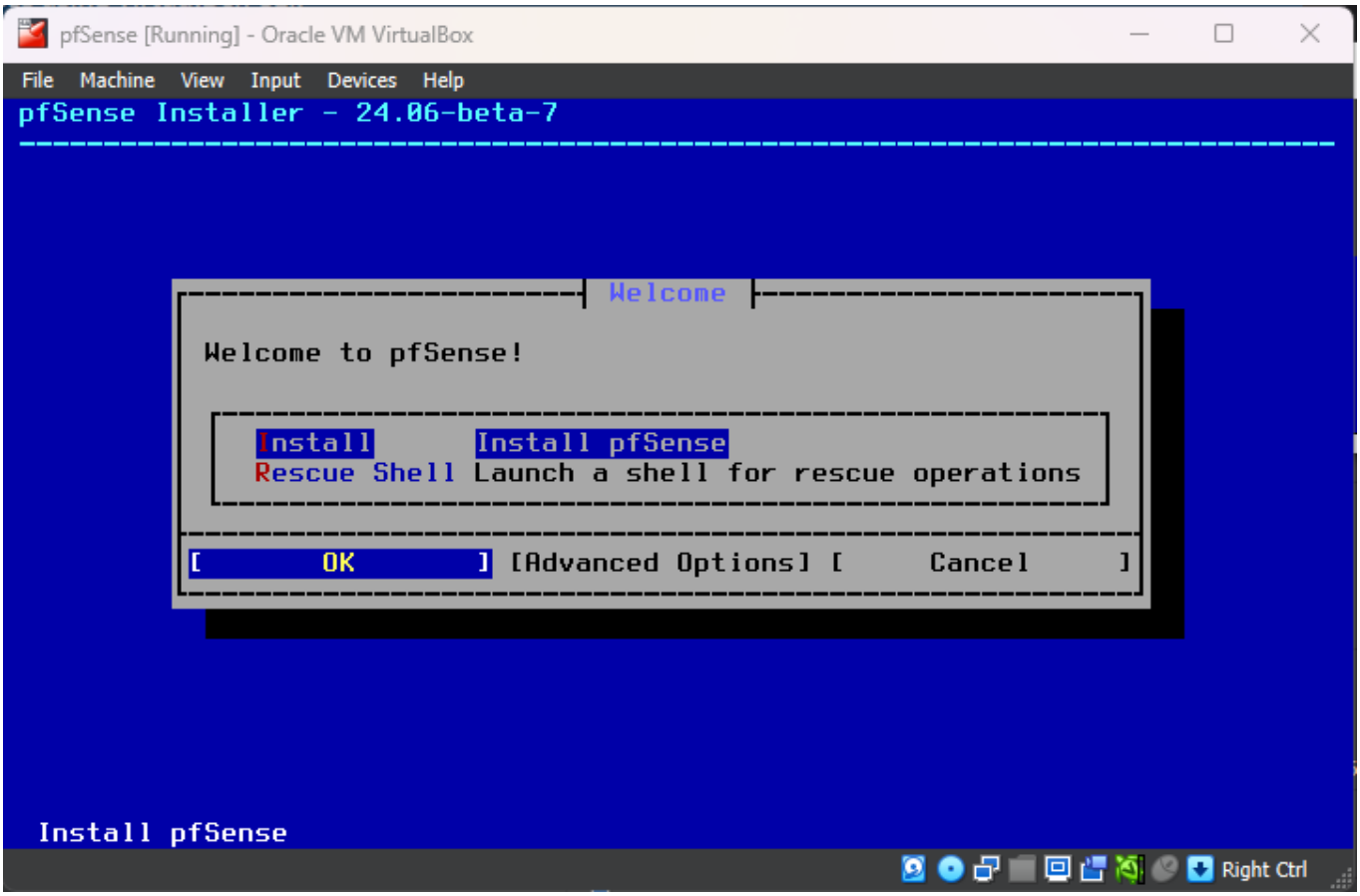
I can now **Start** the machine



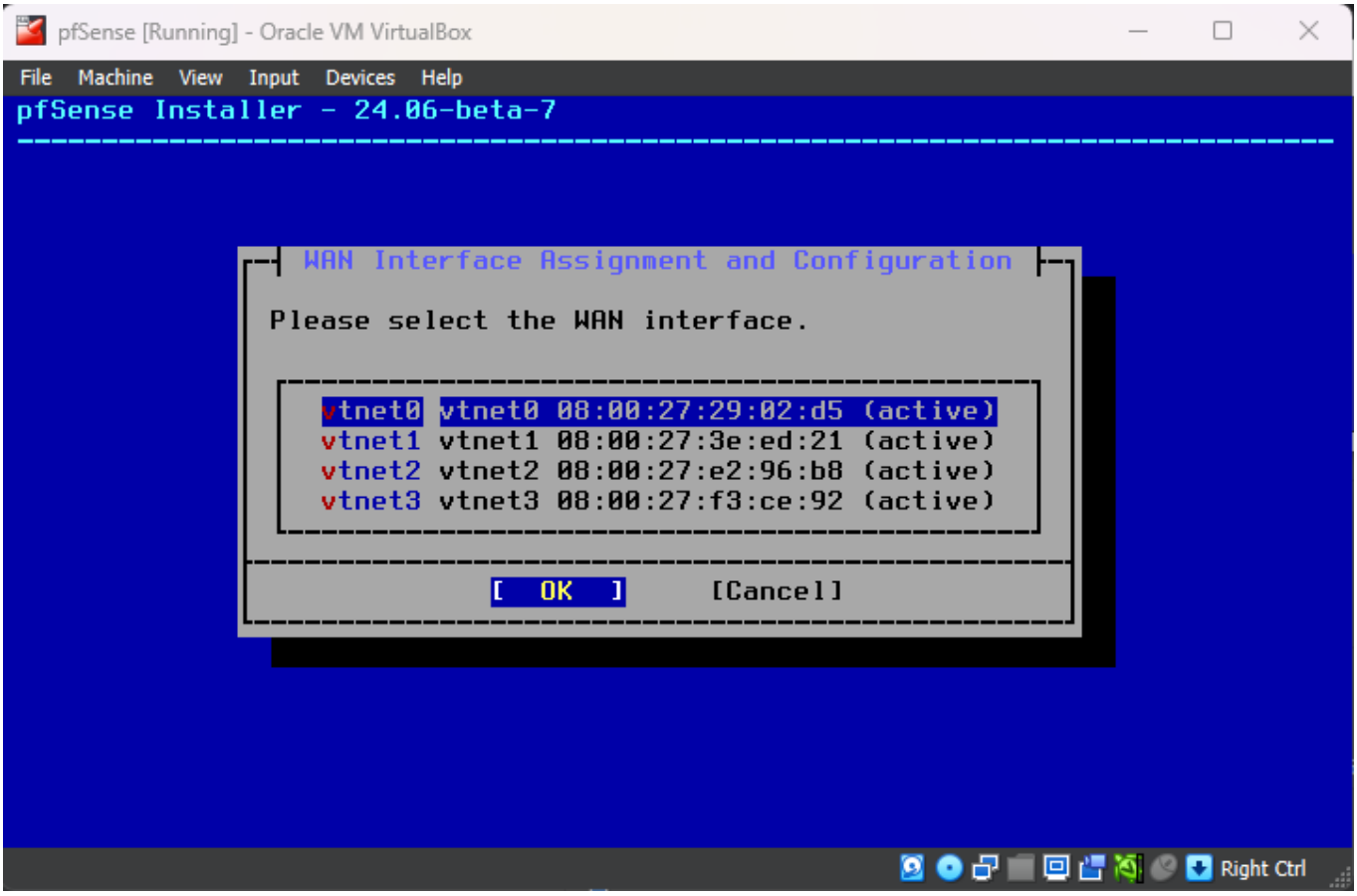
I press **Enter** to Accept the agreement



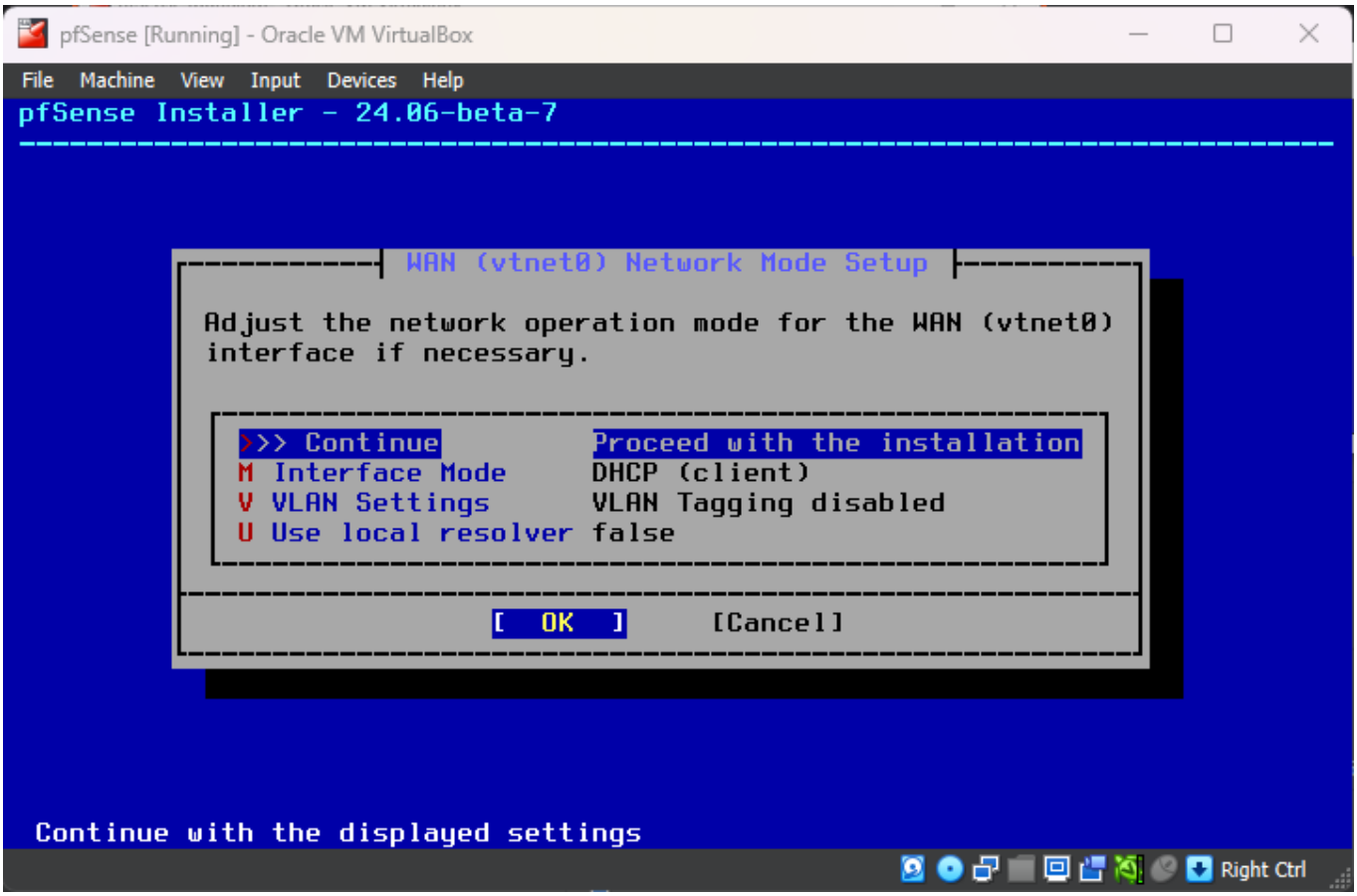
And then press **Enter** again to **Install**



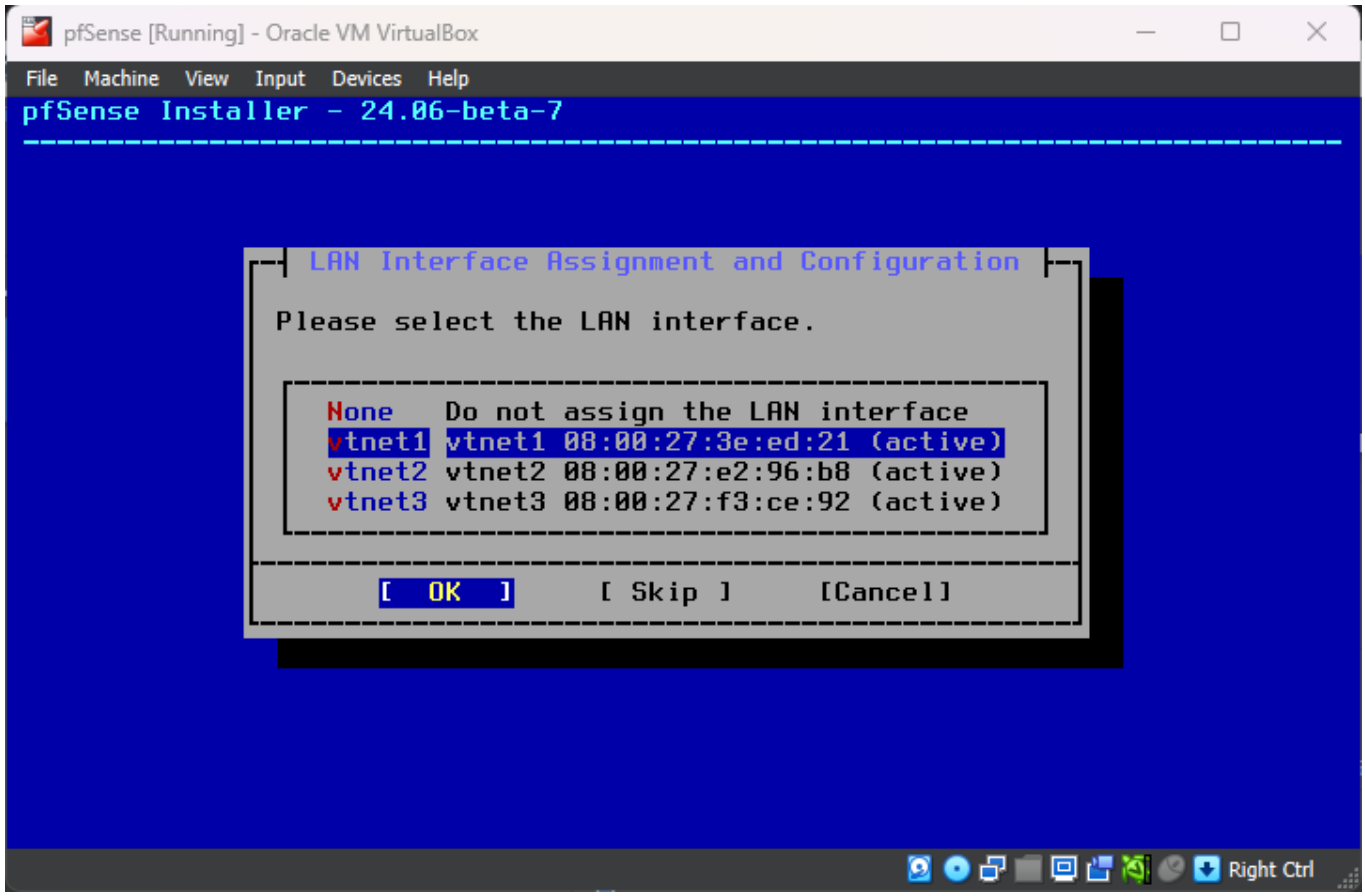
I select **vtnet0** to use as the WAN interface



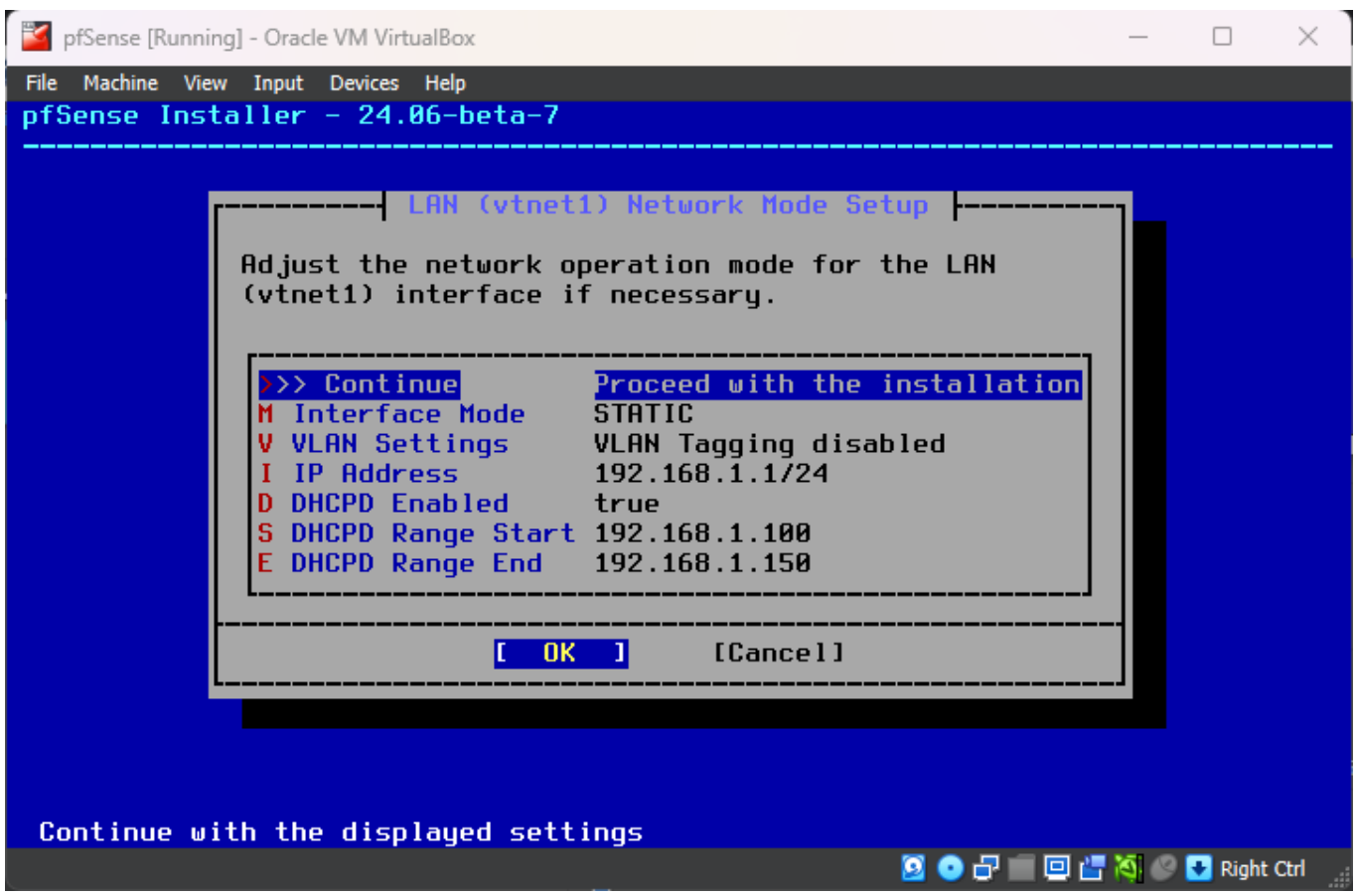
I press **Enter** to leave the settings as default and continue



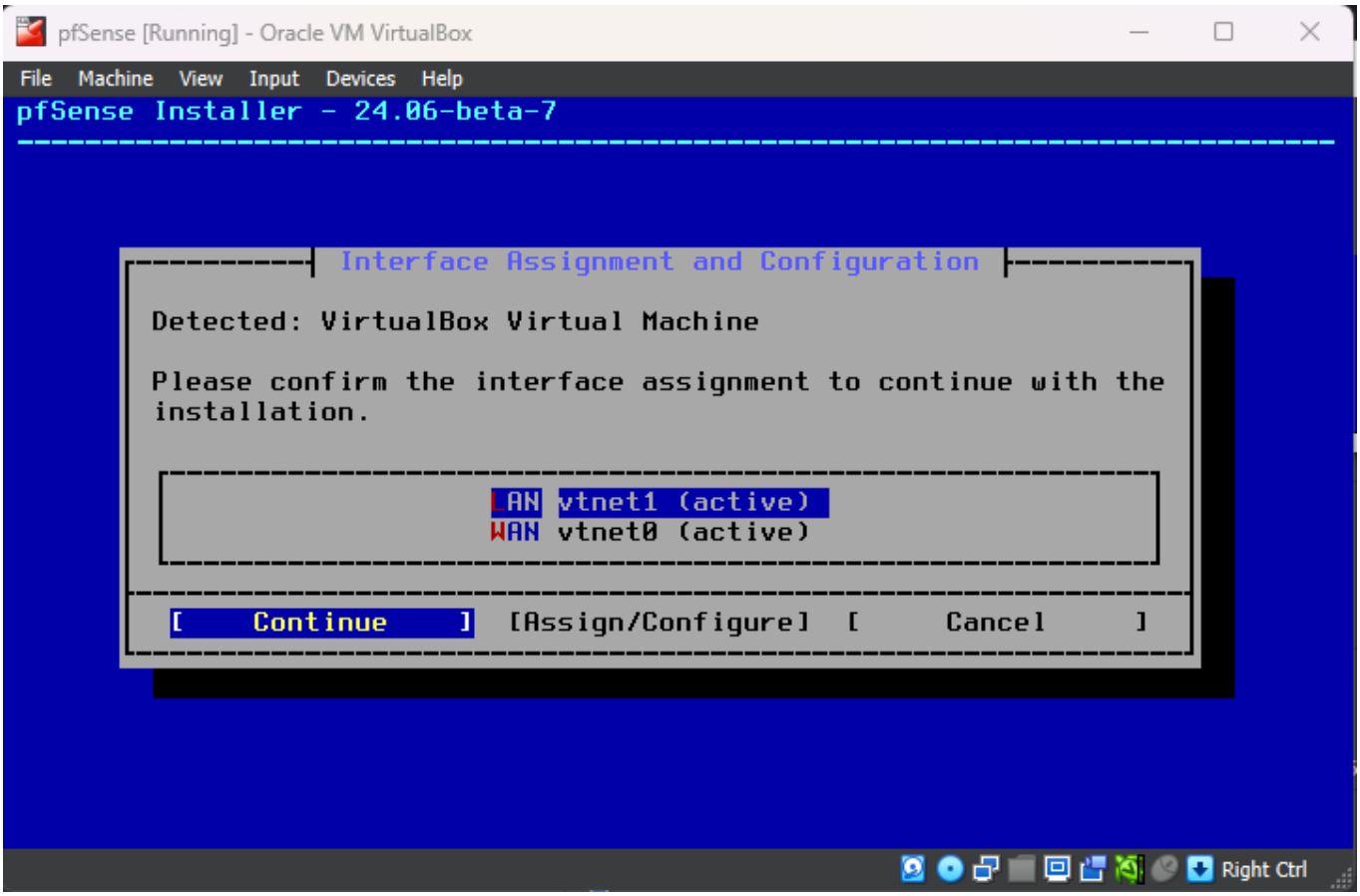
I select **vtnet1** as the **LAN** interface



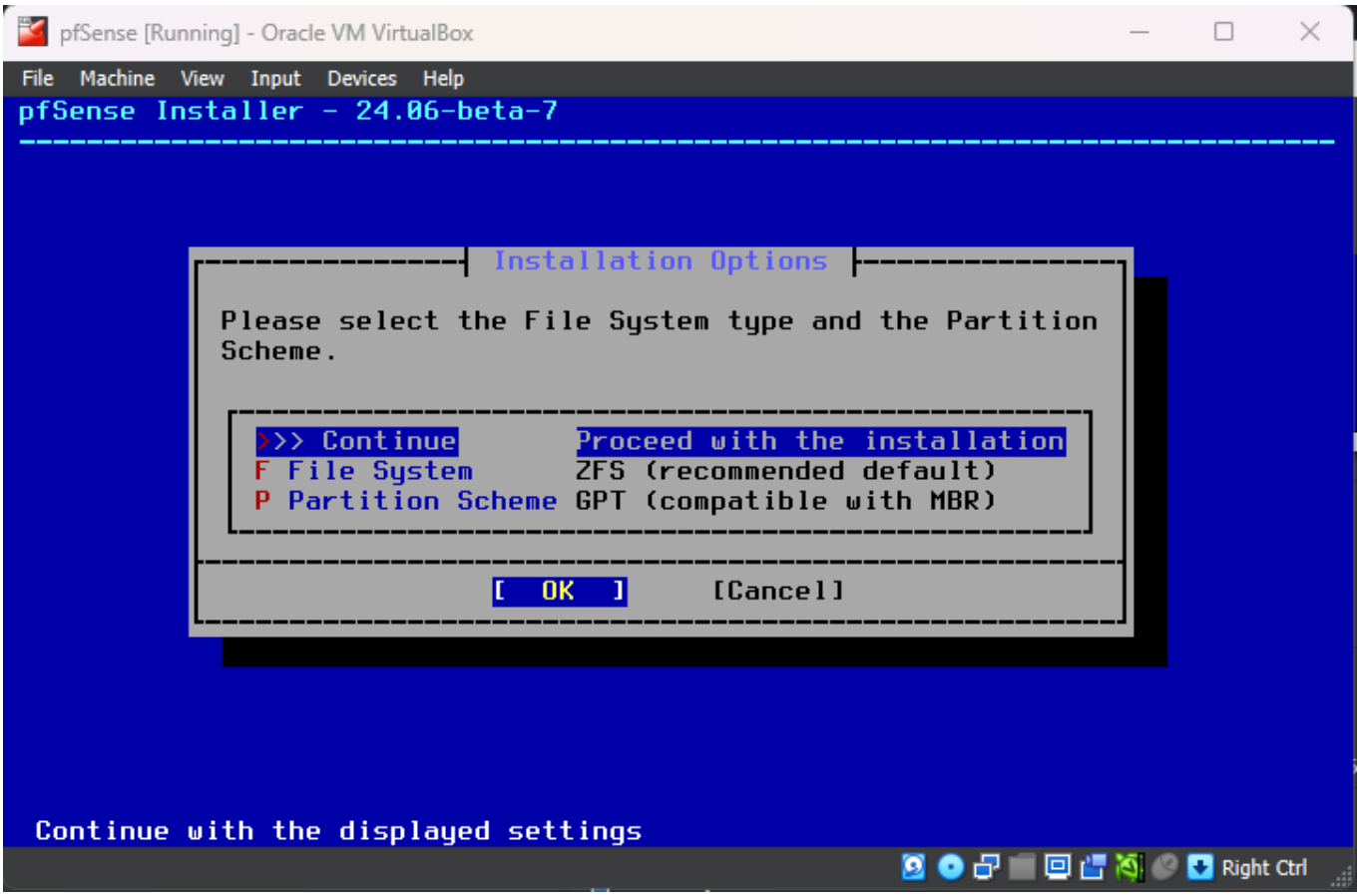
I leave default settings for this as well



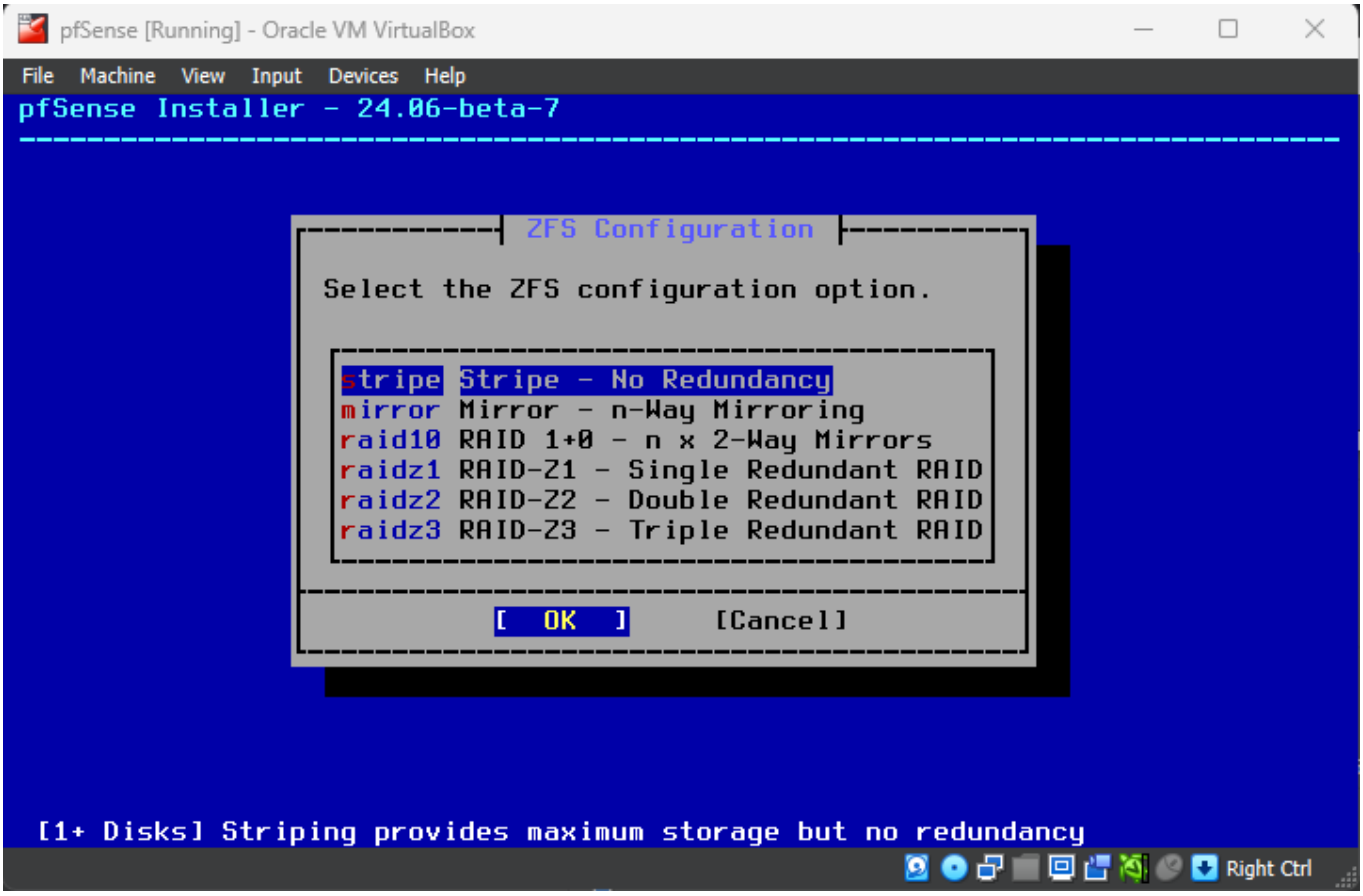
Then I press **Enter** again to **continue** the installation



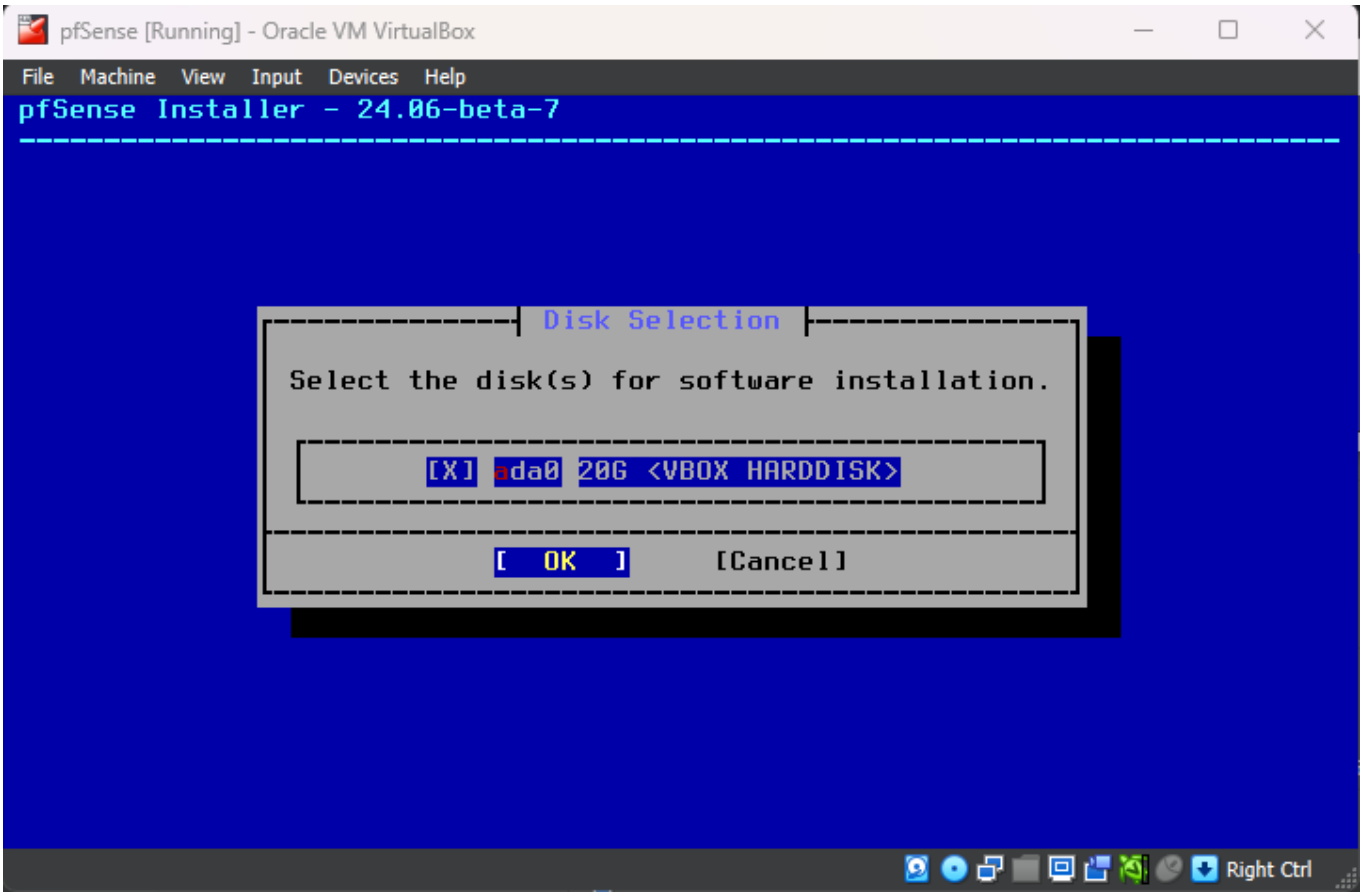
I then **Continue** with the default File System Type and Partition



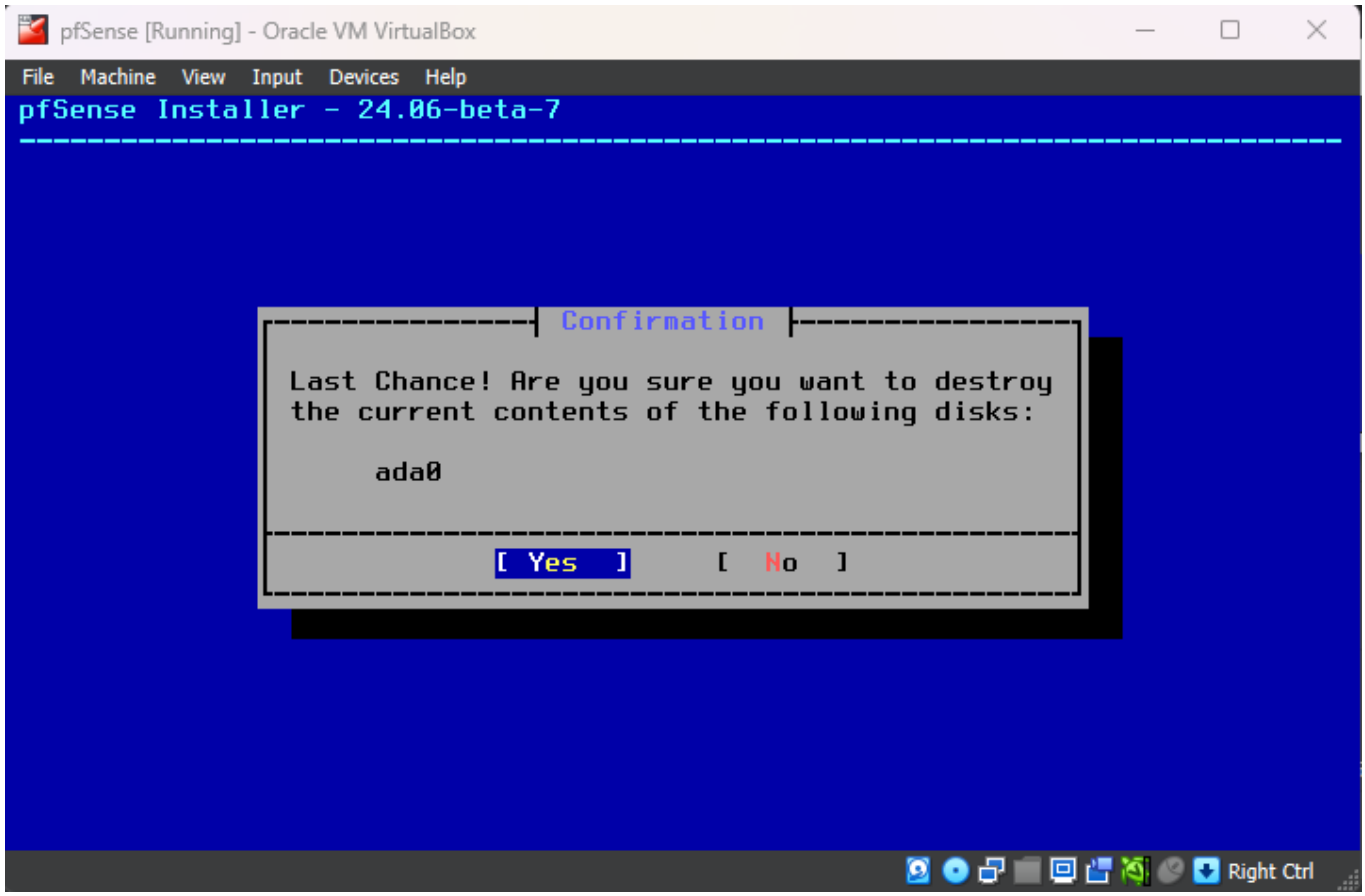
I select **Stripe - No Redundancy**



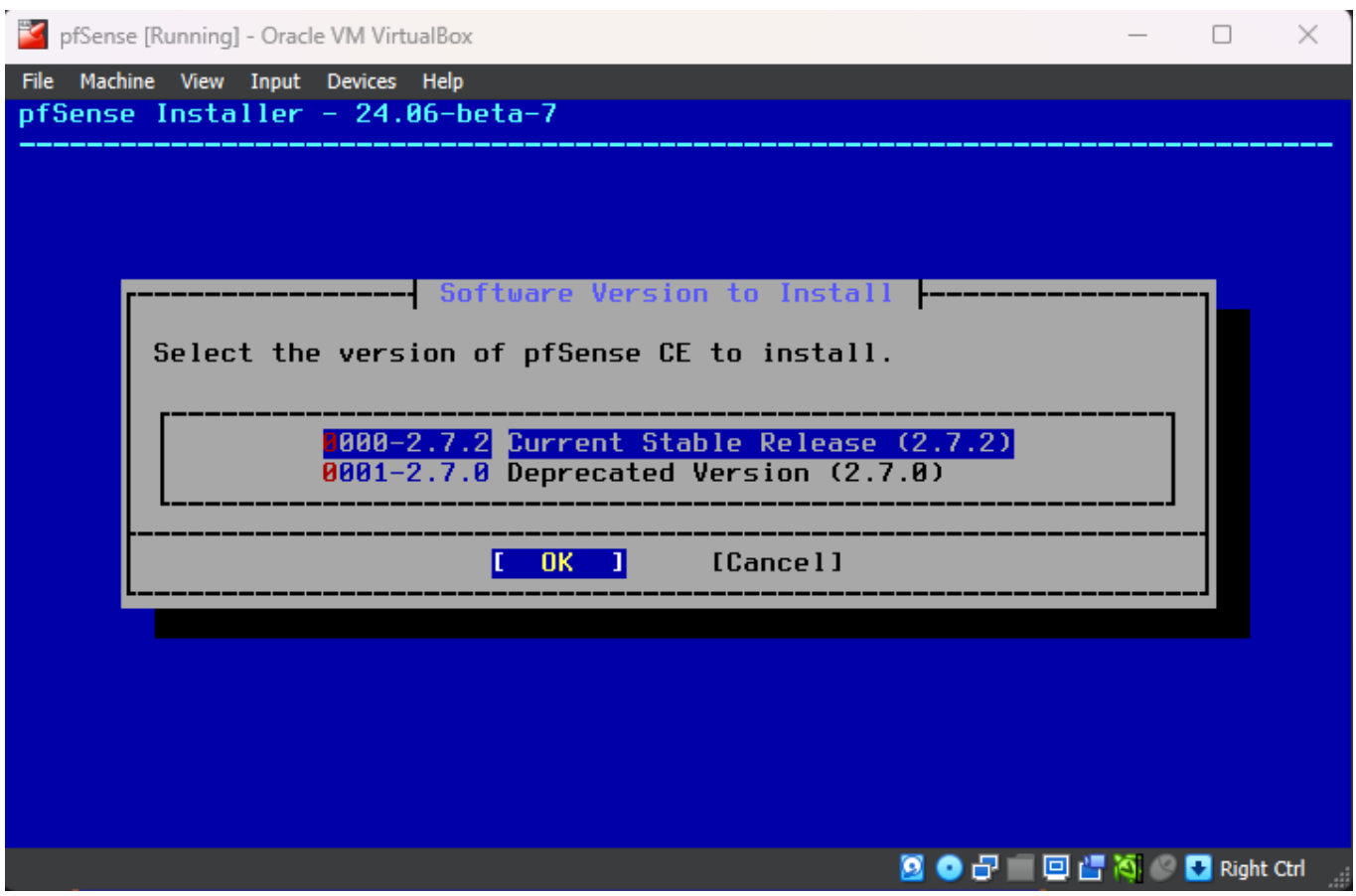
Leave the selected partition and press **Enter**



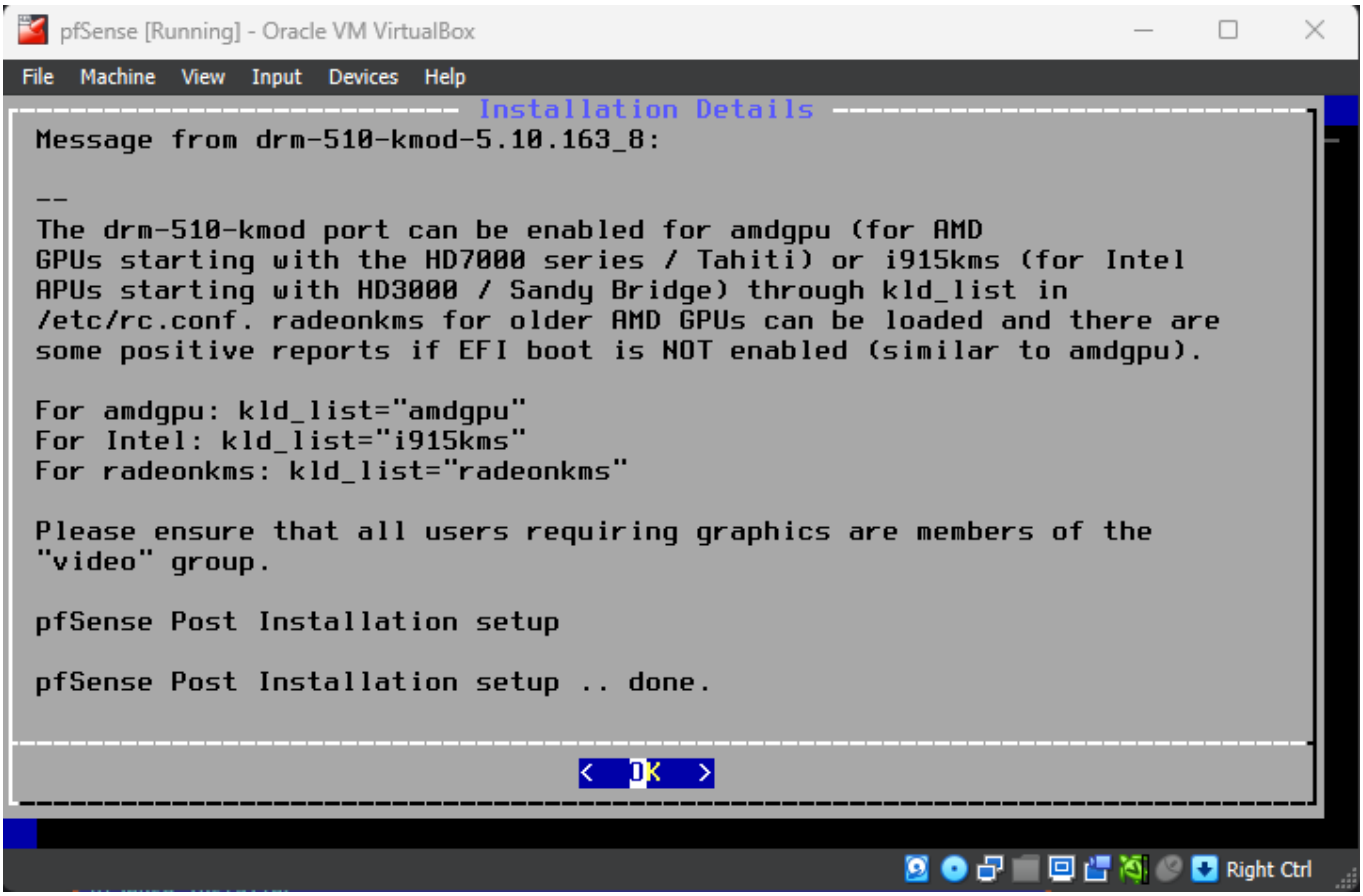
Confirm the partition



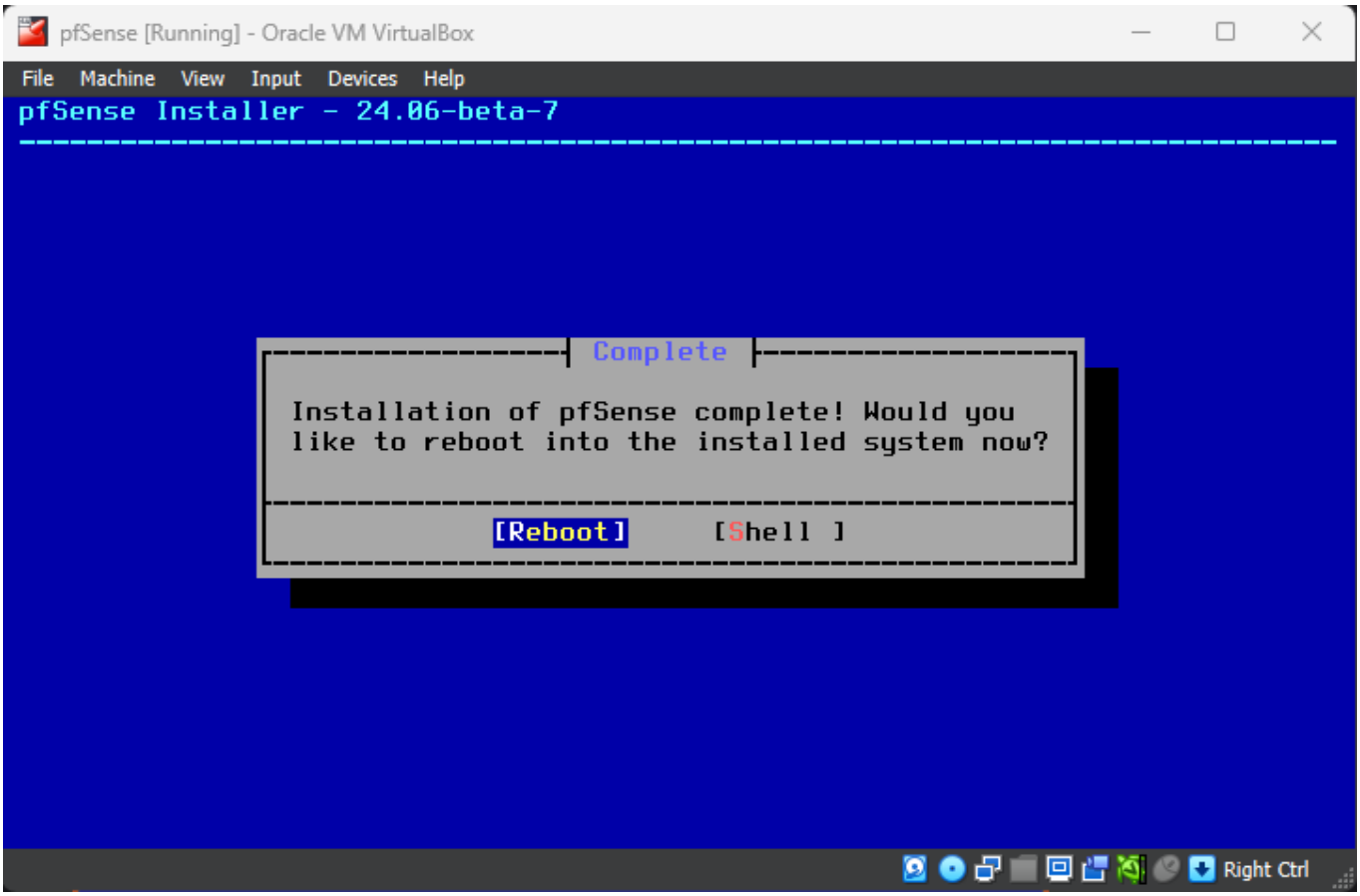
Select the **Current Stable Release** (2.7.2 in my case)



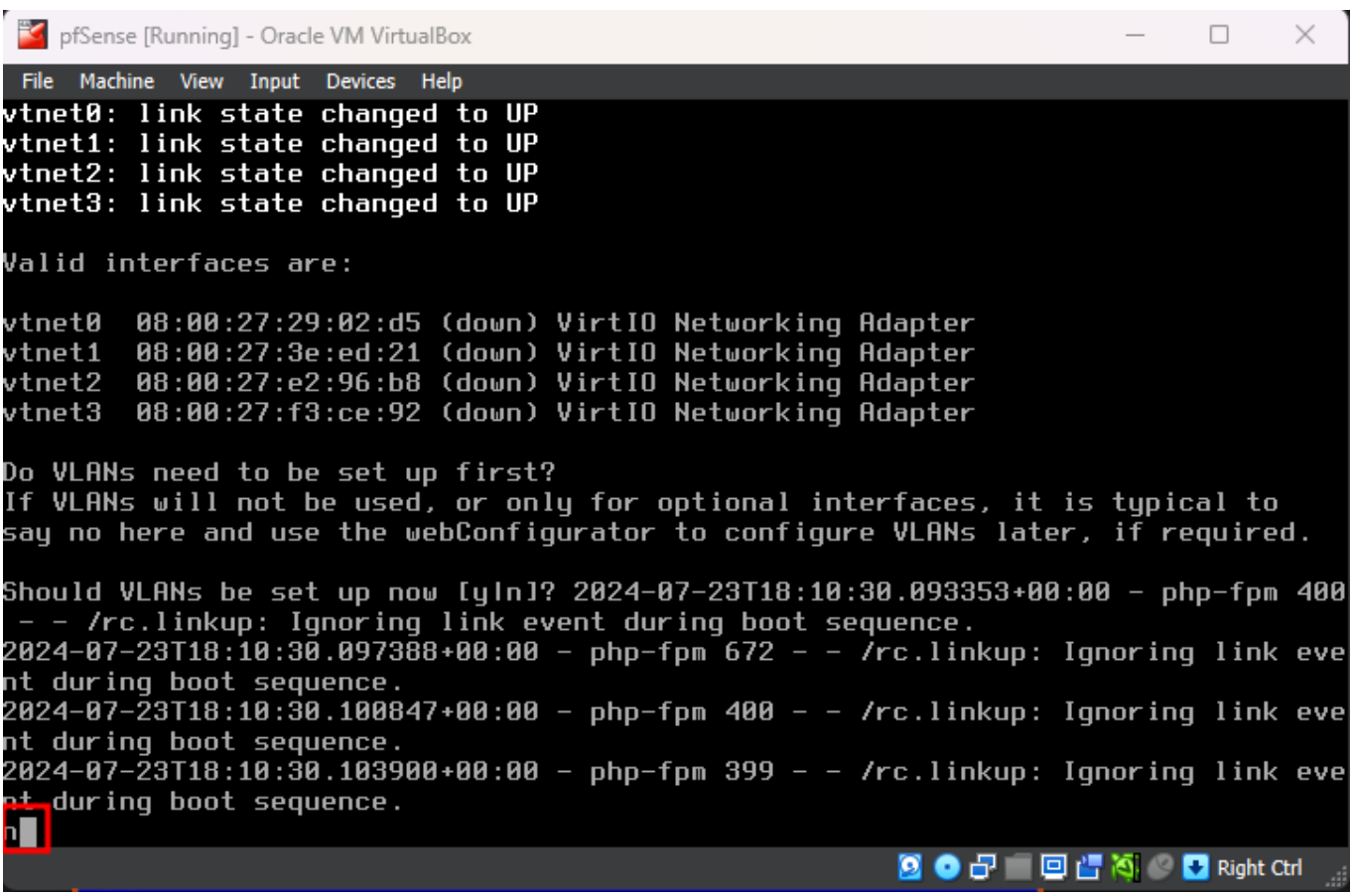
Once it finished it gave me this screen



I then pressed **Enter** to reboot



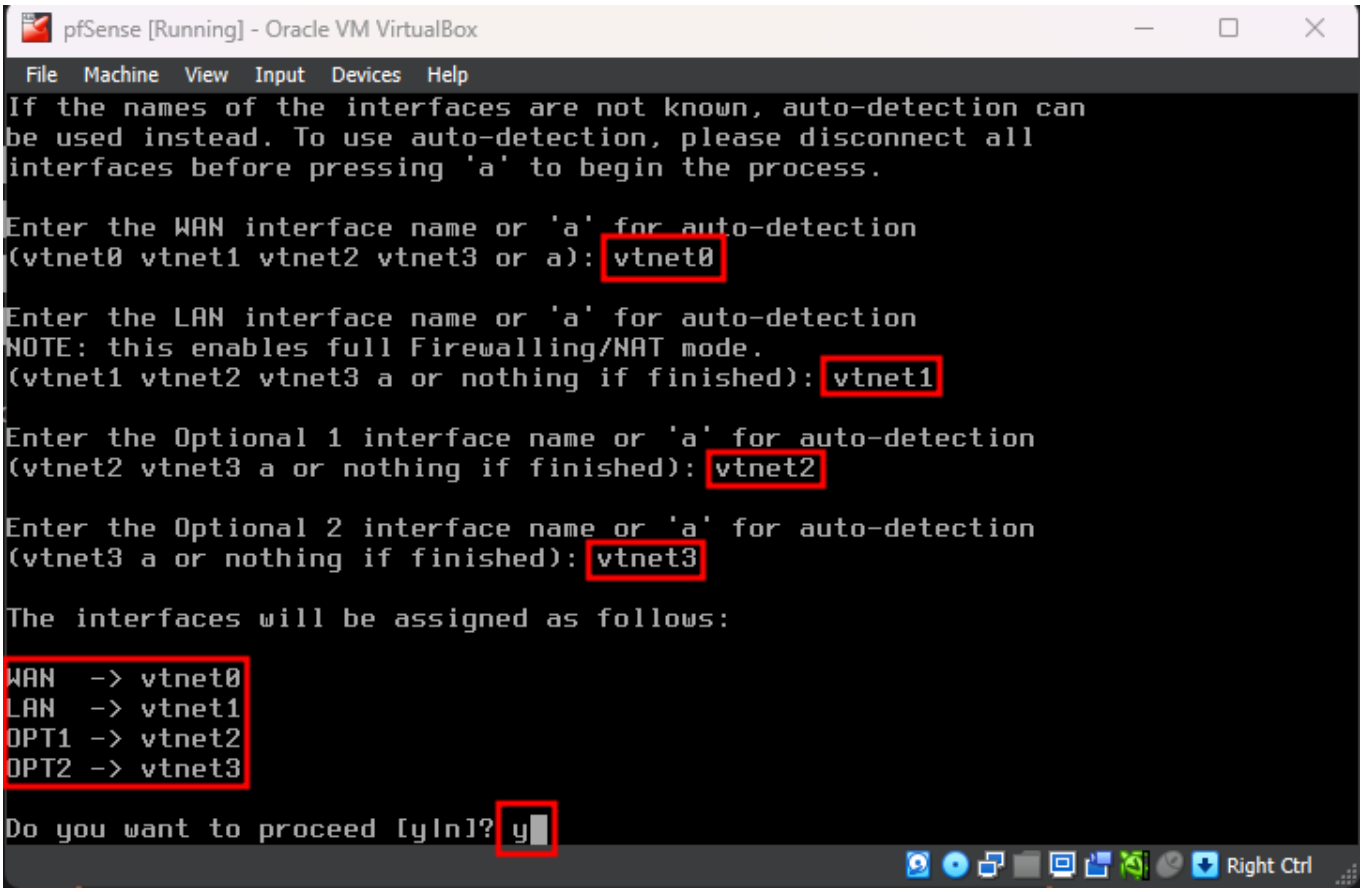
I then press n to not configure VLANs



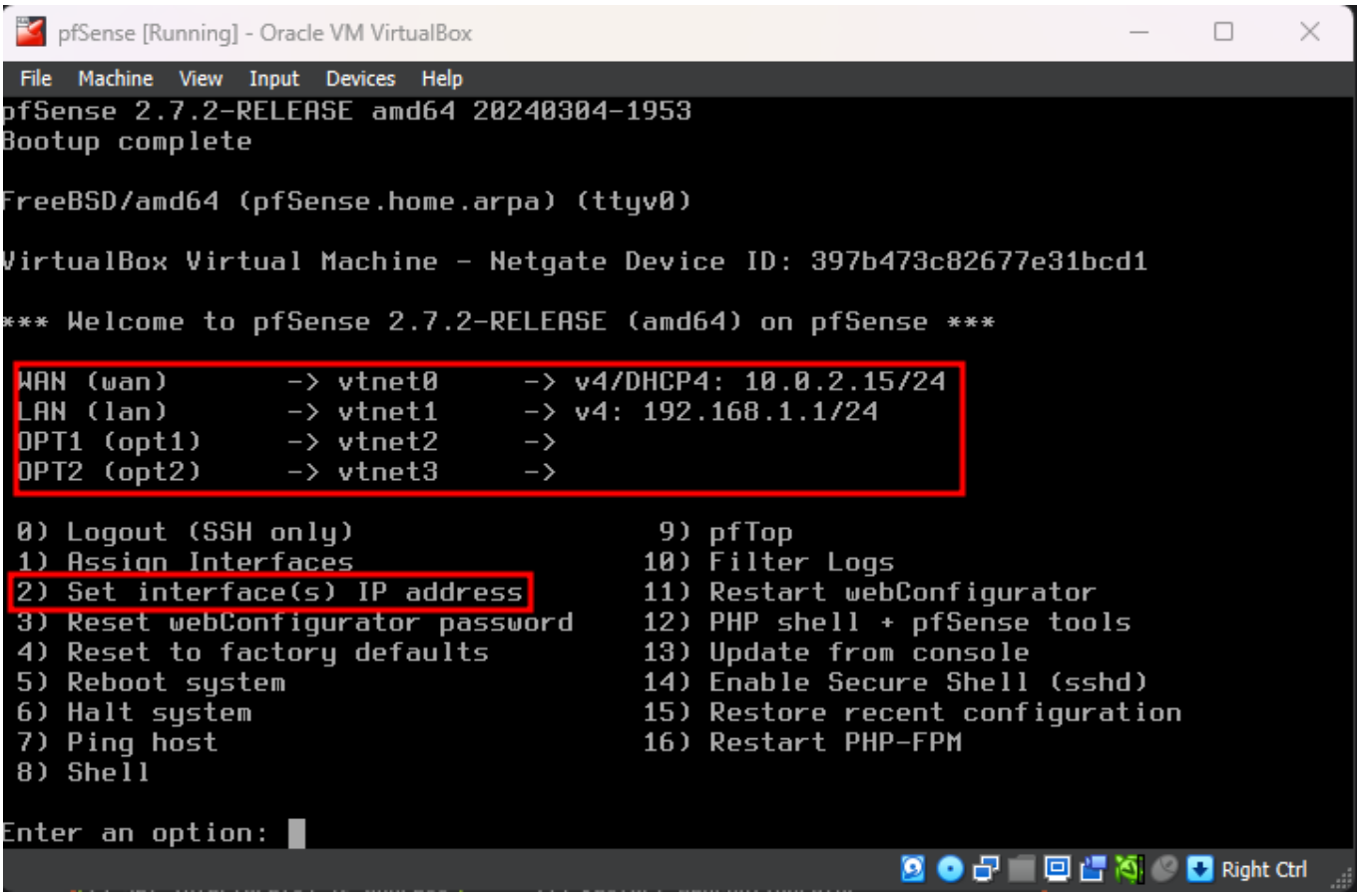
Then i assign the interfaces like this:

Enter the WAN interface name: **vtnet0**
Enter the LAN interface name: **vtnet1**
Enter the Optional 1 interface name: **vtnet2**
Enter the Optional 2 interface name: **vtnet3**

and confirm

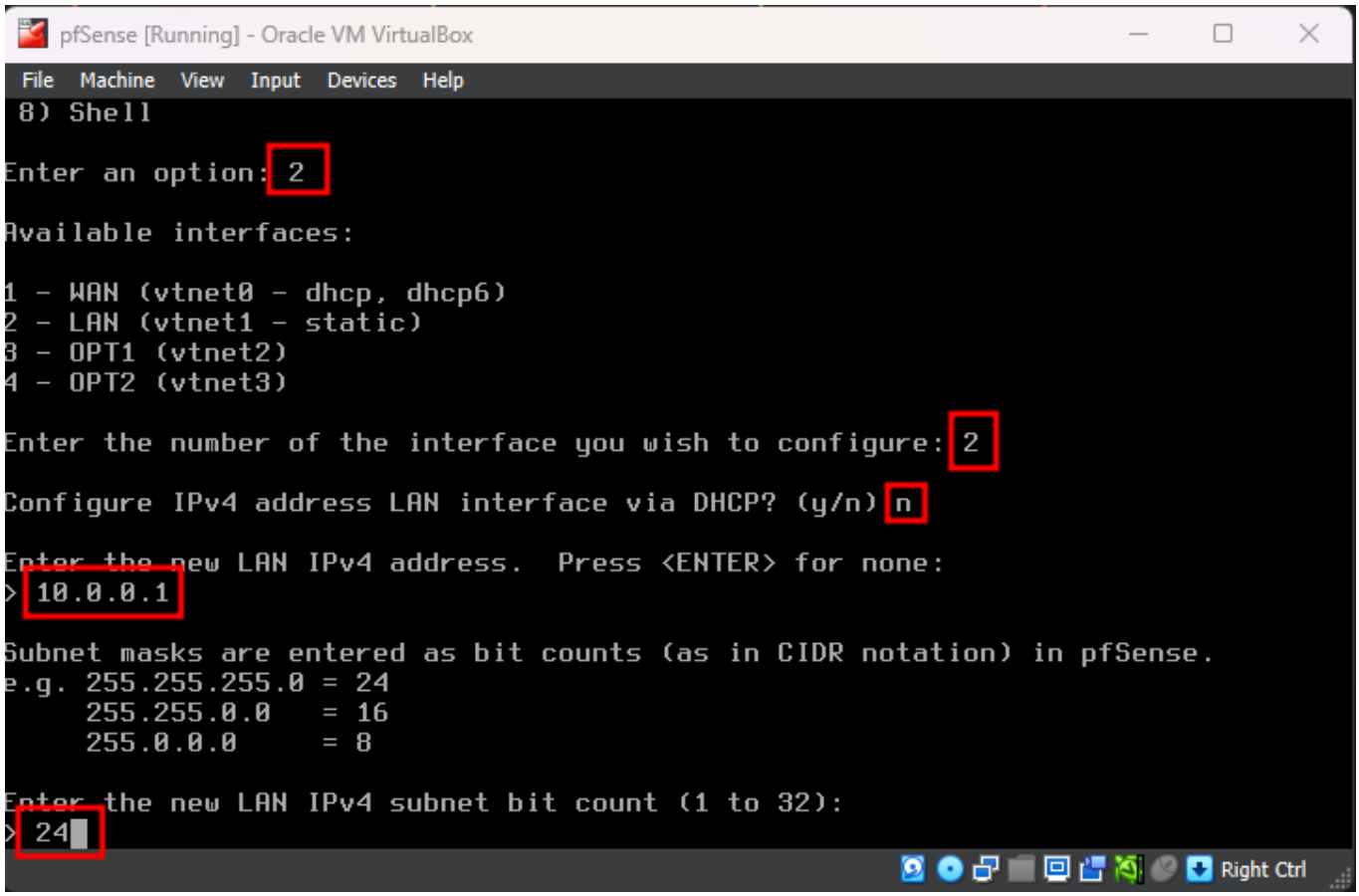


Since the **WAN** interface of pfSense is managed by VirtualBox it has been assigned an IPv4 address by the VirtualBox DHCP server. pfSense has also assigned an IPv4 address to the **LAN** interface using its DHCP service. The **OPT1** and **OPT2** interfaces have not been assigned any IP address. We do not want the IP addresses of the interfaces to change on boot so we will assign static IPv4 addresses to the **LAN**, **OPT1** and **OPT2** interfaces.



So now i configure the LAN (vtnet1). I Enter **2** to select "Set Interface(s) IP address" and enter **2** again to select the **LAN** interface.

Configure IPv4 address LAN interface via DHCP?: **n**
Enter the new LAN IPv4 address: **10.0.0.1**
Enter the new LAN IPv4 subnet bit count: **24**



I then press **Enter** since it's a **LAN** interface and we don't need to worry about configuring the upstream gateway.

Configure IPv6 address LAN interface via DHCP6: **n**
For the new LAN IPv6 address question press **Enter**
Do you want to enable the DHCP server on LAN?: **y**
Enter the start address of the IPv4 client address range: **10.0.0.11**
Enter the end address of the IPv4 client address range: **10.0.0.243**
Do you want to revert to HTTP as the webConfigurator protocol?: **n**

```
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: 10.0.0.11
Enter the end address of the IPv4 client address range: 10.0.0.243
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 10.0.0.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.0.0.1/

Press <ENTER> to continue.
Right Ctrl
```

Now the IP address of the **LAN** interfaces has changed

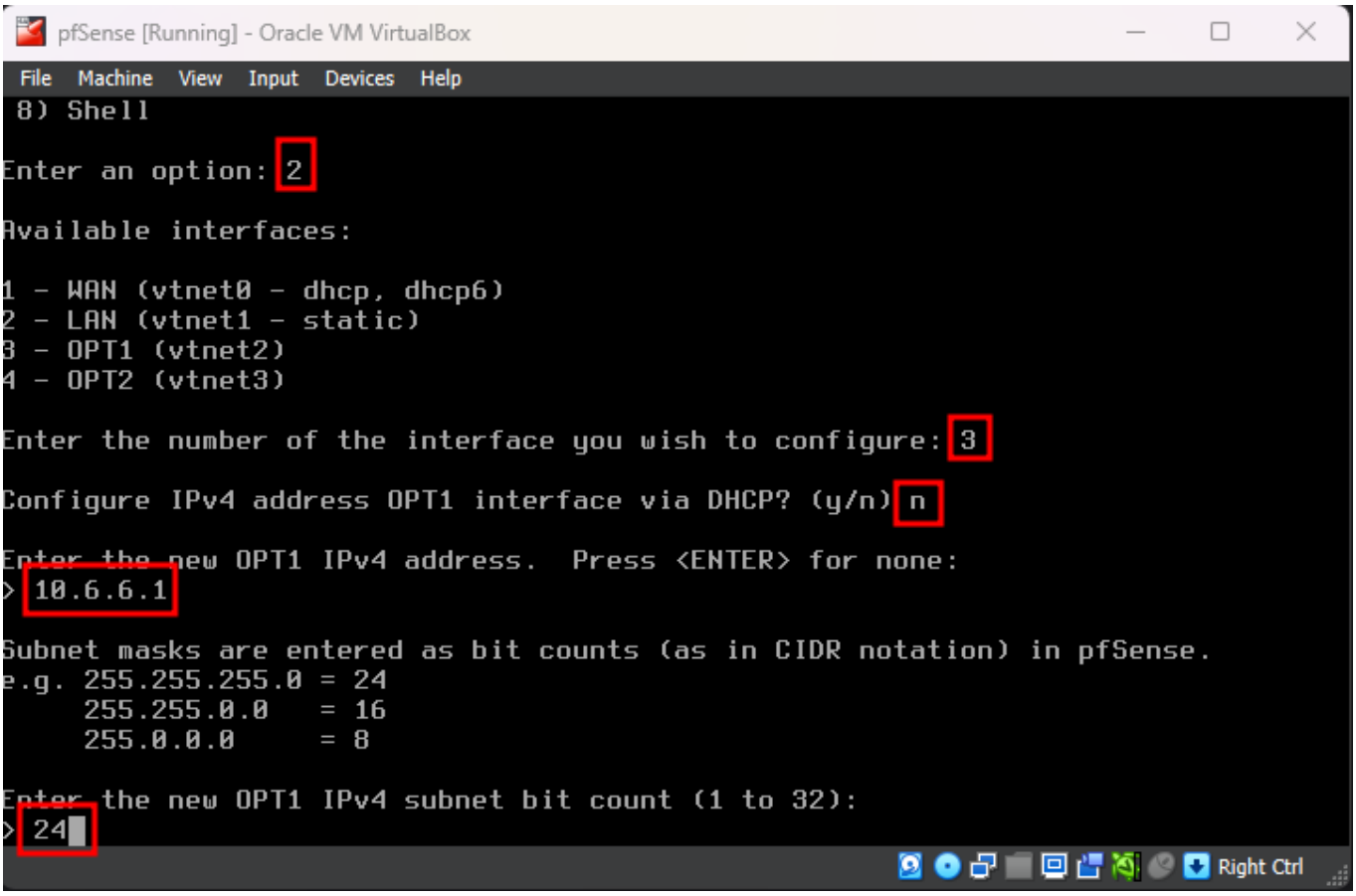
```
pfSense [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.0.0.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 397b473c82677e31bcd1

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 10.0.2.15/24
 LAN (lan)       -> vtnet1     -> v4: 10.0.0.1/24
 OPT1 (opt1)     -> vtnet2     ->
 OPT2 (opt2)     -> vtnet3     ->

 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:
Right Ctrl
```

Then i configure the OPT1(vtnet2) interface. I enter **2** to select “Set interface(s) IP address”. Enter **3** to select the **OPT1** interface.

Configure IPv4 address OPT1 interface via DHCP?: **n**

Enter the new OPT1 IPv4 address: **10.6.6.1**

Enter the new OPT1 IPv4 subnet bit count: **24**



Configure IPv6 address OPT1 interface via DHCP6: **n**

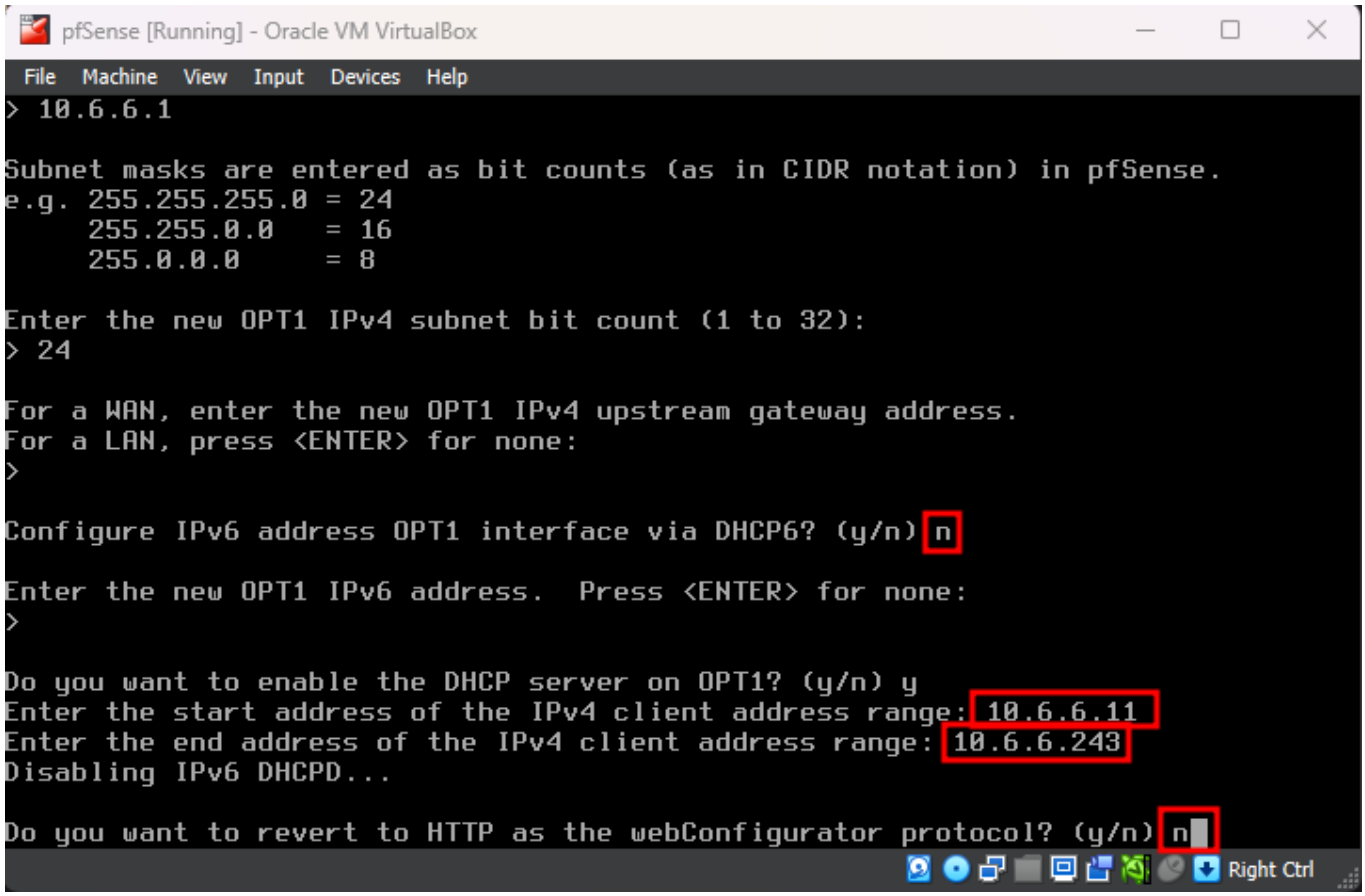
For the new OPT1 IPv6 address question press **Enter**

Do you want to enable the DHCP server on OPT1?: **y**

Enter the start address of the IPv4 client address range: **10.6.6.11**

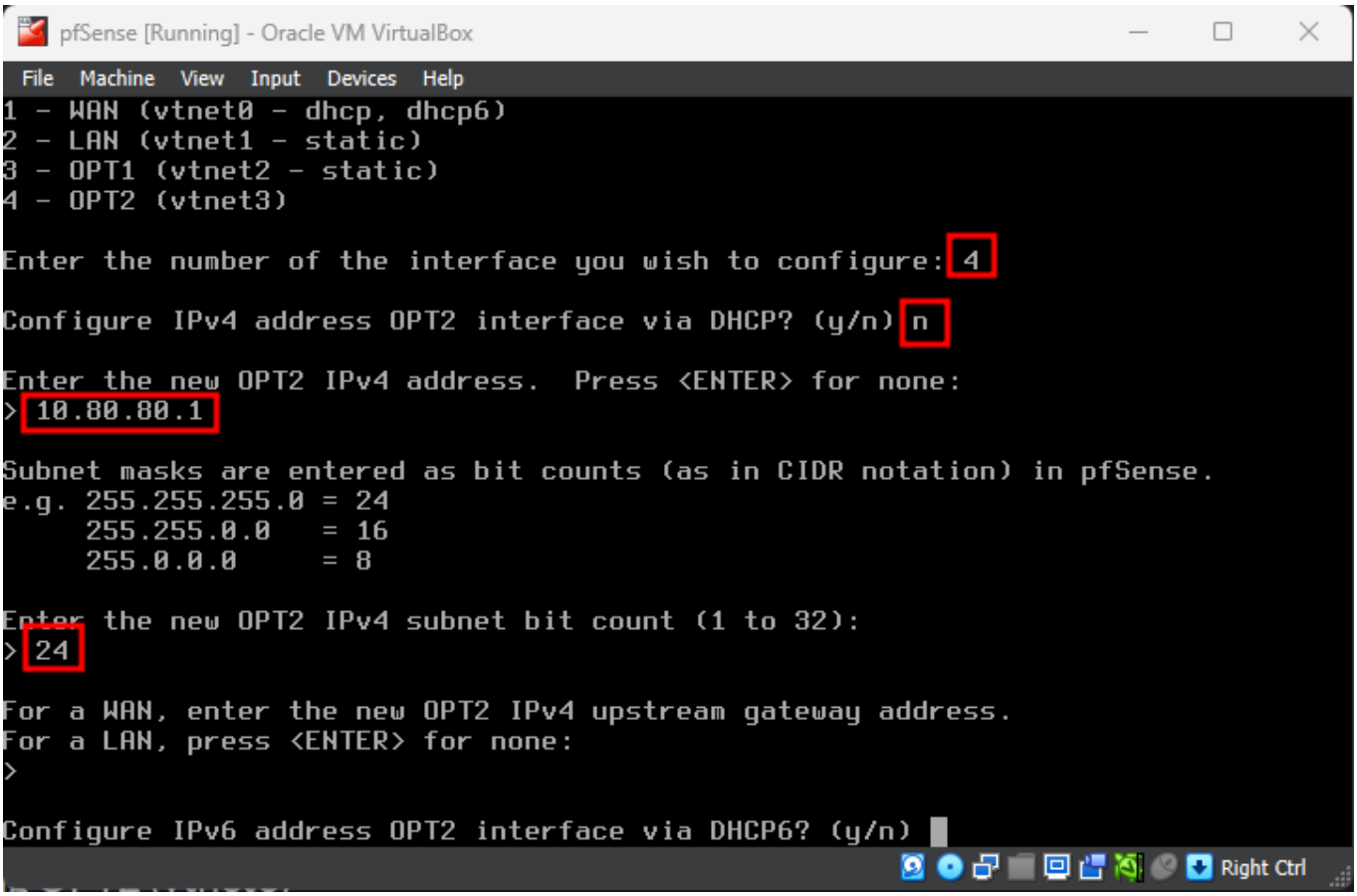
Enter the end address of the IPv4 client address range: **10.6.6.243**

Do you want to revert to HTTP as the webConfigurator protocol?: **n**



Finally I configure the OPT3(vtnet3) interface. I enter **2** to select “Set interface(s) IP address”. Enter **4** to select the **OPT2** interface.

Configure IPv4 address OPT2 interface via DHCP?: **n**
Enter the new OPT2 IPv4 address: **10.80.80.1**
Enter the new OPT2 IPv4 subnet bit count: **24**

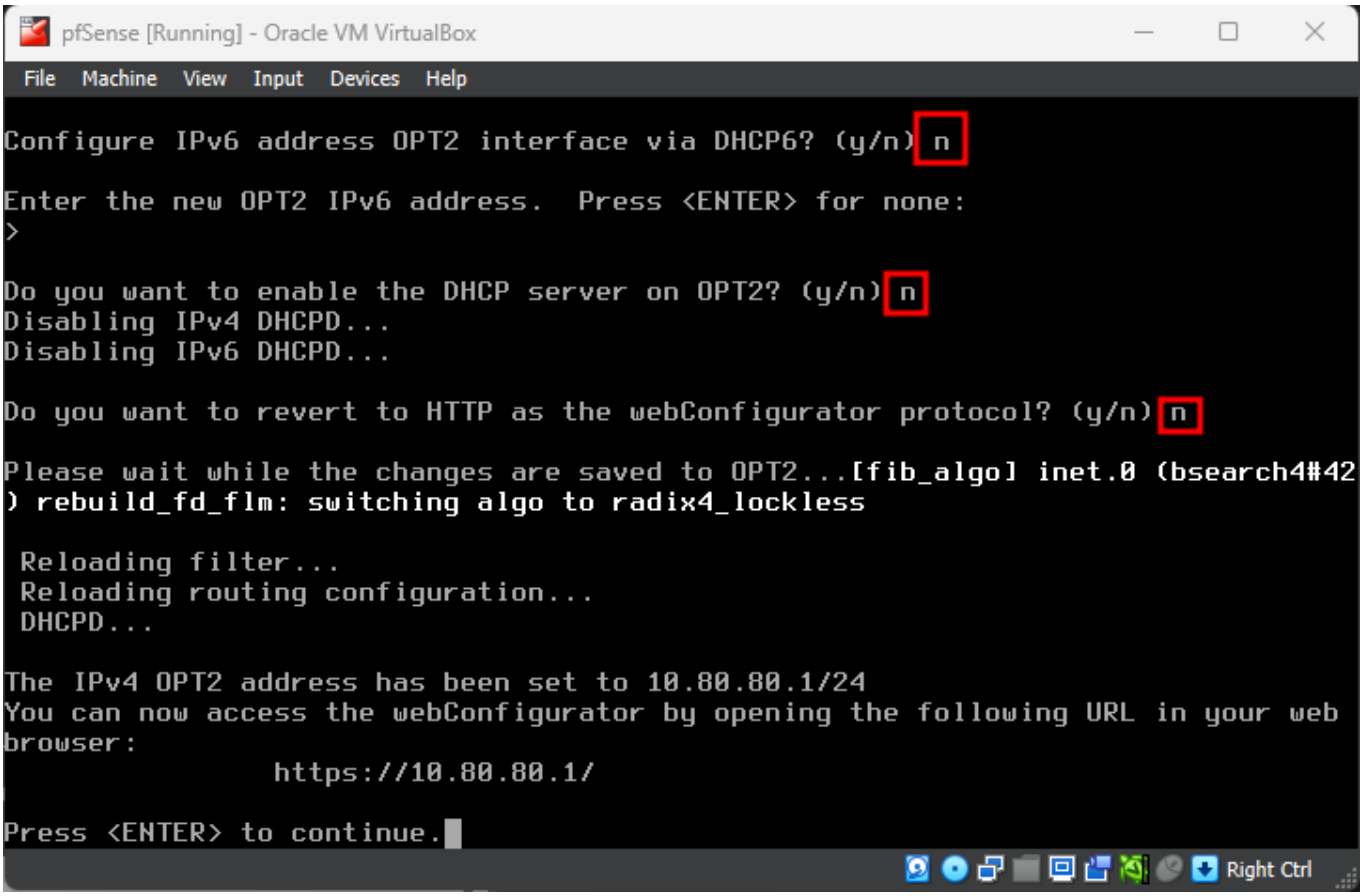


Configure IPv6 address OPT2 interface via DHCP6: **n**

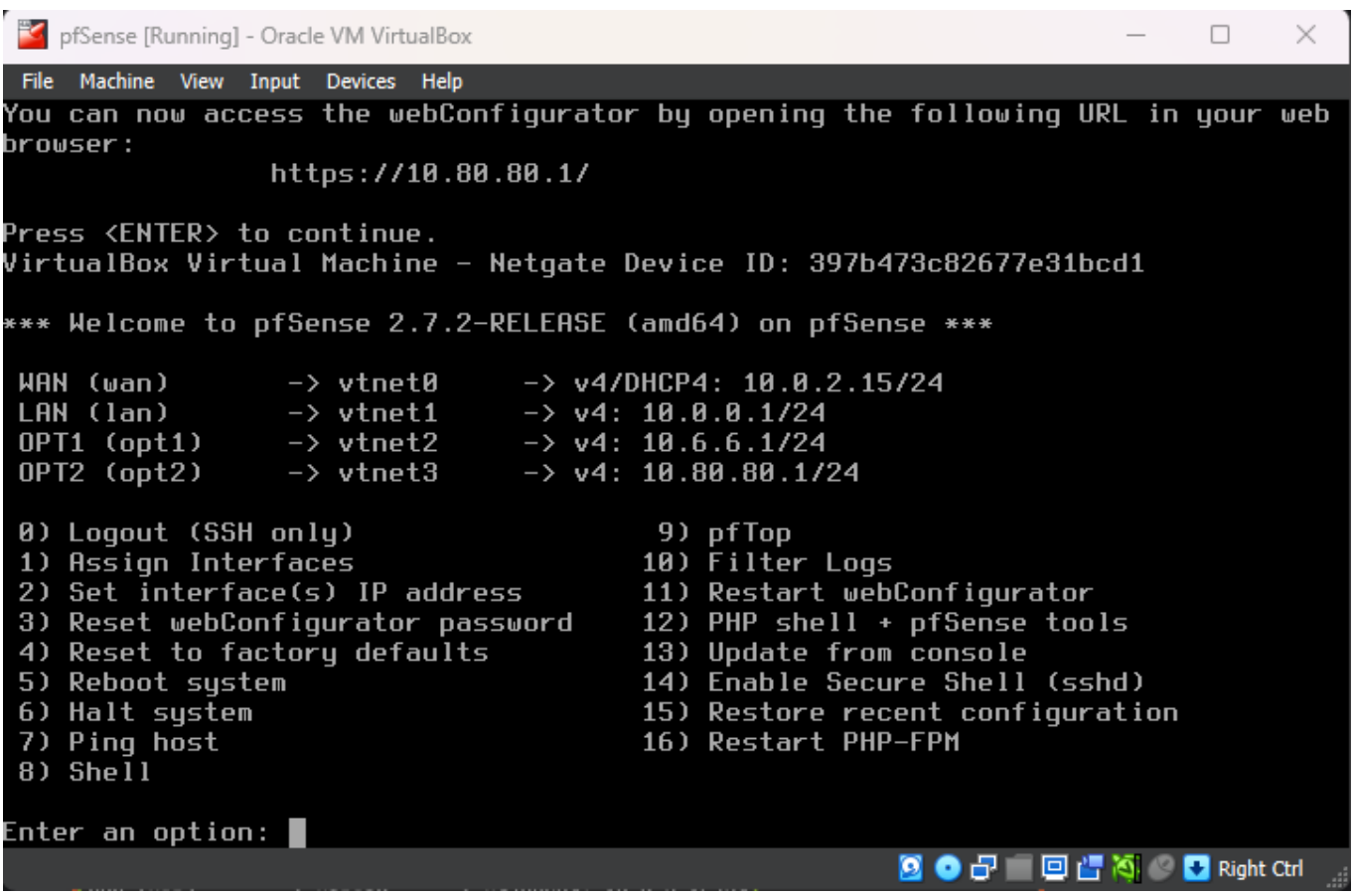
For the new OPT2 IPv6 address question press **Enter**

Do you want to enable the DHCP server on OPT2?: **n**

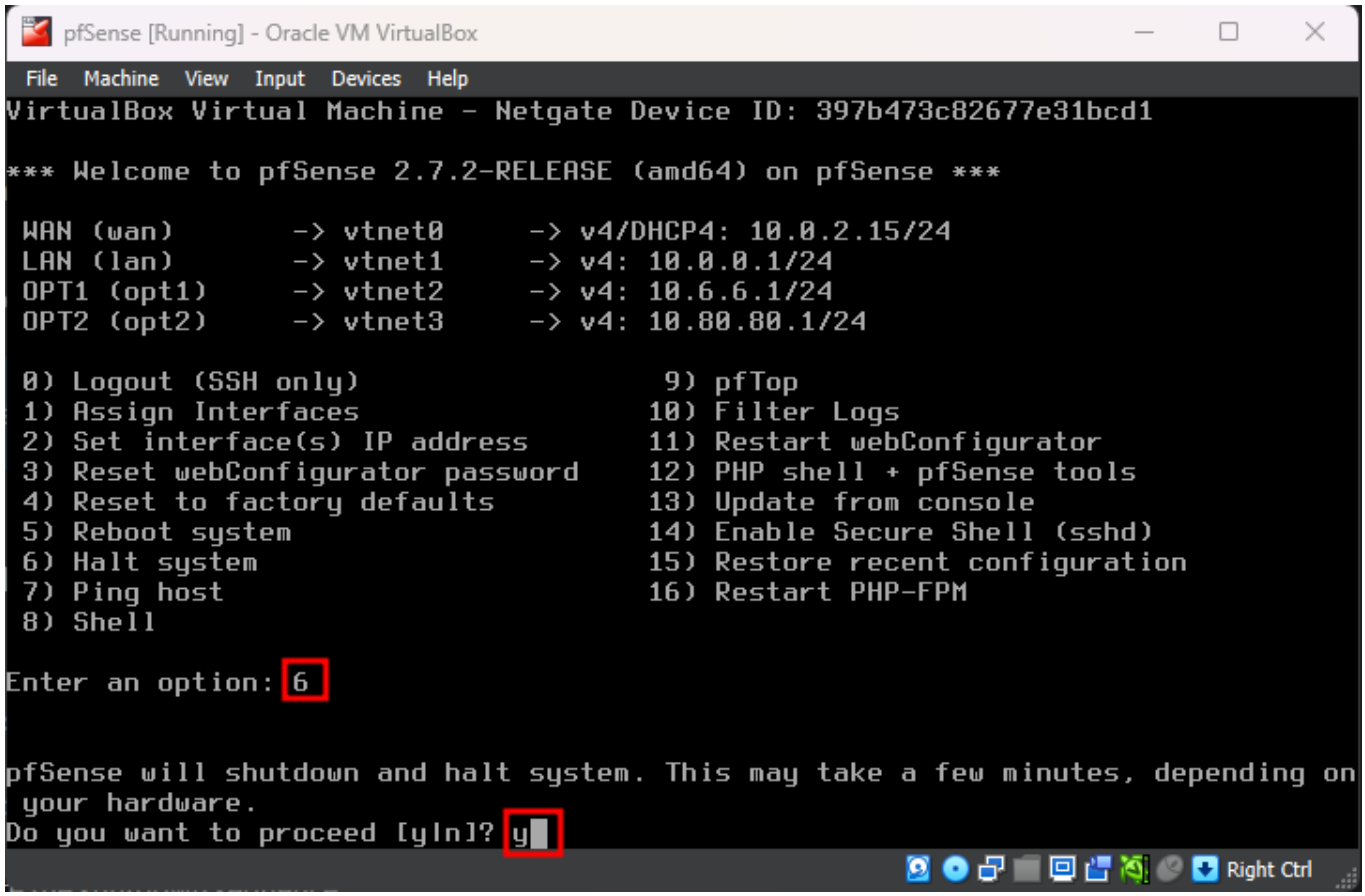
Do you want to revert to HTTP as the webConfigurator protocol?: **n**



Now, all the interfaces are configured

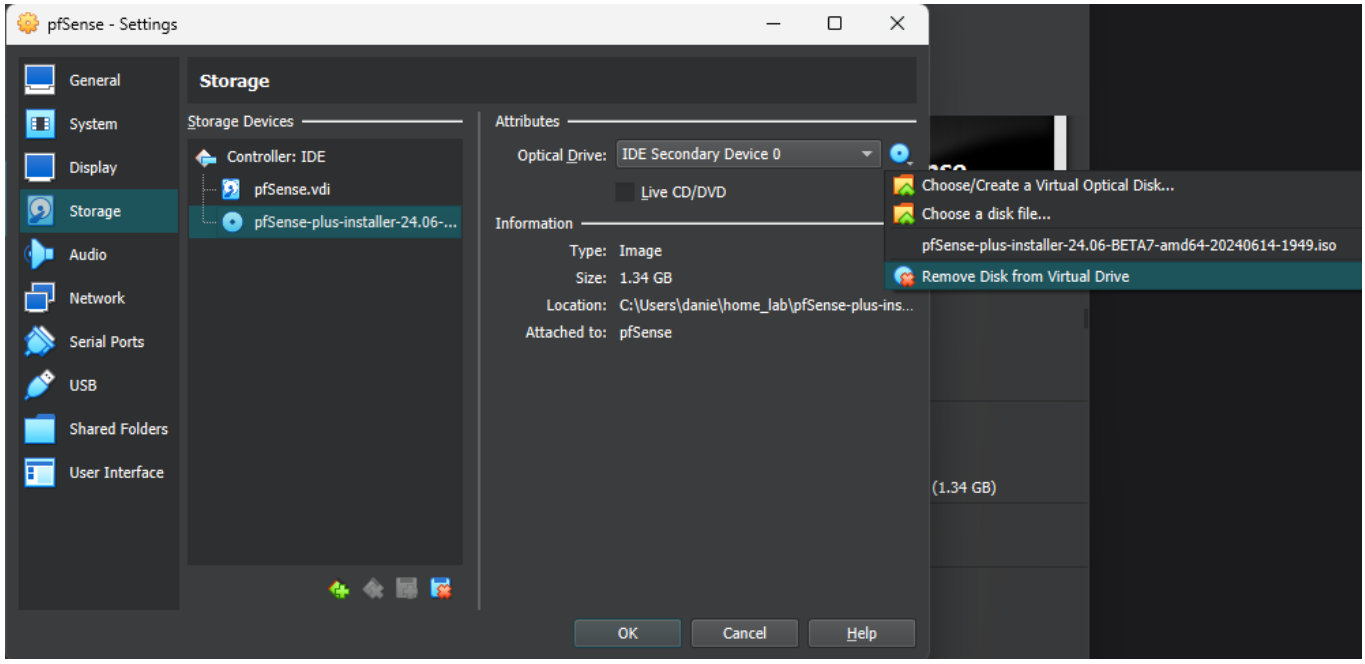


i now shut it down to clean it up



To clean the VM up, i go to **Settings -> Storage**, click on the pfSense **.iso** image and then click on the small disk image.

From the dropdown menu i select **Remove Disk from Virtual Drive** and click **OK**



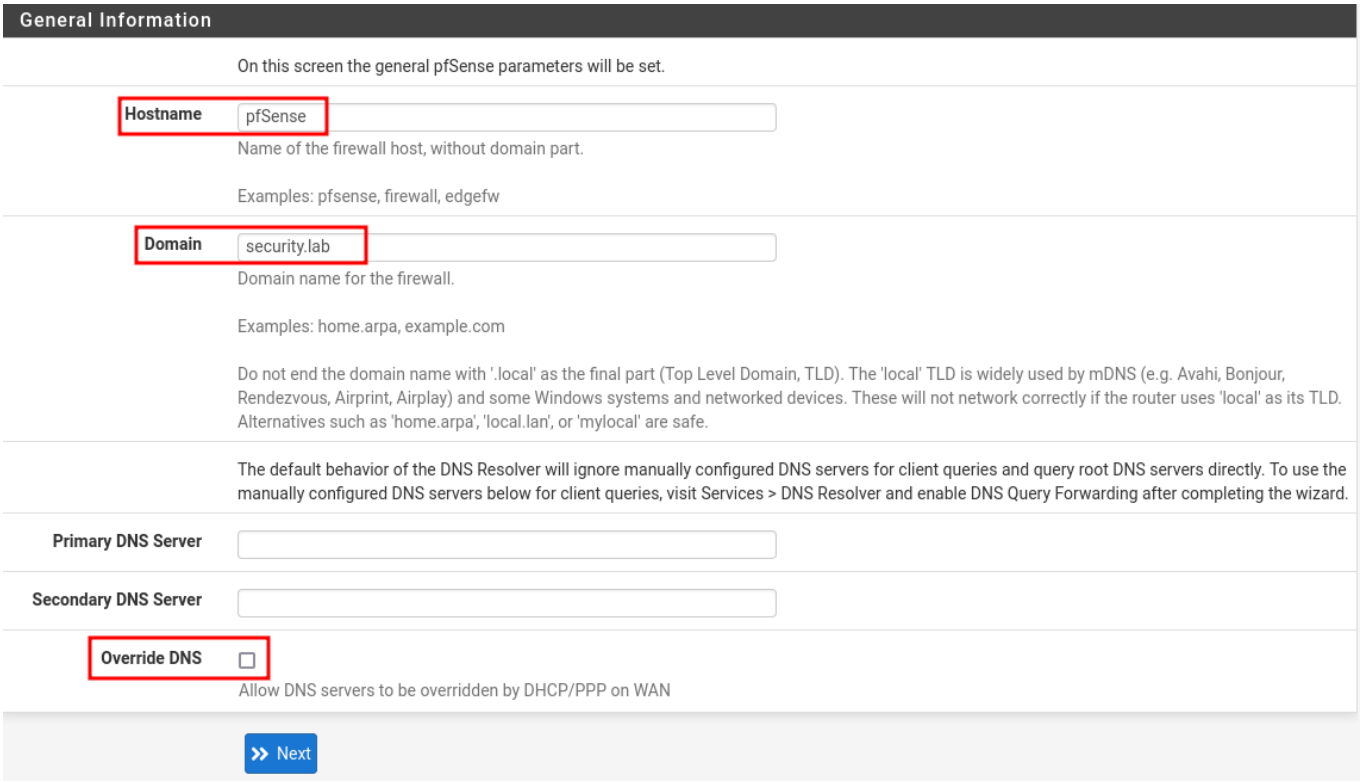
pfSense Configuration

From the managing machine, I navigate to https://10.0.0.1 and login with the default credentials:

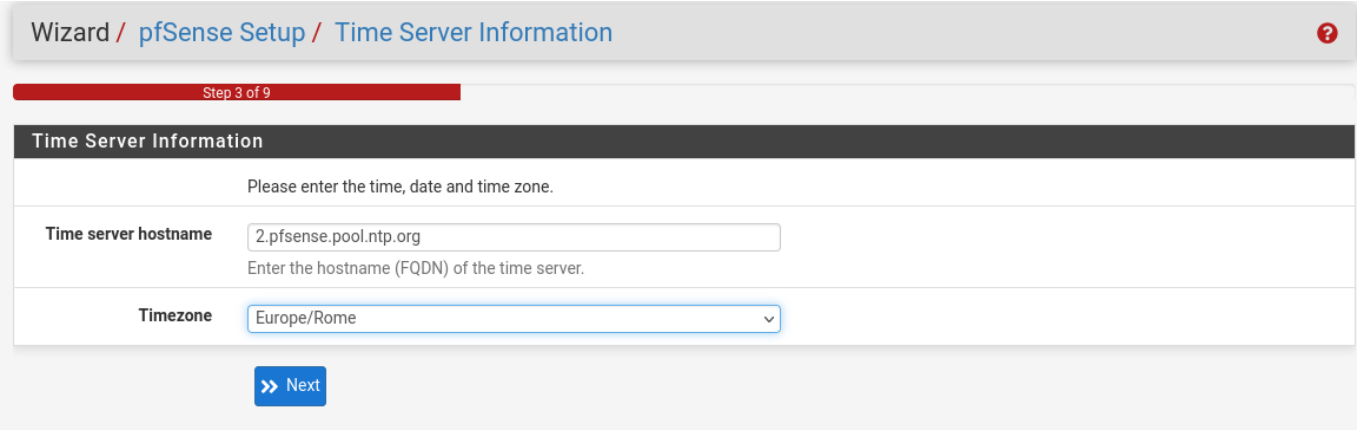
- **username**: admin
- **password**: pfsense

Wizard

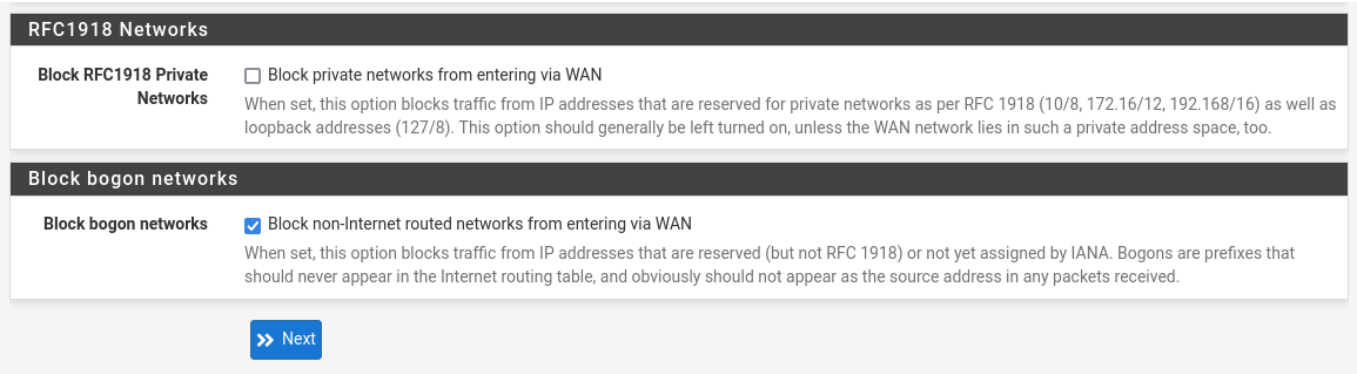
I choose a **hostname** and a **domain** and also disable **DNS override**



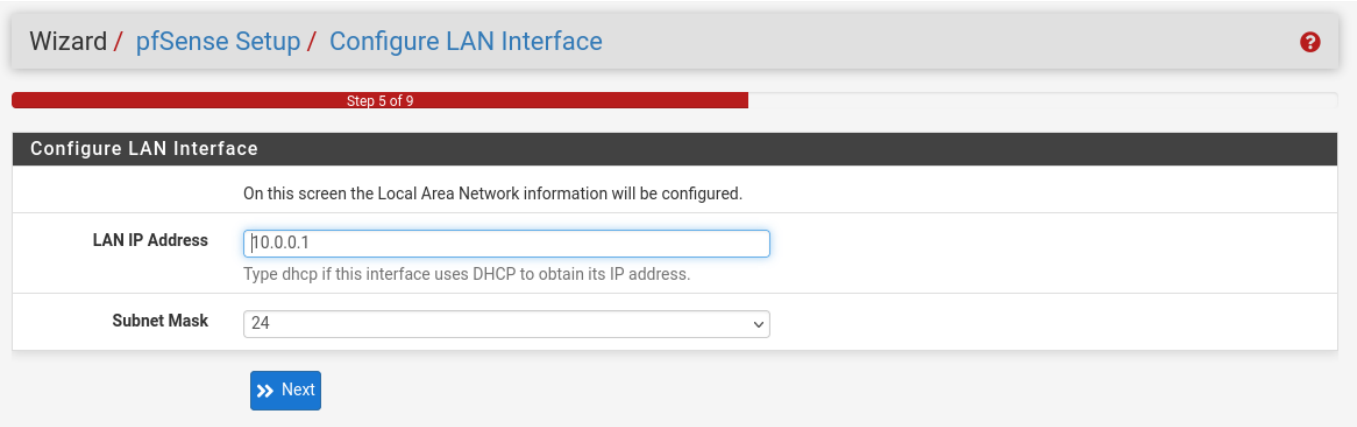
I choose my timezone



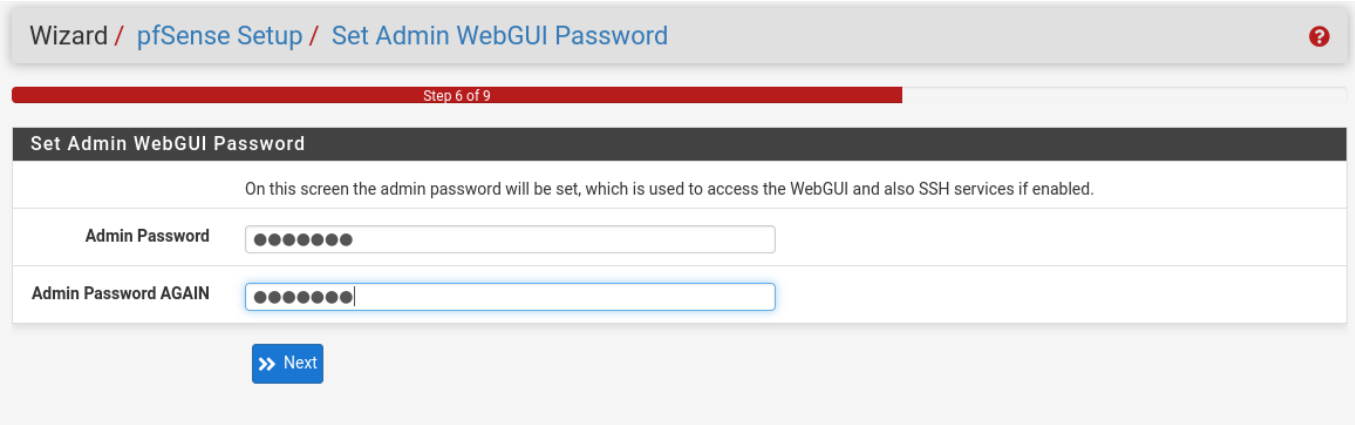
I then scroll to the bottom and uncheck RFC1918



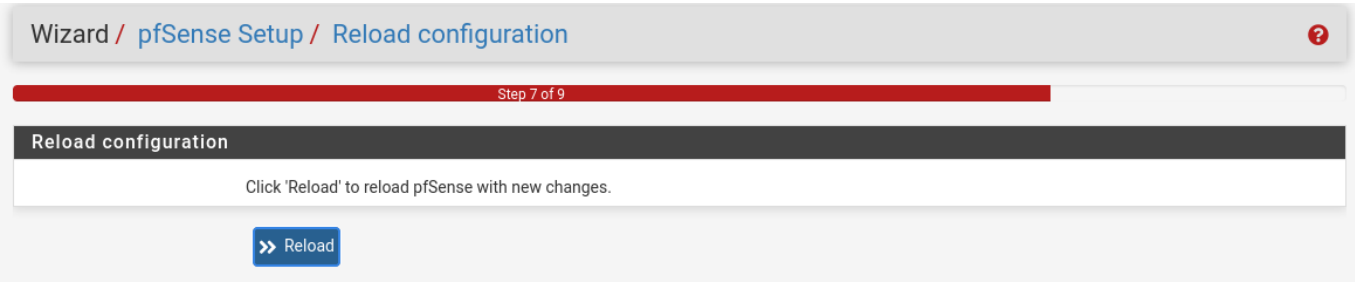
Confirm the LAN interface settings



Choose a new password for the admin account

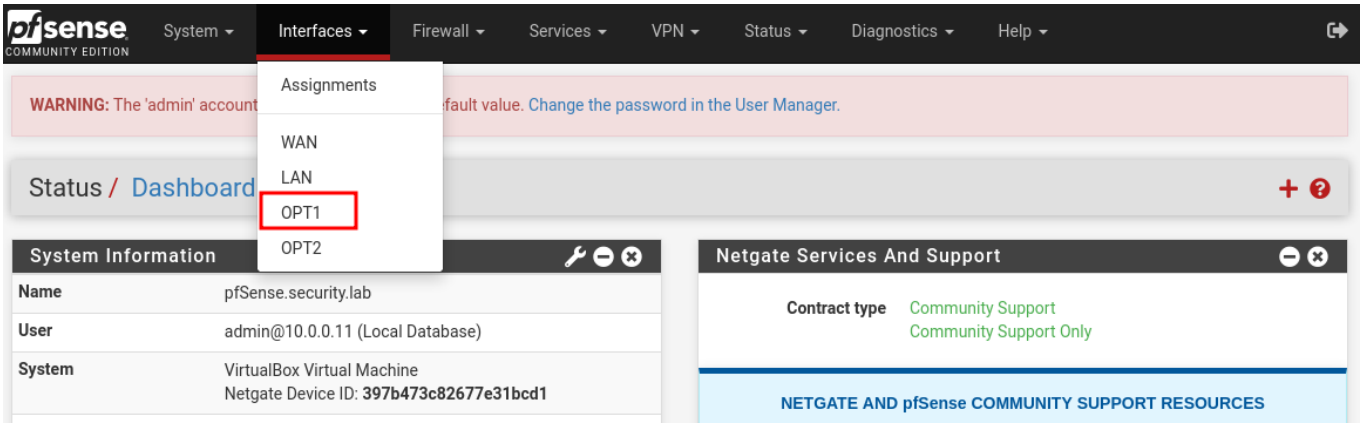


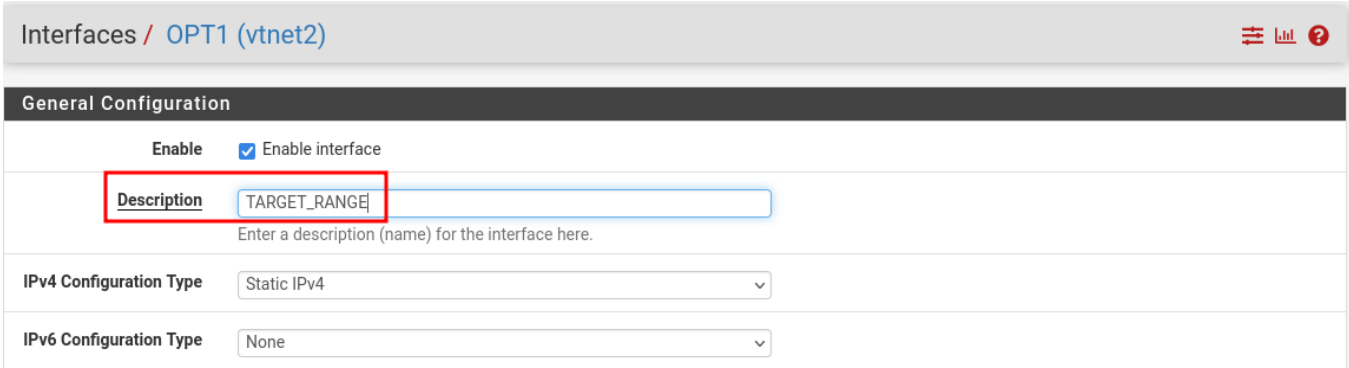
And then I reload pfSense to save the changes



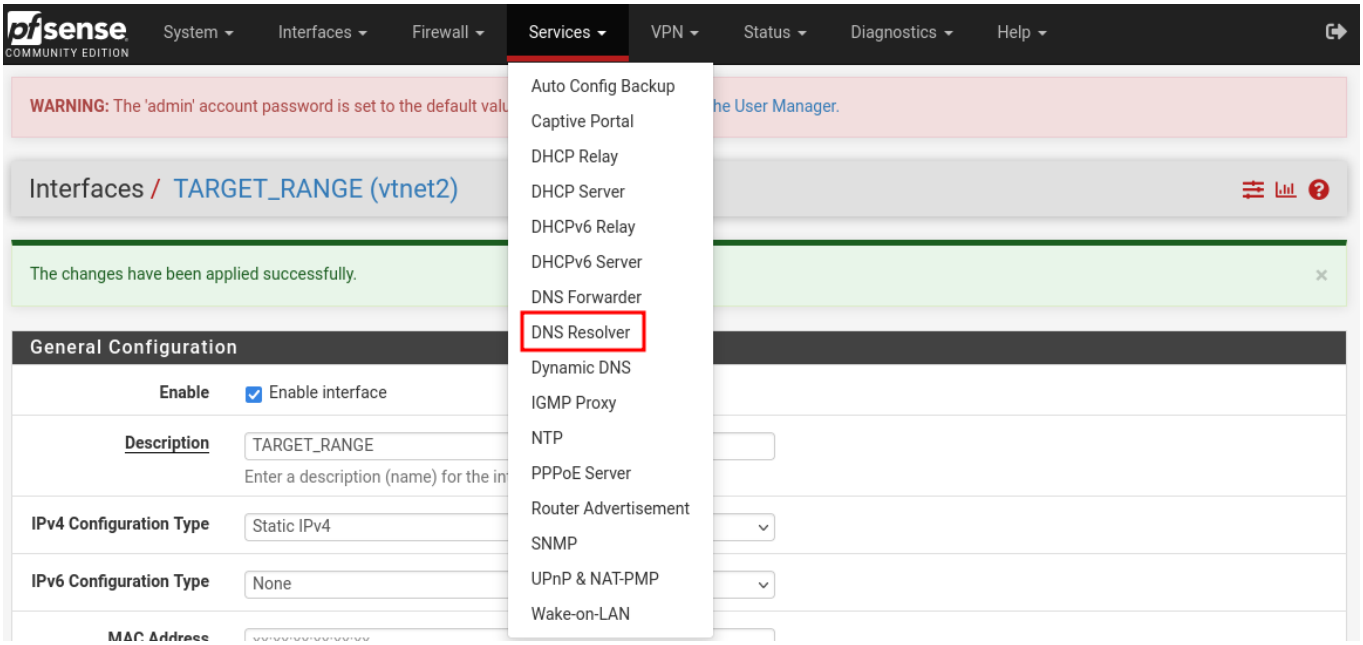
General Configuration

I go to **Interfaces -> OPT1** and rename OPT1 to make it easily understandable

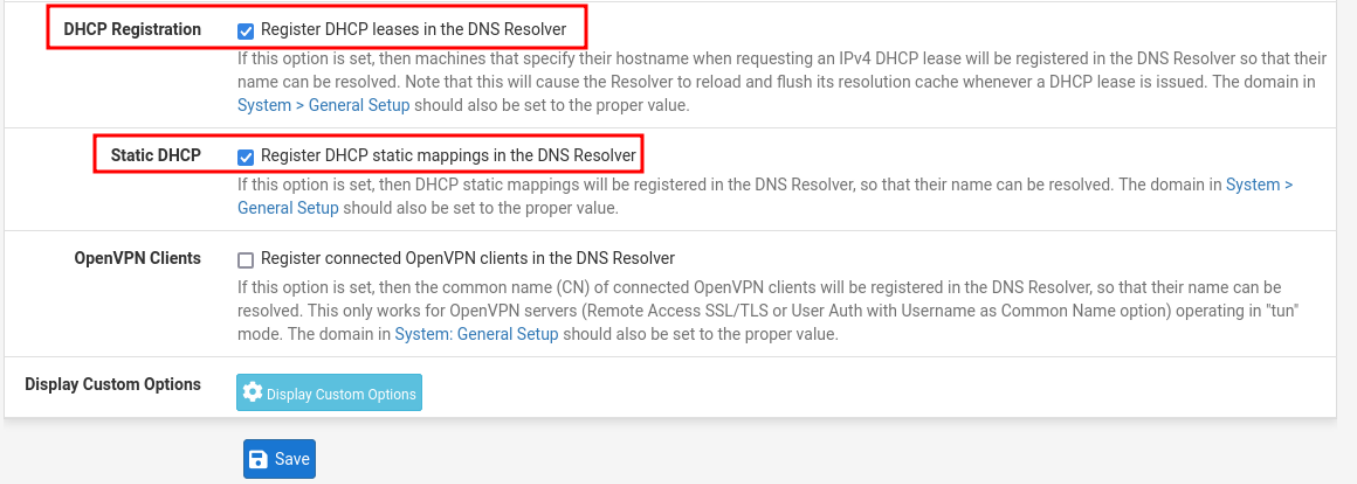




I go to **Services -> DNS Resolver**



And I enable these settings



Services / DNS Resolver / General Settings

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

General Settings | Advanced Settings | Access Lists

General DNS Resolver Options

Enable	☑ Enable DNS resolver
Listen Port	53 The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Advanced Resolver Options

Prefetch Support	☑ Message cache elements are prefetched before they expire to help keep the cache up to date When enabled, this option can cause an increase of around 10% more DNS traffic and load on the server, but frequently requested items will not expire from the cache.
Prefetch DNS Key Support	☑ DNSKEYs are fetched earlier in the validation process when a Delegation signer is encountered This helps lower the latency of requests but does utilize a little more CPU. See: Wikipedia
Harden DNSSEC Data	☑ DNSSEC data is required for trust-anchored zones. If such data is absent, the zone becomes bogus. If Disabled and no DNSSEC data is received, then the zone is made insecure.
Serve Expired	☐ Serve cache records even with TTL of 0 When enabled, allows unbound to serve one query even with a TTL of 0, if TTL is 0 then new record will be requested in the background when the cache is served to ensure cache is updated without latency on service of the DNS request.

Then i go to **System -> Advanced -> Networking

pfsense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

- Advanced
- Certificates
- General Setup
- High Availability
- Package Manager
- Register
- Routing
- Setup Wizard
- Update
- User Manager
- Logout (admin)

WARNING: The d is set to the default value. Change the password in the User Manager.

Services / General Settings

The changes ha fully.

ISC DHCP has r l be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

General Setting s | Access Lists

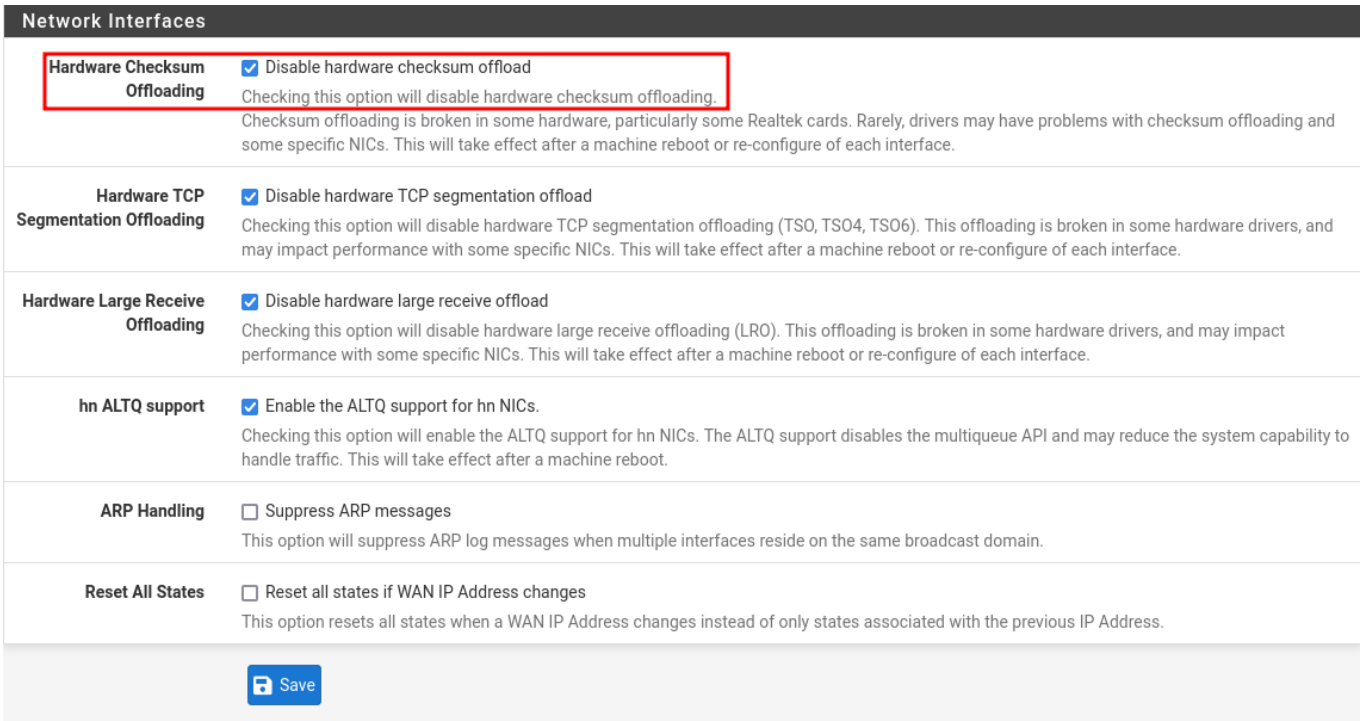
System / Advanced / Admin Access

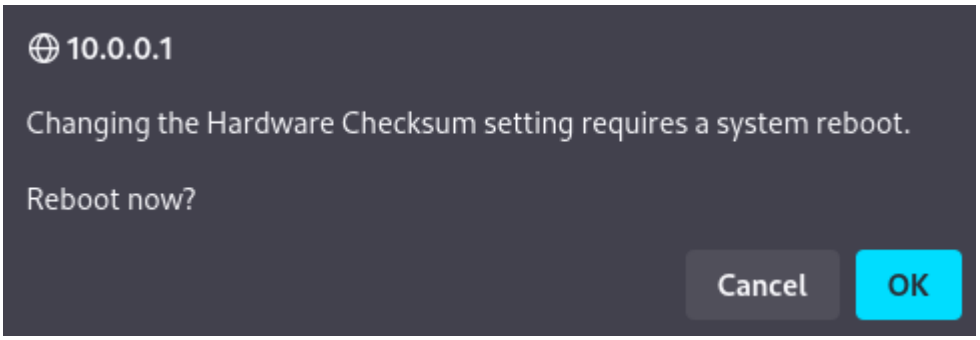
Admin Access | Firewall & NAT | Networking | Miscellaneous | System Tunables | Notifications

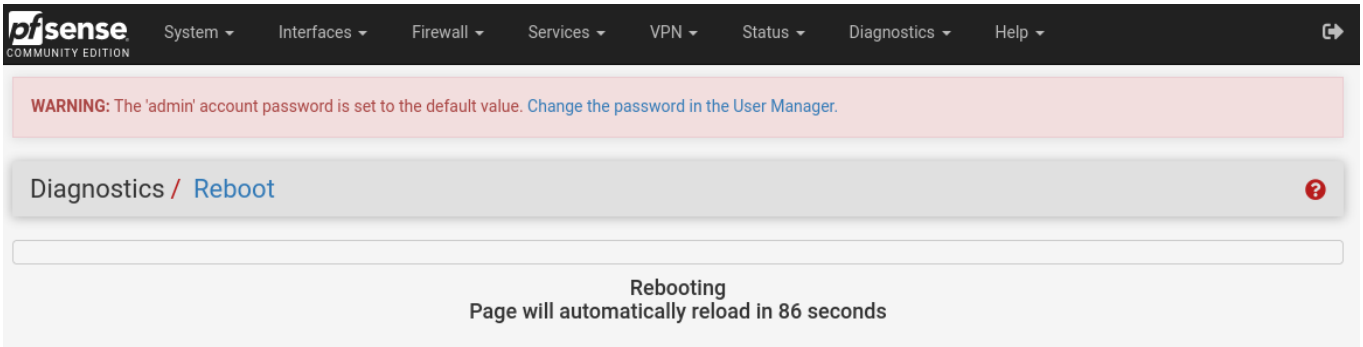
webConfigurator

Protocol	○ HTTP ◉ HTTPS (SSL/TLS)
SSL/TLS Certificate	GUI default (669ff3ab88459) Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
TCP port	Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

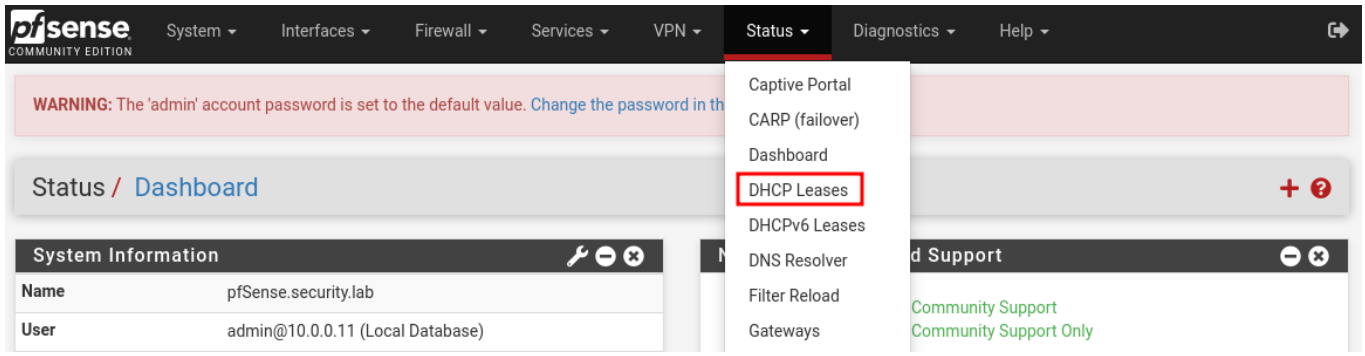
I disable **hardware checksum offloading** and then reboot



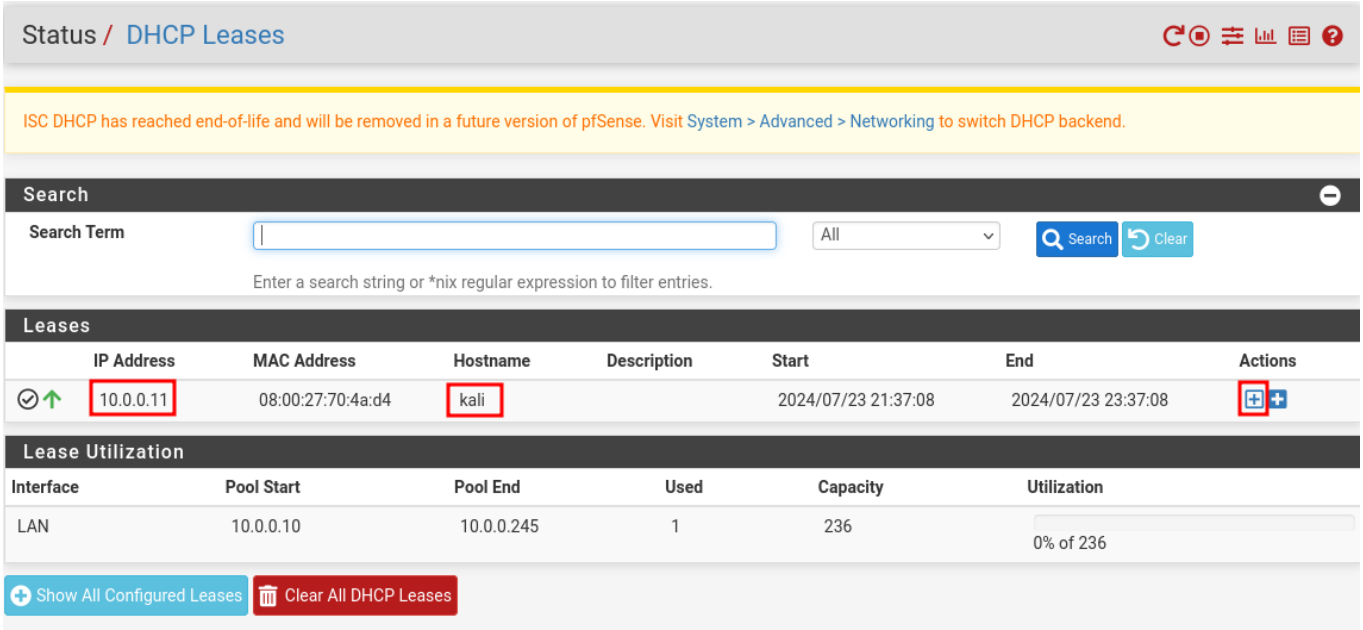




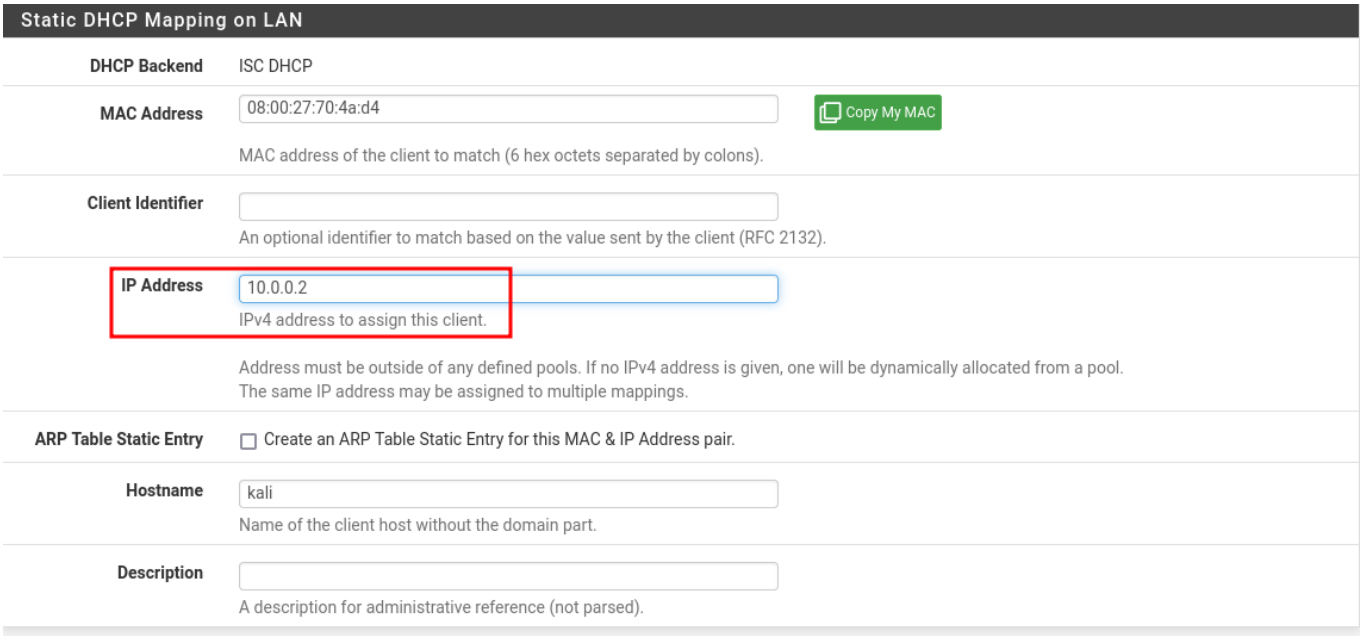
After logging in again i go to **Status -> DHCP Leases**



I click on the + on my managing machine



And assign a static IP to it

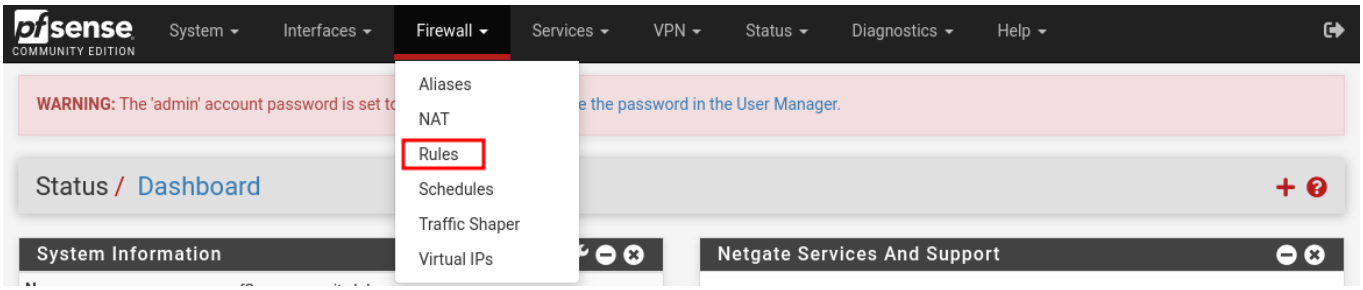


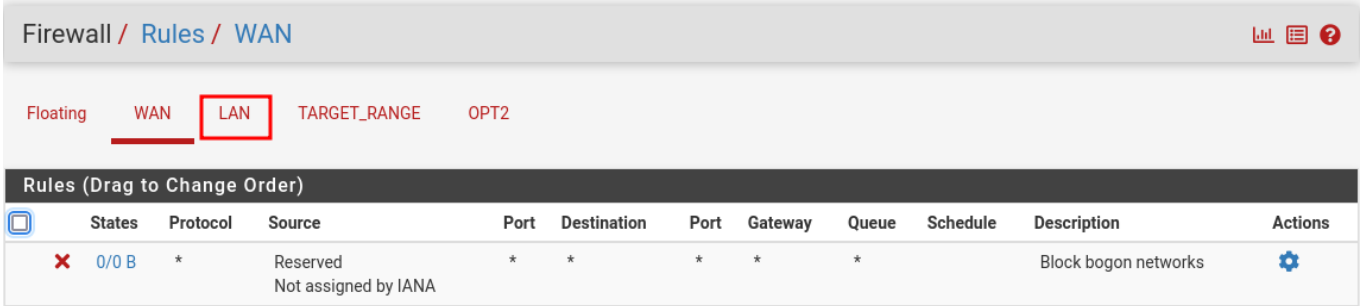
Finally I restart the managing VM's NIC to update its IP

```
┌──(dan㉿kali)-[~]
└─$ ip a l eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:70:4a:d4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.11/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 4929sec preferred_lft 4929sec
    inet6 fe80::a00:27ff:fe70:4ad4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(dan㉿kali)-[~]
└─$ sudo ip l set eth0 down && sudo ip l set eth0 up
[sudo] password for dan:

┌──(dan㉿kali)-[~]
└─$ ip a l eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:70:4a:d4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 7195sec preferred_lft 7195sec
    inet6 fe80::a00:27ff:fe70:4ad4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

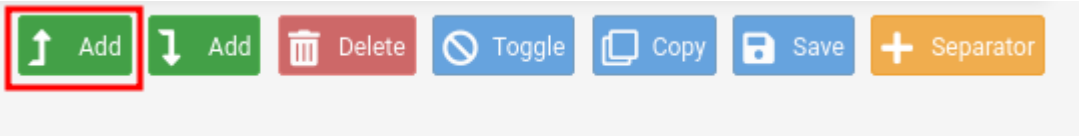
Firewall Rules

I go to **Firewall -> Rules -> LAN**



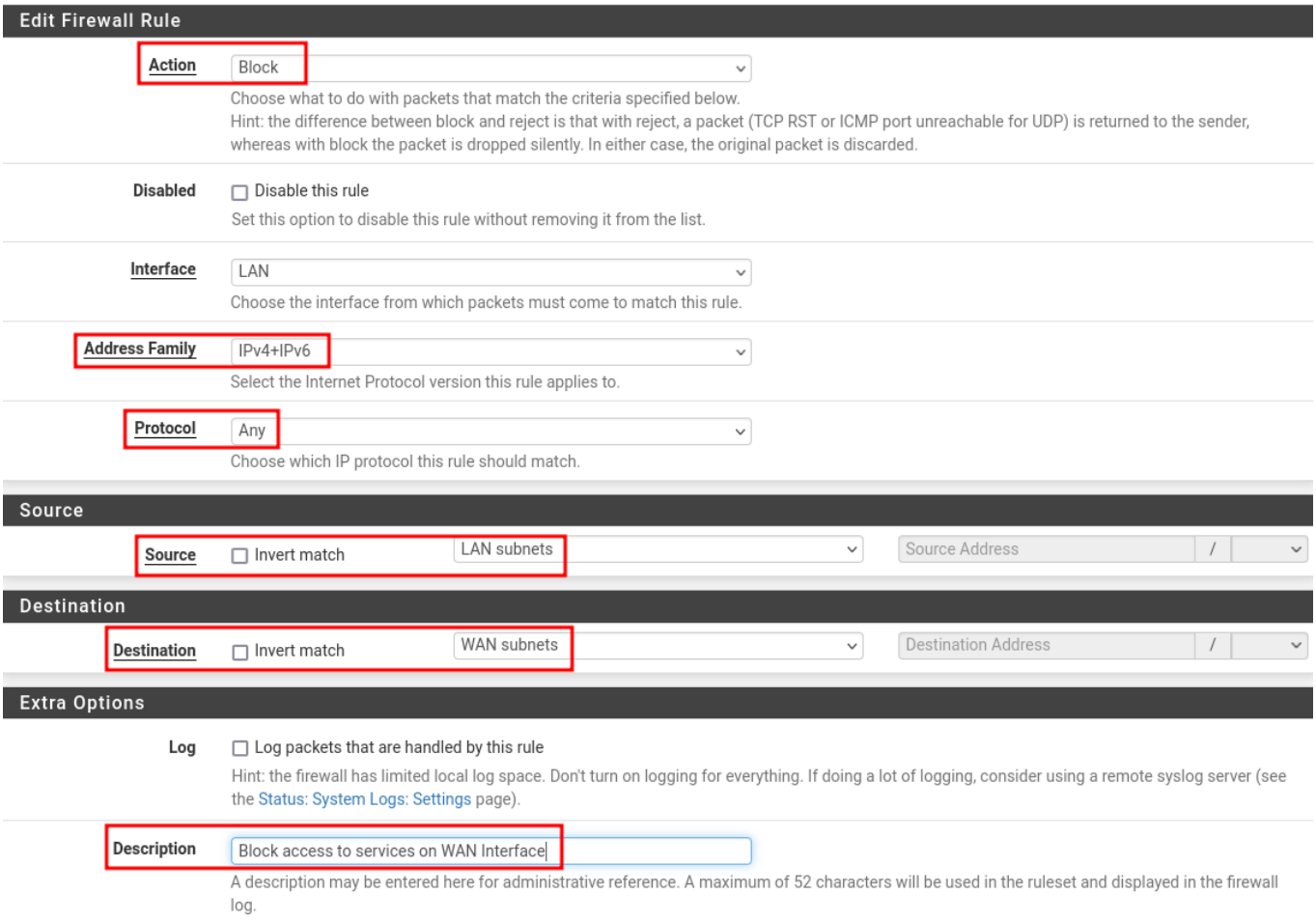


And click on the **Add rule to the top** button

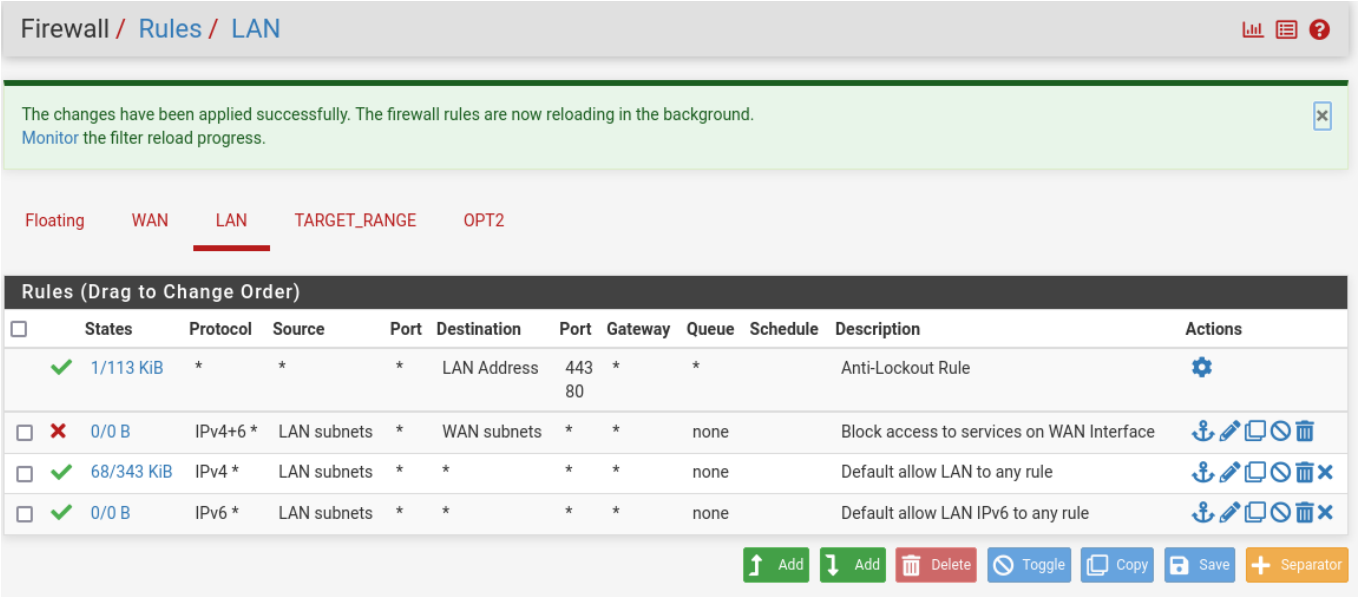


Then i edit the Rule this way:

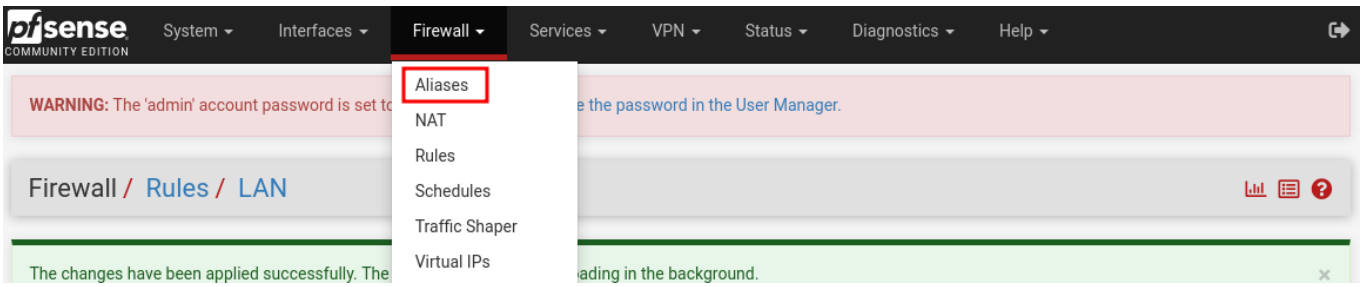
- Action: **Block**
- Address Family: **Ipv4+IPv6**
- Protocol: **Any**
- Source: **LAN subnets**
- Destination: **WAN subnets**
- Description: **Block access to services on WAN interface**

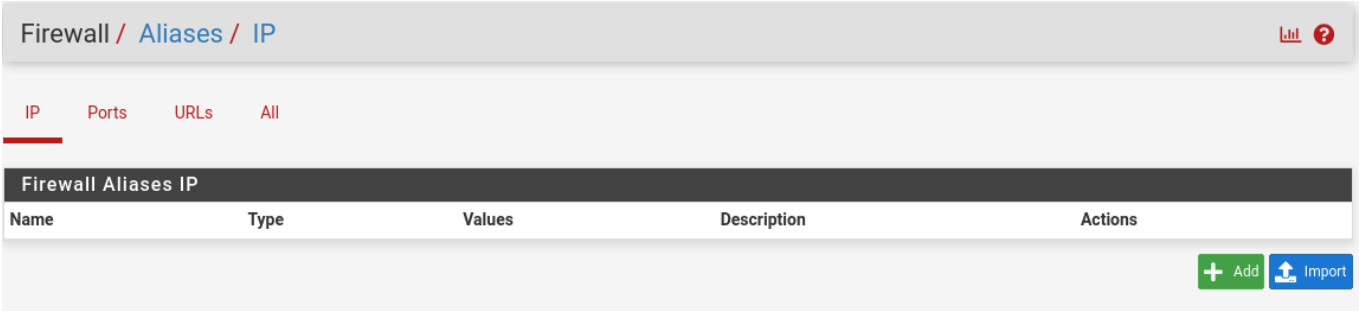


These are the final LAN rules and their order



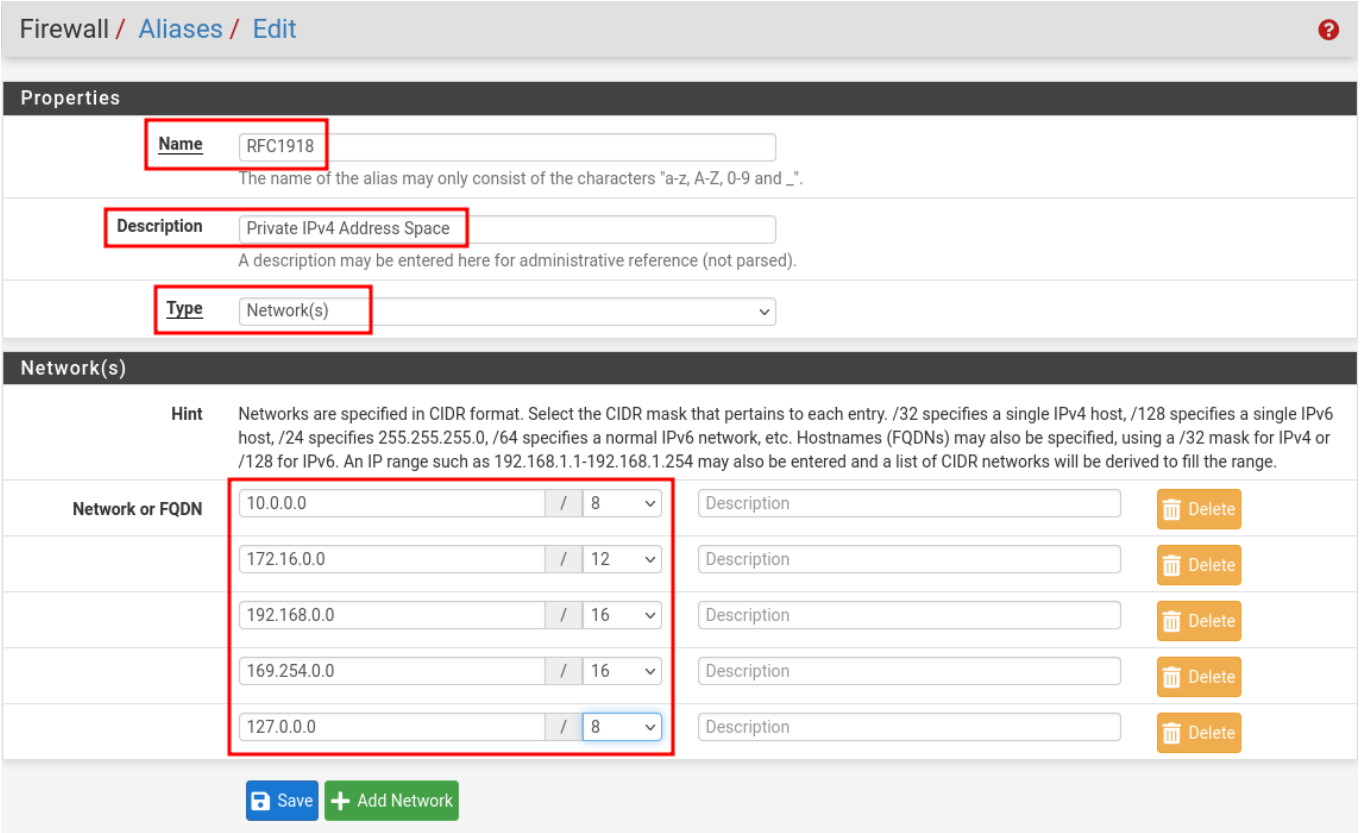
I then go to **Firewall -> Aliases** and add an entry



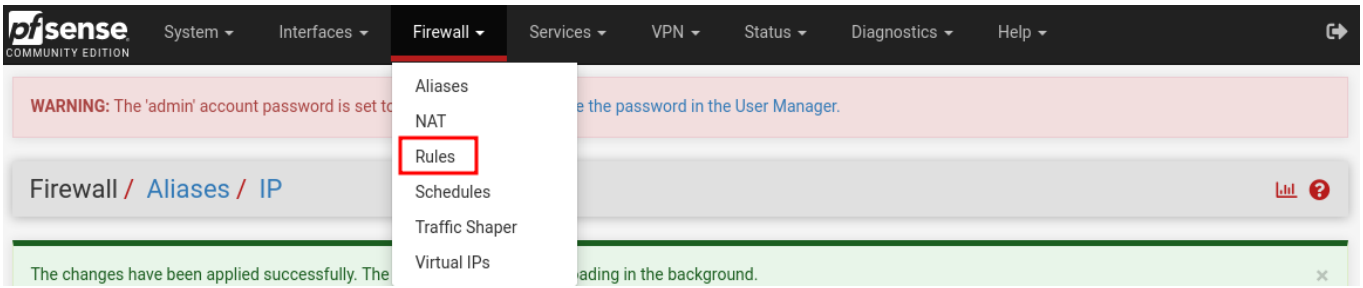


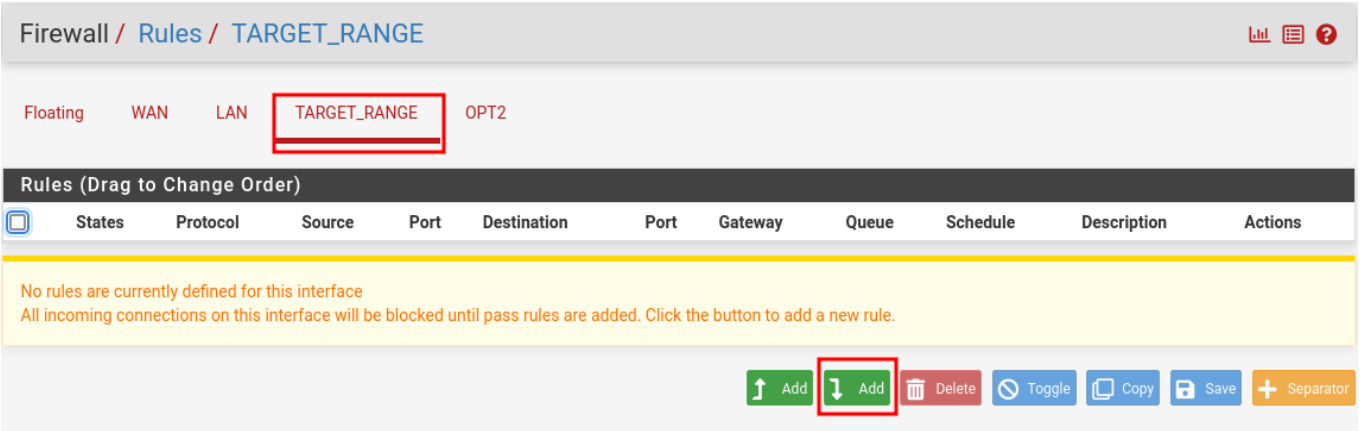
I create this alias:

- Name: **RFC1918**
- Description: **Private IPv4 Address Space**
- Type: **Network(s)**
- Network 1: **10.0.0.0/8**
- Network 2: **172.16.0.0/12**
- Network 3: **192.168.0.0/16**
- Network 4: **169.254.0.0/16**
- Network 5: **127.0.0.0/8**



Then i go to **Firewall -> Rules -> TARGET_RANGE** and click on **Add to the end**

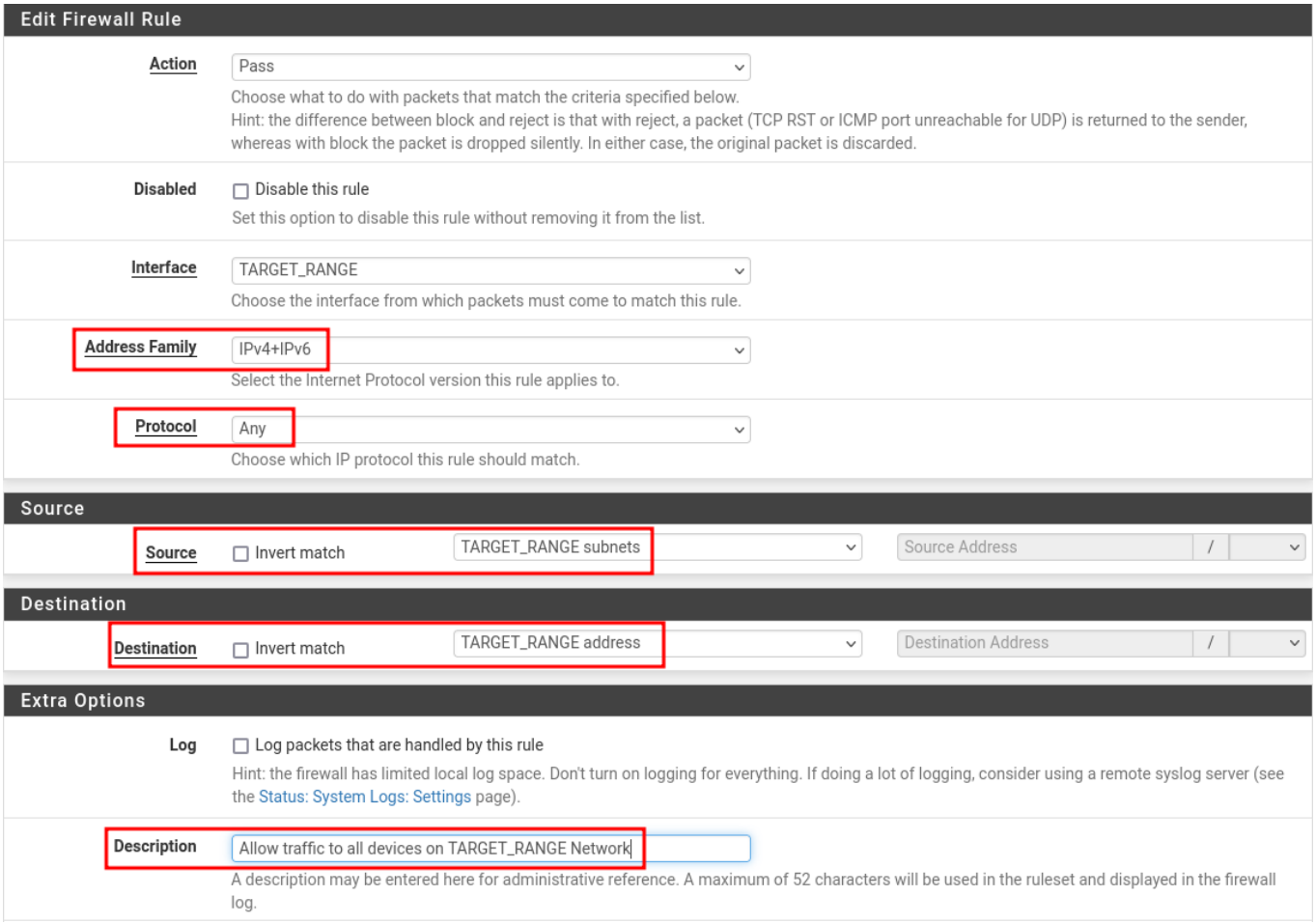




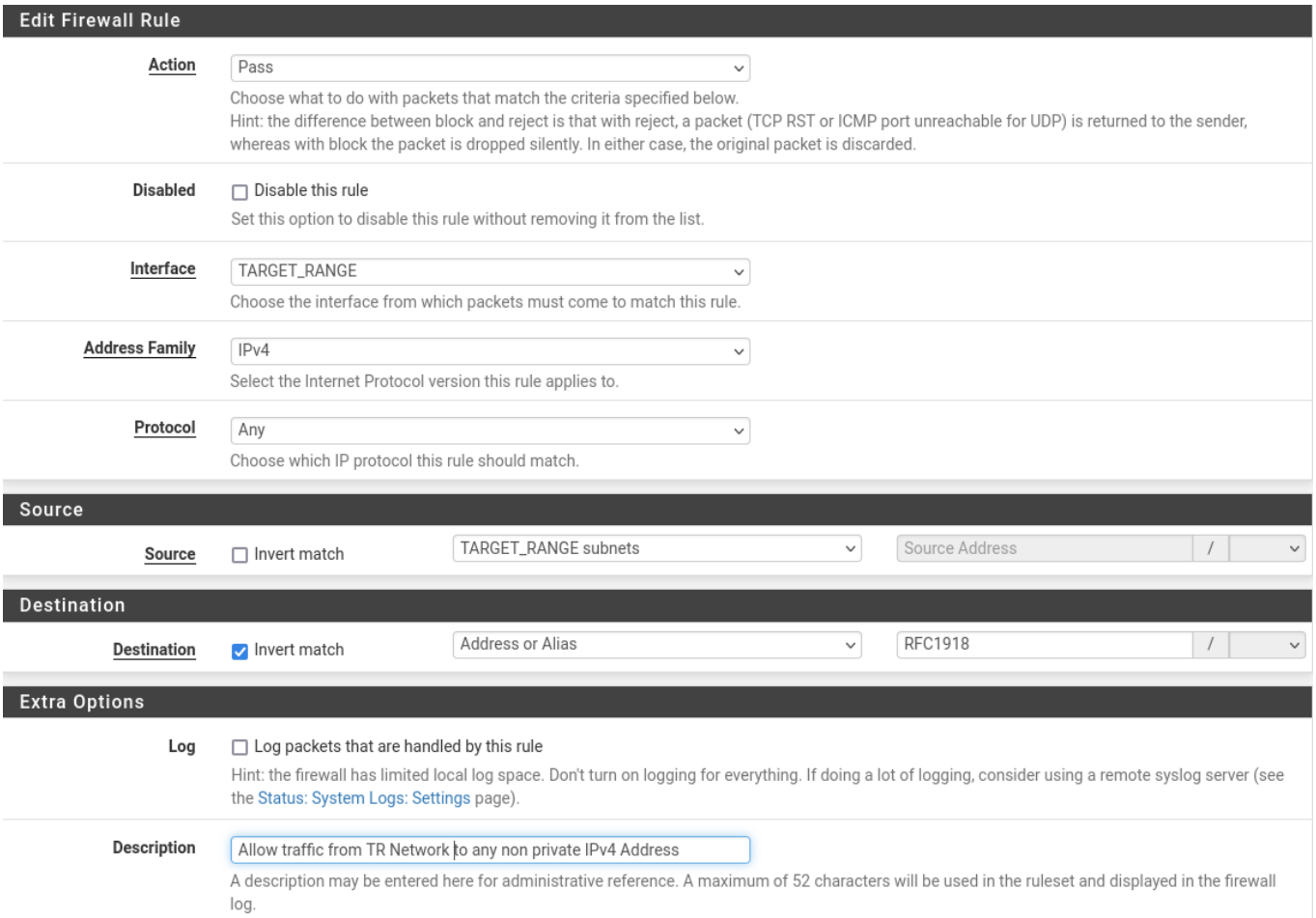
And i create these rules:

- Address Family: **IPv4+IPv6**
- Protocol: **Any**

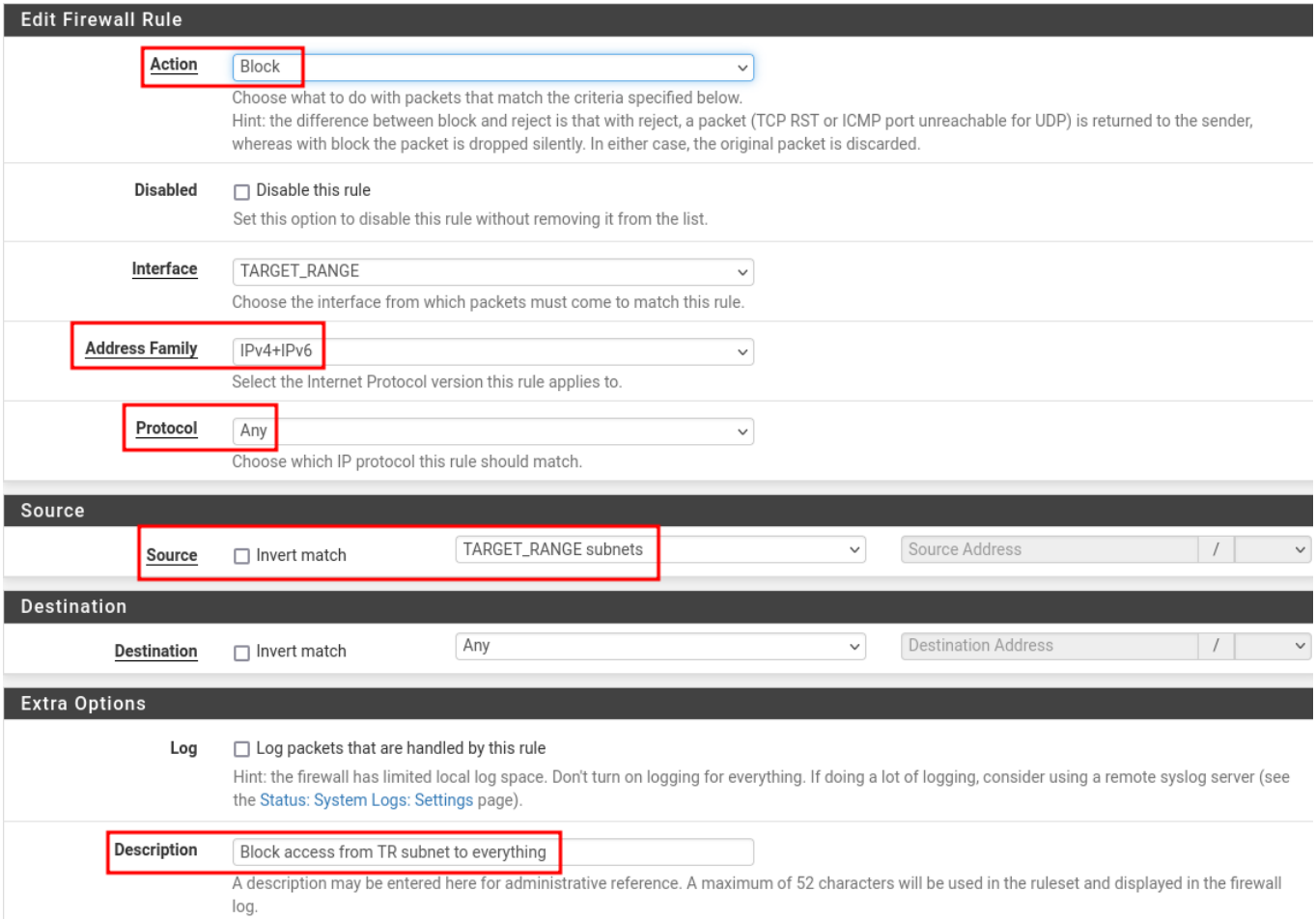
- Source: **TARGET_RANGE subnets**
- Destination: **TARGET_RANGE address**
- Description: **Allow traffic to all devices on the TARGET_RANGE Network**



- Protocol: **Any**
- Source: **TARGET_RANGE subnets**
- Destination: **Address or Alias - RFC1918** (Select Invert match)
- Description: **Allow traffic from TR Network to any non-private IPv4 Address**



- Action: **Block**
- Address Family: **IPv4+IPv6**
- Protocol: **Any**
- Source: **TARGET_RANGE subnets**
- Description: **Block access from TR subnet to everything**



- Protocol: **Any**
- Source: **TARGET_RANGE subnets**
- Destination: **10.0.0.2**
- Description: **Allow traffic to Kali Linux VM**

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 TARGET_RANGE

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 Any

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match | TARGET_RANGE subnets | Source Address | /

Destination

Destination ☐ Invert match | Address or Alias | 10.0.0.2 | /

Extra Options

Log ☐ Log packets that are handled by this rule

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).

Description Allow traffic to Kali Linux VM

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

These are my final rules and rules order

Firewall / Rules / TARGET_RANGE

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating | WAN | LAN | TARGET_RANGE | OPT2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/0 B	IPv4+6 *	TARGET_RANGE subnets	*	TARGET_RANGE address	*	*	none		Allow traffic to all devices on TARGET_RANGE Network	
✓	0/0 B	IPv4 *	TARGET_RANGE subnets	*	! RFC1918	*	*	none		Allow traffic from TR Network to any non private IPv4 Address	
✓	0/0 B	IPv4 *	TARGET_RANGE subnets	*	10.0.0.2	*	*	none		Allow traffic to Kali Linux VM	
✗	0/0 B	IPv4+6 *	TARGET_RANGE subnets	*	*	*	*	none		Block access from TR subnet to everything	

Add | Add | Delete | Toggle | Copy | Save | Separator

Finally I reboot to make sure my changes are successfully updated

pfsense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manage

Status / Dashboard

System Information

Name	pfSense.security.lab
User	admin@10.0.0.2 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: **397b473c82677e31bcd1**
BIOS	Vendor: **innotek GmbH** Version: **VirtualBox** Release Date: **Fri Dec 1 2006**
Version	**2.7.2-RELEASE** (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT *Unable to check for updates*
CPU Type	AMD Ryzen 5 5600H with Radeon Graphics AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 37 Minutes 52 Seconds
Current date/time	Wed Jul 24 0:45:35 CEST 2024
DNS server(s)	• 127.0.0.1

Netgate Ser

Contra

pport
pport Only

NETGA | MUNITY SUPPORT RESOURCES

If you purchase rewall appliance from Netgate and elected **Community Su** or installed pfSense on your own hardware, you h mmunity support resources. This includes the **NETGATE F**

You also may up al Technical Assistance Center (TAC) Support subscri ur team is staffed 24x7x365 and committed to de worldwide support at a price point that is more than comp others in our space.

- **Upgrade Yo** **Community Support Resources**
- Netgate Glo Official pfSense Training by Netgate
- Netgate Pro Visit Netgate.com

If you decide obal TAC Support subscription, you **MUST** have y **NDI)** from your firewall in order to validate supp n your NDI and store it in a safe place. You can purc

ARP Table
Authentication
Backup & Restore
Command Prompt
DNS Lookup
Edit File
Factory Defaults
Halt System
Limiter Info
NDP Table
Packet Capture
pfInfo
pfTop
Ping
Reboot
Routes
S.M.A.R.T. Status
Sockets
States
States Summary
System Activity
Tables
Test Port
Traceroute

Diagnostics / Reboot

Select reboot method

Reboot method Normal reboot

Select "Normal reboot" to reboot the system immediately, or "Reroot" to stop processes, remount disks and re-run startup sequence.

Submit