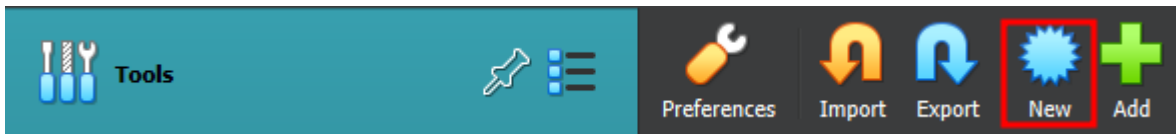


pfSense Setup and Configuration

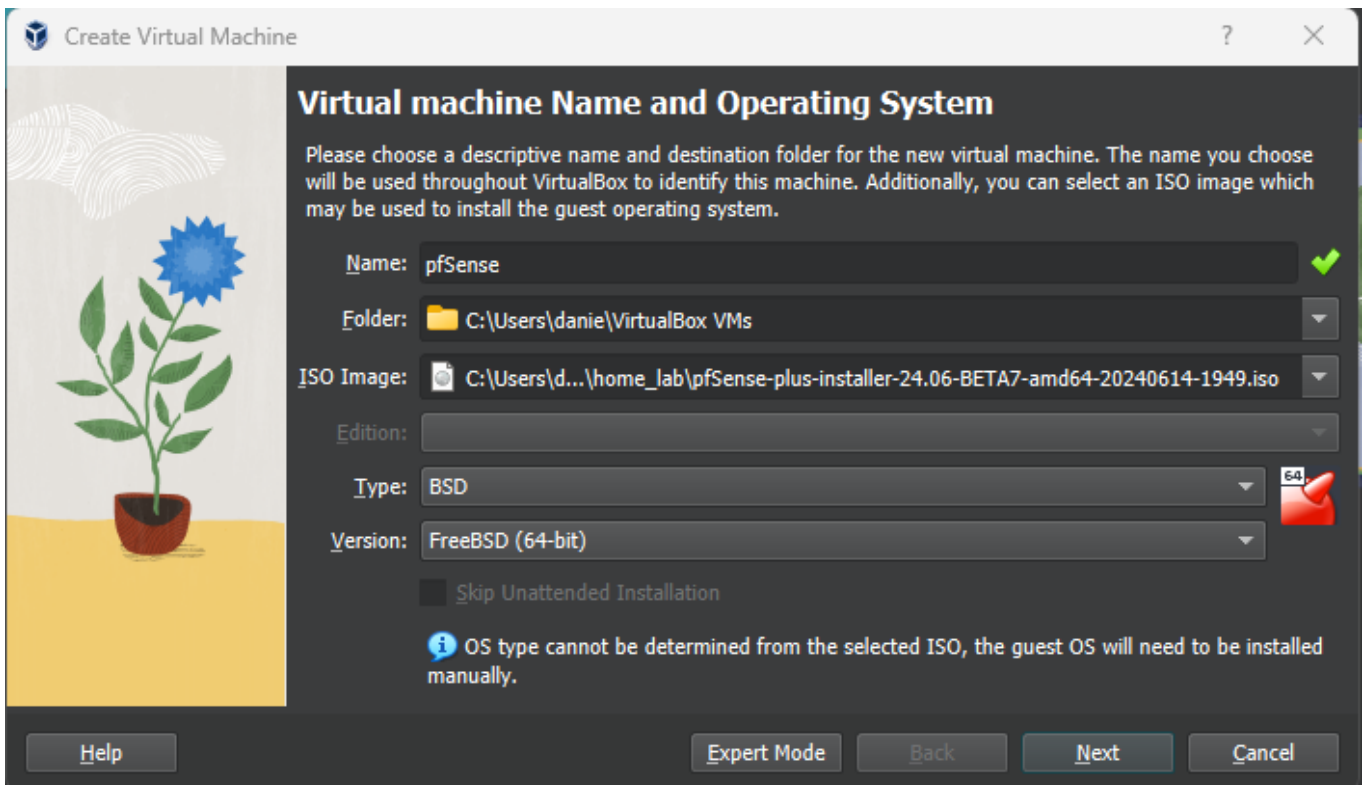
Download: [Download pfSense Installer](#)

VM Setup

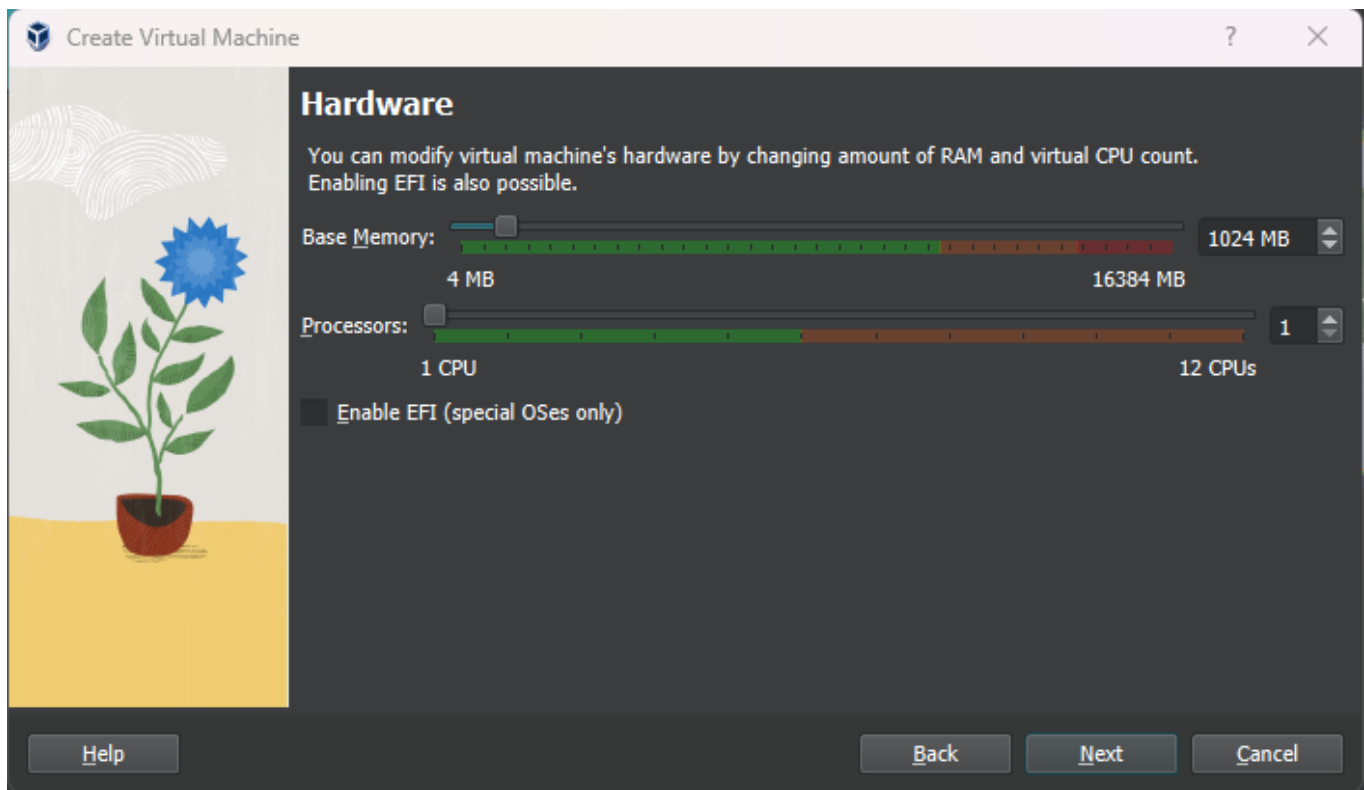
I create a new VM in VirtualBox by clicking on New



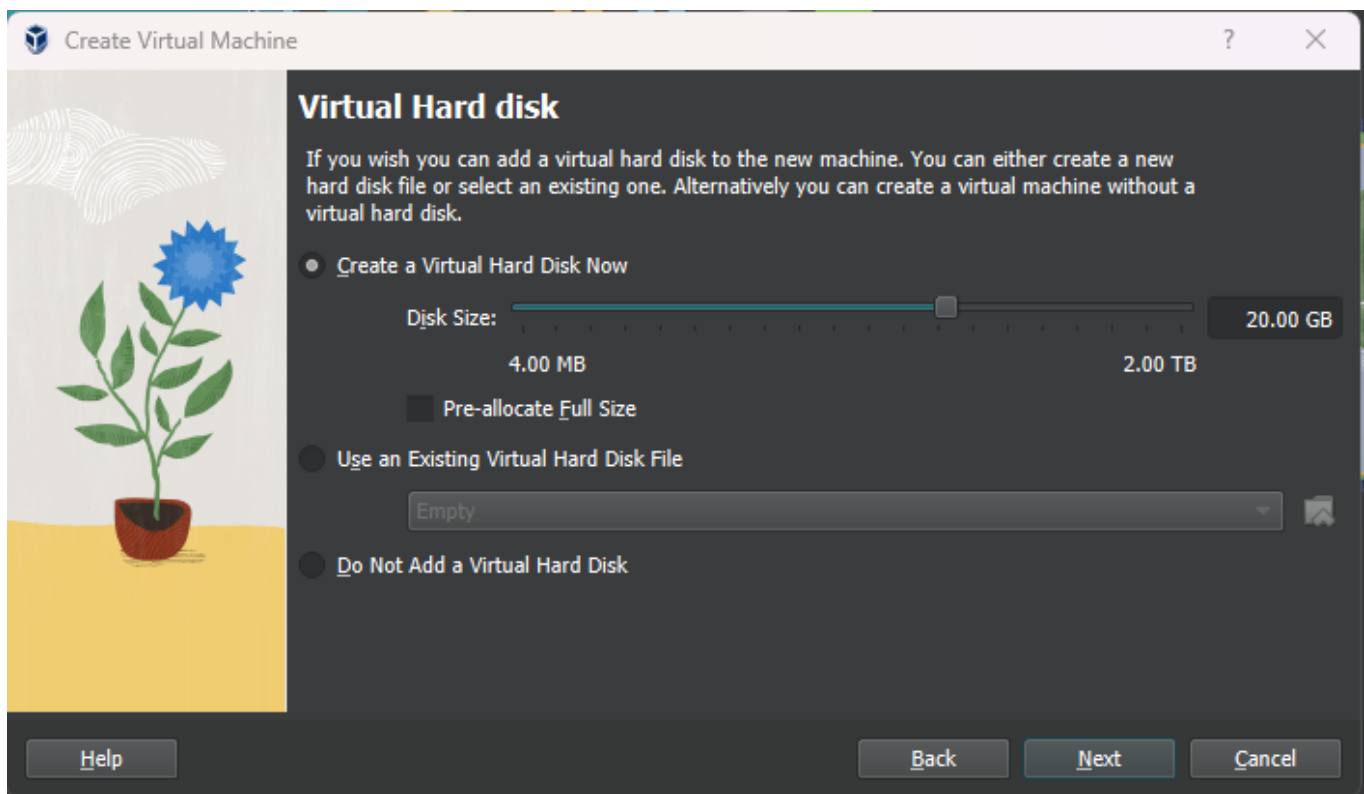
I give it a name, choose where it will be saved and from the ISO Image dropdown select others and then the .iso image I downloaded. As Type I select BSD and as Version I select FreeBSD(64-bit) and then I click on Next



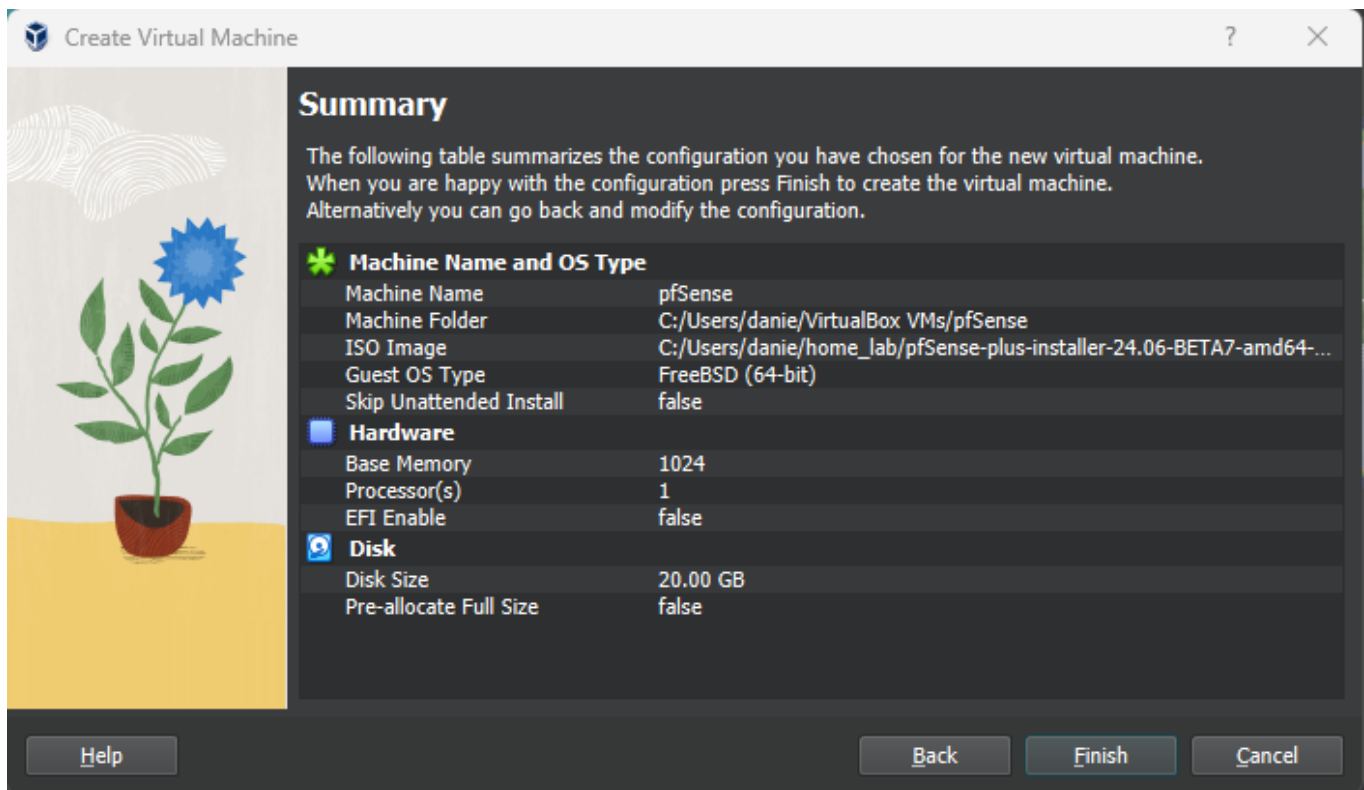
I leave the RAM and CPU setting as default and click on Next



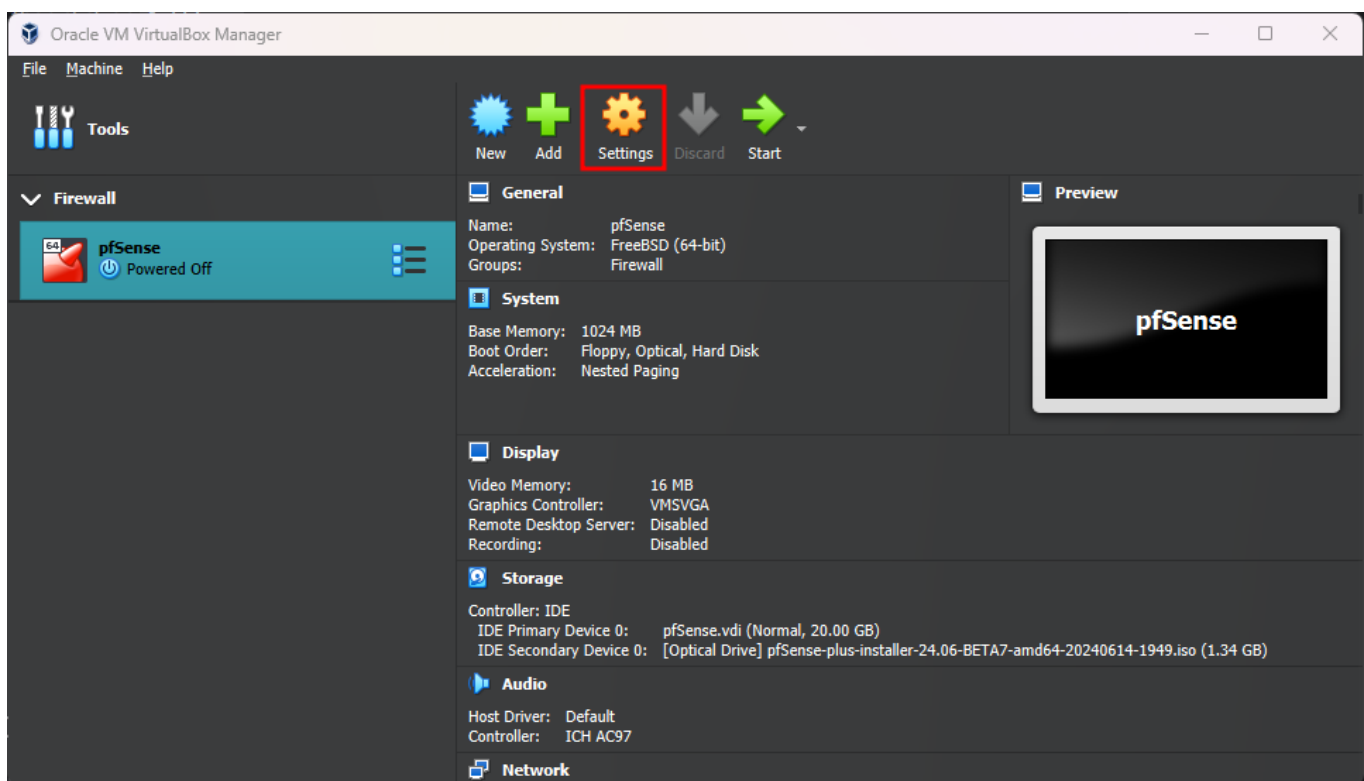
I assign 20GB of storage space to it



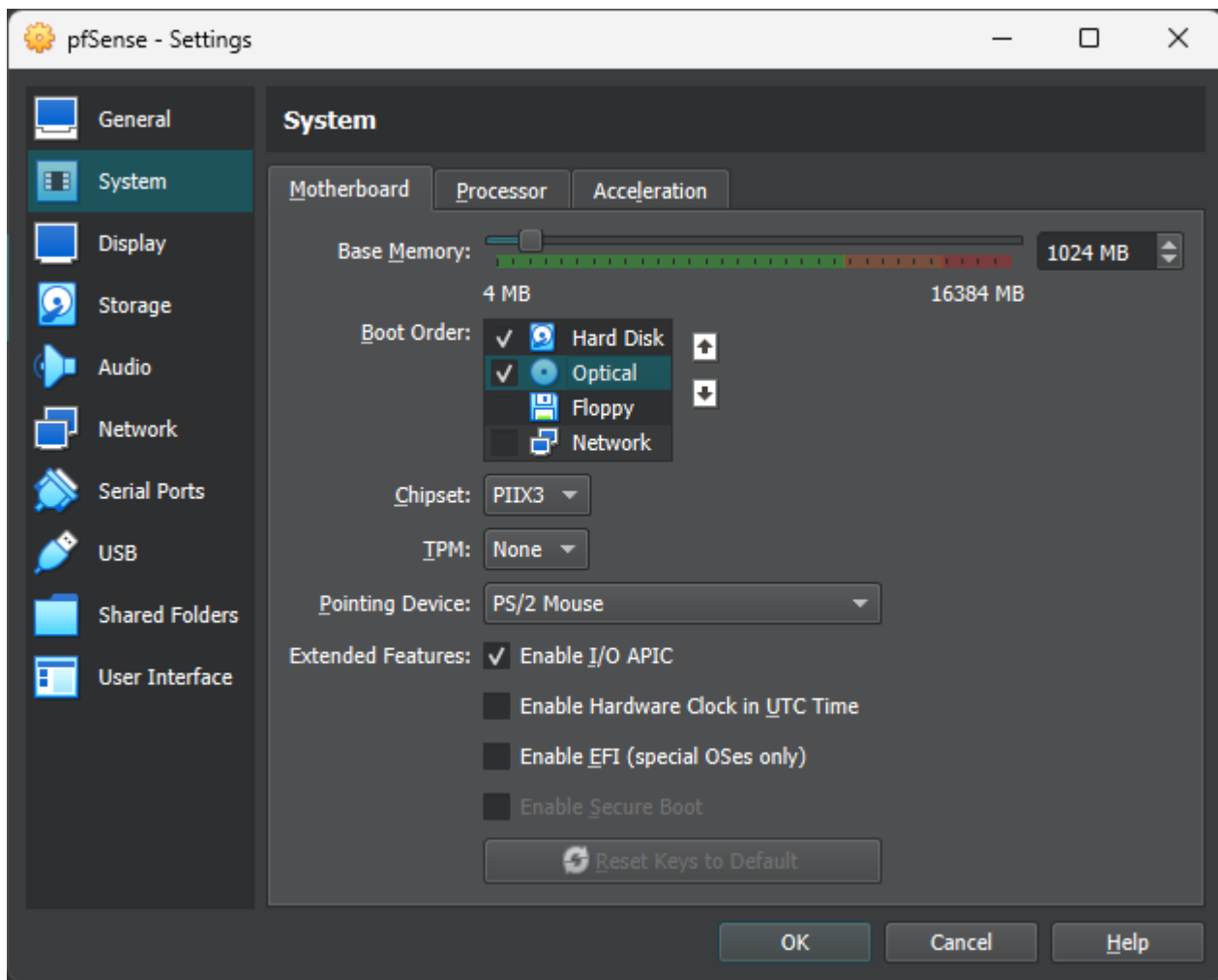
Check if everything is right and then click on **Finish**



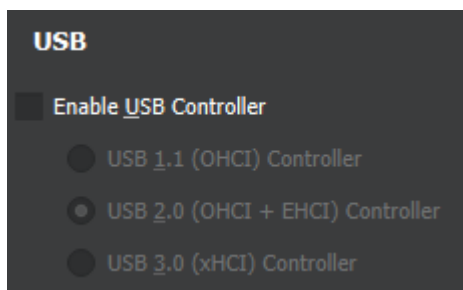
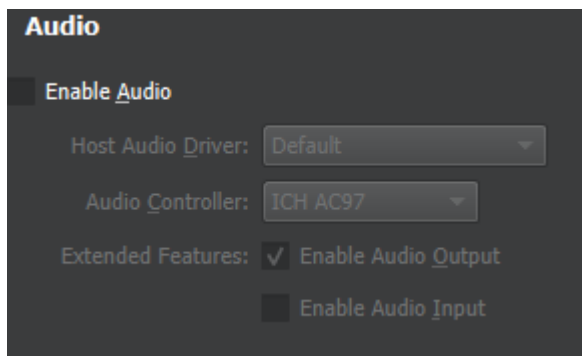
I configure some setting on the machine related to VirtualBox, so I select the pfSense VM and then click on **Settings**



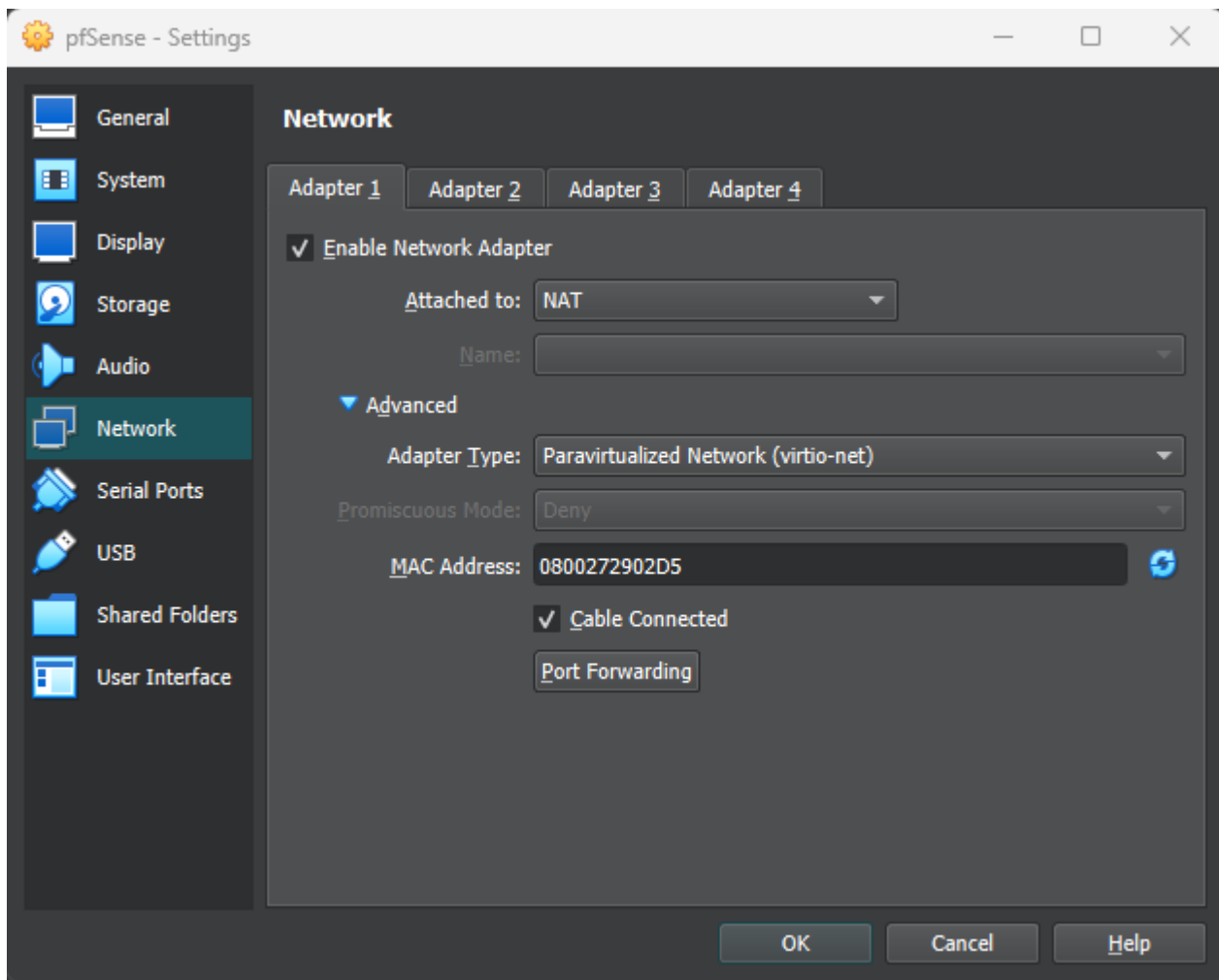
I select **System -> Motherboard** and then change the boot order to have the **Hard Disk** on top, **Optical** and uncheck **Floppy**



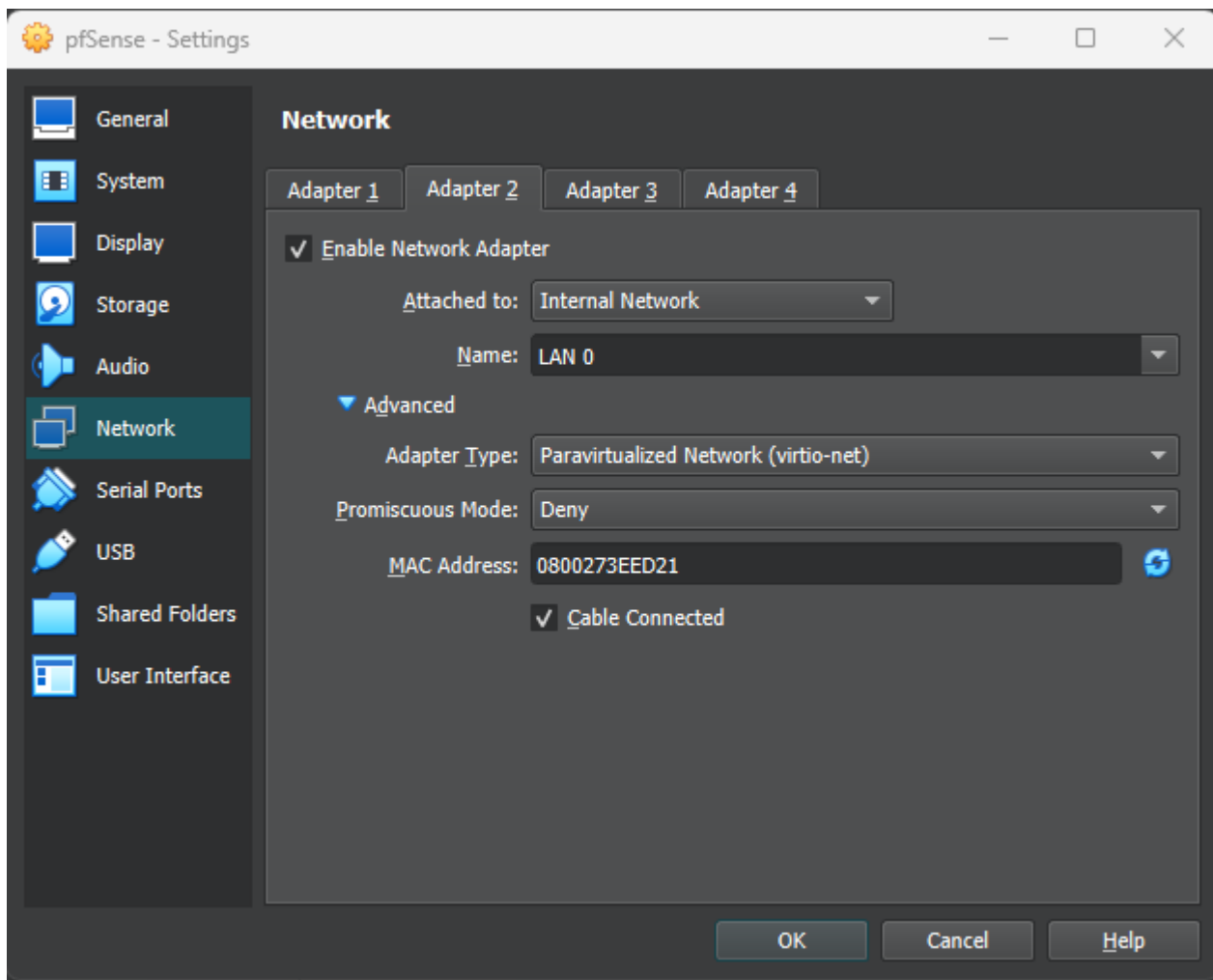
I also disable Audio and USB since I won't need them



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

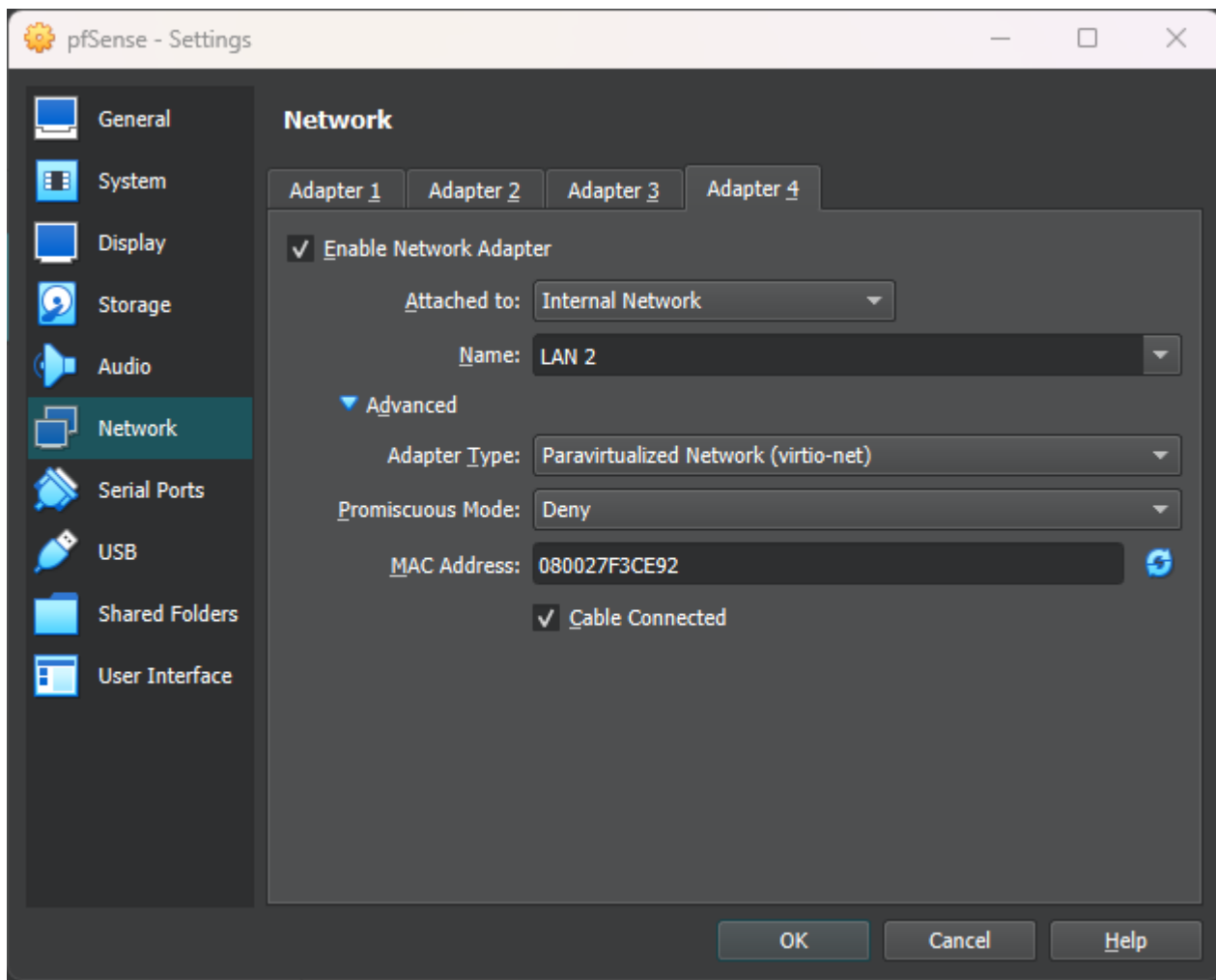
MAC Address: 080027E296B8

☒ Cable Connected

OK

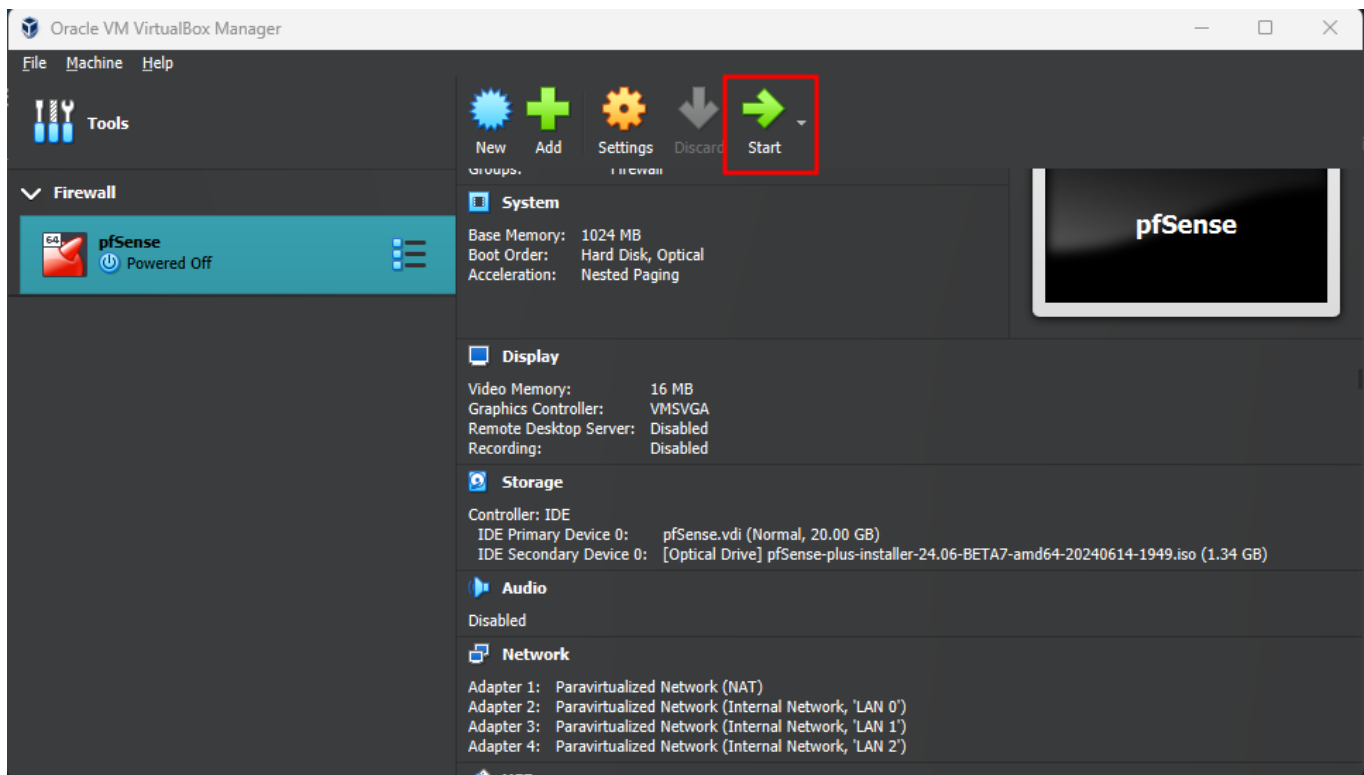
Cancel

Help

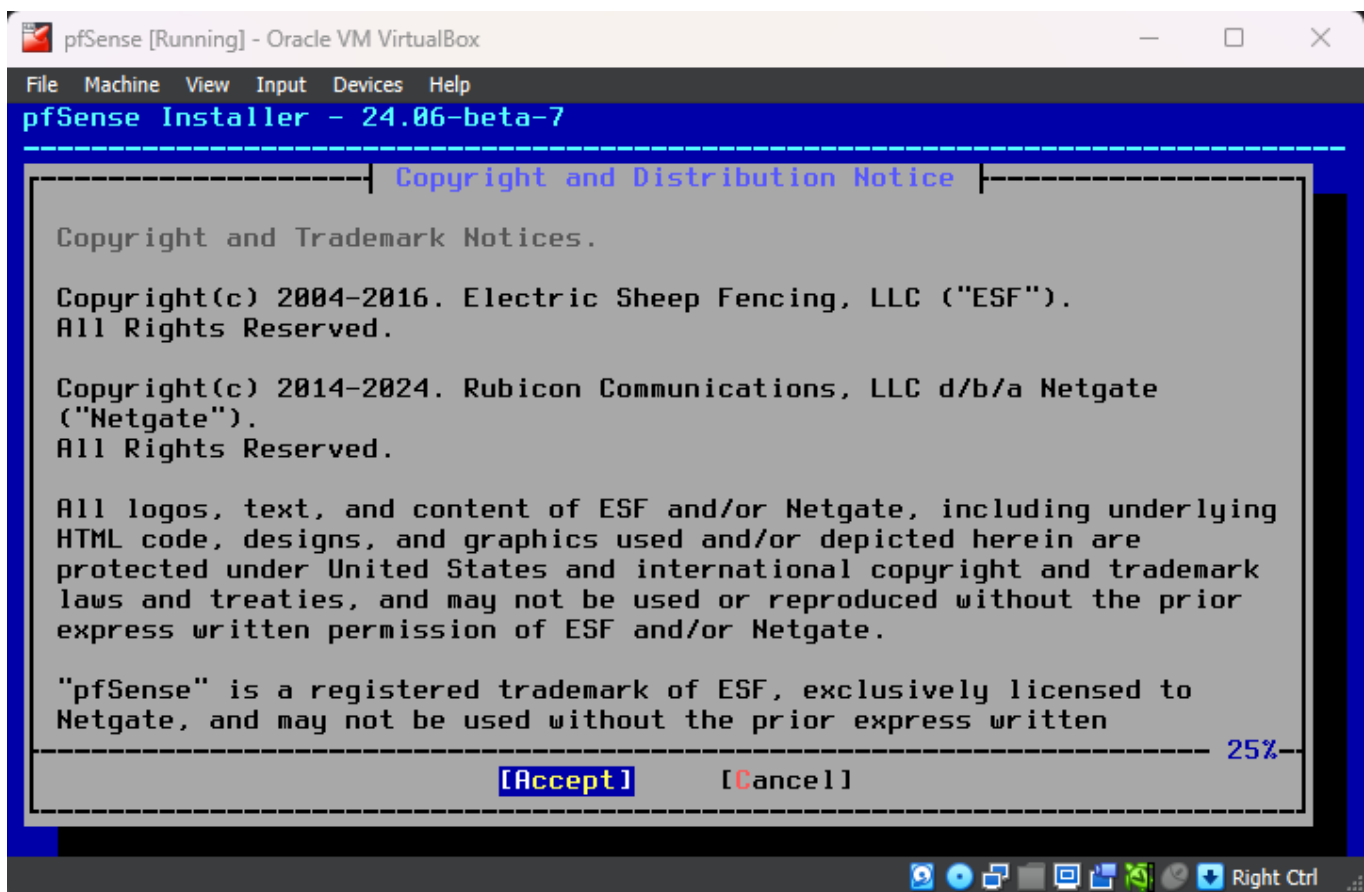


pfSense Installation

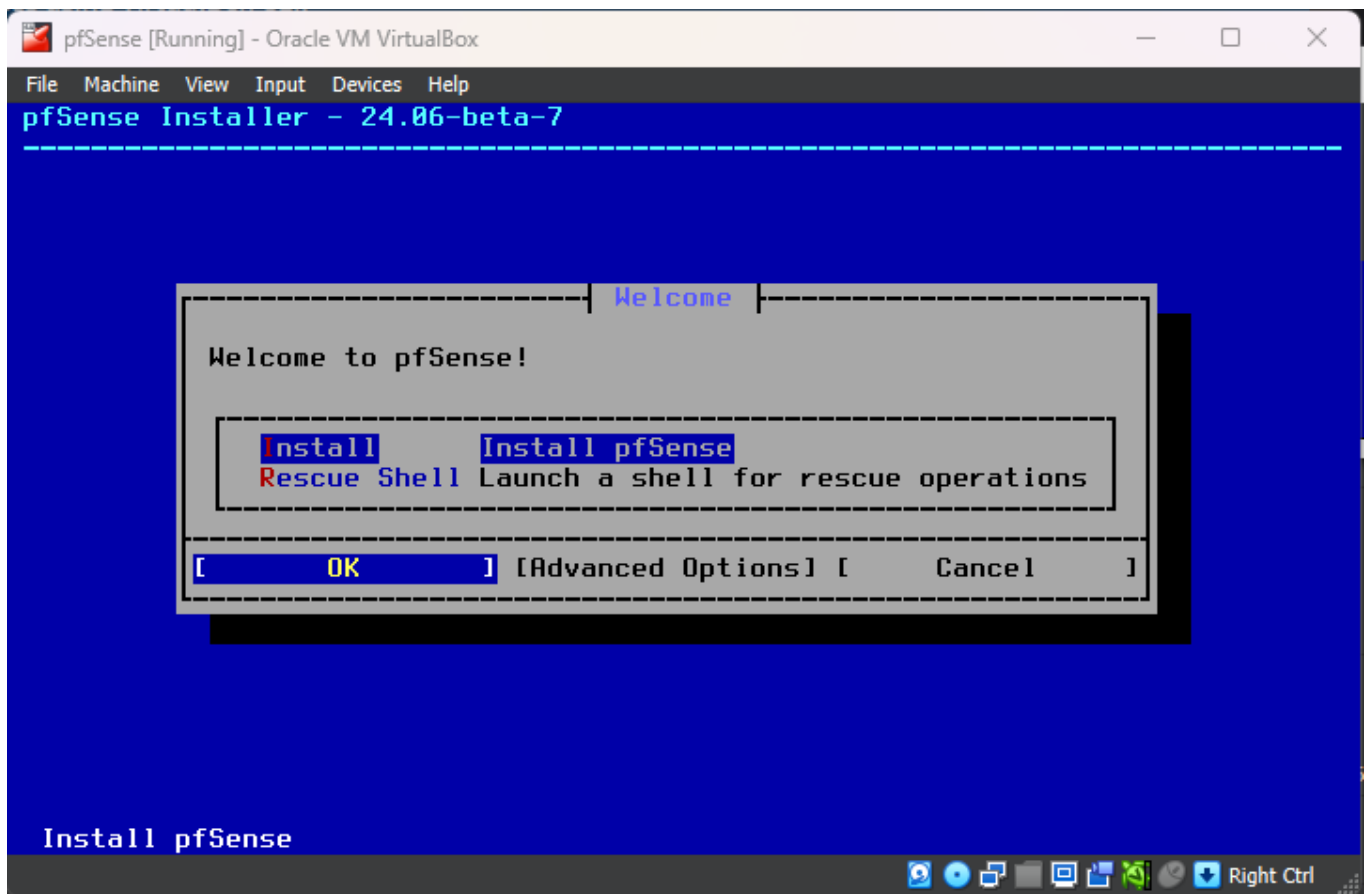
I can now **Start** the machine



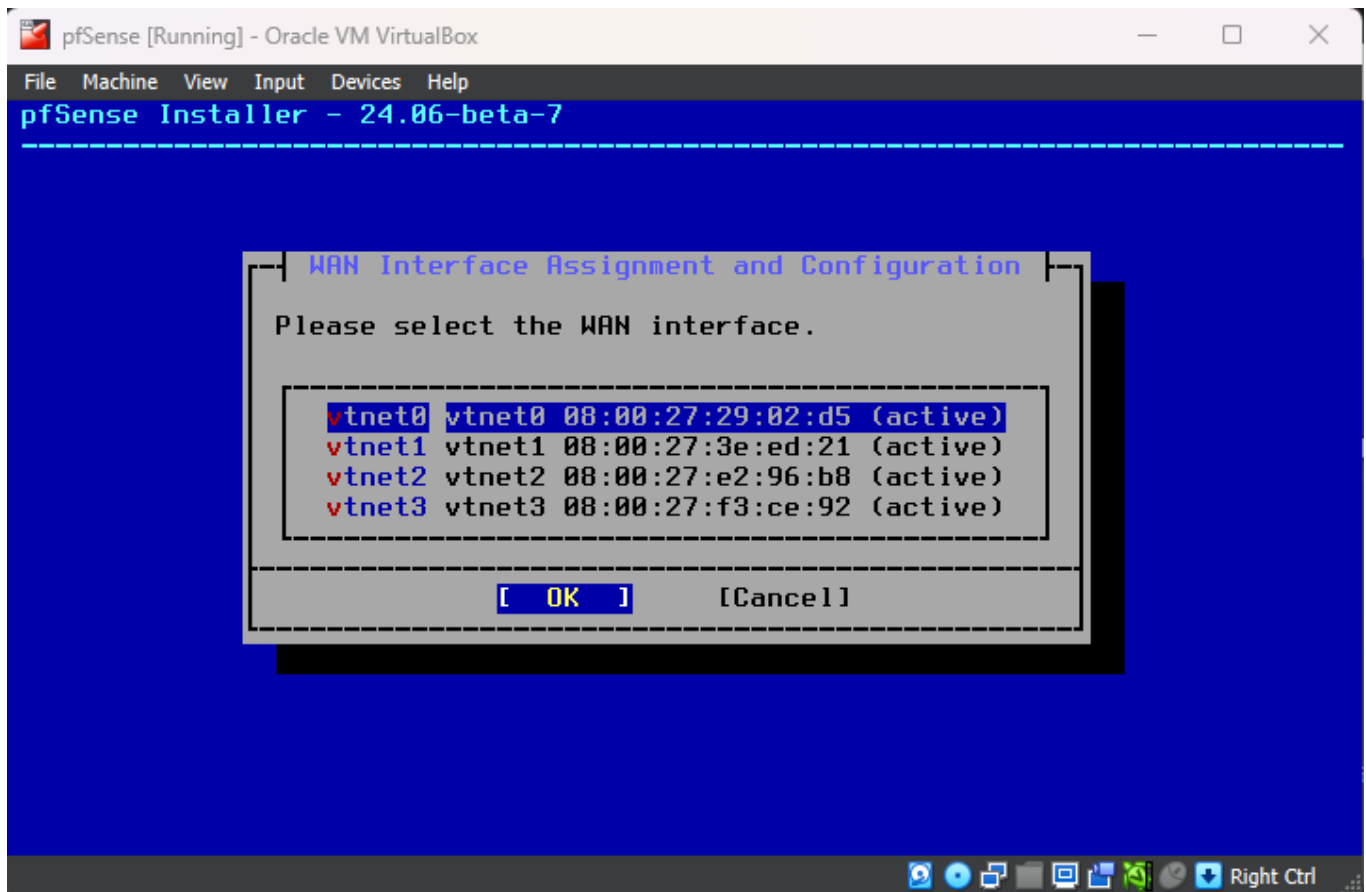
I press Enter to Accept the agreement



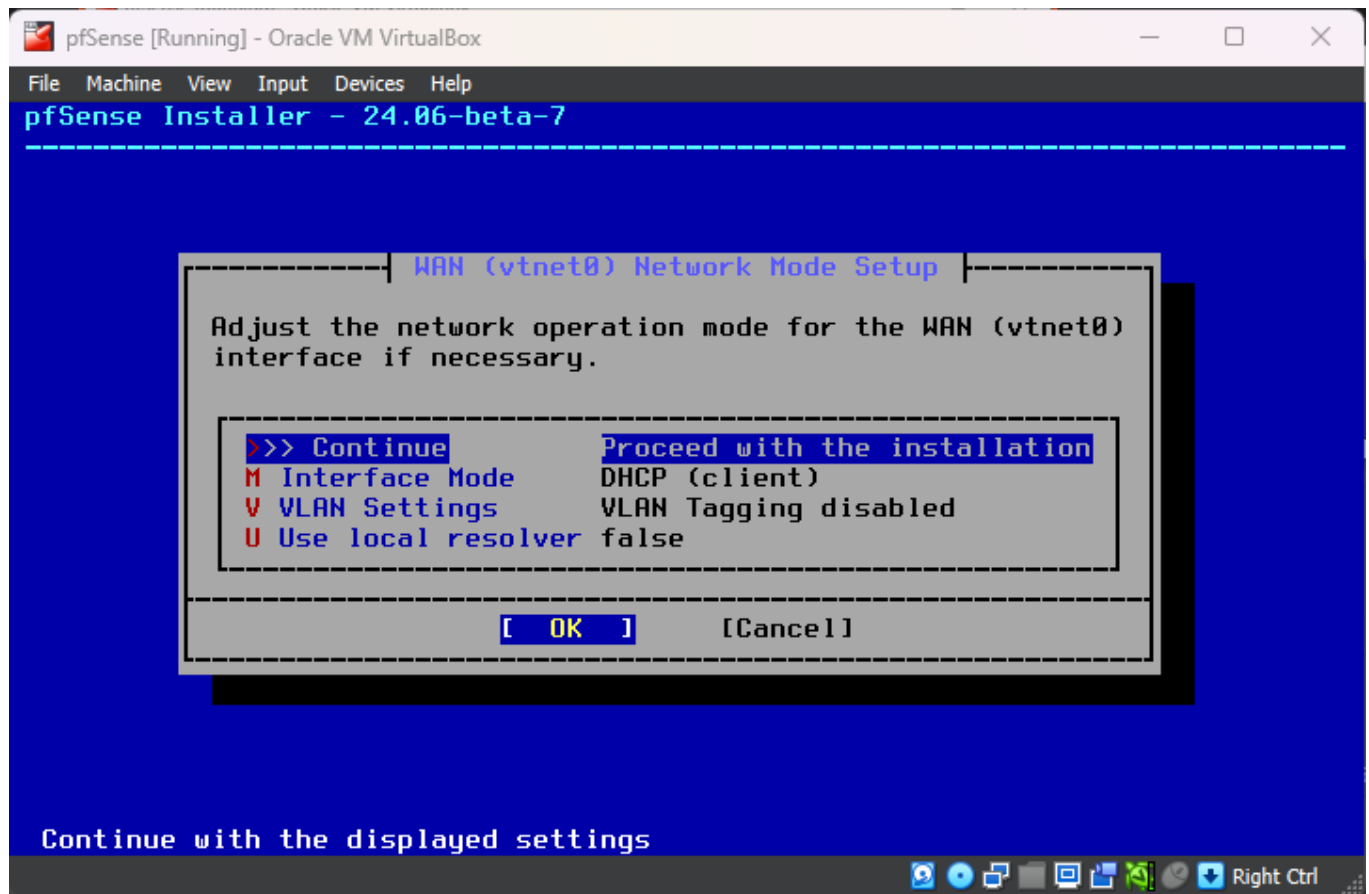
And then press Enter again to Install



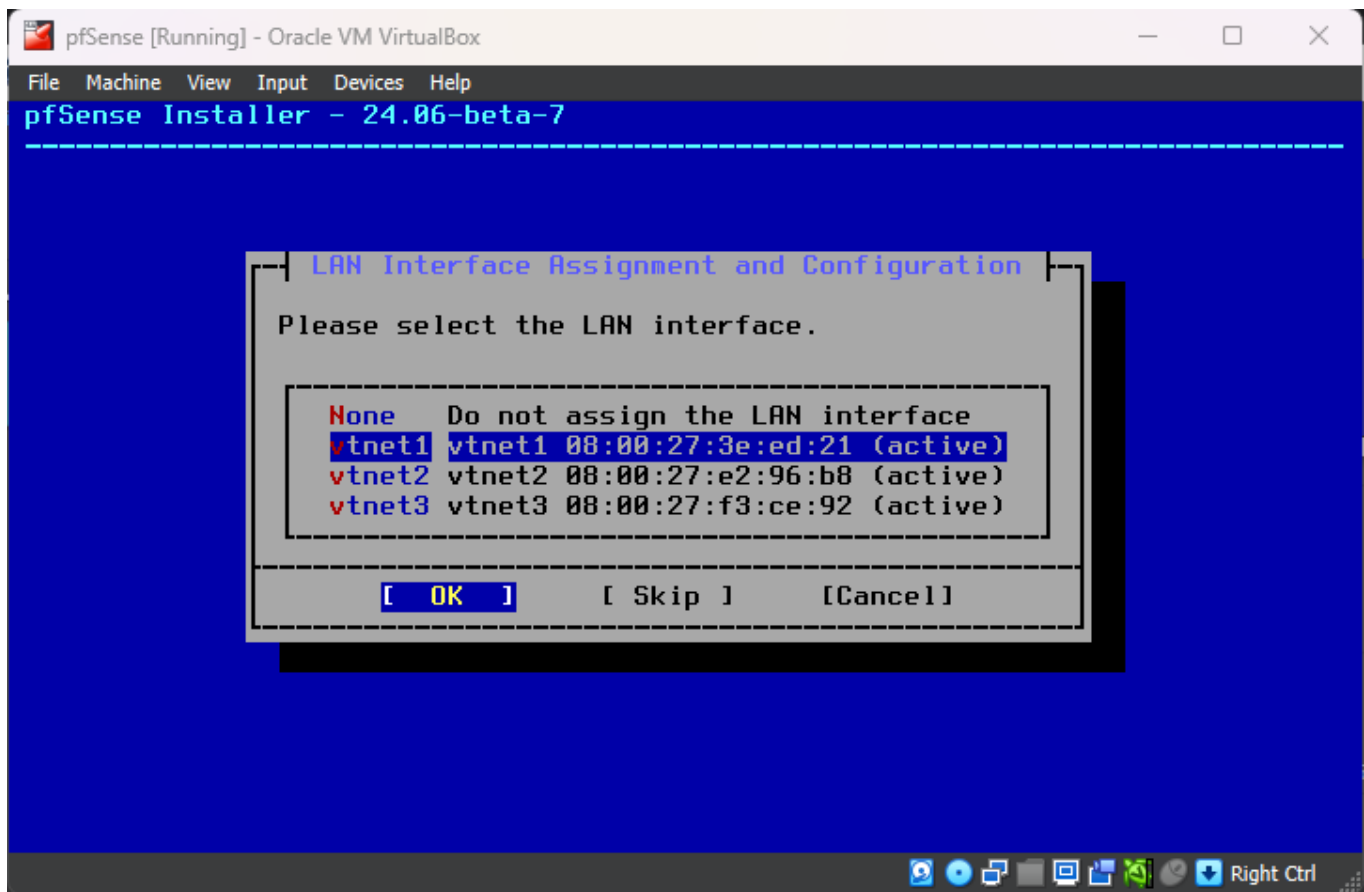
I select vtnet0 to use as the WAN interface



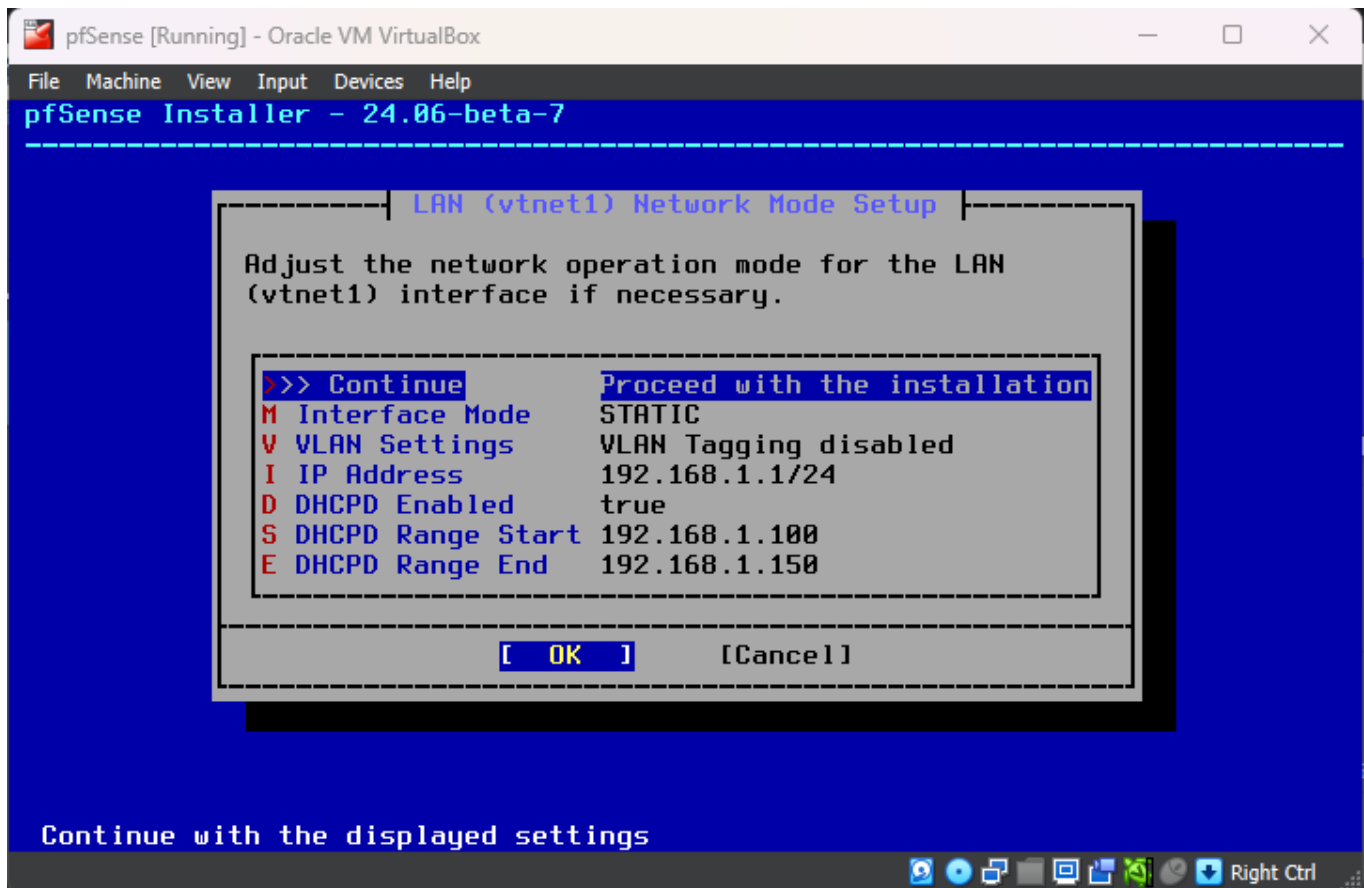
I press **Enter** to leave the settings as default and continue



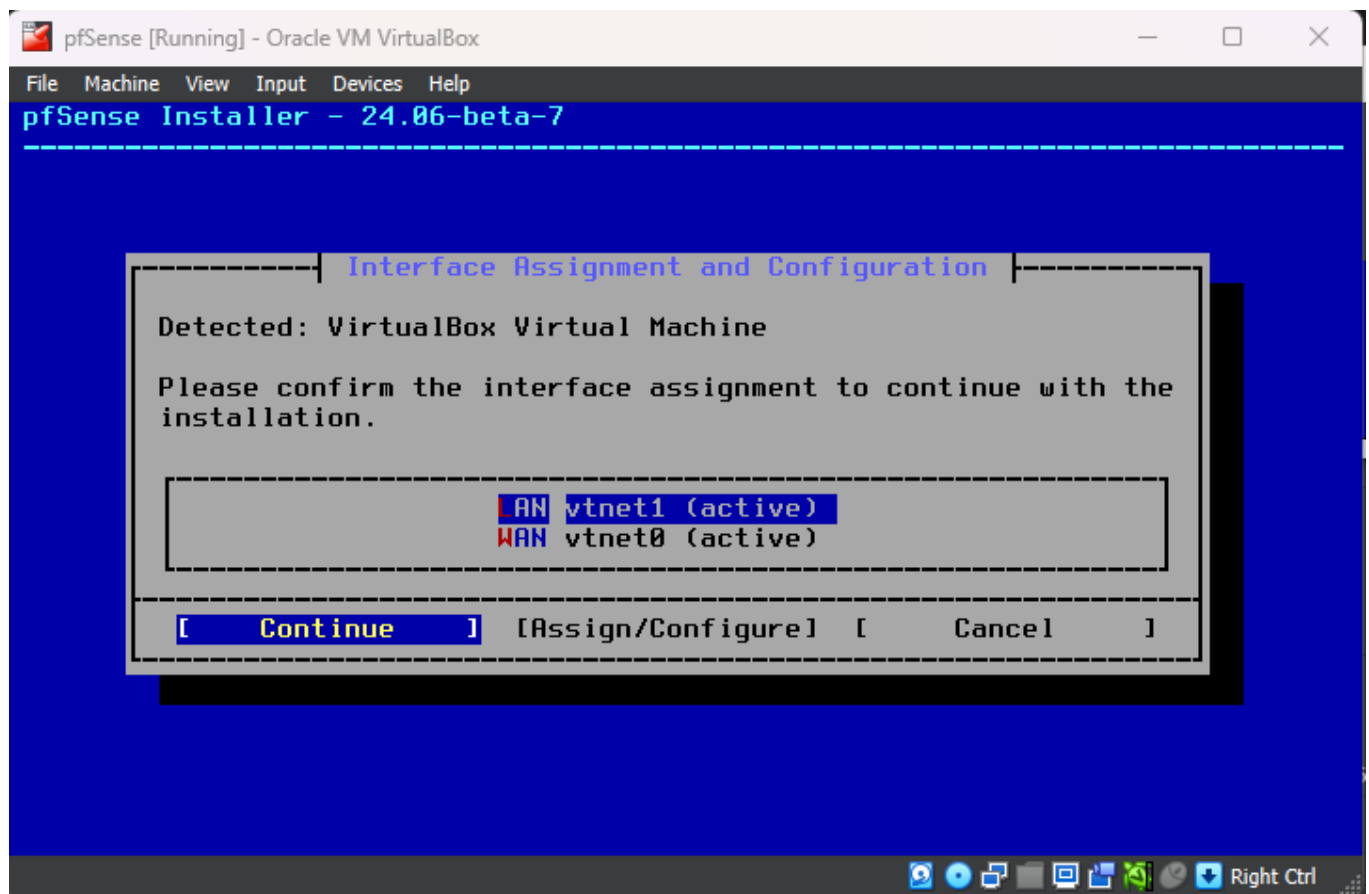
I select **vtnet1** as the LAN interface



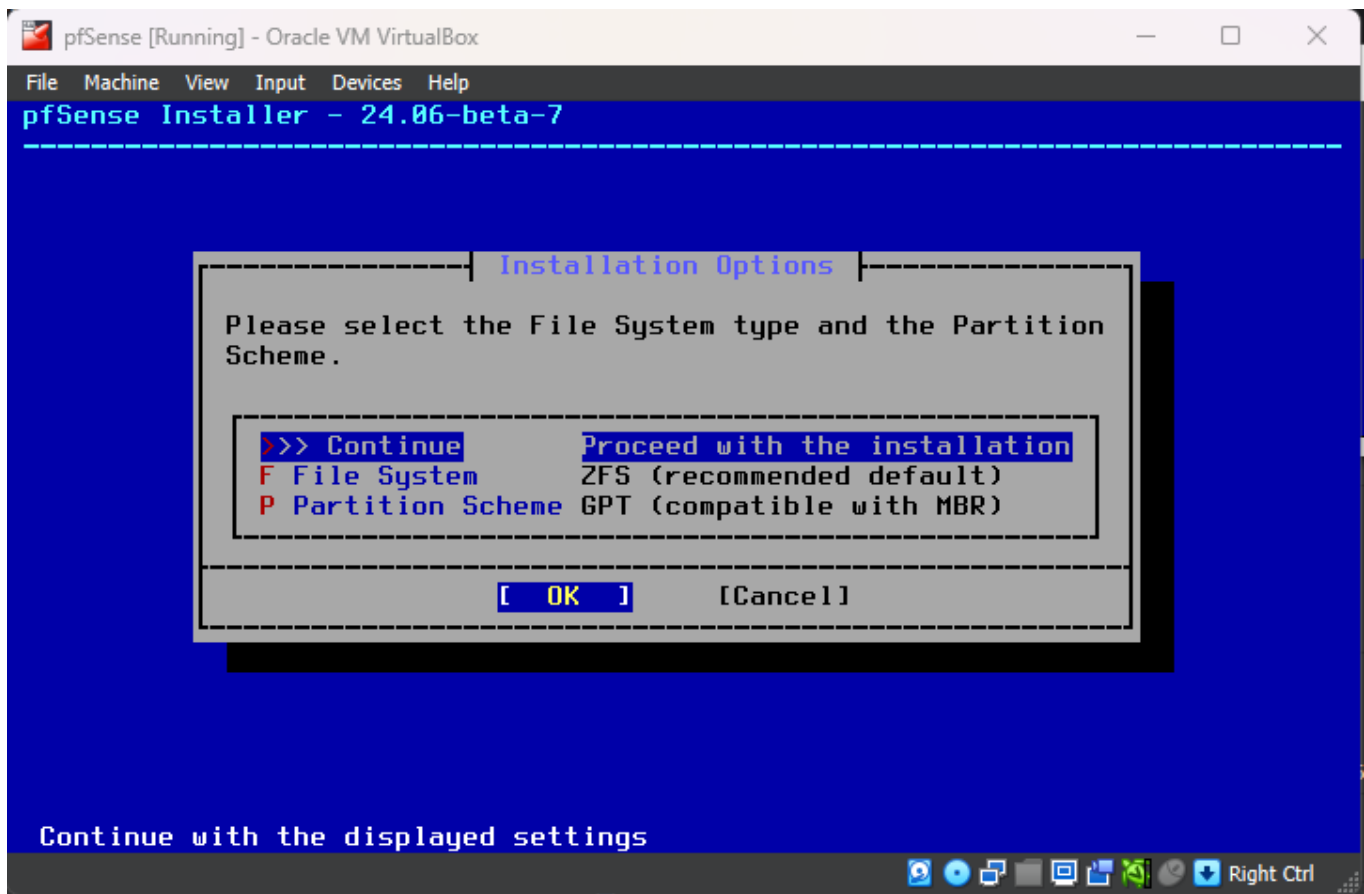
I leave default settings for this as well



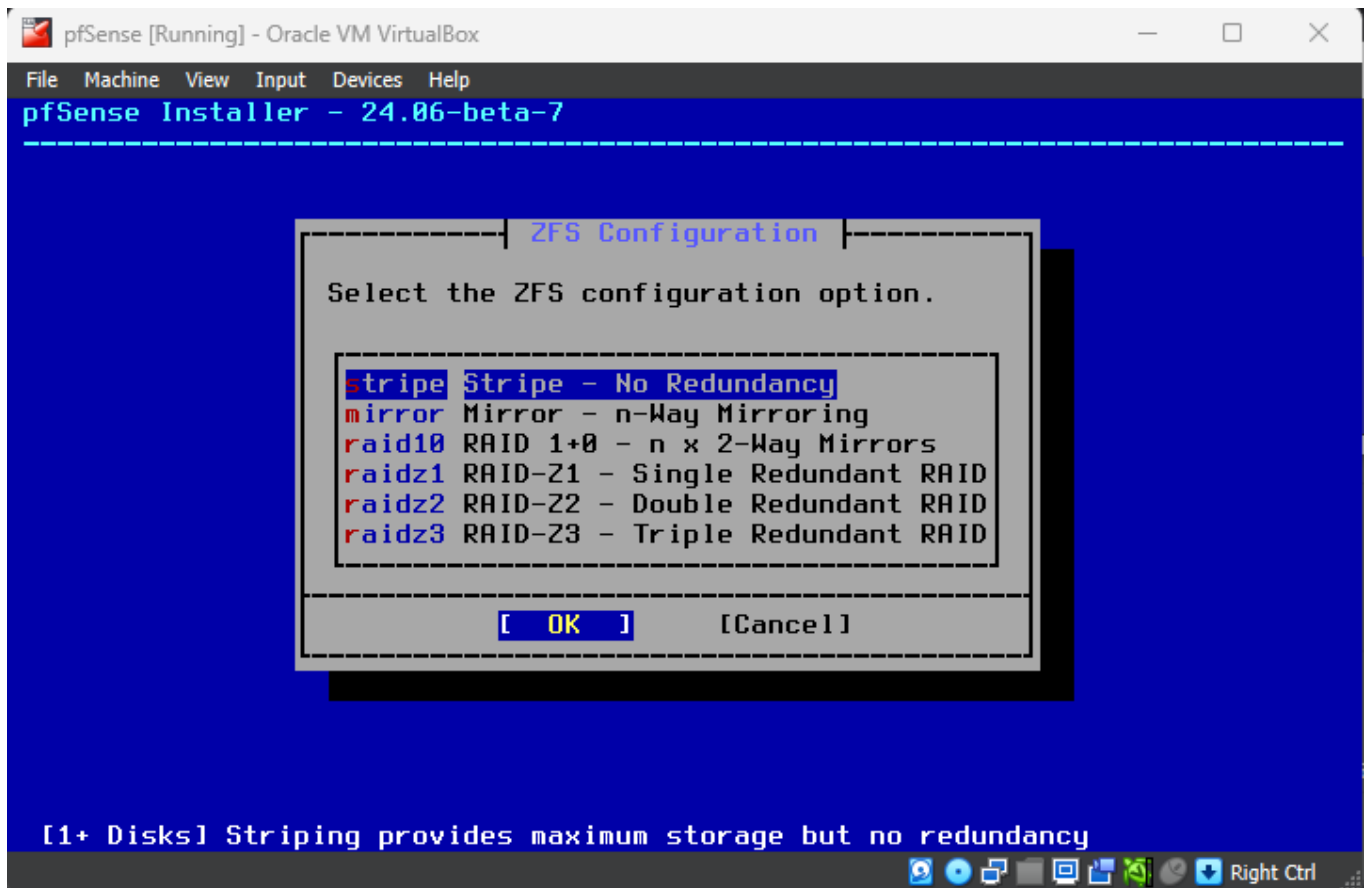
Then I press **Enter** again to continue the installation



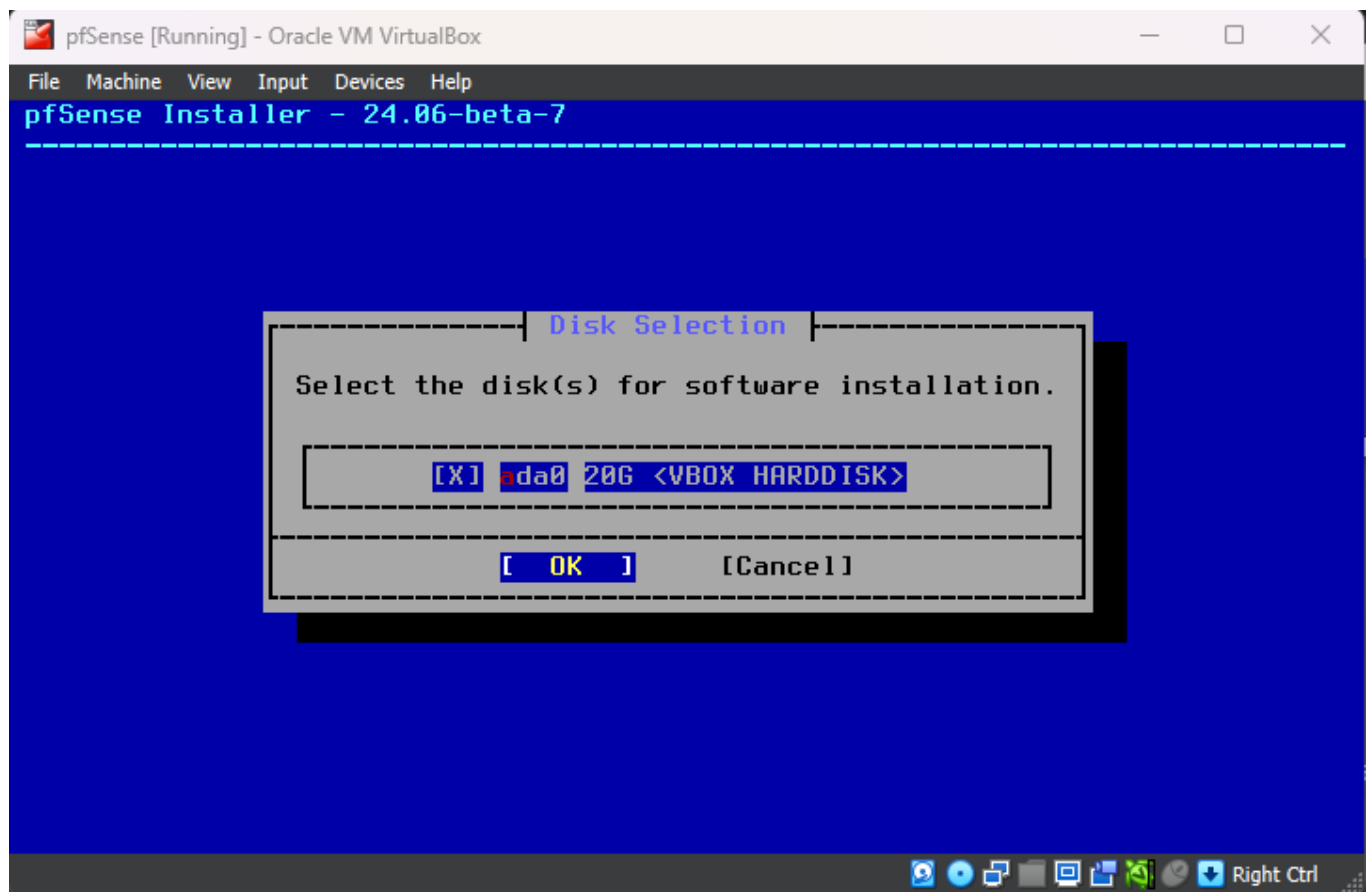
I then **Continue** with the default File System Type and Partition



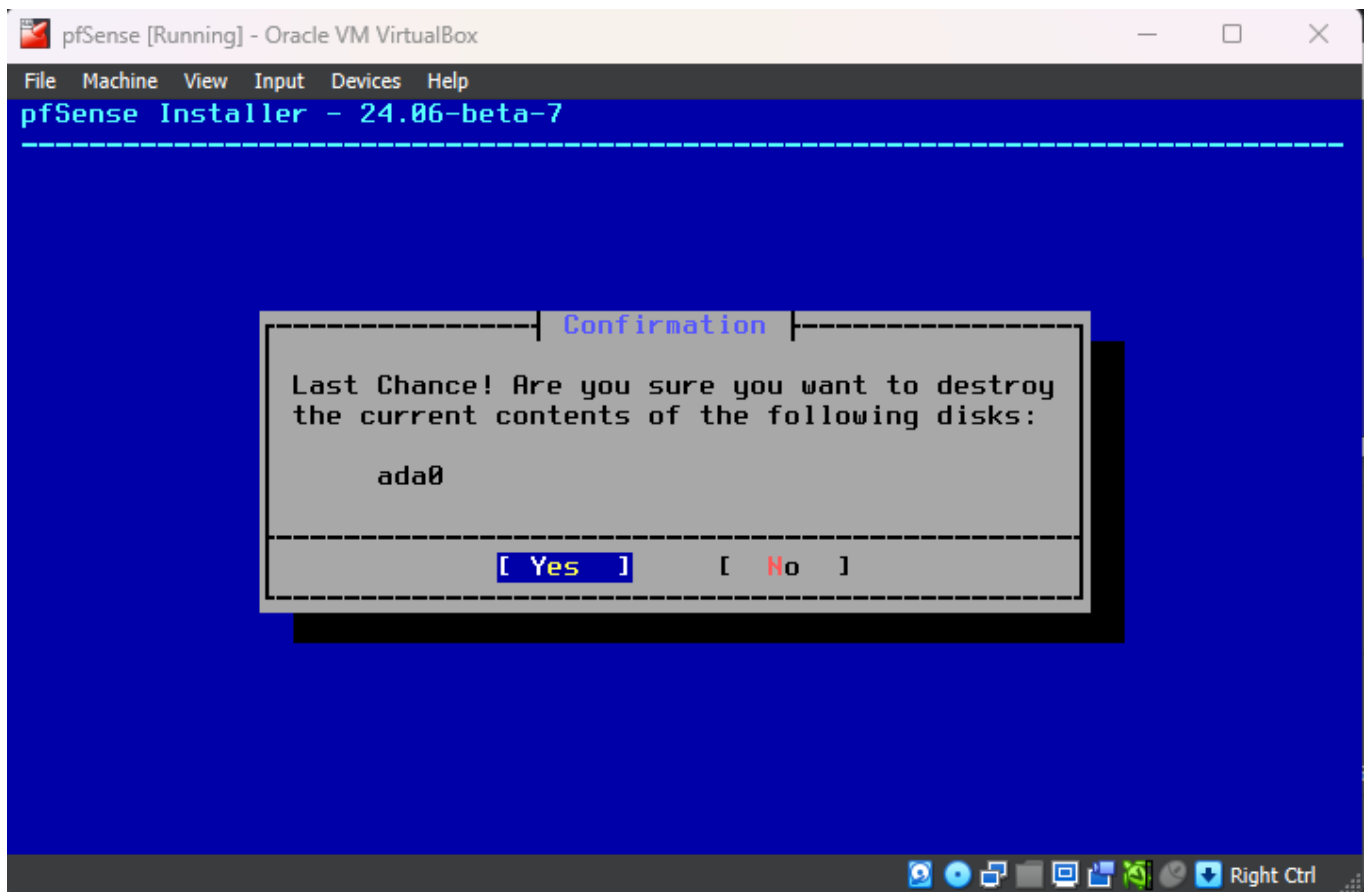
I select Stripe - No Redundancy



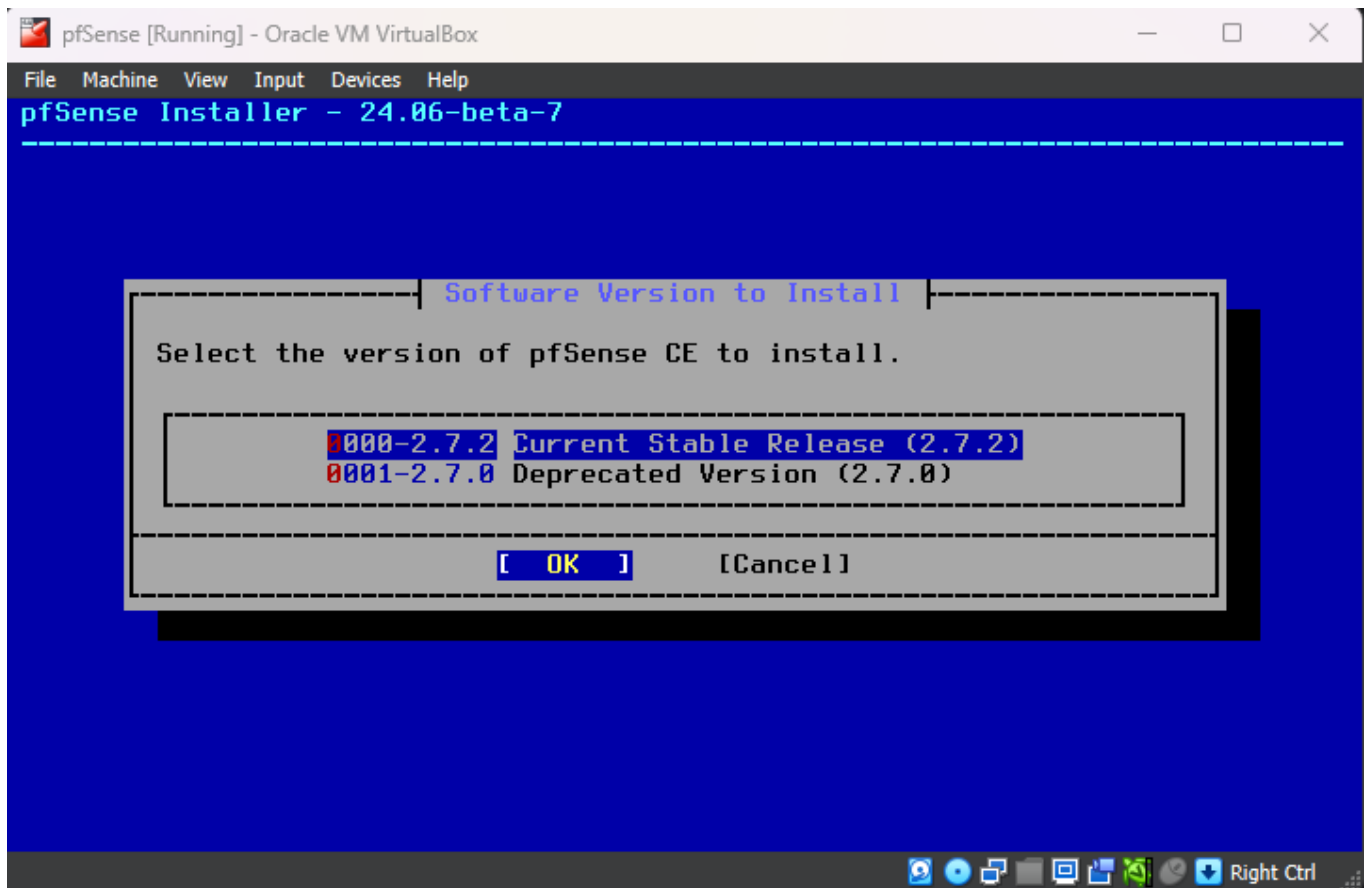
Leave the selected partition and press **Enter**



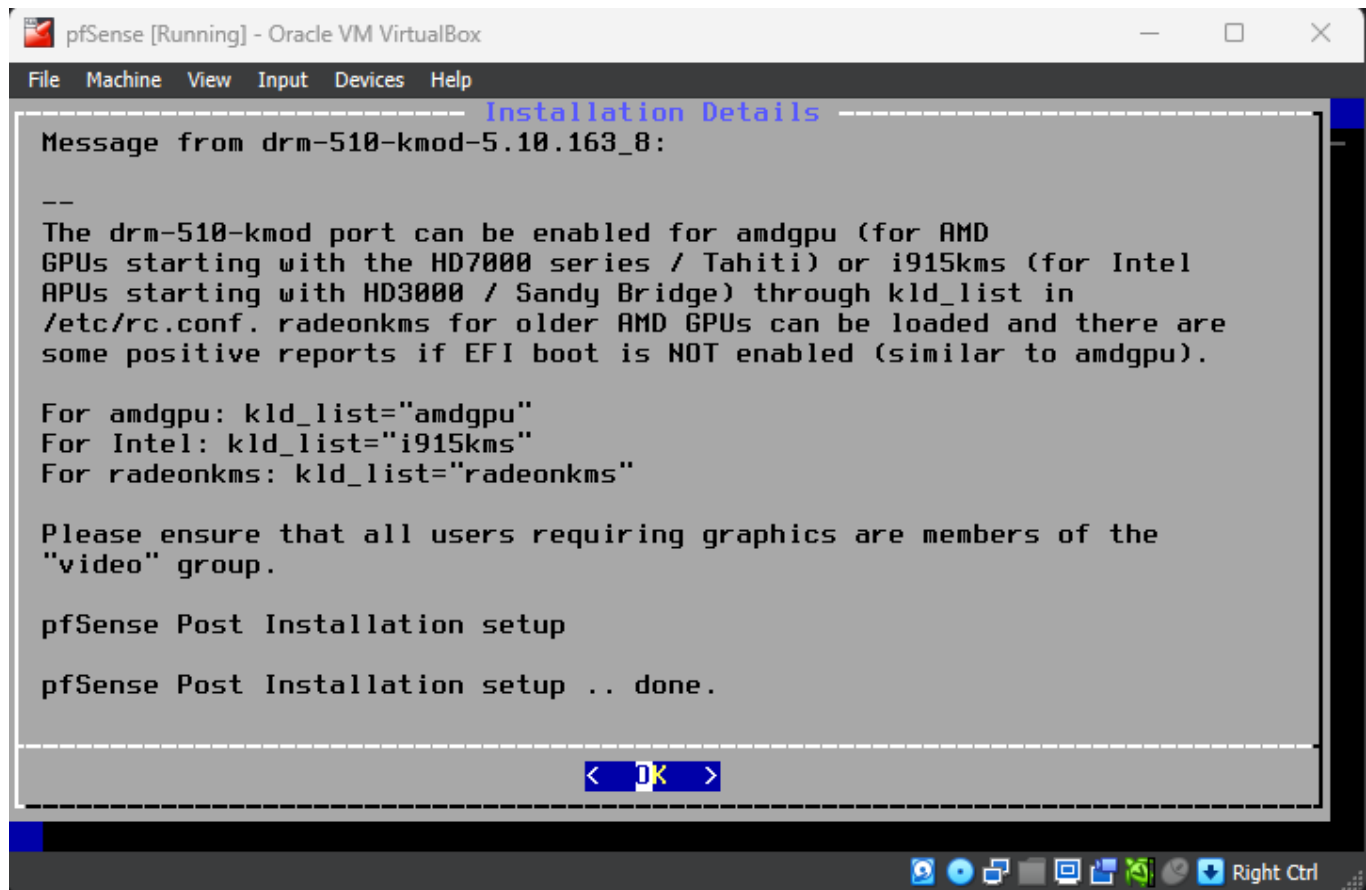
Confirm the partition



Select the Current Stable Release (2.7.2 in my case)



Once it finished it gave me this screen



```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Installation Details
Message from drm-510-kmod-5.10.163_8:
--
The drm-510-kmod port can be enabled for amdgpu (for AMD
GPUs starting with the HD7000 series / Tahiti) or i915kms (for Intel
APUs starting with HD3000 / Sandy Bridge) through kld_list in
/etc/rc.conf. radeonkms for older AMD GPUs can be loaded and there are
some positive reports if EFI boot is NOT enabled (similar to amdgpu).

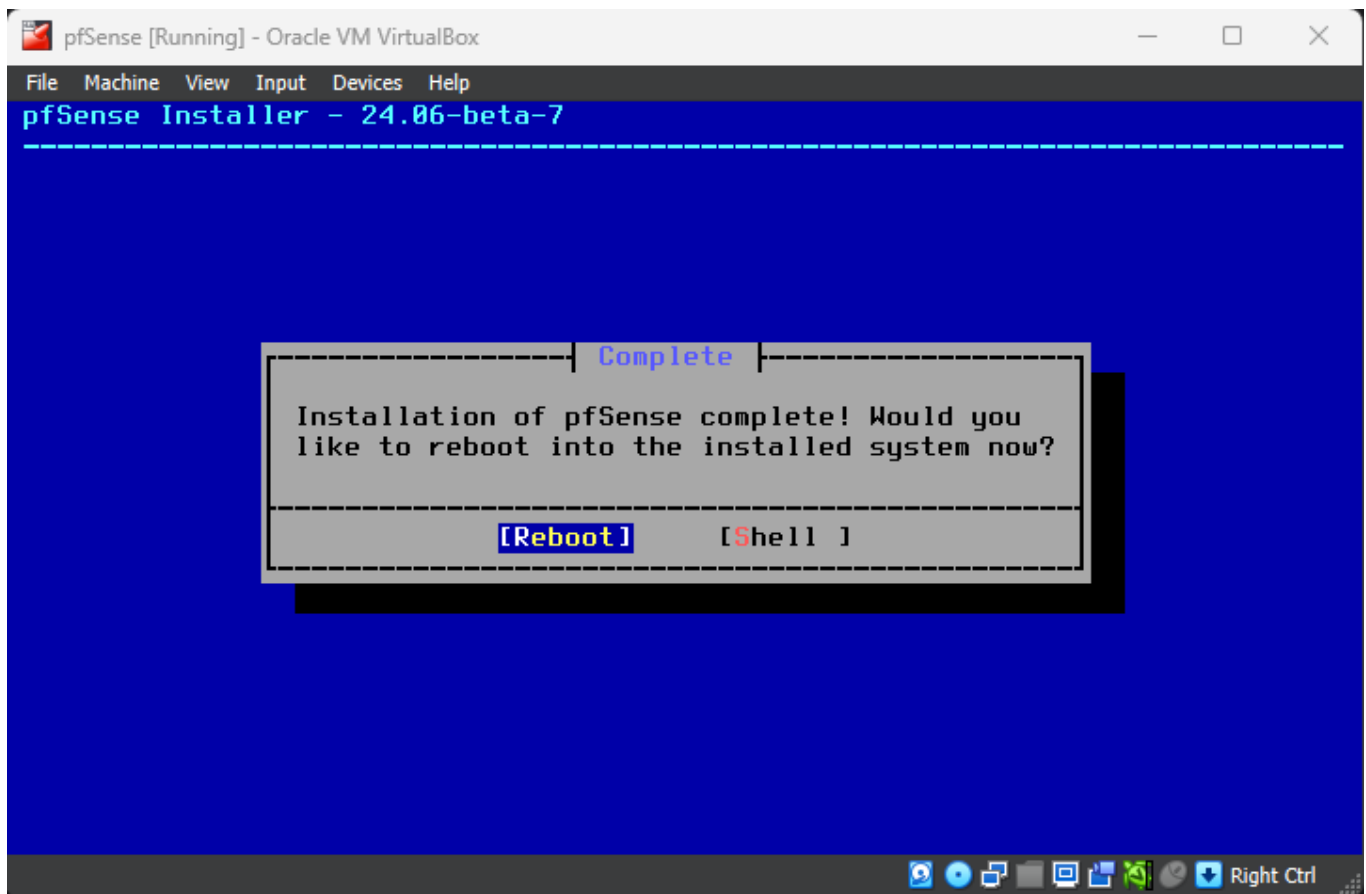
For amdgpu: kld_list="amdgpu"
For Intel: kld_list="i915kms"
For radeonkms: kld_list="radeonkms"

Please ensure that all users requiring graphics are members of the
"video" group.

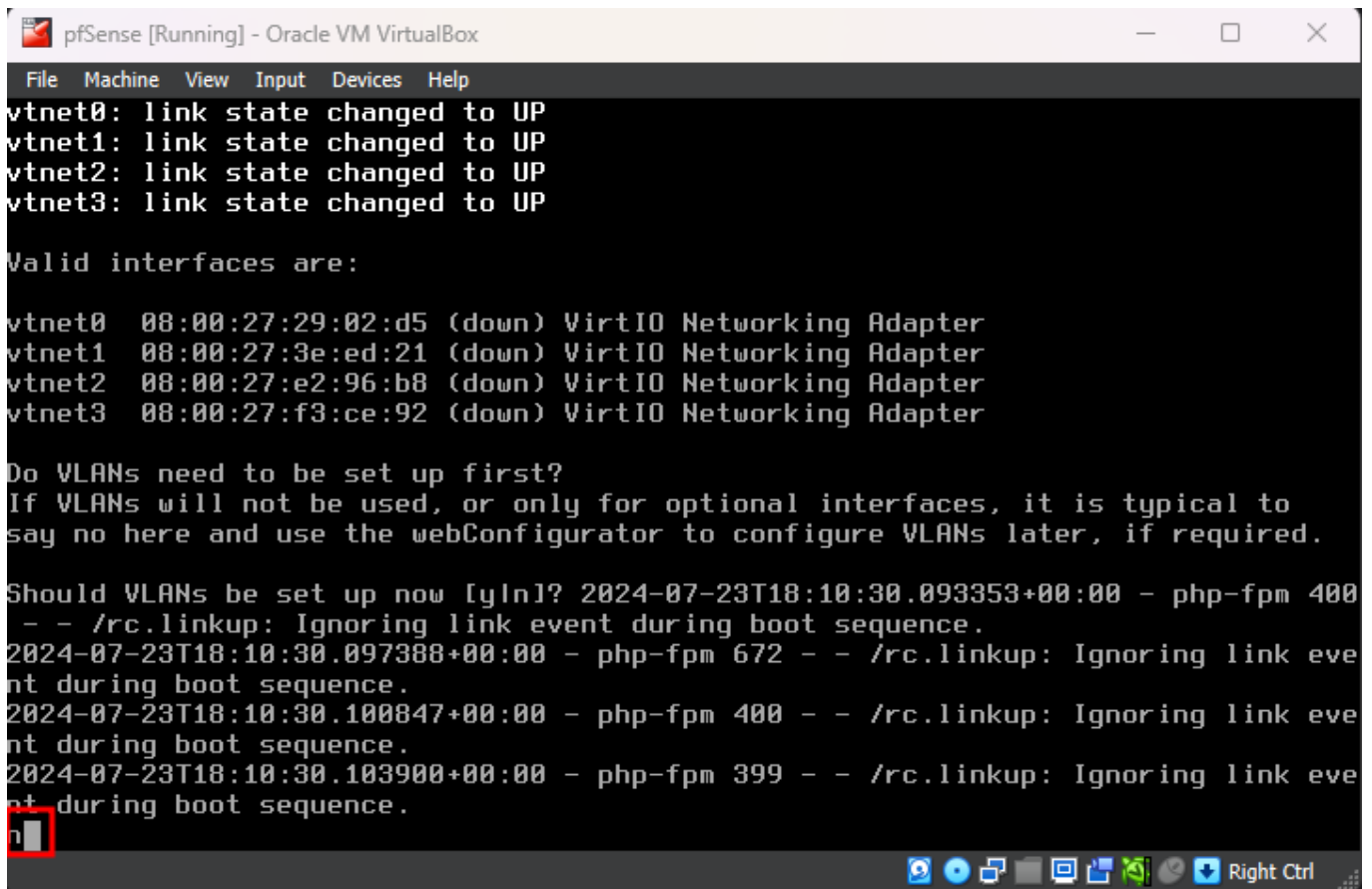
pfSense Post Installation setup
pfSense Post Installation setup .. done.

< OK >
```

I then pressed Enter to reboot



I then press n to not configure VLANs



Then i assign the interfaces like this:

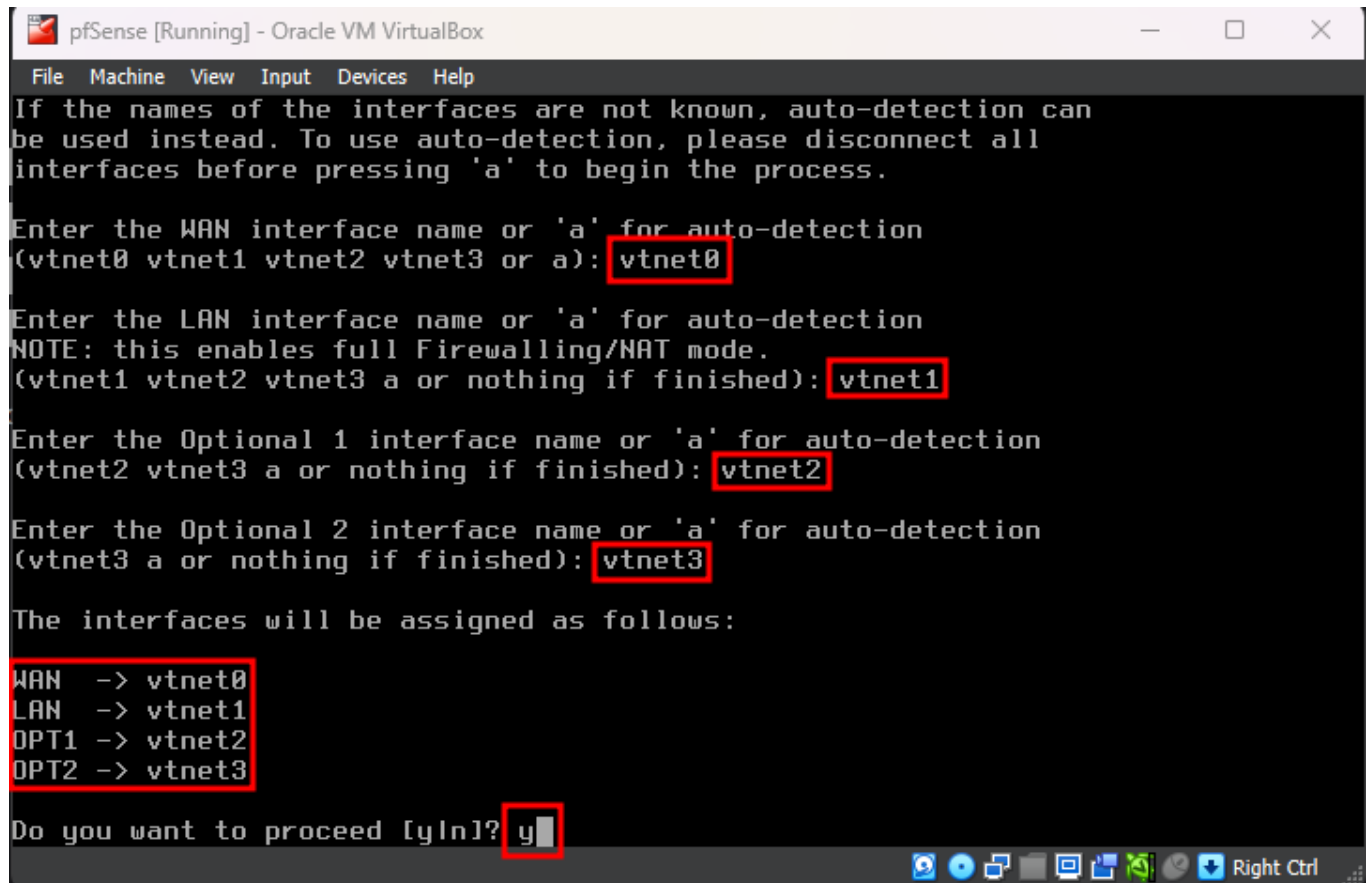
Enter the WAN interface name: **vtnet0**

Enter the LAN interface name: **vtnet1**

Enter the Optional 1 interface name: **vtnet2**

Enter the Optional 2 interface name: **vtnet3**

and confirm

A screenshot of a pfSense terminal window running inside an Oracle VM VirtualBox. The terminal shows the process of assigning network interfaces to pfSense. It prompts the user to enter the WAN interface name, LAN interface name, Optional 1 interface name, and Optional 2 interface name. The user enters vtnet0, vtnet1, vtnet2, and vtnet3 respectively. The terminal then displays the assigned interfaces: WAN -> vtnet0, LAN -> vtnet1, OPT1 -> vtnet2, and OPT2 -> vtnet3. Finally, it asks if the user wants to proceed, and the user enters 'y'.

```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 vtnet2 vtnet3 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 vtnet2 vtnet3 a or nothing if finished): vtnet1

Enter the Optional 1 interface name or 'a' for auto-detection
(vtnet2 vtnet3 a or nothing if finished): vtnet2

Enter the Optional 2 interface name or 'a' for auto-detection
(vtnet3 a or nothing if finished): vtnet3

The interfaces will be assigned as follows:
WAN -> vtnet0
LAN -> vtnet1
OPT1 -> vtnet2
OPT2 -> vtnet3

Do you want to proceed [y/n]? y
```

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.

```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

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

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: 192.168.1.1/24
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

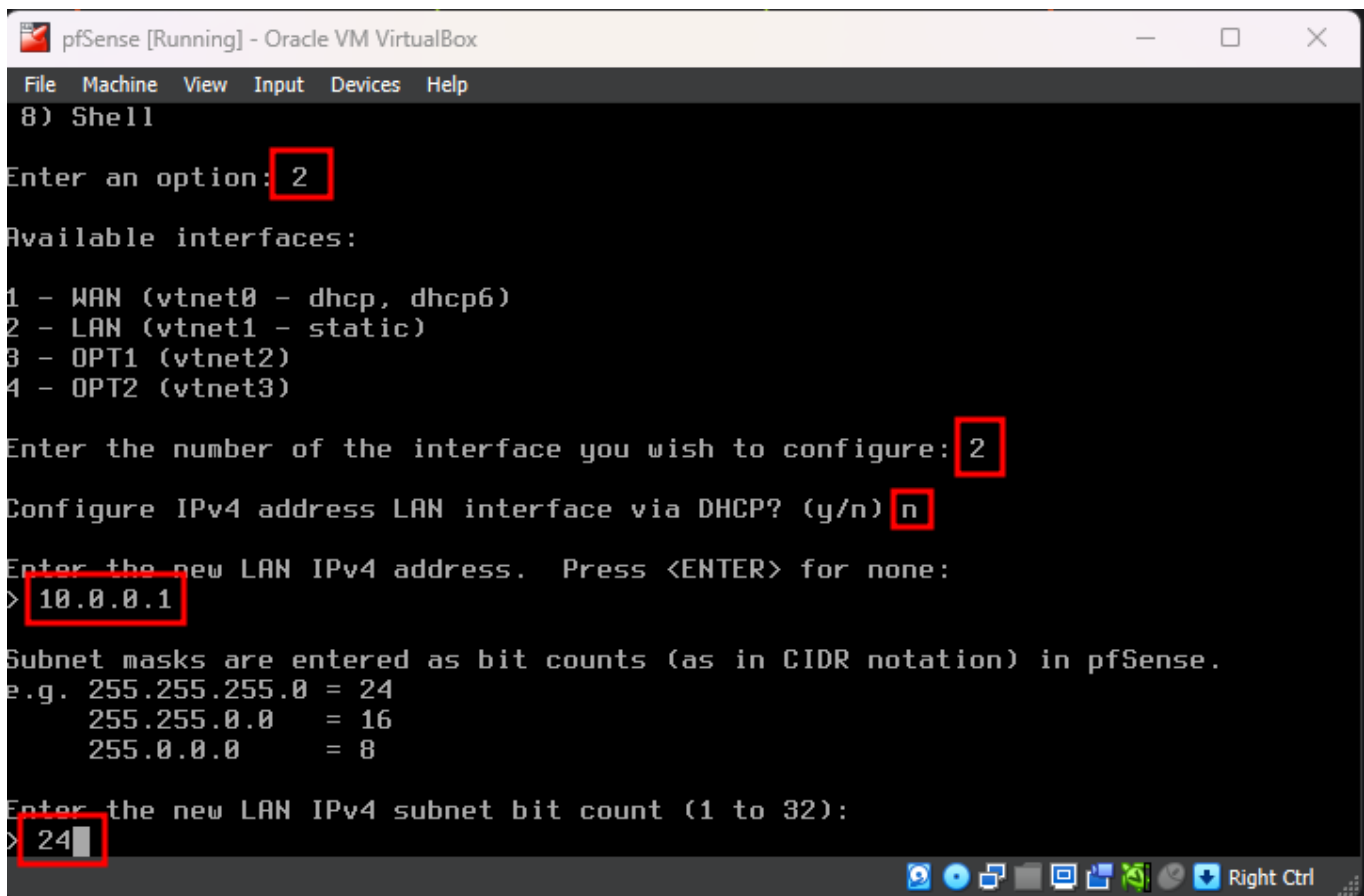
Enter an option: 
```

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



```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
8) Shell
Enter an option: 2
Available interfaces:
1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2)
4 - OPT2 (vtnet3)
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
    255.255.0.0   = 16
    255.0.0.0    = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 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.
```

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

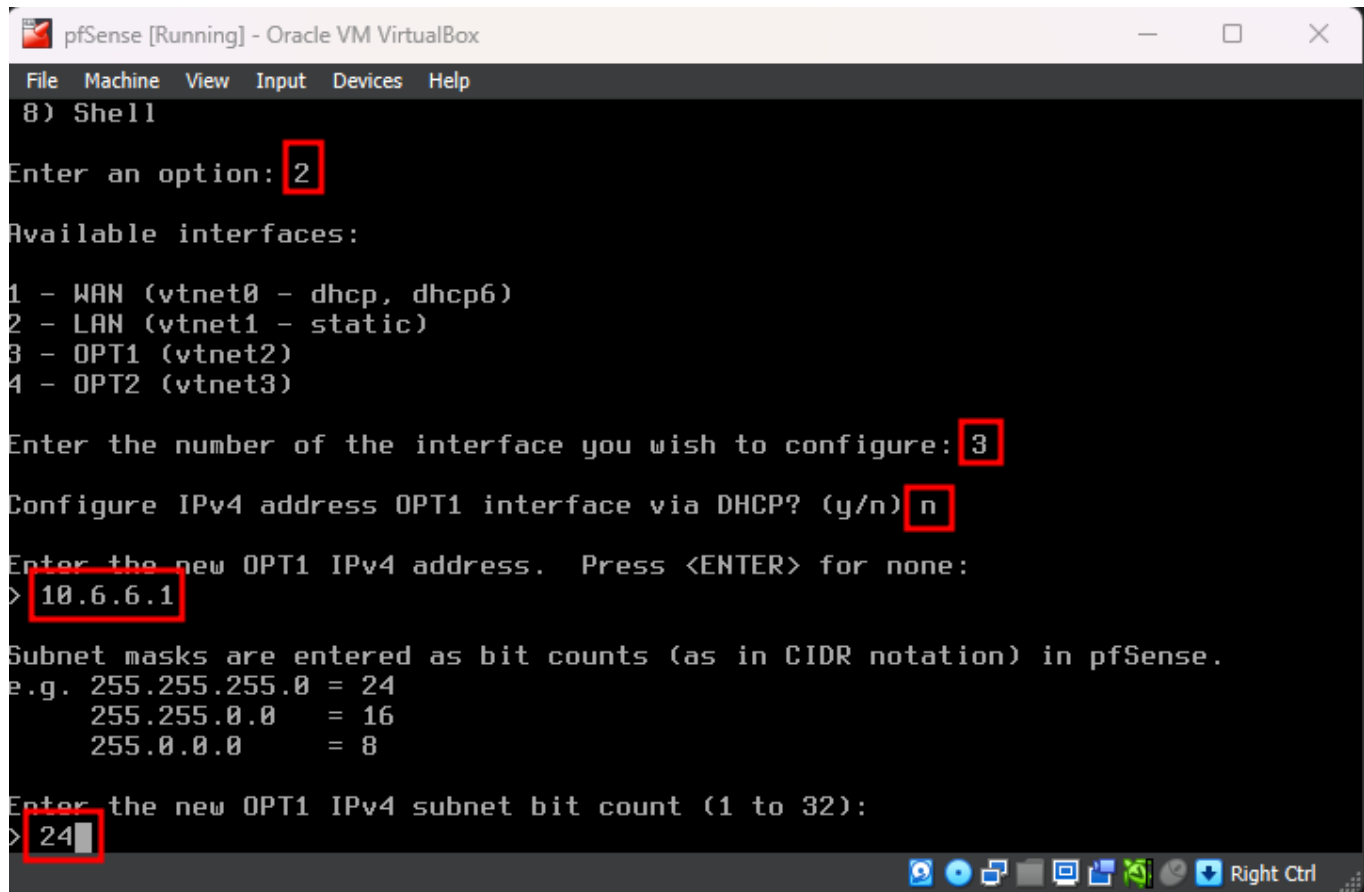
Enter an option:
```

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

A screenshot of a pfSense terminal window running in Oracle VM VirtualBox. The window title is "pfSense [Running] - Oracle VM VirtualBox". The terminal shows the configuration steps for the OPT1 interface. The user enters '2' to select "Set interface(s) IP address". The terminal lists available interfaces: 1 - WAN (vtnet0 - dhcp, dhcp6), 2 - LAN (vtnet1 - static), 3 - OPT1 (vtnet2), and 4 - OPT2 (vtnet3). The user enters '3' to select the OPT1 interface. The terminal asks "Configure IPv4 address OPT1 interface via DHCP? (y/n)" and the user enters 'n'. The terminal asks "Enter the new OPT1 IPv4 address. Press <ENTER> for none:" and the user enters '10.6.6.1'. The terminal shows examples of subnet masks and bit counts: "Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24, 255.255.0.0 = 16, 255.0.0.0 = 8". The terminal asks "Enter the new OPT1 IPv4 subnet bit count (1 to 32):" and the user enters '24'.

```
8) Shell
Enter an option: 2
Available interfaces:
1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2)
4 - OPT2 (vtnet3)
Enter the number of the interface you wish to configure: 3
Configure IPv4 address OPT1 interface via DHCP? (y/n) n
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.6.6.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
    255.255.0.0   = 16
    255.0.0.0    = 8
Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 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

```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
> 10.6.6.1

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

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) 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
Disabling IPv6 DHCPD...

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


```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2 - static)
4 - OPT2 (vtnet3)

Enter the number of the interface you wish to configure: 4

Configure IPv4 address OPT2 interface via DHCP? (y/n) n

Enter the new OPT2 IPv4 address. Press <ENTER> for none:
> 10.80.80.1

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

Enter the new OPT2 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT2 interface via DHCP6? (y/n) 
```

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

```
pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Configure IPv6 address OPT2 interface via DHCP6? (y/n) n
Enter the new OPT2 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) n
Disabling IPv4 DHCPD...
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 OPT2...[fib_algo] inet.0 (bsearch4#42)
) rebuild_fd_flm: switching algo to radix4_lockless

Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT2 address has been set to 10.80.80.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://10.80.80.1/

Press <ENTER> to continue.
```

Now, all the interfaces are configured

```
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://10.80.80.1/

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

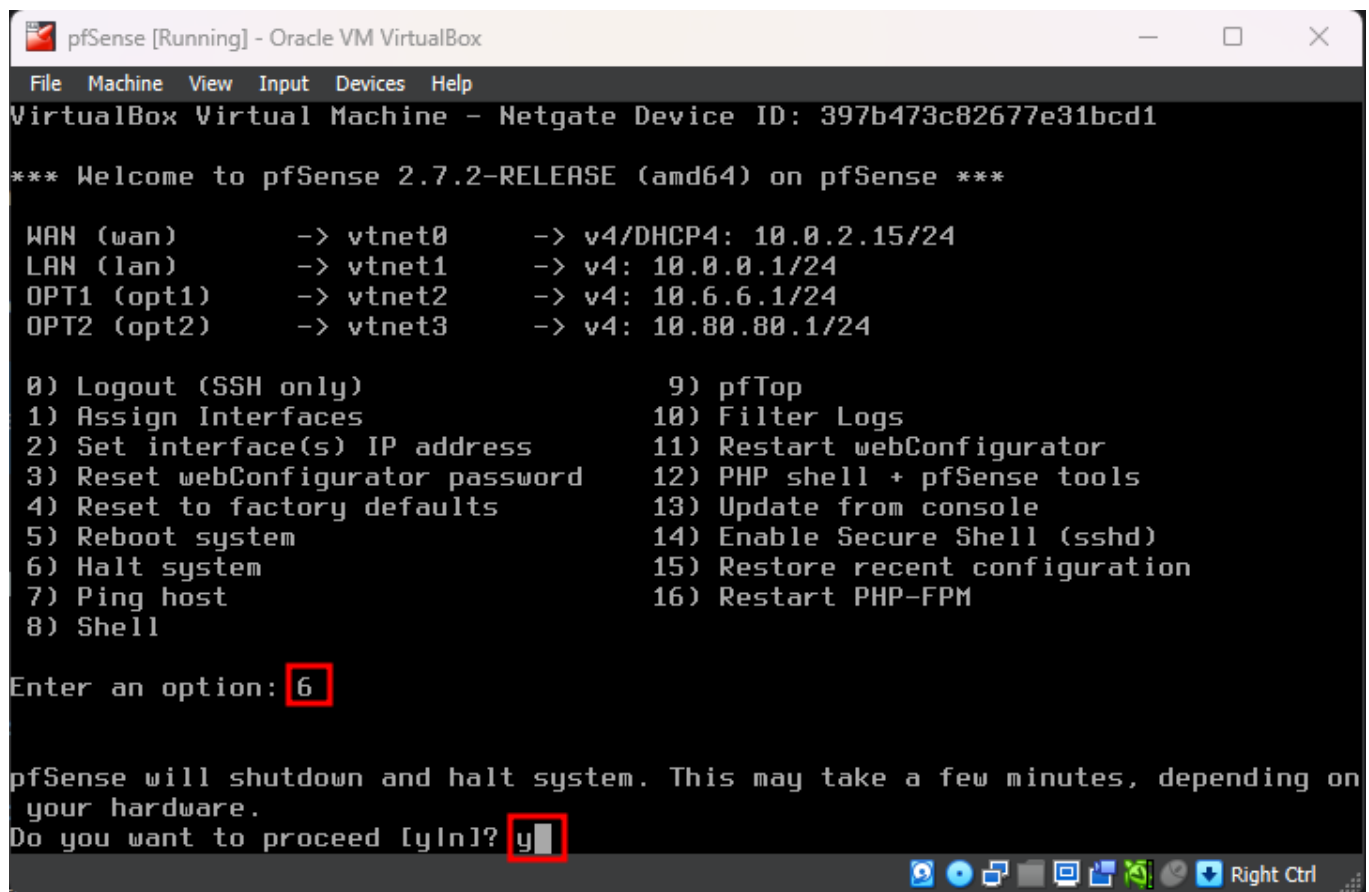
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet1      -> v4: 10.0.0.1/24
OPT1 (opt1)    -> vtnet2      -> v4: 10.6.6.1/24
OPT2 (opt2)    -> vtnet3      -> v4: 10.80.80.1/24

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

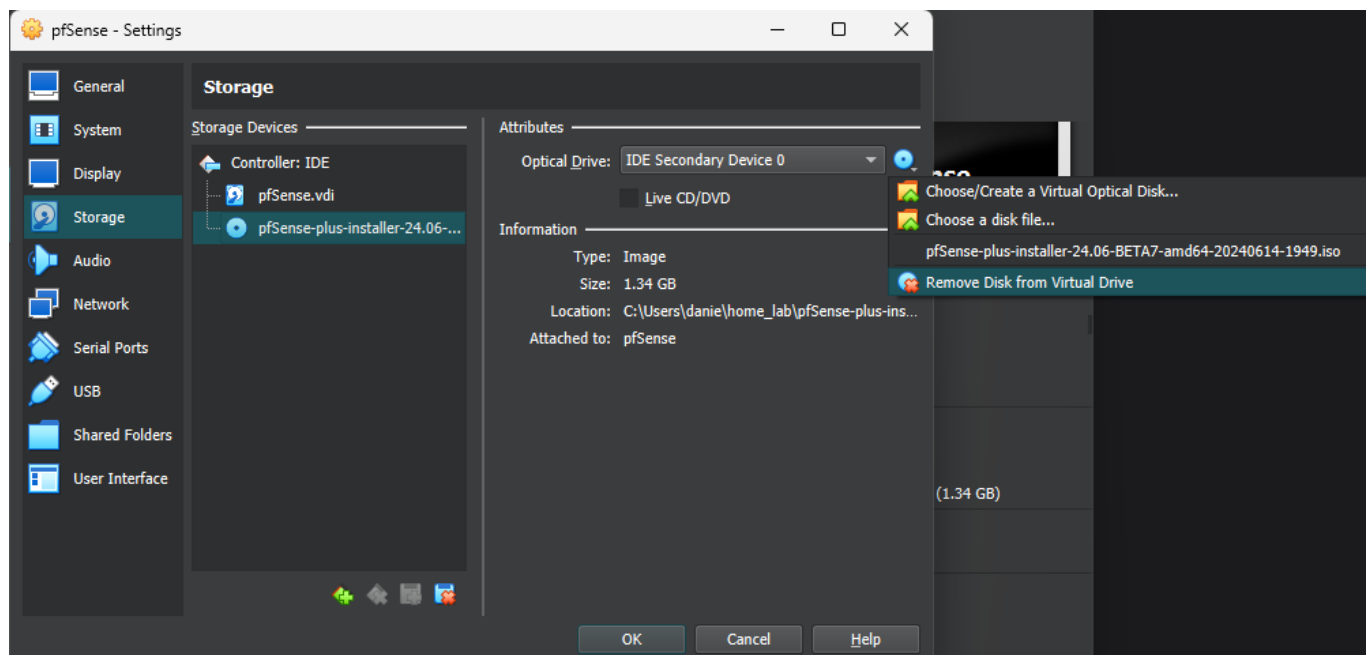
Enter an option:
```

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**

General Information

On this screen the general pfSense parameters will be set.

Hostname

pfSense

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

security.lab

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS

☐

Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

I choose my timezone

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname	<input type="text" value="2.pfsense.pool.ntp.org"/>
Enter the hostname (FQDN) of the time server.	
Timezone	<input type="text" value="Europe/Rome"/>

>> Next

I then scroll to the bottom and uncheck RFC1918

RFC1918 Networks

Block RFC1918 Private Networks	<input type="checkbox"/> Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.	

Block bogon networks

Block bogon networks	<input checked="" type="checkbox"/> Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.	

>> Next

Confirm the LAN interface settings

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	<input type="text" value="10.0.0.1"/>
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	<input type="text" value="24"/>

>> Next

Choose a new password for the admin account

Wizard / pfSense Setup / Set Admin WebGUI Password ?

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

[» Next](#)

And then I reload pfSense to save the changes

Wizard / pfSense Setup / Reload configuration ?

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

[» Reload](#)

General Configuration

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

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

Status / Dashboard + ?

- Assignments
- WAN
- LAN
- OPT1**
- OPT2

System Information	
Name	pfSense.security.lab
User	admin@10.0.0.11 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 397b473c82677e31bcd1

Netgate Services And Support

Contract type **Community Support**
Community Support Only

[NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES](#)

Interfaces / OPT1 (vtnet2)

General Configuration

Enable ☒ Enable interface

Description TARGET_RANGE
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

I go to Services -> DNS Resolver

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ **Services ▾** VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. Please change it immediately.

Interfaces / TARGET_RANGE (vtnet2)

The changes have been applied successfully.

General Configuration

Enable ☒ Enable interface

Description TARGET_RANGE
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server
- DNS Forwarder
- DNS Resolver**
- Dynamic DNS
- IGMP Proxy
- NTP
- PPPoE Server
- Router Advertisement
- SNMP
- UPnP & NAT-PMP
- Wake-on-LAN

And I enable these settings

DHCP Registration ☒ Register DHCP leases in the DNS Resolver
If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in [System > General Setup](#) should also be set to the proper value.

Static DHCP ☒ Register DHCP static mappings in the DNS Resolver
If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

OpenVPN Clients ☐ Register connected OpenVPN clients in the DNS Resolver
If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in [System: General Setup](#) should also be set to the proper value.

Display Custom Options [Display Custom Options](#)

[Save](#)

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 SettingsAdvanced SettingsAccess 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

SystemInterfacesFirewallServicesVPNStatusDiagnosticsHelp

Advanced

Certificates

General Setup

High Availability

Package Manager

Register

Routing

Setup Wizard

Update

User Manager

Logout (admin)

WARNING: The password for the root user is set to the default value. [Change the password in the User Manager.](#)

Services / General Settings

The changes have been applied successfully.

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 SettingsAccess Lists

System / Advanced / Admin Access

Admin AccessFirewall & NATNetworkingMiscellaneousSystem TunablesNotifications

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.

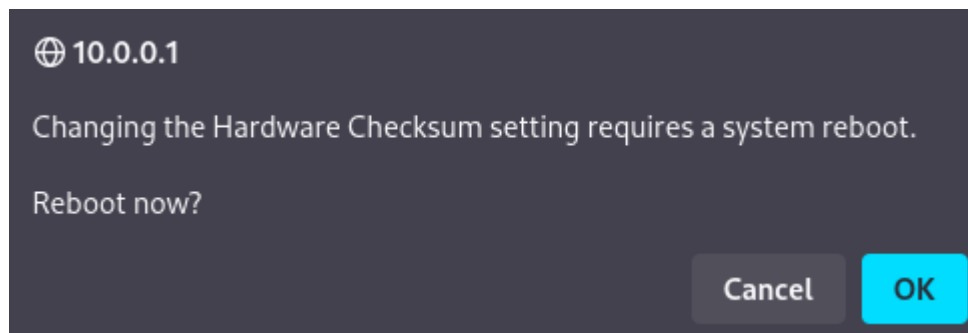
TCP port



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


Network Interfaces	
Hardware Checksum Offloading	<input checked="" type="checkbox"/> Disable hardware checksum offload Checking this option will disable hardware checksum offloading. Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
Hardware TCP Segmentation Offloading	<input checked="" type="checkbox"/> Disable hardware TCP segmentation offload Checking this option will disable hardware TCP segmentation offloading (TSO, TSO4, TSO6). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
Hardware Large Receive Offloading	<input checked="" type="checkbox"/> Disable hardware large receive offload Checking this option will disable hardware large receive offloading (LRO). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
hn ALTQ support	<input checked="" type="checkbox"/> Enable the ALTQ support for hn NICs. Checking this option will enable the ALTQ support for hn NICs. The ALTQ support disables the multiqueue API and may reduce the system capability to handle traffic. This will take effect after a machine reboot.
ARP Handling	<input type="checkbox"/> Suppress ARP messages This option will suppress ARP log messages when multiple interfaces reside on the same broadcast domain.
Reset All States	<input type="checkbox"/> Reset all states if WAN IP Address changes This option resets all states when a WAN IP Address changes instead of only states associated with the previous IP Address.

 Save



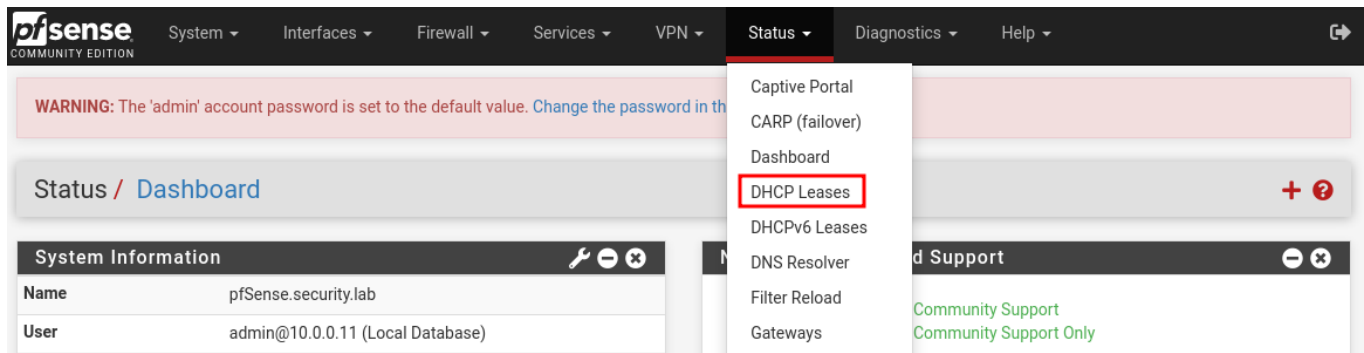
 System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 

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

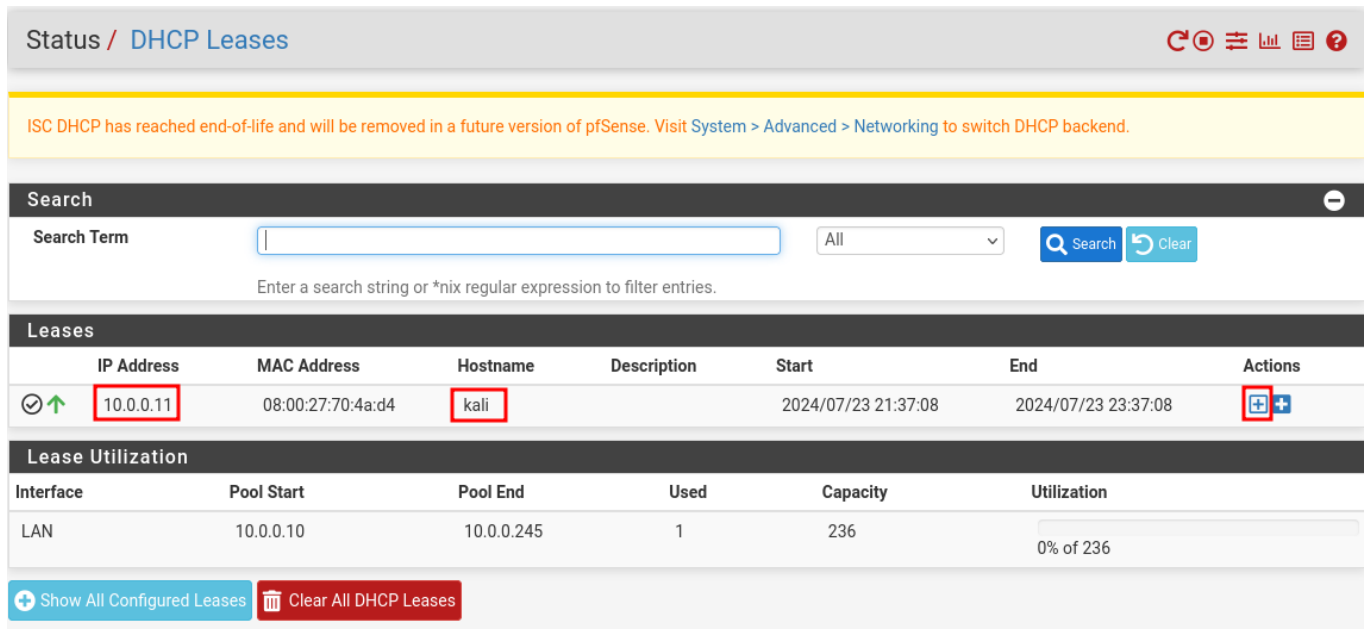
Diagnostics / [Reboot](#) 

Rebooting
Page will automatically reload in 86 seconds

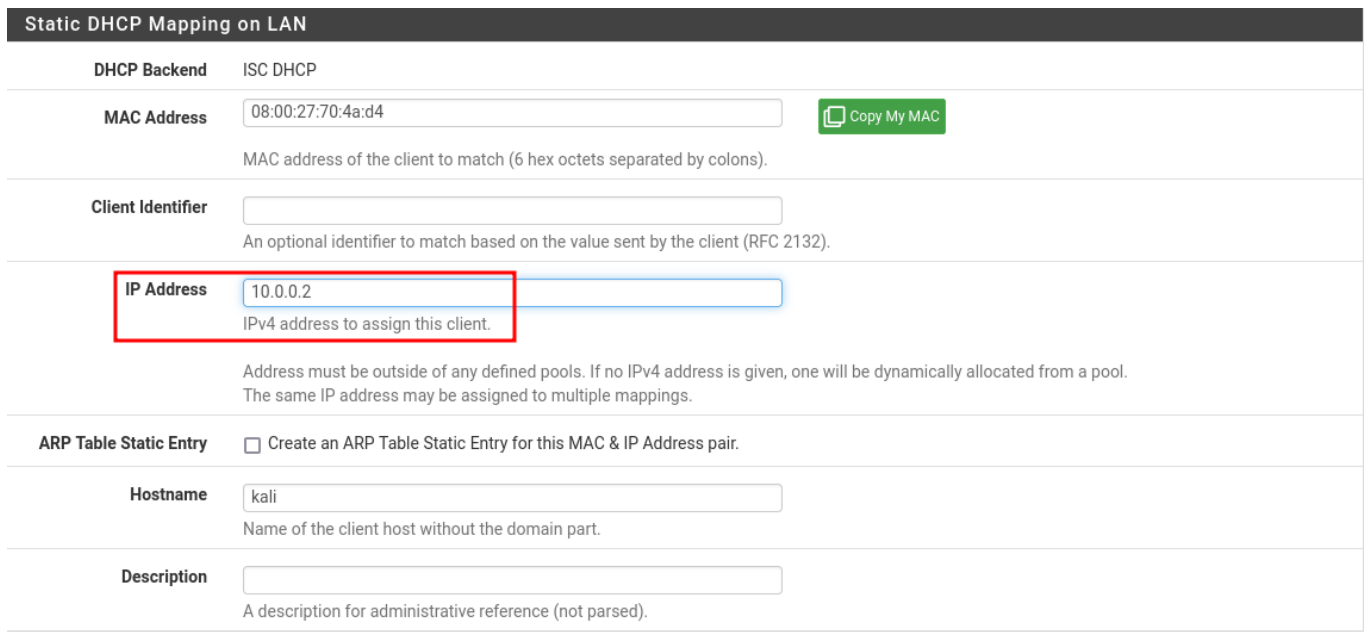
After logging in again i go to **Status -> DHCP Leases**



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 group 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)-[~] / DHCP Server / LAN
$ 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 group 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

WARNING: The 'admin' account password is set to [redacted]. Please change the password in the User Manager.

Status / Dashboard

System Information

Netgate Services And Support

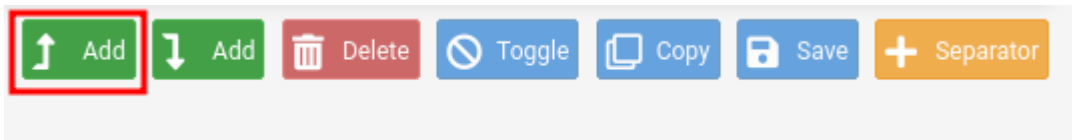
Firewall / Rules / WAN

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	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️

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**

Edit Firewall Rule

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

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

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

Address Family IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source
Source ☐ Invert match LAN subnets Source Address /

Destination
Destination ☐ Invert match WAN subnets Destination Address /

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 Block access to services on WAN Interface
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 the final LAN rules and their order

Firewall / Rules / LAN

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
✓ 1/113 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
✗ 0/0 B	IPv4+6 *	LAN subnets	*	WAN subnets	*	*	none		Block access to services on WAN Interface	⚓ ✎ 📄 🚫 🗑️
✓ 68/343 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ 📄 🚫 🗑️ ✖️
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ 📄 🚫 🗑️ ✖️

↑ Add ↓ Add 🗑️ Delete 🚫 Toggle 📄 Copy 💾 Save + Separator

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

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to ...
 ... the password in the User Manager.

Firewall / Rules / LAN

Aliases
 NAT
 Rules
 Schedules
 Traffic Shaper
 Virtual IPs

The changes have been applied successfully. The ...
 ... loading in the background.

Firewall / Aliases / IP

IP Ports URLs All

Firewall Aliases IP

Name	Type	Values	Description	Actions
------	------	--------	-------------	---------

+ Add 📄 Import

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

Firewall / Aliases / Edit

Properties

Name RFC1918
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description Private IPv4 Address Space
A description may be entered here for administrative reference (not parsed).

Type Network(s)

Network(s)

Hint Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN		Description	
10.0.0.0	/ 8	Description	Delete
172.16.0.0	/ 12	Description	Delete
192.168.0.0	/ 16	Description	Delete
169.254.0.0	/ 16	Description	Delete
127.0.0.0	/ 8	Description	Delete

Save + Add Network

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

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the password in the User Manager.

Firewall / Aliases / IP

The changes have been applied successfully. The

loading in the background.

Firewall / Rules / TARGET_RANGE

Floating WAN LAN TARGET_RANGE OPT2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.										

↑ Add ↓ Add Delete Toggle Copy Save + Separator

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**

Edit Firewall Rule	
Action	<div>Pass</div> <div>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.</div>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
Interface	<div>TARGET_RANGE</div> <div>Choose the interface from which packets must come to match this rule.</div>
Address Family	<div>IPv4+IPv6</div> <div>Select the Internet Protocol version this rule applies to.</div>
Protocol	<div>Any</div> <div>Choose which IP protocol this rule should match.</div>
Source	
Source	<div><input type="checkbox"/> Invert match</div> <div>TARGET_RANGE subnets</div> <div>Source Address /</div>
Destination	
Destination	<div><input type="checkbox"/> Invert match</div> <div>TARGET_RANGE address</div> <div>Destination Address /</div>
Extra Options	
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <div>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).</div>
Description	<div>Allow traffic to all devices on TARGET_RANGE Network</div> <div>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.</div>

- 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**

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

RFC1918

/

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 from TR Network to any non private IPv4 Address

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.

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

Edit Firewall Rule

Action Block

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+IPv6

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 Any Destination Address /

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 Block access from TR subnet to everything

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.

- 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)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4+6 *	TARGET_RANGE subnets	*	TARGET_RANGE address	*	*	none	Allow traffic to all devices on TARGET_RANGE Network	   
<input type="checkbox"/>	✓	0/0 B	IPv4 *	TARGET_RANGE subnets	*	!RFC1918	*	*	none	Allow traffic from TR Network to any non private IPv4 Address	   
<input type="checkbox"/>	✓	0/0 B	IPv4 *	TARGET_RANGE subnets	*	10.0.0.2	*	*	none	Allow traffic to Kali Linux VM	   
<input type="checkbox"/>	✗	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

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

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 Services

Contr...

NETGATE

If you purchase a pfSense firewall appliance from Netgate and elected to use the Community Support resources, you have committed to the NETGATE Firewall Community Support resources. This includes:

- Upgrade Your pfSense Firewall
- Netgate Global Technical Assistance Center (TAC)
- Netgate Professional Support

You also may wish to consider a Support subscription, which is committed to deliver more than complete support resources. This includes:

- Upgrade Your pfSense Firewall
- Netgate Global Technical Assistance Center (TAC)
- Netgate Professional Support

If you decide to purchase a Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support. You can purchase a Support subscription from your firewall in order to validate support. You can purchase a Support subscription from your firewall in order to validate support.

- 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