Setting up pfSense: Protecting a Virtual Internal Network
Requirements:
Oracle VirtualBox
pfSense version 2.7.2
A file archiver (in this instance, **WINRAR**)
An ISO of an operating system (in this instance, **Manjaro Xfce**)
A router (in this instance, **172.20.10.1/28**)

Part 1: Obtaining Requirements

1. To download Oracle VirtualBox, go to https://www.virtualbox.org/wiki/Downloads and select on the platform (operating system) that you use.

a. Once downloaded, proceed through the setup wizard to complete the installation of Oracle VirtualBox.

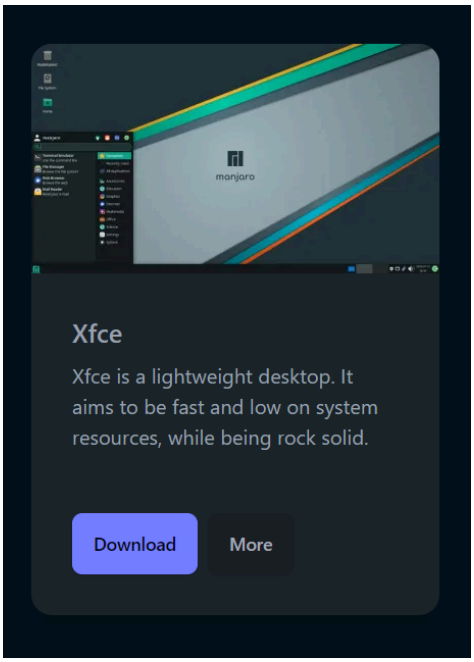
2. To download pfSense version 2.7.2, go to https://atxfiles.netgate.com/mirror/downloads/ and click on pfSense-CE-2.7.2-RELEASE-amd64.iso.gz. You can install this version of pfSense on the pfSense website, however, you will need to log into an account. The mirror link avoids this extra step.

Index of /mirror/downloads/

../		
old/	06-Jun-2024 19:18	-
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz	31-Jan-2022 20:31	437073513
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz.sha256	31-Jan-2022 20:32	114
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz	29-Jun-2023 20:11	495733706
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz.sha256	29-Jun-2023 20:11	114
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz	17-Nov-2023 00:47	574639430
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz.sha256	17-Nov-2023 00:47	114
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz	08-Dec-2023 18:27	574277009
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.sha256	08-Dec-2023 18:27	114
pfSense-CE-memstick-2.6.0-RELEASE-amd64.img.gz	31-Jan-2022 20:40	438161574
pfSense-CE-memstick-2.6.0-RELEASE-amd64.img.gz...>	31-Jan-2022 20:40	123
pfSense-CE-memstick-2.7.0-RELEASE-amd64.img.gz	29-Jun-2023 20:11	499043832
pfSense-CE-memstick-2.7.0-RELEASE-amd64.img.gz...>	29-Jun-2023 20:11	123
pfSense-CE-memstick-2.7.1-RELEASE-amd64.img.gz	17-Nov-2023 00:47	575598913
pfSense-CE-memstick-2.7.1-RELEASE-amd64.img.gz...>	17-Nov-2023 00:47	123
pfSense-CE-memstick-2.7.2-RELEASE-amd64.img.gz	08-Dec-2023 18:27	576633377
pfSense-CE-memstick-2.7.2-RELEASE-amd64.img.gz...>	08-Dec-2023 18:27	123
pfSense-CE-memstick-ADI-2.6.0-RELEASE-amd64.img.gz	31-Jan-2022 20:48	440116418
pfSense-CE-memstick-ADI-2.6.0-RELEASE-amd64.img..>	31-Jan-2022 20:49	127
pfSense-CE-memstick-ADI-2.7.0-RELEASE-amd64.img.gz	29-Jun-2023 20:11	496977920
pfSense-CE-memstick-ADI-2.7.0-RELEASE-amd64.img..>	29-Jun-2023 20:11	127
pfSense-CE-memstick-ADI-2.7.1-RELEASE-amd64.img.gz	17-Nov-2023 00:47	576330254
pfSense-CE-memstick-ADI-2.7.1-RELEASE-amd64.img..>	17-Nov-2023 00:47	127

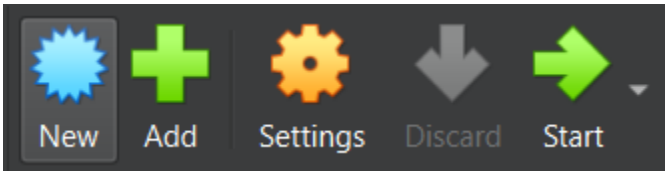
a. Once downloaded, unzip the archive folder through any file archiver software (in this instance, **WinRAR**).

3. For this step, an ISO for an operating system needs to be obtained. It does not matter which operating system since the purpose of it is to be protected by pfSense and access the Graphical User Interface (GUI) to set up firewall rules. For this instance, **Manjaro Xfce**, a distribution of Linux, will be used. If you wish to download Manjaro, go to https://manjaro.org/products/download/x86 and click the download button under Xfce.

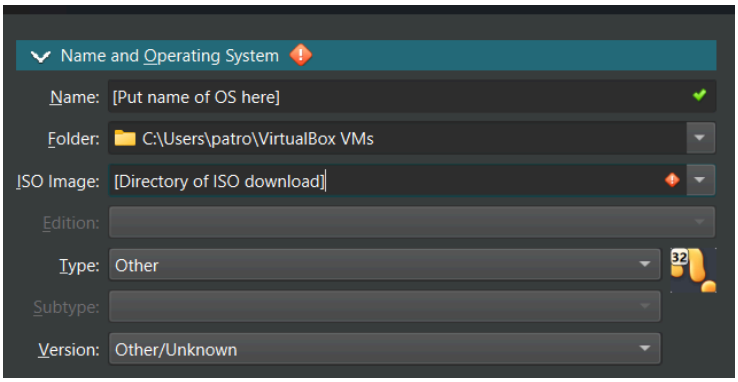


Part 2: Setting up pfSense

1. Open Oracle VirtualBox, and select the **New** icon. Alternatively, you can locate the Machine tab in the top left corner of the window, and click New (or Ctrl + n).



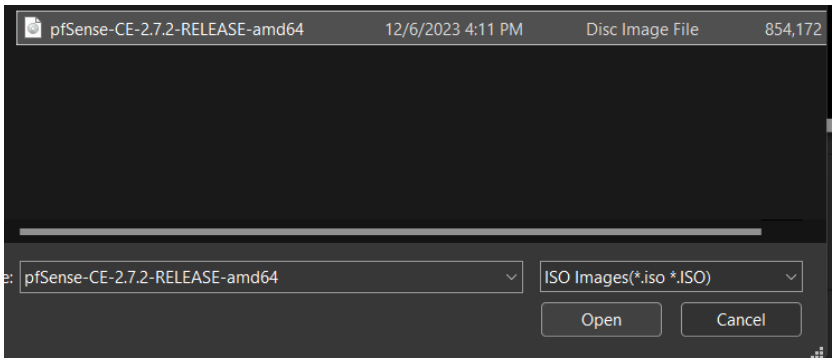
a. You will be presented with a screen with a Name, Folder, ISO Image, Type, and Version.

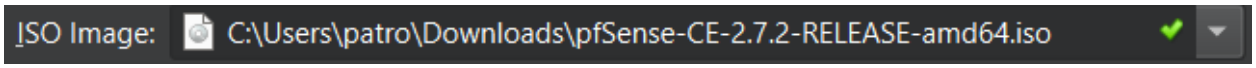


b. In the **Name** field, type in **pfSense**.

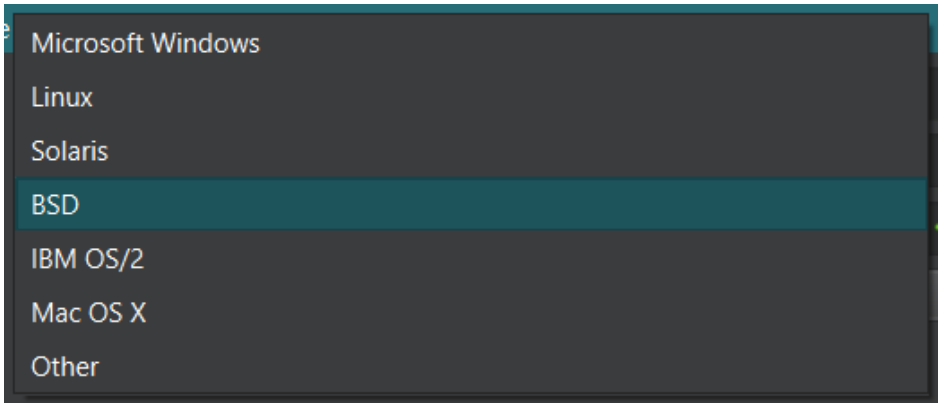
c. The folder field is where the virtual machines are stored on your computer. You do not have to edit this, although if you wish to store the virtual machines elsewhere on your computer, select the down arrow, select **Other**, proceed to the directory where you would store them, and select **Select Folder**.

d. The ISO Image field is where you locate the ISO file of pfSense-CE-2.7.2-RELEASE-amd64.iso. Select the down arrow by the **ISO Image** field, select **Other**, proceed to the directory where it is located, and select **Open**. The ISO file should now be presented in the field.





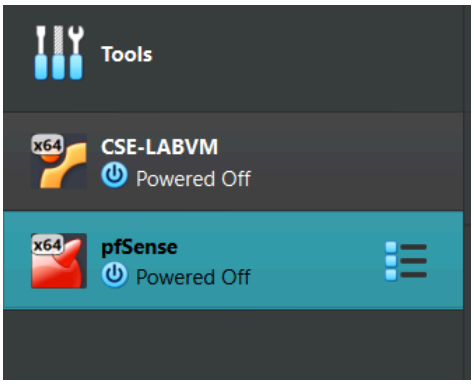
e. Under the type field, select **BSD**.



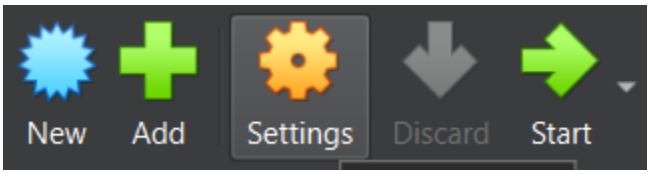
f. Under the version field, select **FreeBSD (64 bit)**.

g. Other tabs, such as Unattended Install, Hardware, and Hard Disk do not have to be edited. The software we are installing on the virtual machine does need a lot of space or power, so the default settings will work.

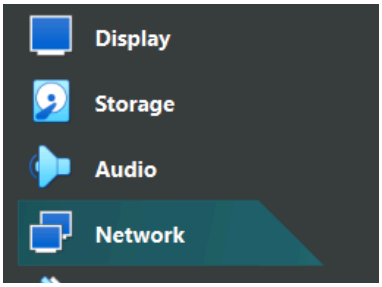
h. Select finish, and now pfSense should appear in the options for Virtual Machines.



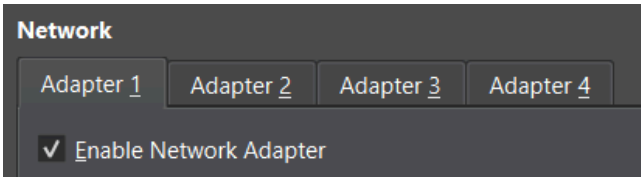
2. While pfSense is highlighted on the left (if it is not, select the general area in between the text and tab icon), select the **Settings** icon.



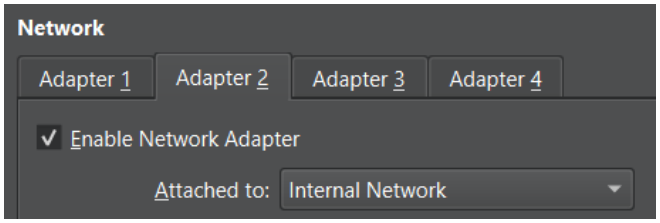
a. A screen will display various options for the virtual machine. Select the **Network** section.



b. Under the **Adapter 1** tab, ensure that the check box has a mark for **Enable Network Adapter.**

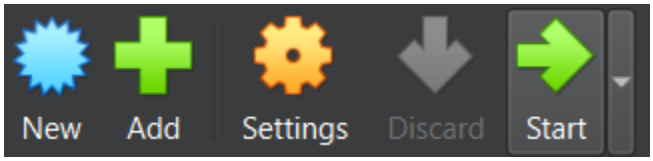


c. Under the **Adapter 2** tab, check the box for **Enable Network Adapter**, and under the Attached to section, select **Internal Network**.

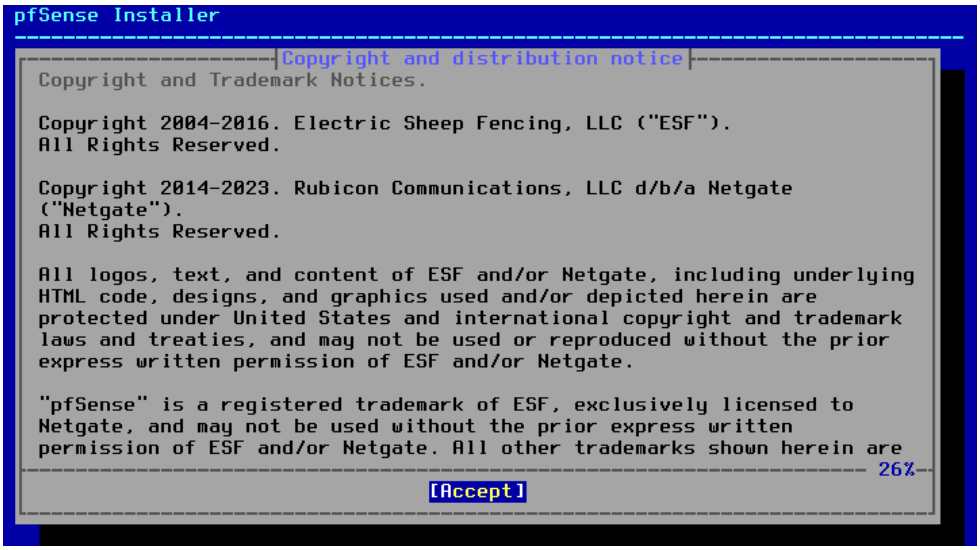


d. Repeat step c under the **Adapter 3 tab**.
e. Select **OK**.

3. To boot up the virtual machine, select the **Start** icon.



a. The virtual machine will boot up pfSense, and it will proceed to load on its own for a couple of moments. Once the screen below appears, we will start the setup by pressing **Enter** to **Accept**.



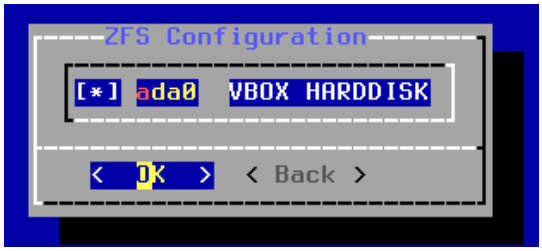
b. On the next screen, press **Enter** to **Install**.

c. On the next screen, press **Enter** to select **Auto (2FS)**.

d. On the next screen, press **Enter** to **Install**.

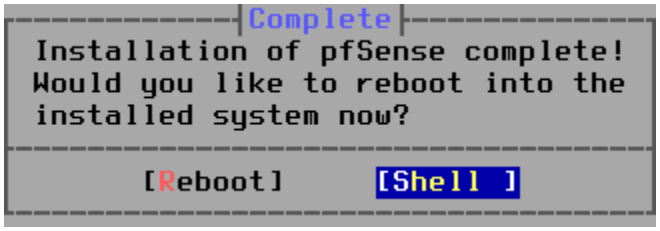
e. On the next screen, press **Enter** to select **Stripe**.

f. On the next screen, you will need to place a character to represent the 2FS Configuration. Press **Space** and *, an asterisk, should fill in the blank field. Press **Enter** to select **OK**.

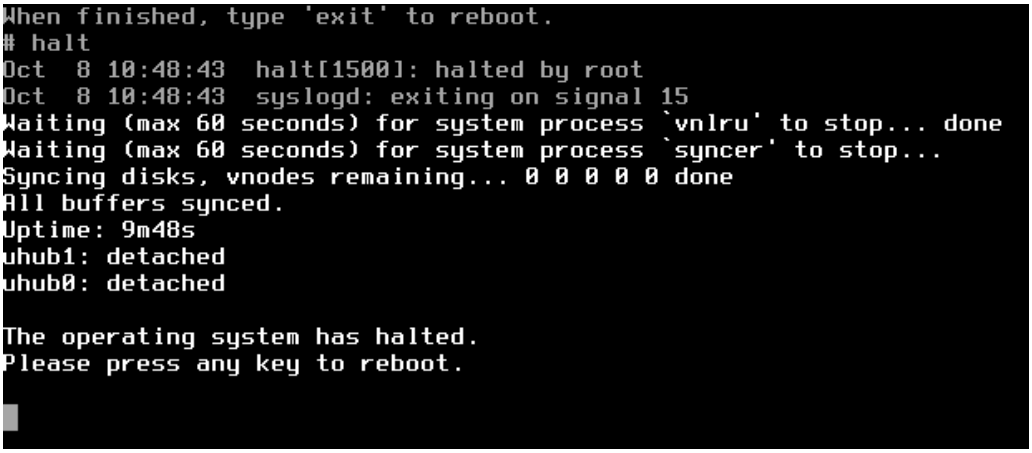


g. On the next screen, use your arrow key to highlight **YES** and press **Enter**.

h. The setup will extract distribution files, and once that is completed, it will ask you if you want to **Reboot** or access the **Shell**. Use the arrow key to select **Shell**, and press **Enter**.



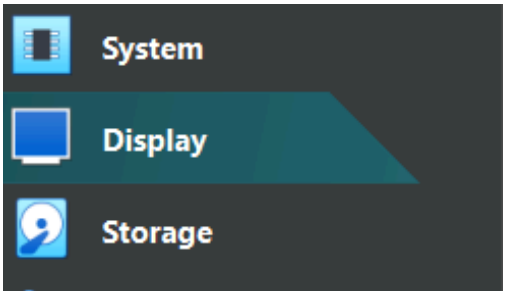
i. Once you enter the shell, type **halt**. It will halt the operating system, and it will ask you to reboot.

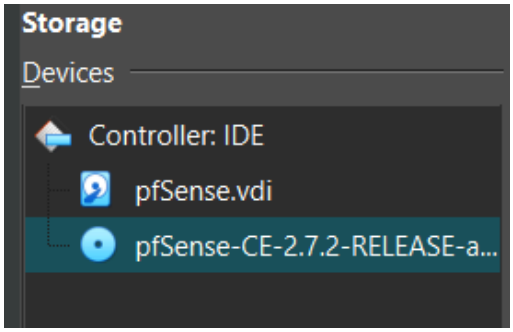


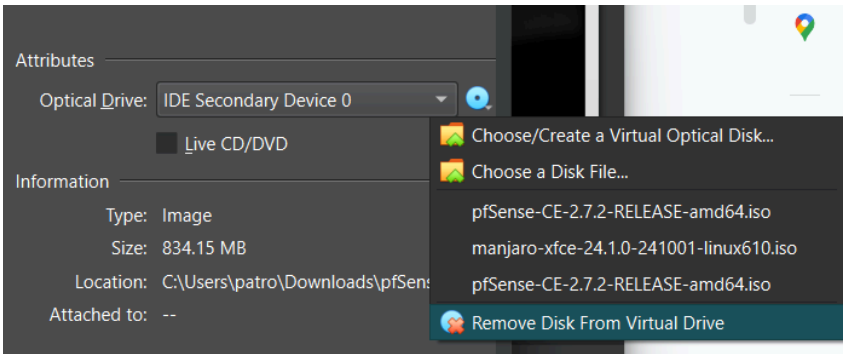
j. Once this screen appears, you can select the X icon on the top right corner of the window, select **Power off the machine**, and select **OK**.

k. Now, we will be deleting the optical drive to bypass the setup process of pfSense. While pfSense is highlighted on the left, select the **Settings** icon.

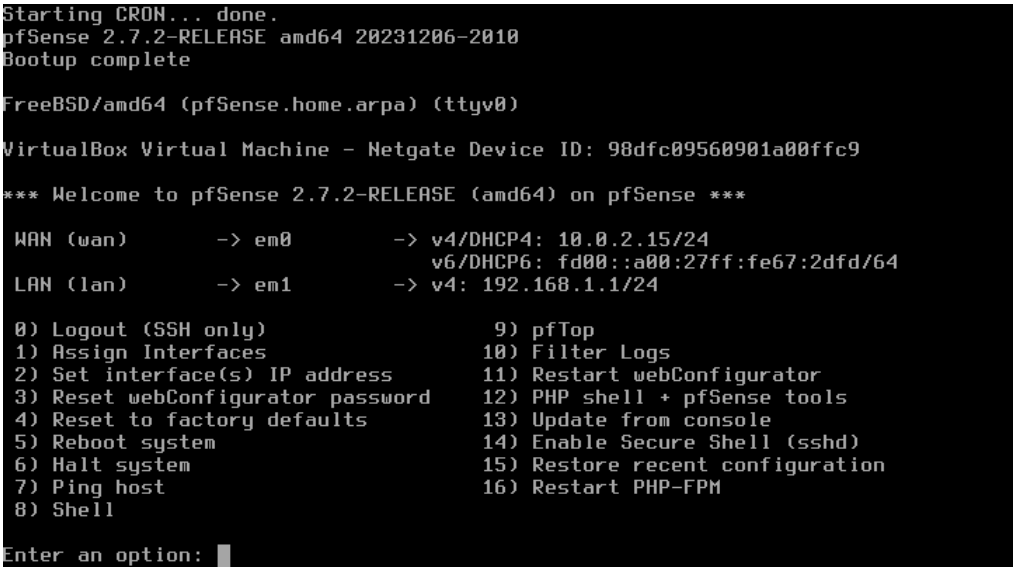
l. Select the **Storage** tab on the left side of the window, and select the ISO file at the bottom of the **Storage Devices** section. Under the **Attributes** section, select the disk icon, and select **Remove Disk from Virtual Drive**. Select **OK**.



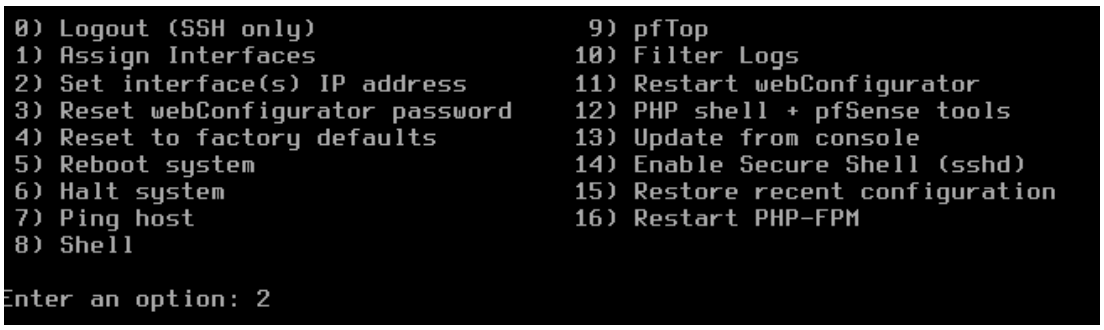




m. Boot up pfSense with the **Start** icon. Let it boot until presented with this screen:



2. We are going to edit the LAN interface. Press **2** to select Set interface IP address, then press **Enter**.



a. Press **2** to select the LAN interface, then press **Enter**.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - DMZ (em2)

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

b. pfSense will ask you if you would like to configure the IPv4 address LAN interface with DHCP. Since we are setting up a static IP address and do not have a DHCP server, press **n** for No, then press **Enter**.

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

c. It will then ask you to enter an IPv4 address for the LAN interface. It is important that you do not use an IP address that is already in use on the network you are currently on. For this instance, we will set up the LAN interface with the IPv4 address with **192.168.168.1**. Press **Enter**.

```
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.168.1
```

d. For the subnet bit count, type **24**, then press **Enter**.

```
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
```

e. It will ask for an upstream gateway address for the WAN. Since we are just using a LAN, we can press **Enter** for none.

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

f. pfSense will ask you if you would like to configure the IPv6 address LAN interface with DHCP. Press **n**, then press **Enter**.

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

g. Press **Enter** for no IPv6 LAN interface.

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

h. Press **y** to enable the DHCP server on the LAN.

```
Do you want to enable the DHCP server on LAN? (y/n) y
```

i. For the start address range, type **192.168.168.100**, then press **Enter**.

```
Enter the start address of the IPv4 client address range: 192.168.168.100
```

j. For the end address, type **192.168.168.199**, then press **Enter**.

```
Enter the end address of the IPv4 client address range: 192.168.168.199
```

k. For reverting to HTTP, press **n** and then **Enter**.

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

You should now be able to access the webConfigurator by using **https://192.168.168.1/**.

```
The IPv4 LAN address has been set to 192.168.168.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.168.1/
```

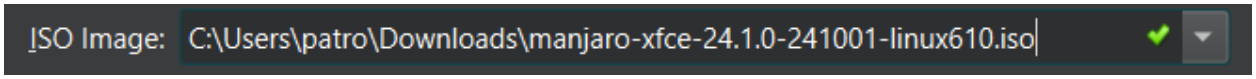
Part 3: Initial Setup of Manjaro

1. Click the **New** icon in VirtualBox.

a. In the name field, type in **Manjaro**.

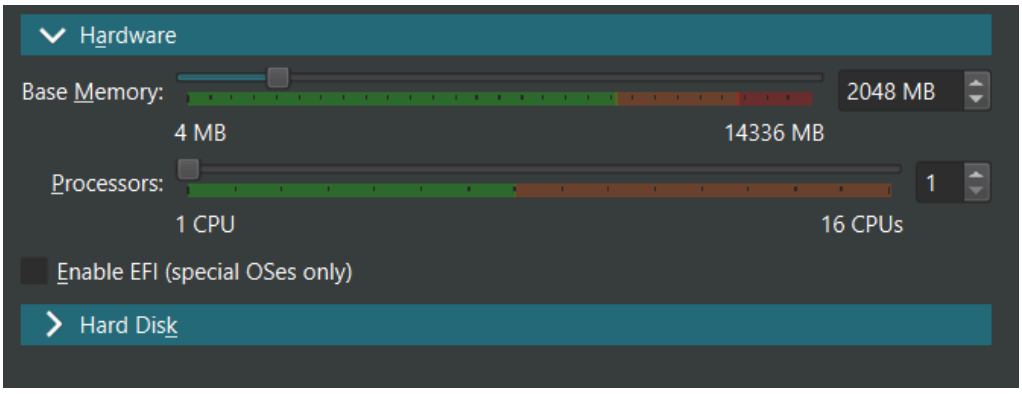
b. You do not have to edit the folder field, although you can store the virtual machine elsewhere on the computer.

c. Locate the ISO file of manjaro-xfce-24.1.0-241001-linux610 in the ISO file section. Under the type section, select **Linux**.



d. In the version field, select **ArchLinux**.

e. Expand the **Hardware** section, and edit the base memory to **2048 MB** by typing it in the field on the right. Select **Finish**.

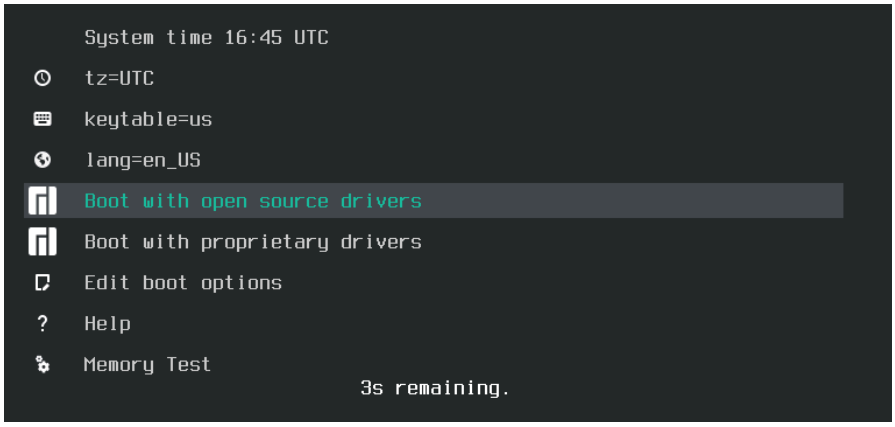


f. While Manjaro is highlighted on the left, select the **Settings** icon.

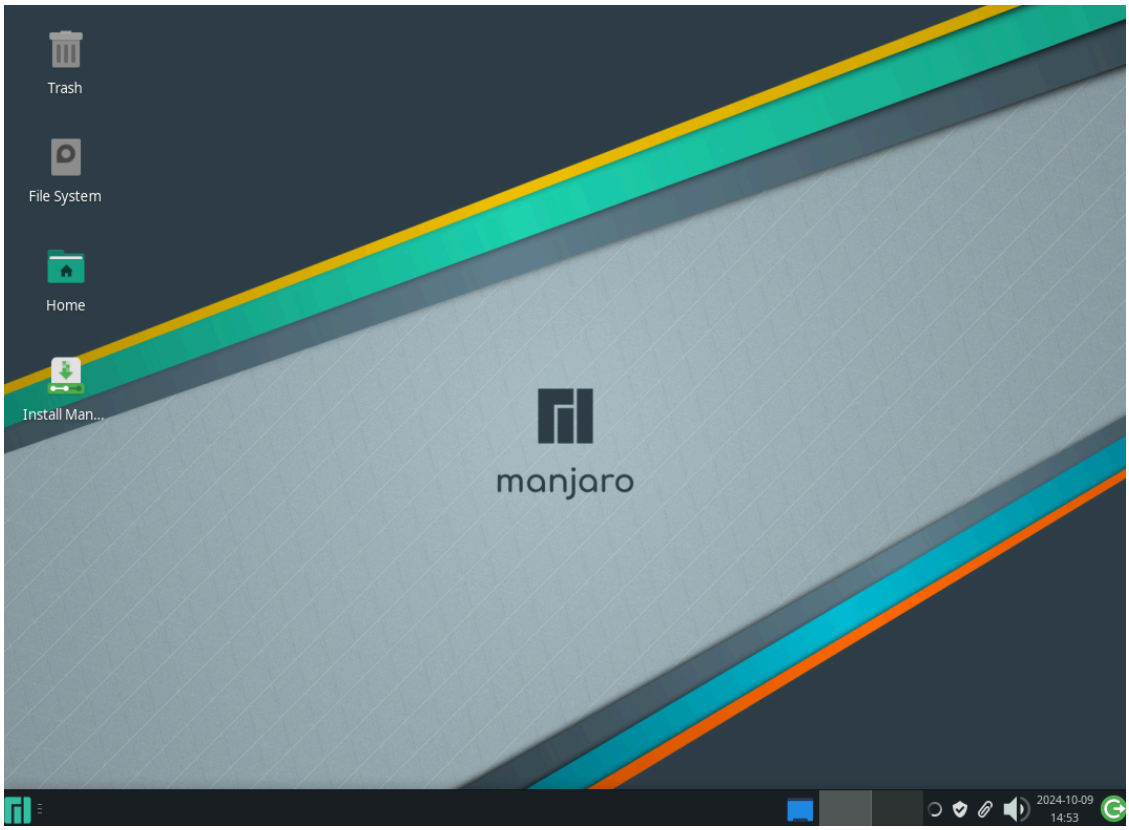
g. Select the **Network** tab, and under Adapter 1 section, change the field of Attached to: to **Internal network**. Select **OK**.

2. Boot up Manjaro by selecting the **Start** icon.

a. On the boot screen, press **Enter** to select **Boot with open source drivers**.

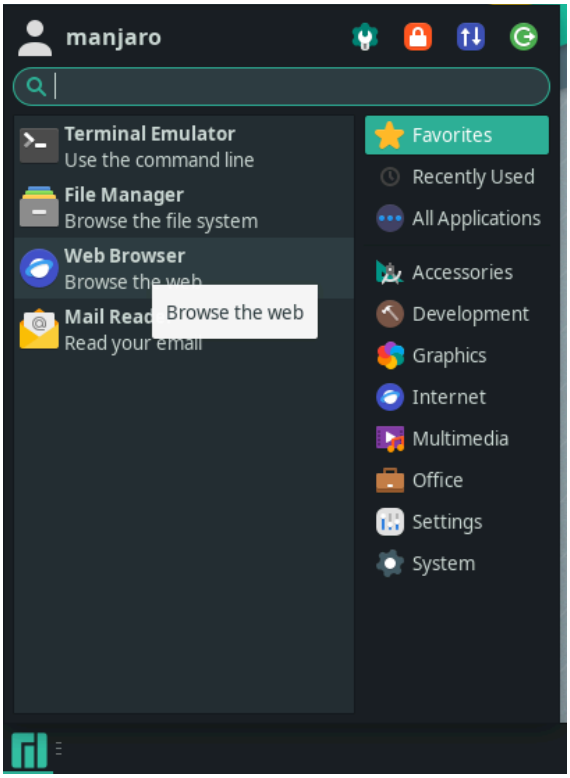


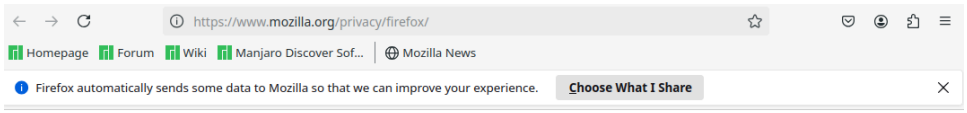
The operating system will boot on its own, and then the GUI will be presented shortly after.



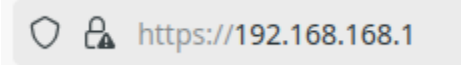
Part 4: Initial Setup of pfSense GUI

1. In the bottom left corner is the **Applications** icon. Select the icon, then select **Web Browser** from the list. Notice how the privacy notice tab does not load in.

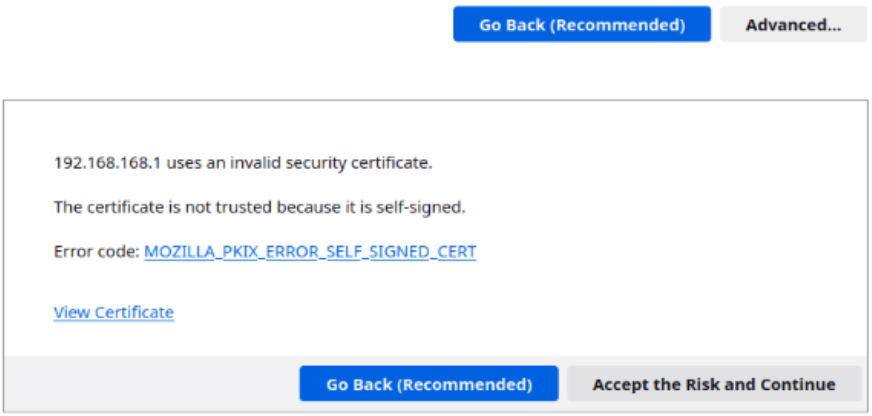




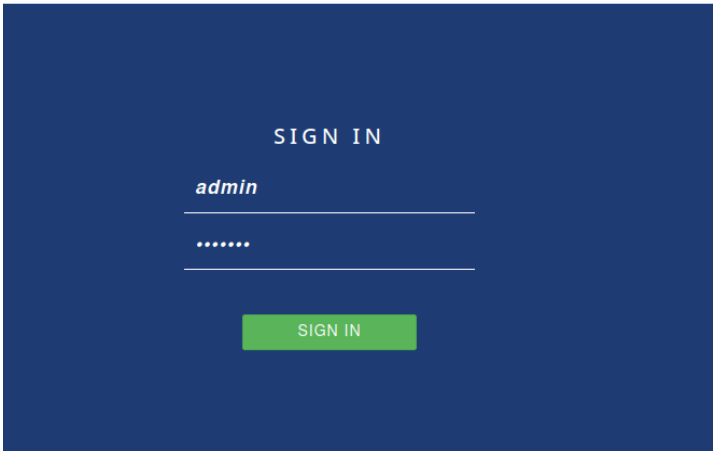
a. In the search bar, type in the address for the router that was configured in pfSense, **192.168.168.1**, then press **Enter**.



b. Firefox is going to detect this as a potentially unsafe website since it is not an official certificate. Select **Advanced** then **Accept the Risk and Continue** to proceed.

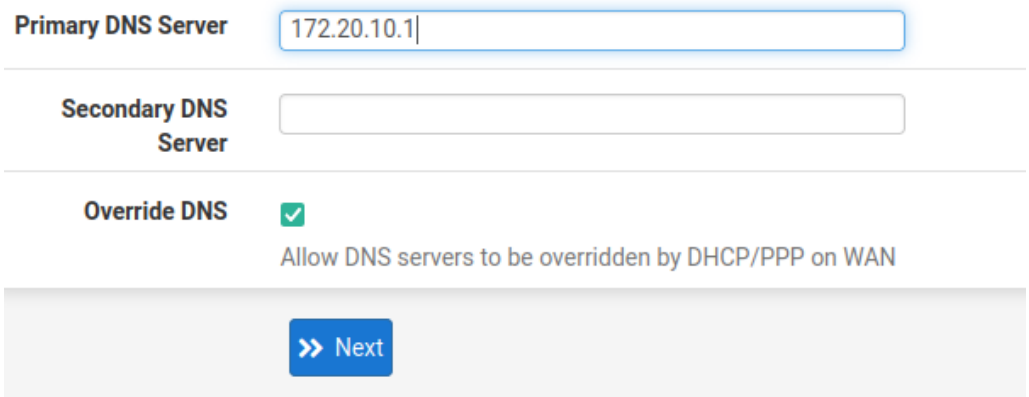


c. On the sign in page, type in **admin** for the username and **pfsense** for the password. Select **SIGN IN**.

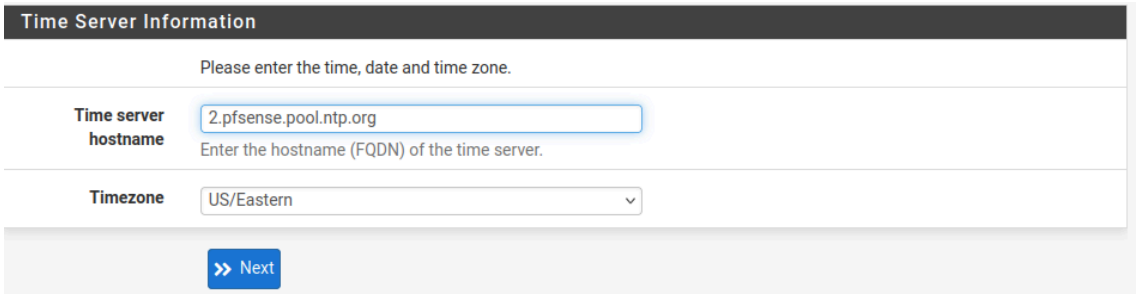


2. You will now be presented with the setup wizard. For the first two pages, Select **Next**.

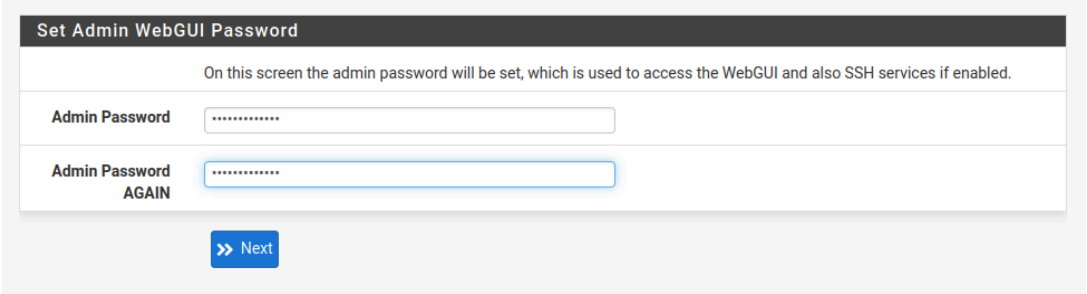
a. On the step 2 page, set the **Primary DNS server** field to your home router. The home router is going to be emulated as a DNS server. In this instance, **172.20.10.1** with a subnet mask of **255.255.255.240 (/28)** will be used. Select **Next** at the bottom of the page.



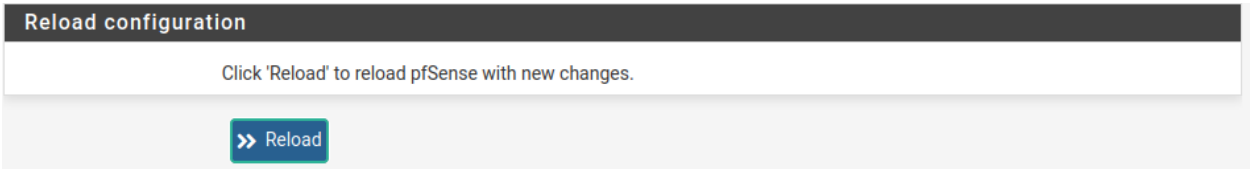
b. On the step 3 page, set the **Timezone** field to **your preferred time zone (in this instance, US/Eastern)**, then select **Next**.



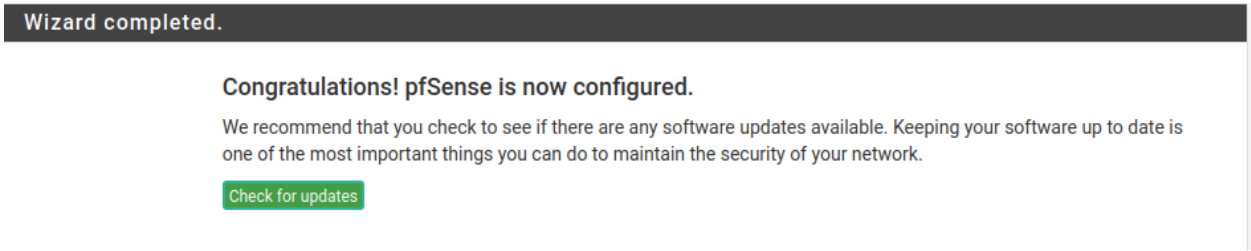
c. For steps 4 and 5, select **Next**. On the step 6 page, it is recommended to configure a more secure password. This is because the default username and passwords to routers can be looked up on the internet, making the current interface vulnerable. For this instance, the administrator password will be changed to **InAJiffy5060!**. Type your password of choice in both the **Admin Password** and **Admin Password AGAIN** fields. Select **Next**.



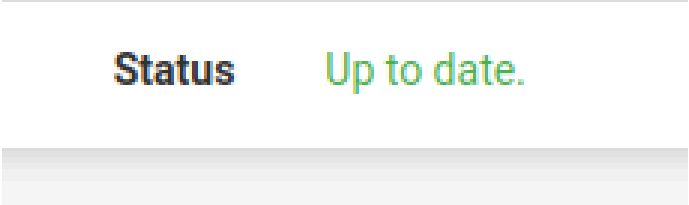
d. pfSense will ask you to reload the page to confirm the changes. Select **Reload**.



e. After the page reloads, It will bring you to the last step. Select **Check for Updates** to ensure our interface is up-to-date.



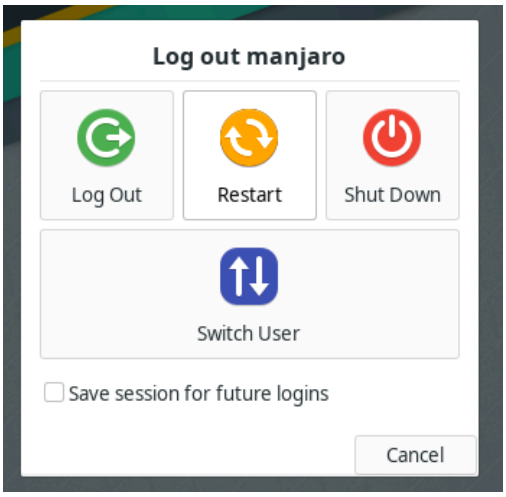
f. Wait for the status to load, and it should display **Up to date**.



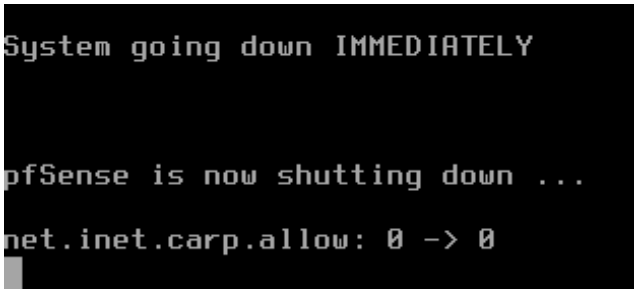
Part 5: Rebooting Virtual Machines

Typically, you do not want to restart a router as it is vital for devices to communicate inside a network. However, in this scenario, restarting the devices in order for the DNS server to be updated is necessary.

1. Once a status is shown (last step in the previous part), reboot Manjaro by selecting the green **Sign out** icon in the bottom right corner of your taskbar, and select the **Restart** icon.

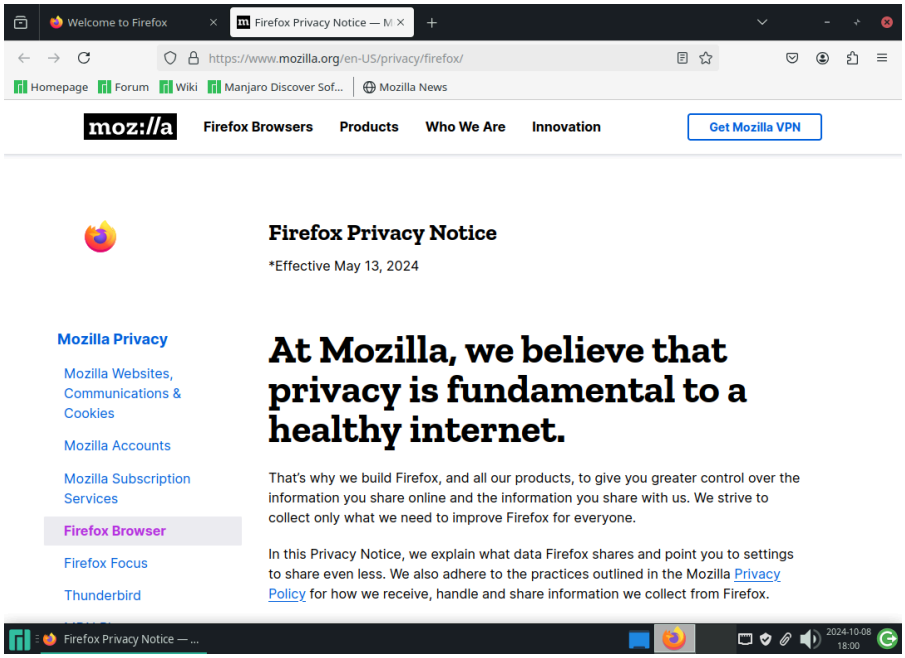


2. In the pfSense virtual machine, press **6** then **Enter** to halt the system. Once it asks if you are sure, press **y**, then press **Enter**. It will shut down on its own.



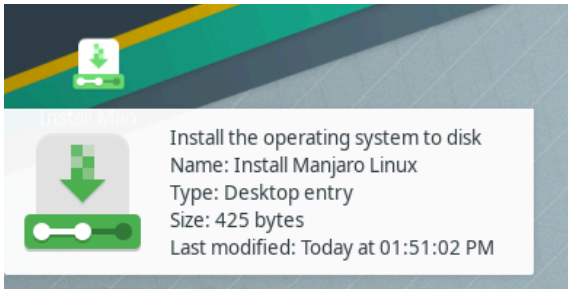
a. Reboot pfSense to ensure it is working.

3. Reboot Manjaro, press **Enter** on the boot screen, and wait for the GUI to load. Once it is done loading, select the **Applications** icon, and select **Web Browser** under the list. If the DNS is properly working, the privacy notice tab should now load in.

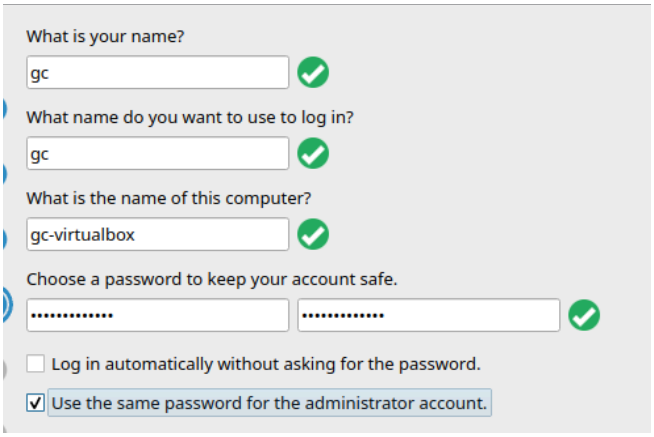


Part 5: Installing Manjaro Linux

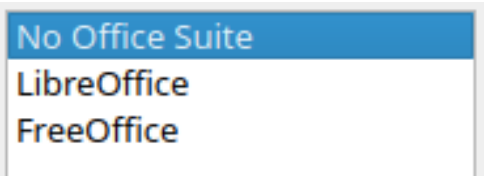
1. On the desktop, open **Install Manjaro Linux**.



a. Select **Next** until you get to the Users section. Fill in the information in the fields as necessary, and select **Use the same password for the administrator account**. Select **Next**.



b. Under the **Office Suite** list, select **No Office Suite**. Select **Next**.



c. Select **Install,** then **Install Now** to install Manjaro Linux.

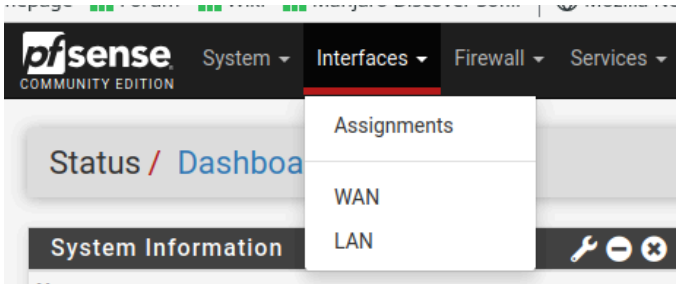
Part 6: Setting up Additional Settings in pfSense

While Manjaro Linux installs in the background, there is some time to configure firewall rules:

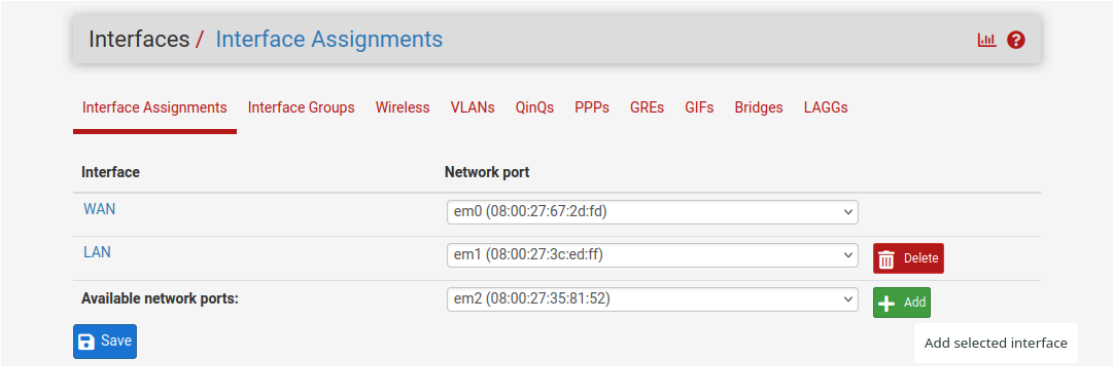
1. In the web browser, type in **192.168.168.1** into the search bar. The reboot restarted the token for the certificate, so you will have to select **Advanced** then **Accept the Risk and Continue** to proceed again.

a. Login into the pfSense interface with **admin** as the username and the new administrator password that was configured in the setup wizard. If additional windows popup on the dashboard, select **Accept** then **Close**.

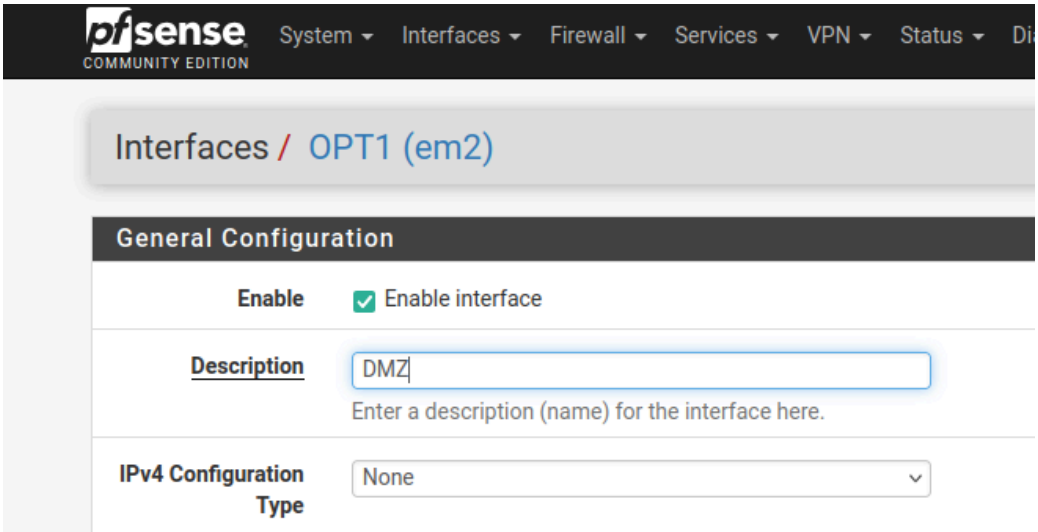
2. On the top of the interface, select **Interfaces**, then **Assignments**.



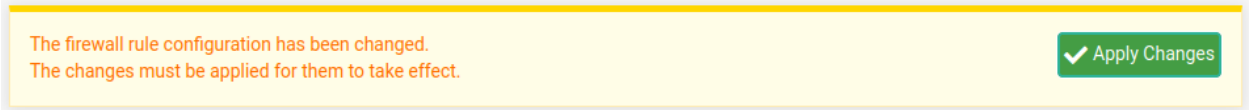
a. During the configuration of the pfSense virtual machine, three adapters were enabled. Two are currently enabled, the LAN and WAN, but the third has not been configured in the GUI. This third interface will be our demilitarized zone (DMZ). Select **Add** by **em2**.



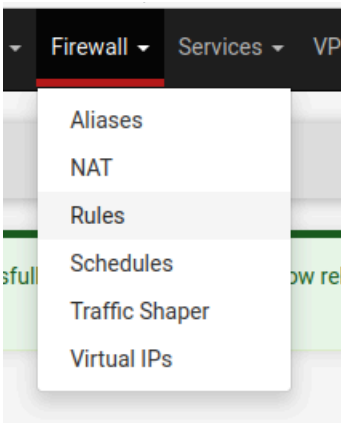
b. The interface will be created as **OPT1**. Select the blue text of **OPT1**, select **Enable Interface**, and change the name to **DMZ**. At the bottom of the page, select **Save**.



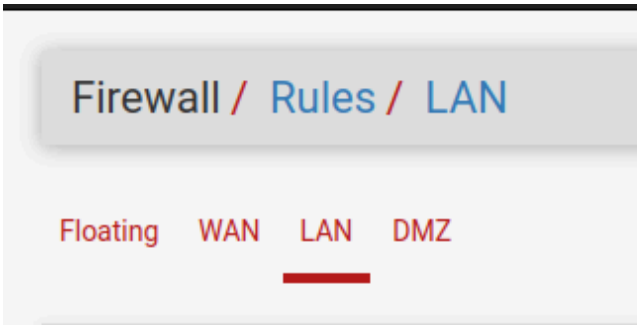
c. pfSense will load back into the interfaces page and a green box will pop up, indicating that the changes must be applied in order to be taken into effect. Select **Apply Changes**.

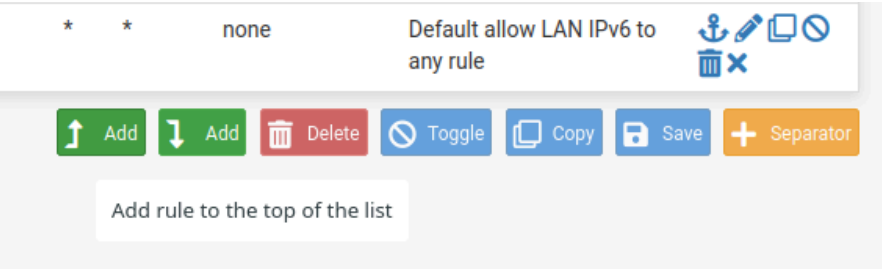


3. On the top of the interface, select **Firewall**, then select **Rules**.



a. The WAN interface firewall rules will be presented by default. Select the **LAN** tab, then select the **Add** button with the up arrow. The rule that is going to be created is going to be first priority when traffic hits the LAN.





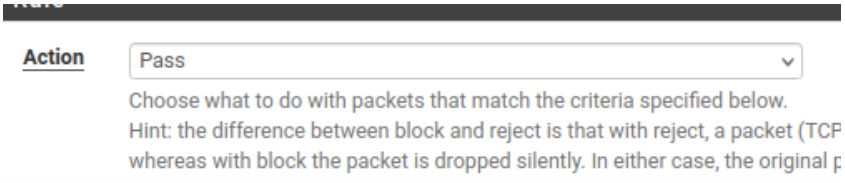
b. For this rule, we want the home network (172.168.1.0) to be blocked on the LAN interface. In the **Action** field, select **Block**.

c. Under the **Protocol** field, select **Any**. No traffic should be allowed to go to the home router.

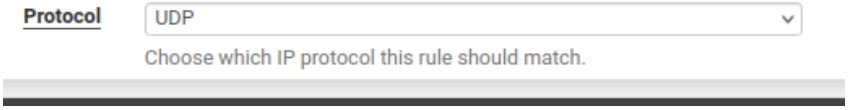
d. Under the **Destination** section, select **Network**, **172.20.10.0** for the destination address, and **/28** as the subnet. At the bottom of the page, select **Save**, then **Apply Changes**.

4. Add another rule selecting the **Add** button with an up arrow.

a. For this rule, DNS traffic is going to be allowed going to the DNS server, **172.20.10.1**. Under the **Action** field, select **Pass**.

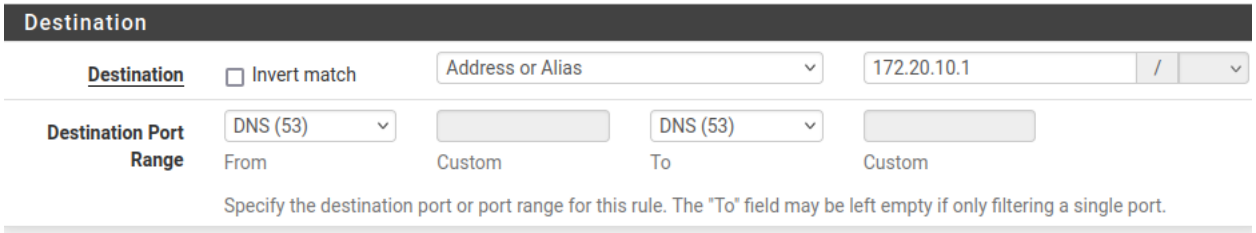


b. In the **Protocol** field, select **UDP**.

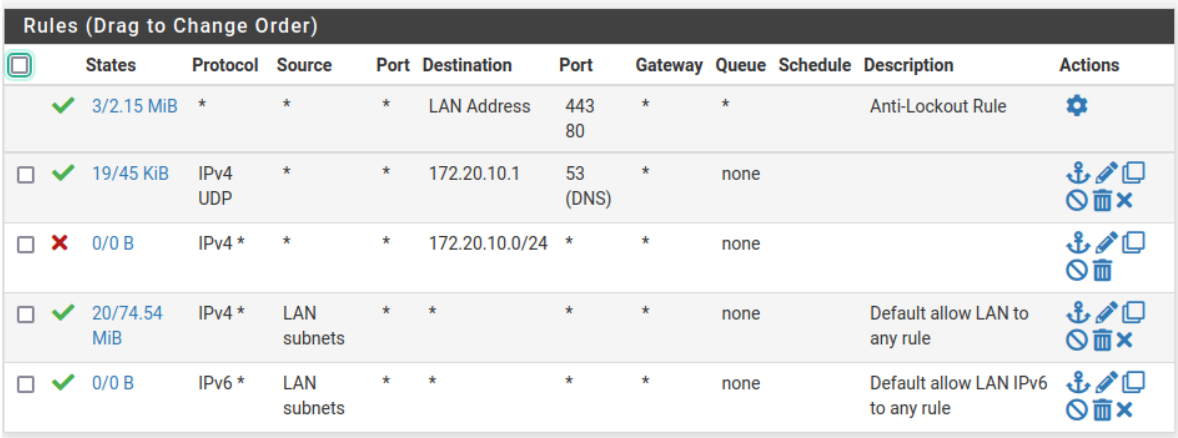


c. Under the **Destination** section, select **Address or Alias**, then type **172.20.10.1** in the destination address field.

d. For **Destination Port Range**, select **DNS (53)** for From and To (it should automatically fill in the same option for to).



e. At the bottom of the page, select **Save**, and then **Apply Changes**.
f. The firewall rules should be configured at the top of the ruleset. If you did not select the **Add** button with the up arrow, you can move the rules that need to be on top by selecting and dragging with your mouse.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	3/2.15 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓	19/45 KiB	IPv4 UDP	*	*	172.20.10.1	53 (DNS)	*	none			
✗	0/0 B	IPv4 *	*	*	172.20.10.0/24	*	*	none			
✓	20/74.54 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

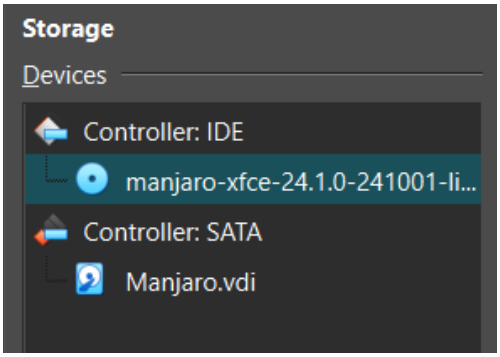
This is the correct order of the firewall rules.

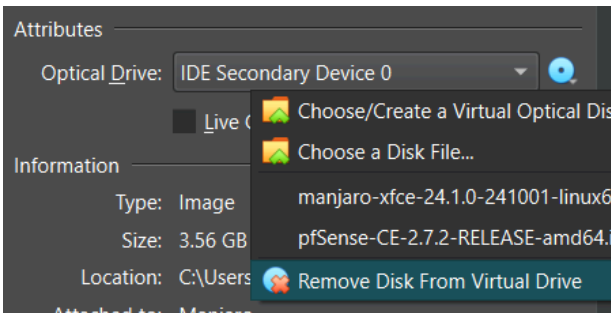
Part 7: Confirm Changes

Once the rules in the previous step have been configured, Manjaro should be done installing.

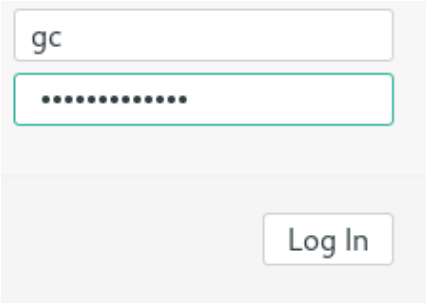
1. In the installation window, select **Finish**. Select the **green Sign out** icon in the bottom right corner of your taskbar, and select the **red Shutdown** icon.

a. While Manjaro is highlighted, select the **Settings** icon.
b. Select the **Storage** tab, and under the **Devices** section, and select manjaro-xfce-24.1.0-241001-linux610.
c. Select the disk icon on the far right, and select **Remove Disk From Virtual Drive**. This is to ensure the optical drive won't boot. Select **OK**.

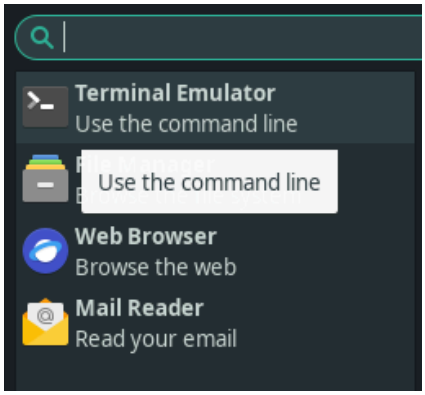




2. Select the **Start** button for Manjaro. Notice how it skips the initial boot process and presents you a login screen.
   a. Use the username and password created during the Manjaro installation process. Select **Log In**.

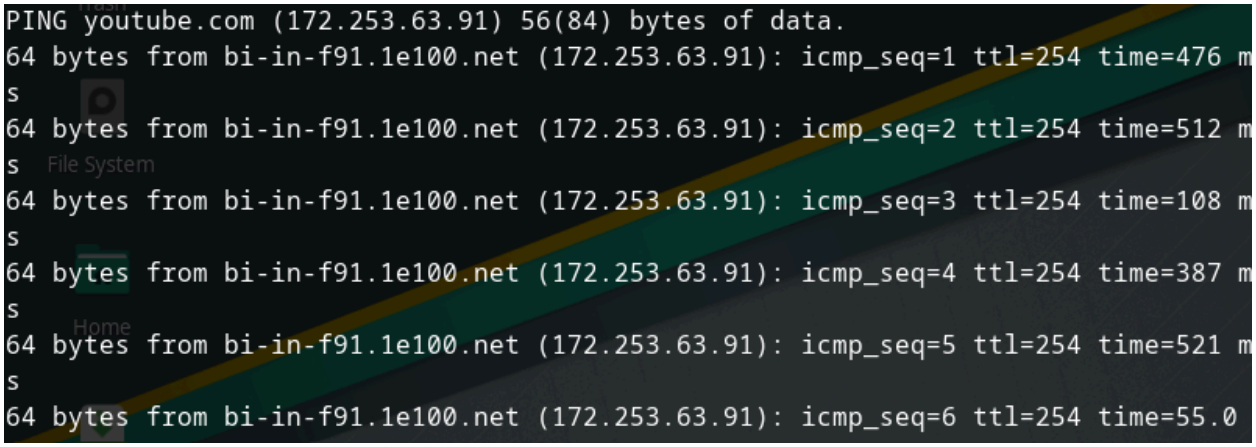


3. Once logged in, Select the **Applications** icon, then select **Terminal Emulator** icon.



   a. In the command line, type **cat /etc/resolv.conf**. It should display **172.20.10.1** as the DNS server.

   b. Ping a website. In this instance, **www.youtube.com** will be used. Type **ping www.youtube.com** in the command line. Responses will come back with 64 bytes of data. To stop the pings, press **Ctrl + C**.



c. In the web browser, type **172.20.10.1** in the web browser. Because of the block rule that we made in the LAN interface for the **172.20.10.0** network, the page will not load.