INDUSTRIAL TRAINING REPORT

Submitted in partial fulfilment for the
requirements for the award of

Bachelor Of Computer Applications (BCA) Hons Cybersecurity

Ansh Infotech (AIT)

Submitted by

Maxwell Appiah

Department of Computer

School of Engineering and Technology

CT UNIVERSITY, LUDHIANA

2023

INDUSTRIAL TRAINING REPORT

Submitted in partial fulfilment for the
requirements for the award of

Bachelor Of Computer Applications (BCA) Hons Cybersecurity

International Business Machines Corporation (IBM)

Submitted by

Maxwell Appiah

Department of Computer

School of Engineering and Technology

CT UBIVERSITY, LUDHIANA

July – August 2023

TABLE OF CONTENTS

Firewall Configuration using pfsense Technology

What is pfesense?

pfSense is a free and open-source firewall and router that also features unified threat management, load balancing, multi-WAN, and more.

What is the purpose of pfsense?

pfSense software is primarily used as a router and firewall software and is frequently set up as a DHCP server, DNS server, Wi-Fi access point, and VPN server, all on the same physical device

Aims & Objectives

In this project, I'm demonstrating how to secure your local network or home network traffic over the internet.

Aims

To allow only my G-Host Virtual machine to access my admin GUI of pfsense but can't ping the server.

Objectives

- Pfsense must only permit LAN to reach any destination.
- Pfsense restrict the access of connection from the internet to my network

Tools

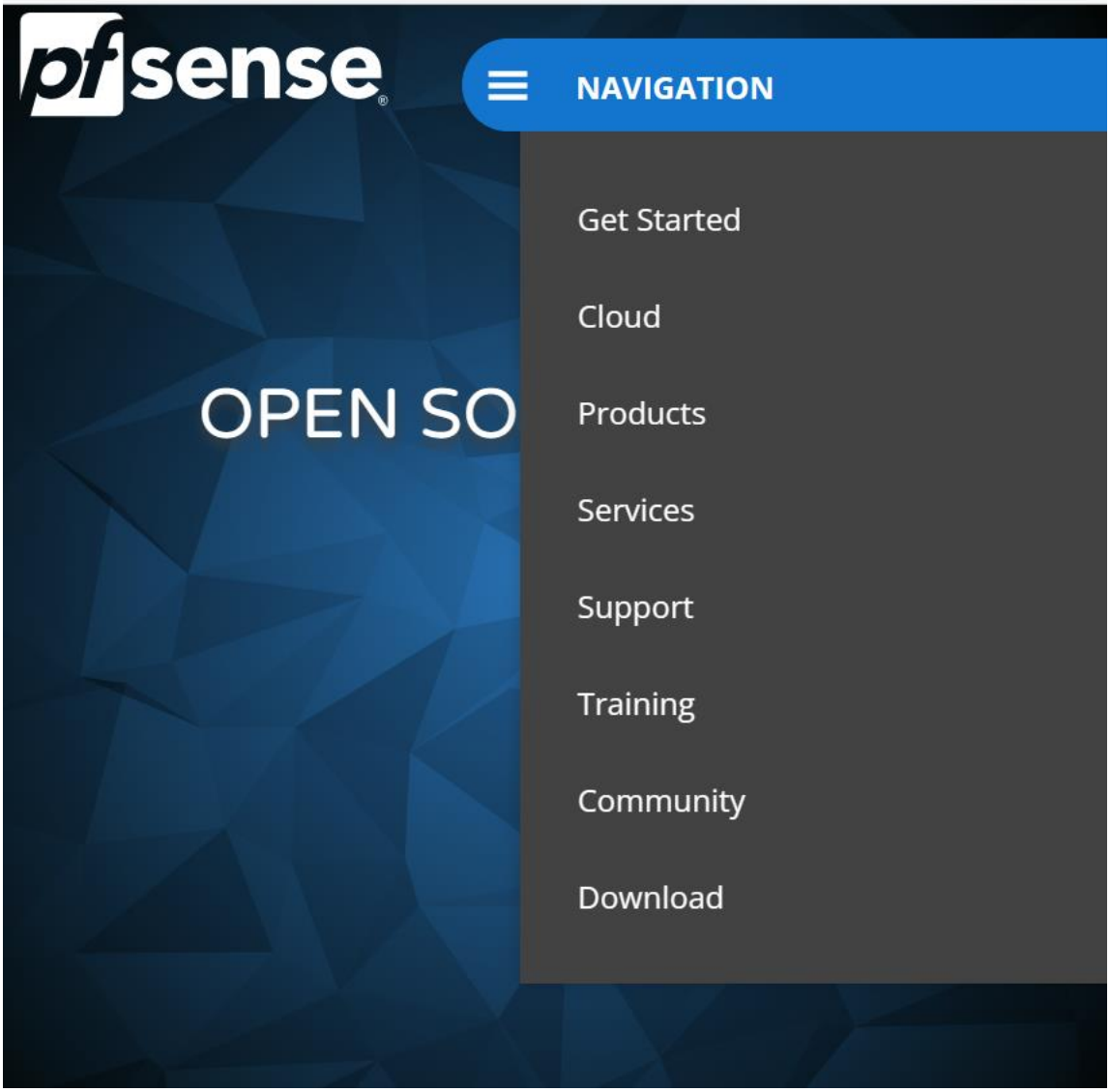
1. VMware workstation
2. pfsense
3. Win 10 OS
4. Ubuntu 64 11

Introduction

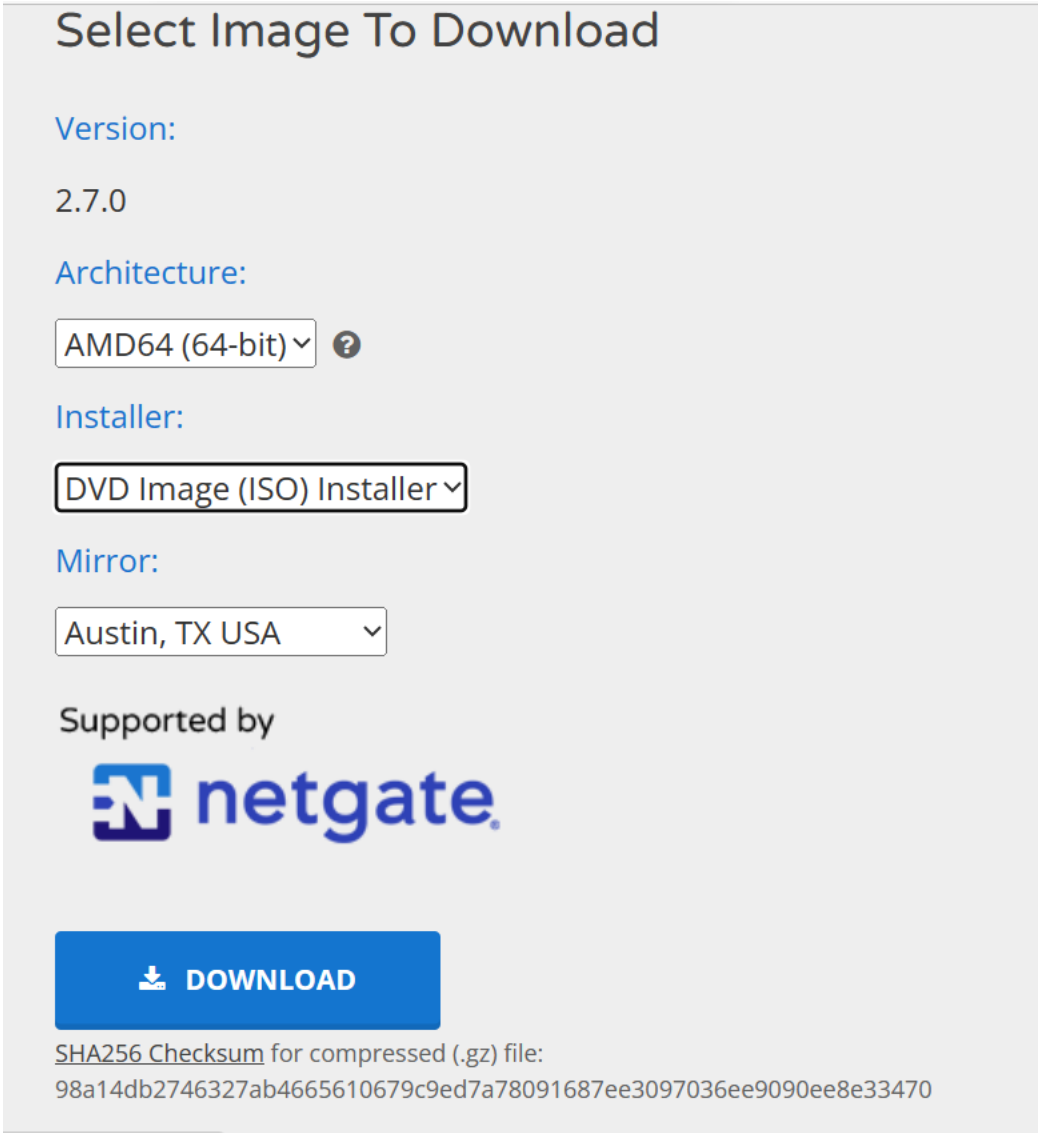
Firstly, we need to set up the environment needed to carry out our operation. To configure firewall rules using pfsense, we must first download our tools including VMware workstation, pfsense, Host os (kali os, win os, ubuntu os).

Let get started installing our tools.

Open your browser and download pfsense (src=" pfSense® - World's Most Trusted Open Source Firewall")



Click on download as shown below



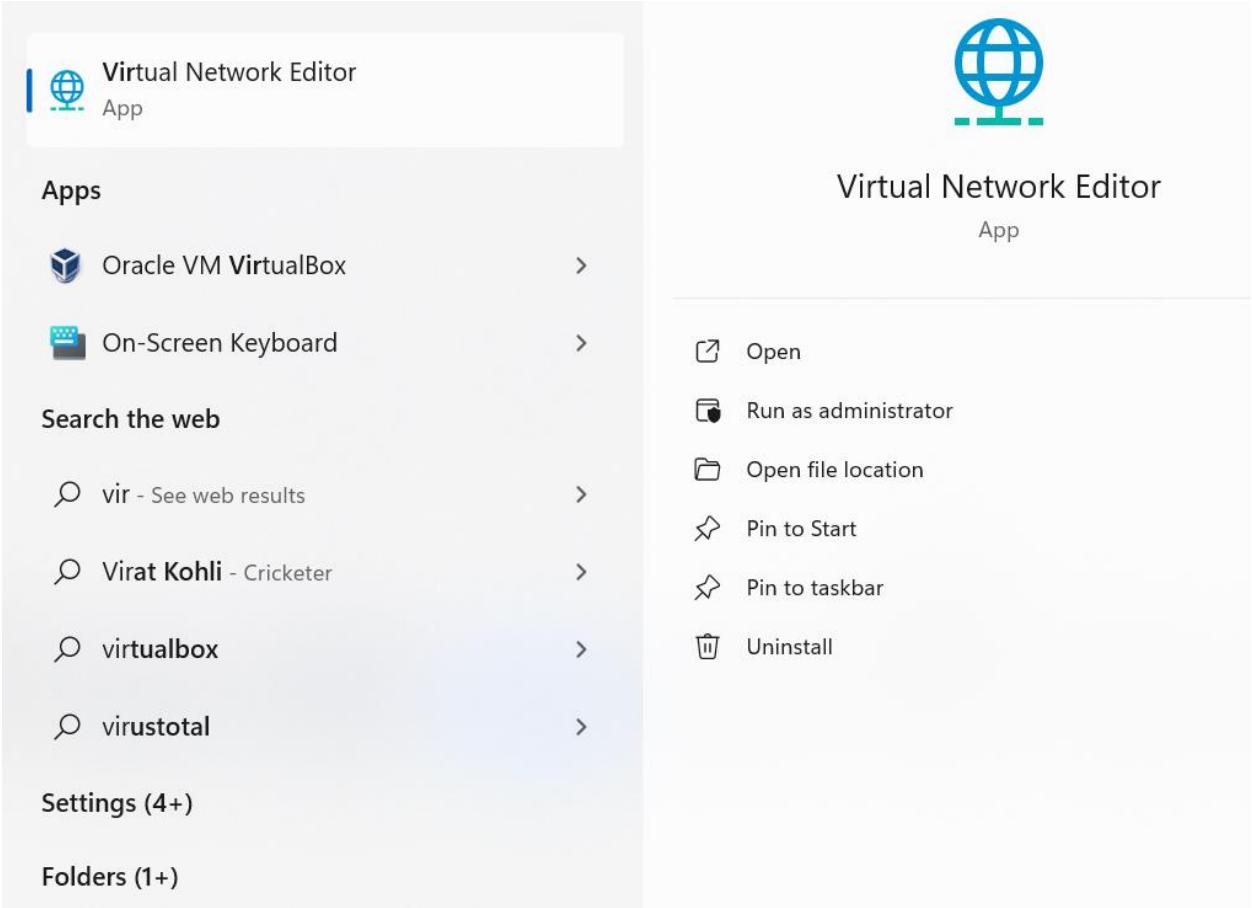
Pfsense will automatically start downloading.

Now we have our tools (pfsense, os, workstation) downloaded, we need to set up the environment then apply our control access list.

Before that, we have to configure our virtual network that will allow us to access gui interface.

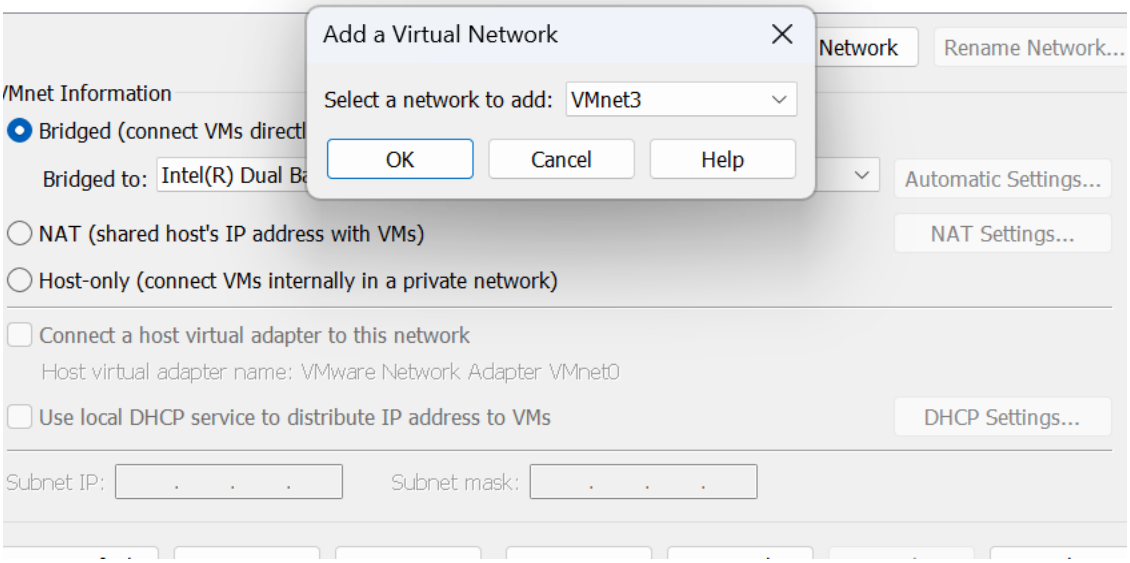
Go to search bar on your taskbar, search Virtual Network Editor

Run as administrator



Now after open VTE, click on add network and click on “okay”

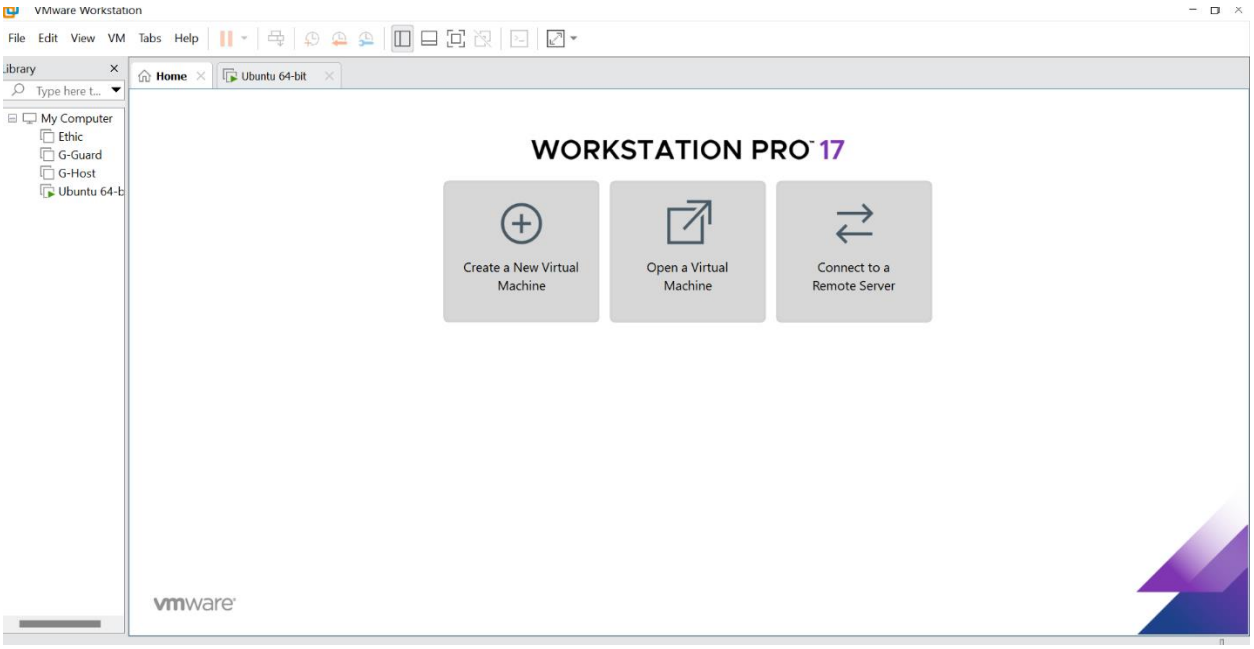
Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Intel(R) Dual Band Wireless-A...	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.5.0
VMnet2	Host-only	-	Connected	-	192.168.80.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.71.0



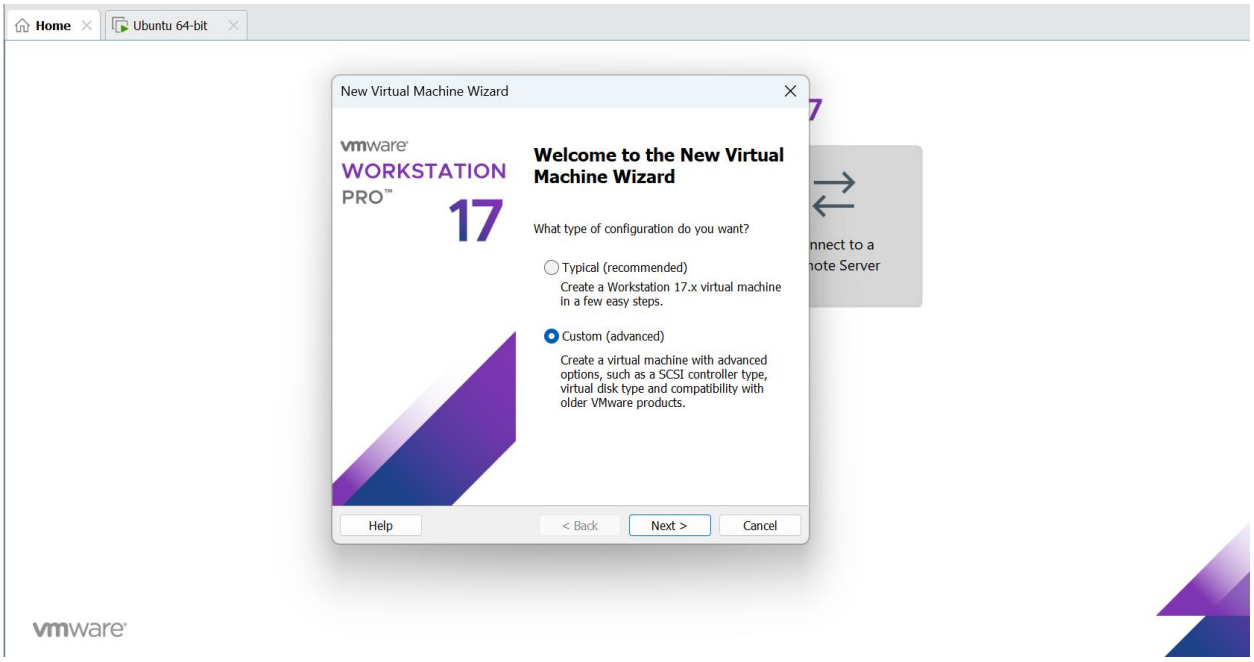
Now make sure you disable local dhcp server then click on apply

Let’s get started

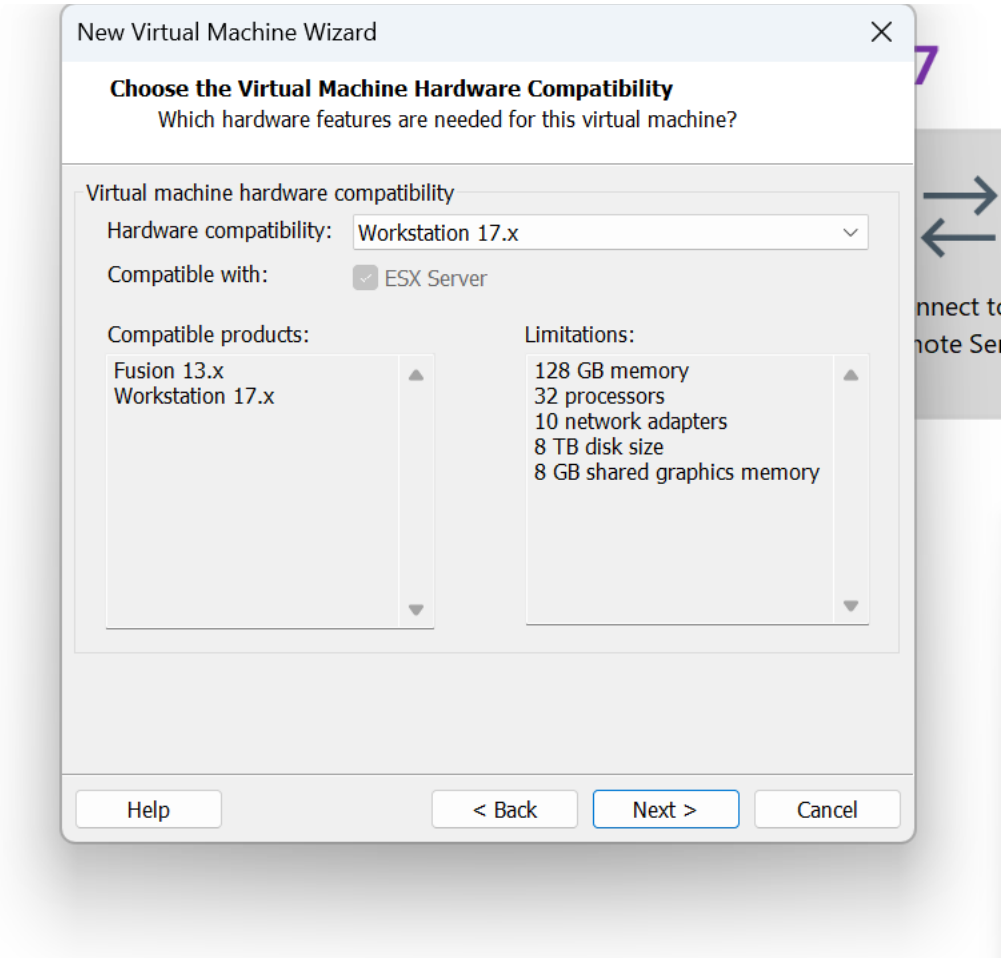
Open VMware workstation



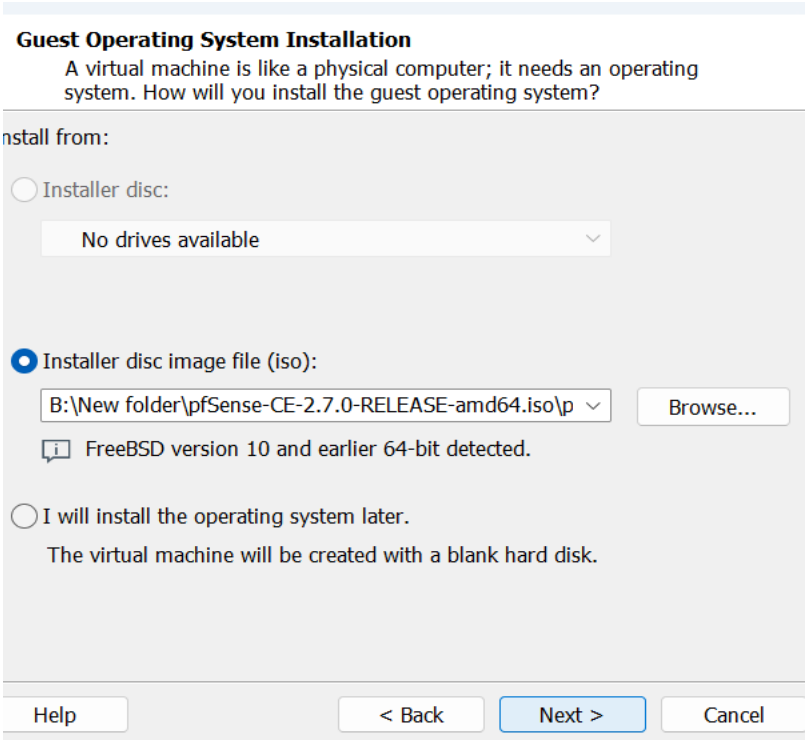
Click on create a New virtual machine



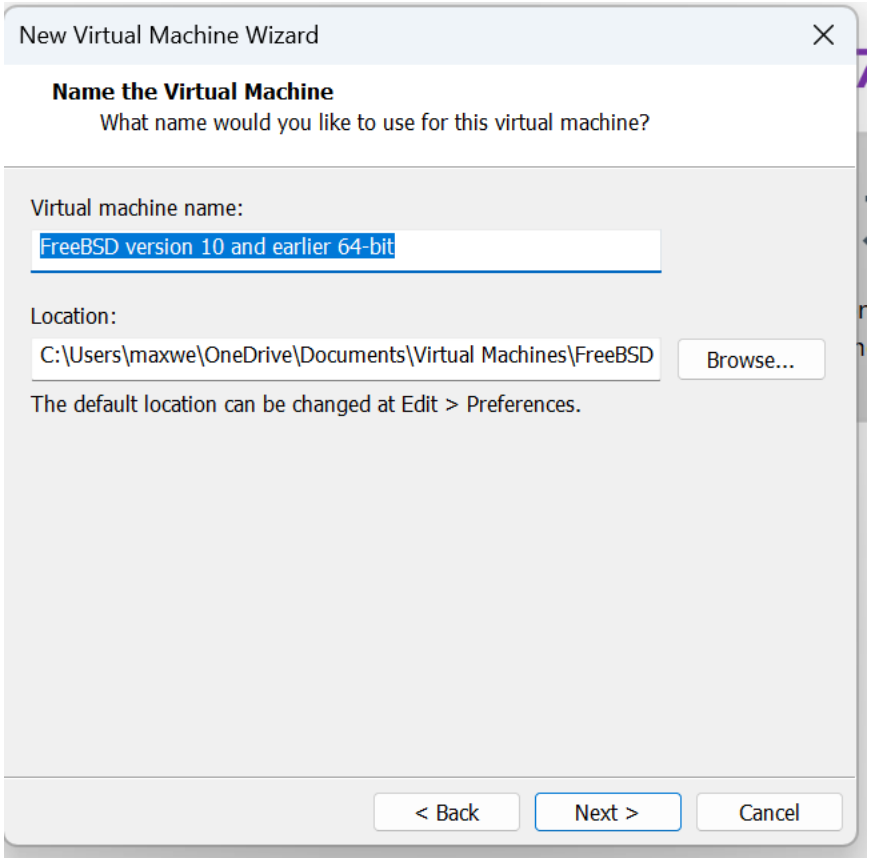
Click on Next



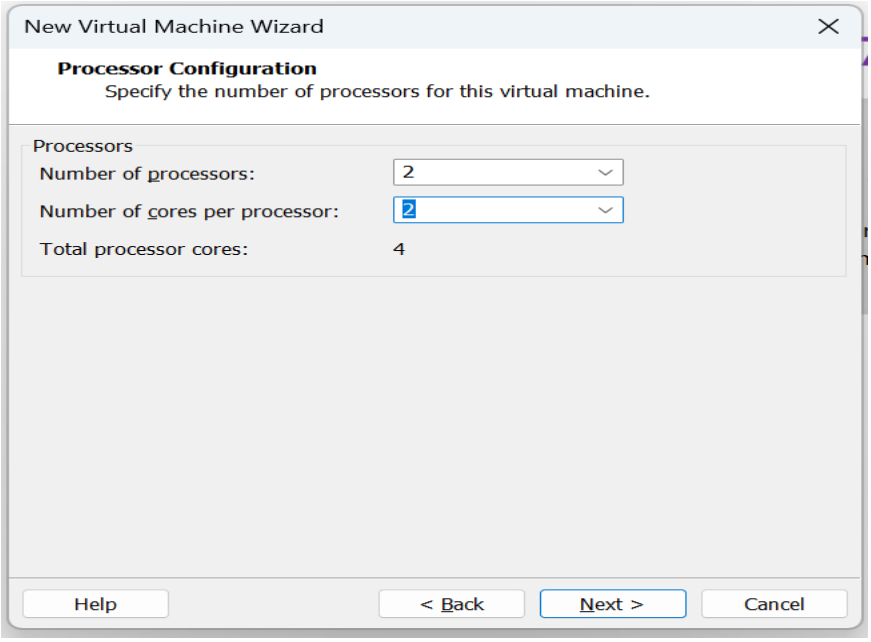
Click on Next



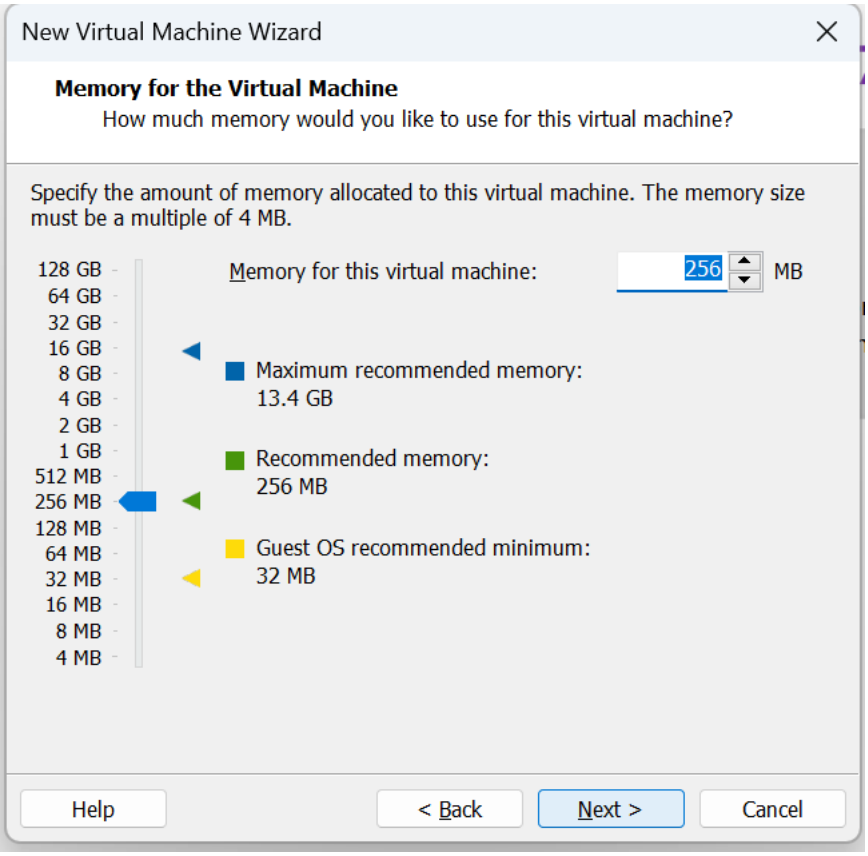
You click on browse to location of the iso file, select the file
Click on Next,



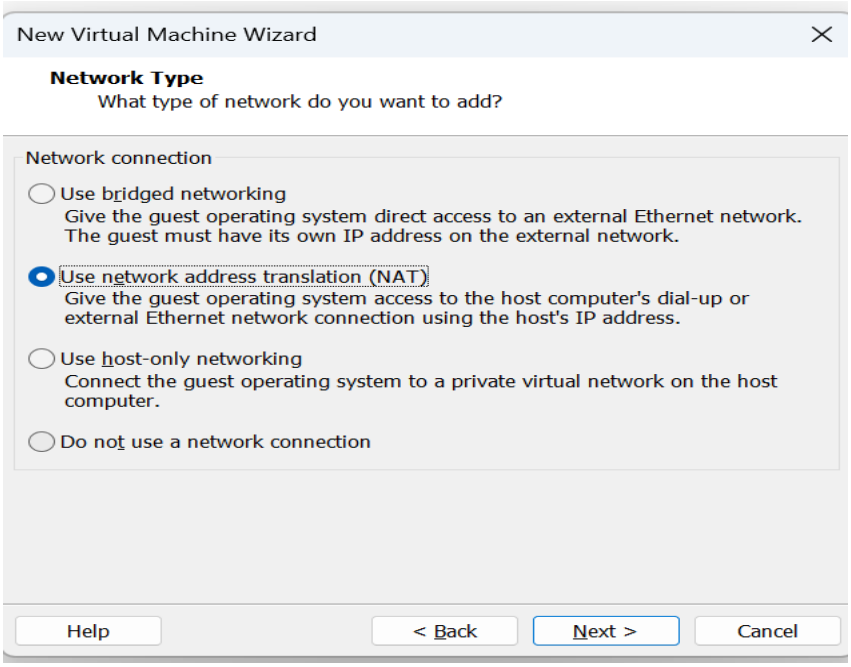
Click on Next,



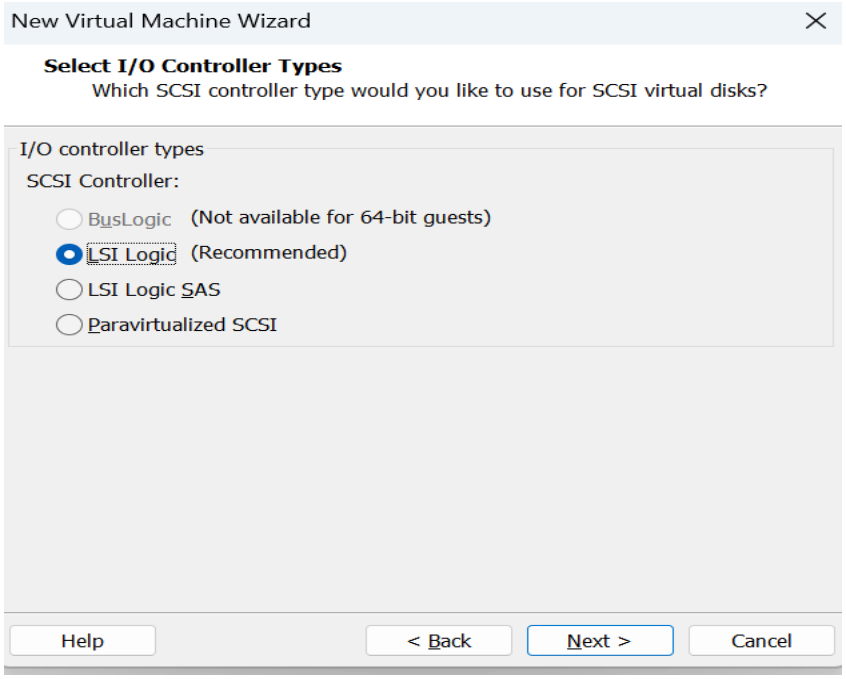
You configure your processor and click Next.



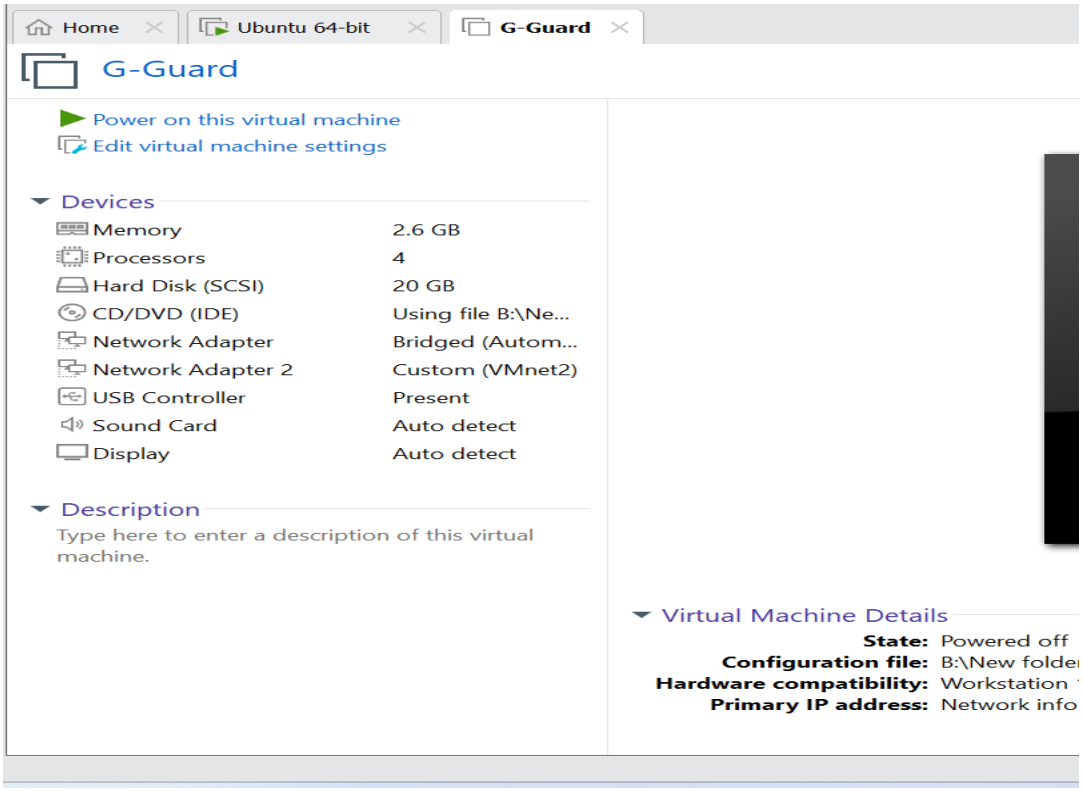
Now on this page you give storage capacity to the pfsense.



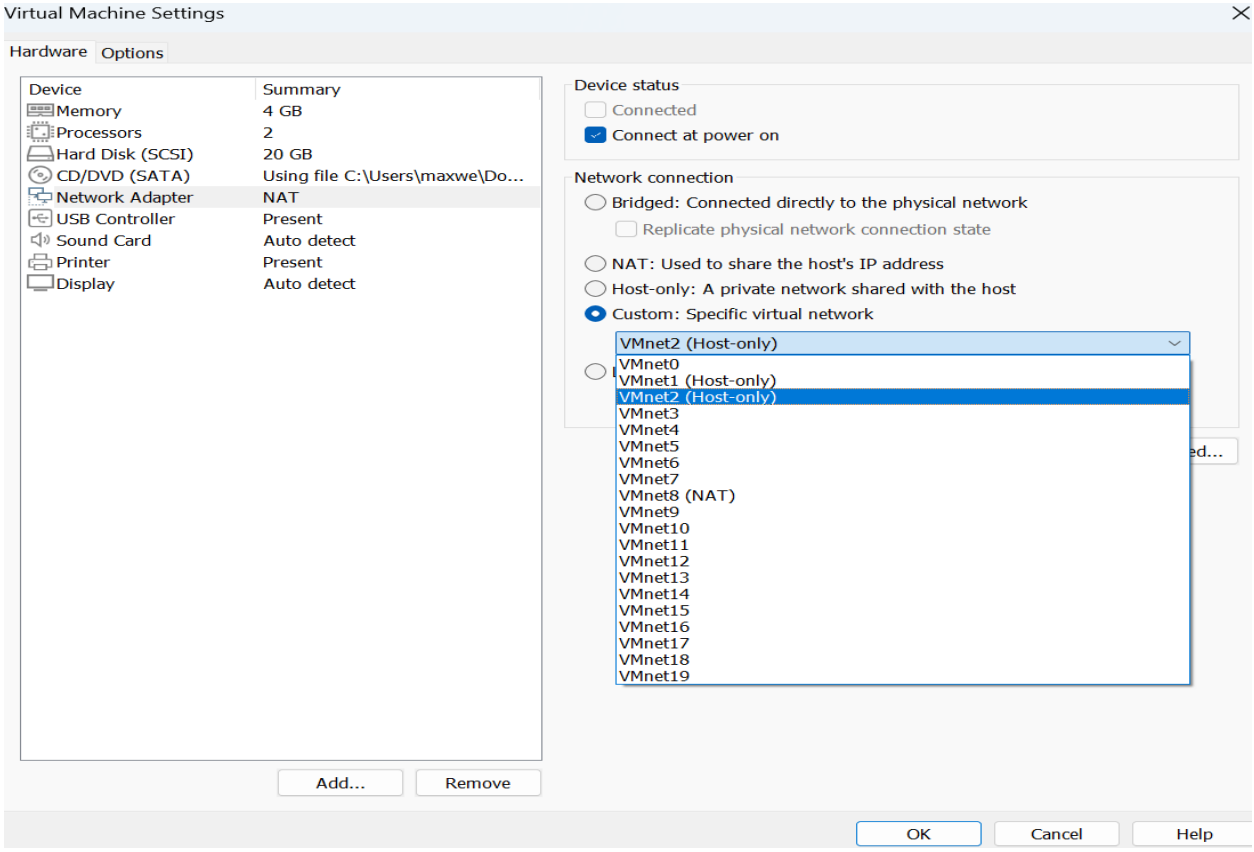
Click on next



Click on next to all next pages
After pfsense will boot to start running,
power off the pfsense and click on edit virtual machine settings

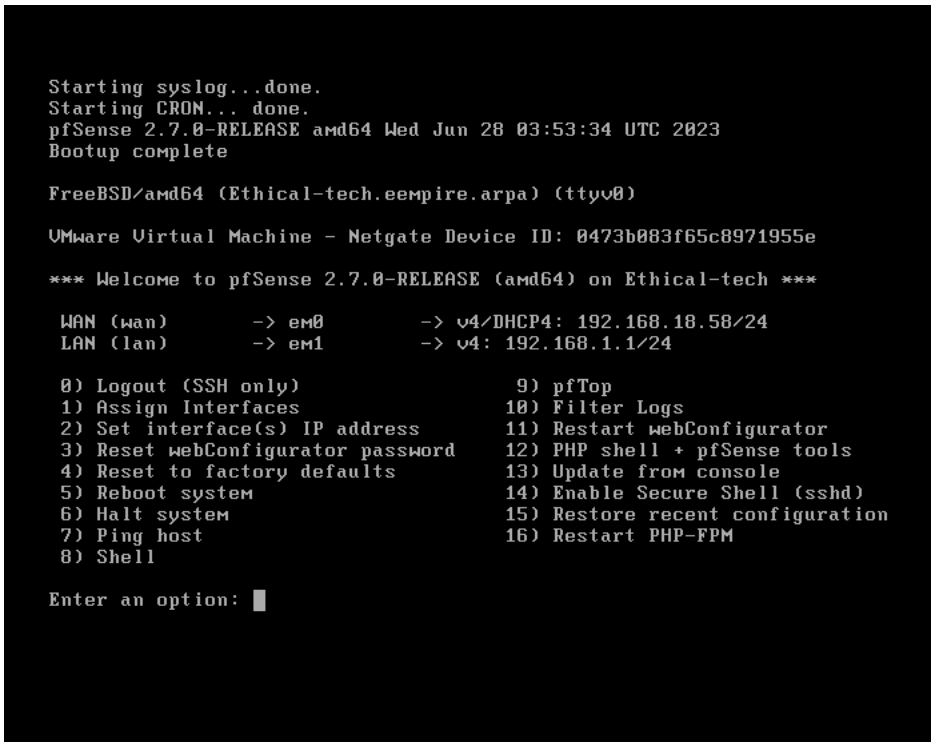


Click on add to and new Network adaptor,
Click on the second Network adaptor and select custom then you choose the specific virtual network you created.

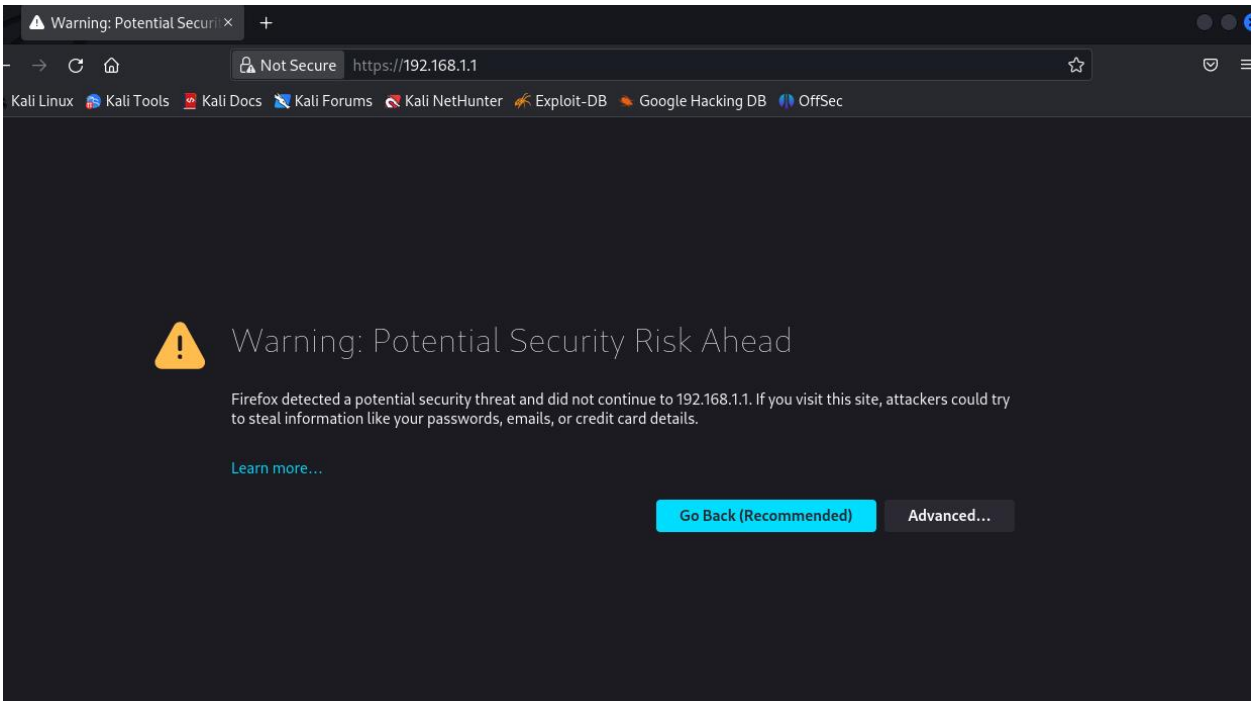


After this power on the pfsense.
Go to the OS and on the Network adaptor select the custom and choose the specific virtual network created which was assign to the pfsense Network adaptor you created then power it on.

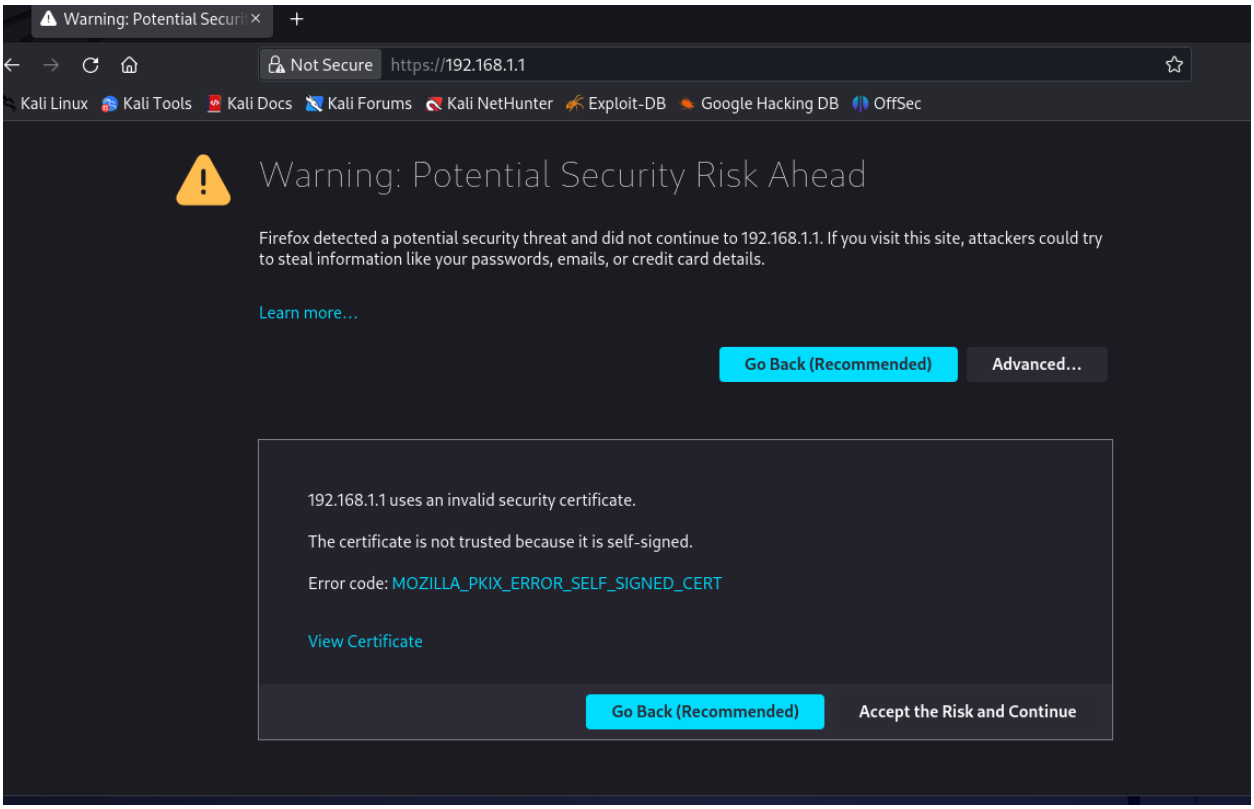
When pfsense is on, you will see the interface as the fig below



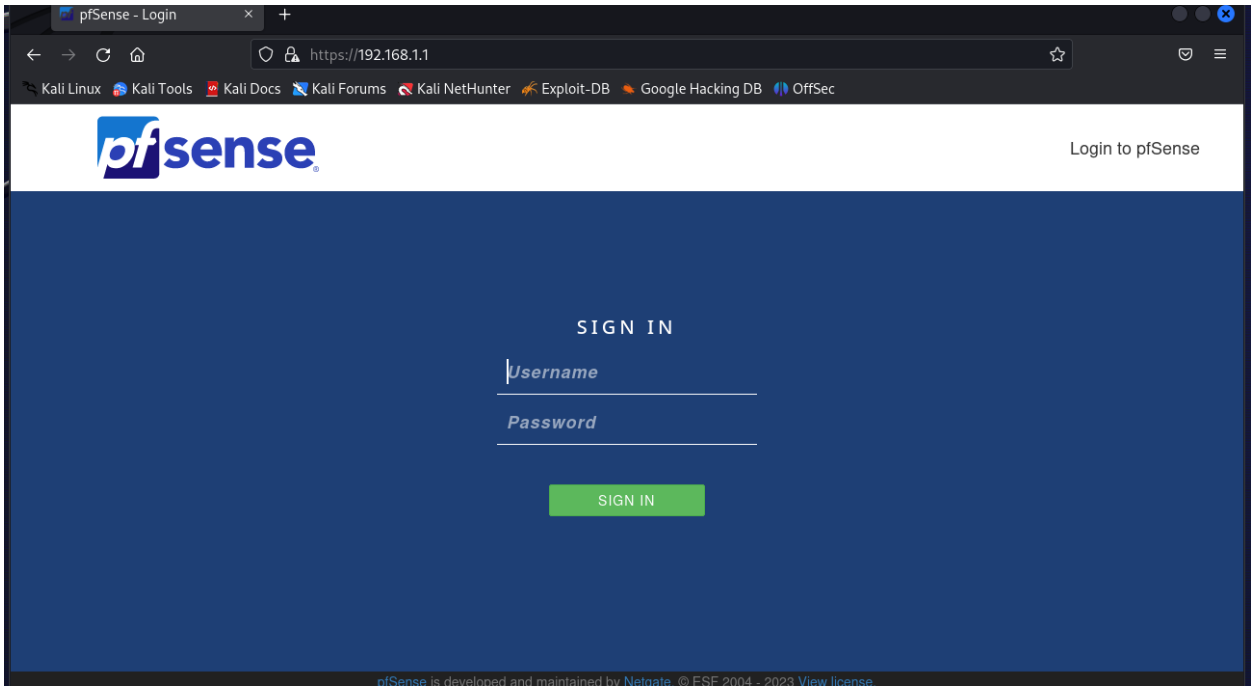
Now go to your browser on your OS configured with specific virtual network (custom) and input the LAN ip address(mine is 192.168.1.1) as shown above



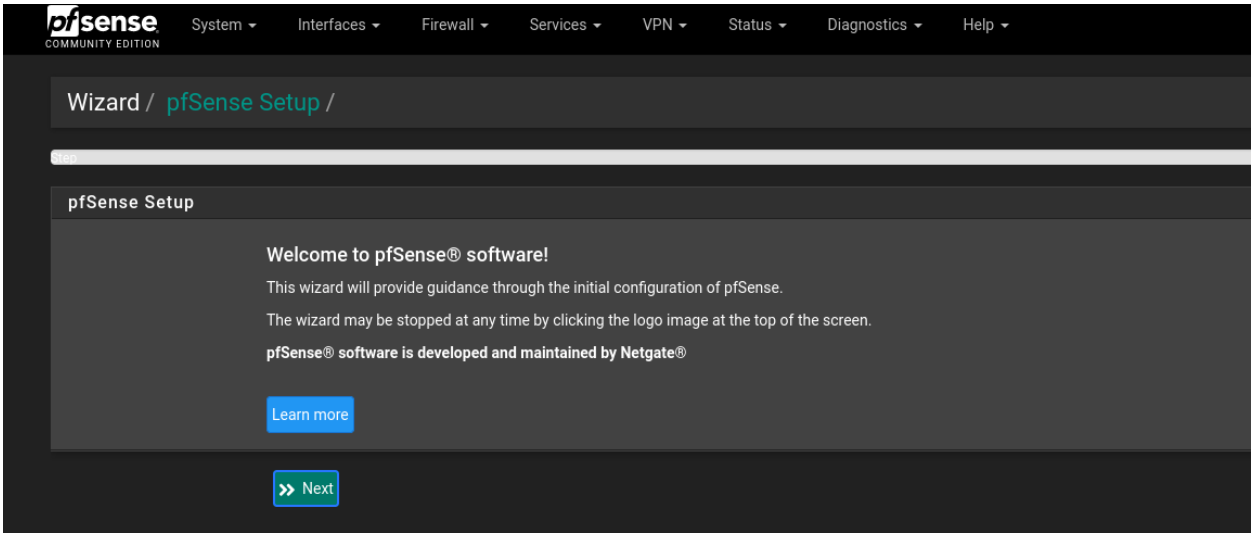
Click on advance



Click on accept the Risk and Continue,

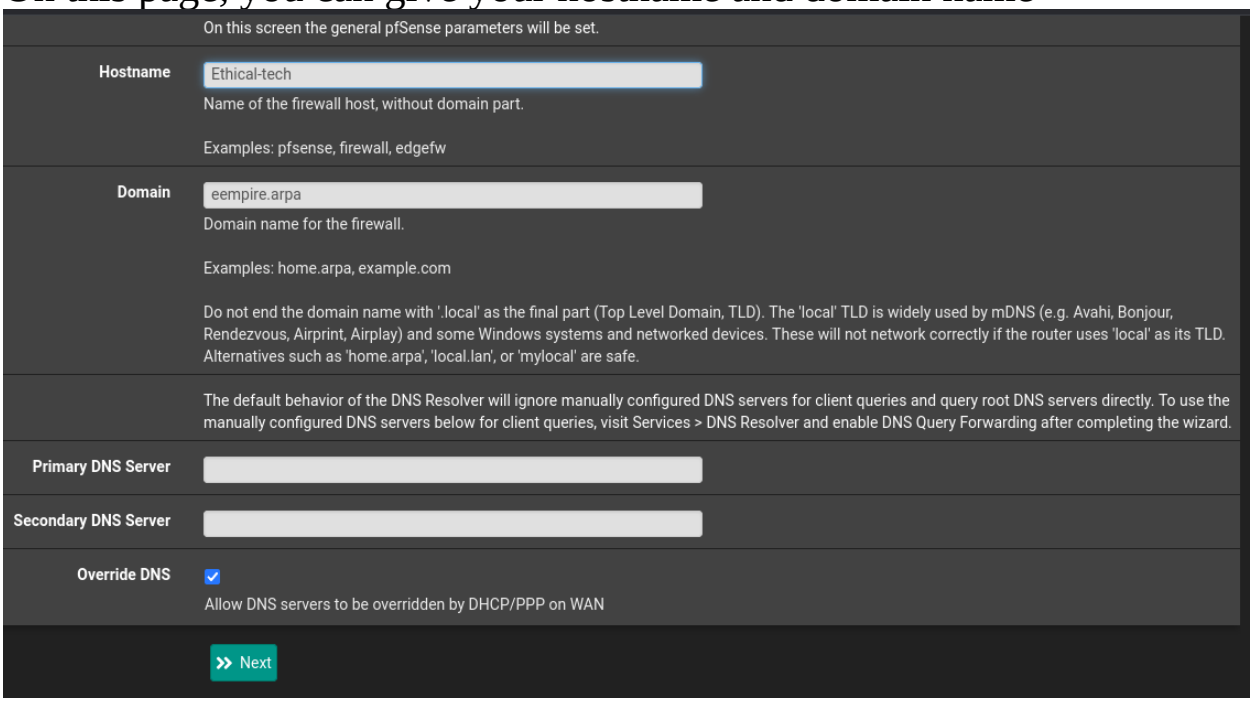


Default log in credentials
Username: admin
Password: pfsense

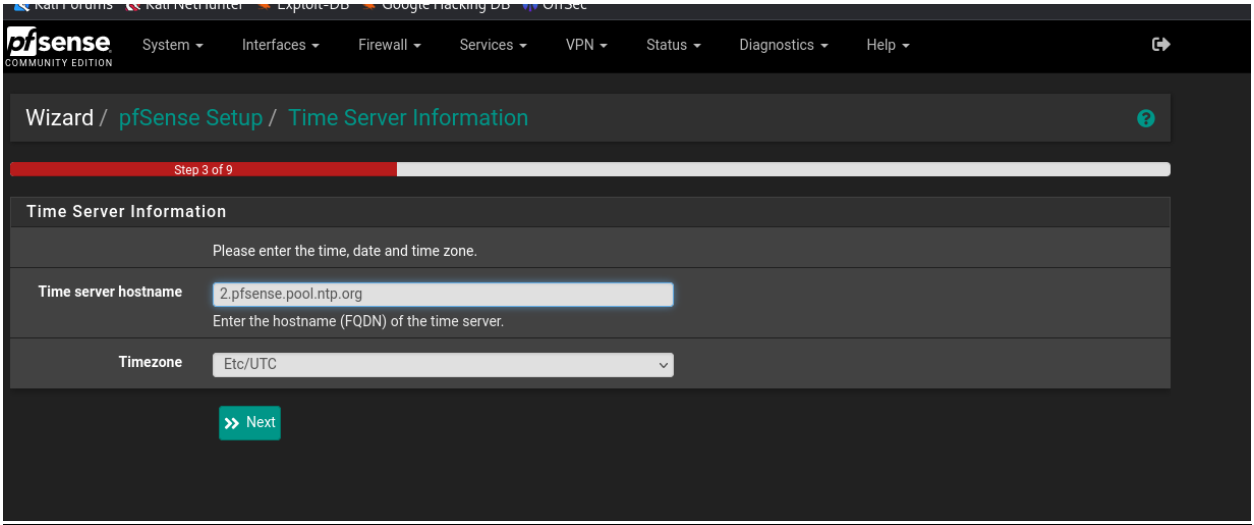


Now it has opened the set-up wizard, click on next

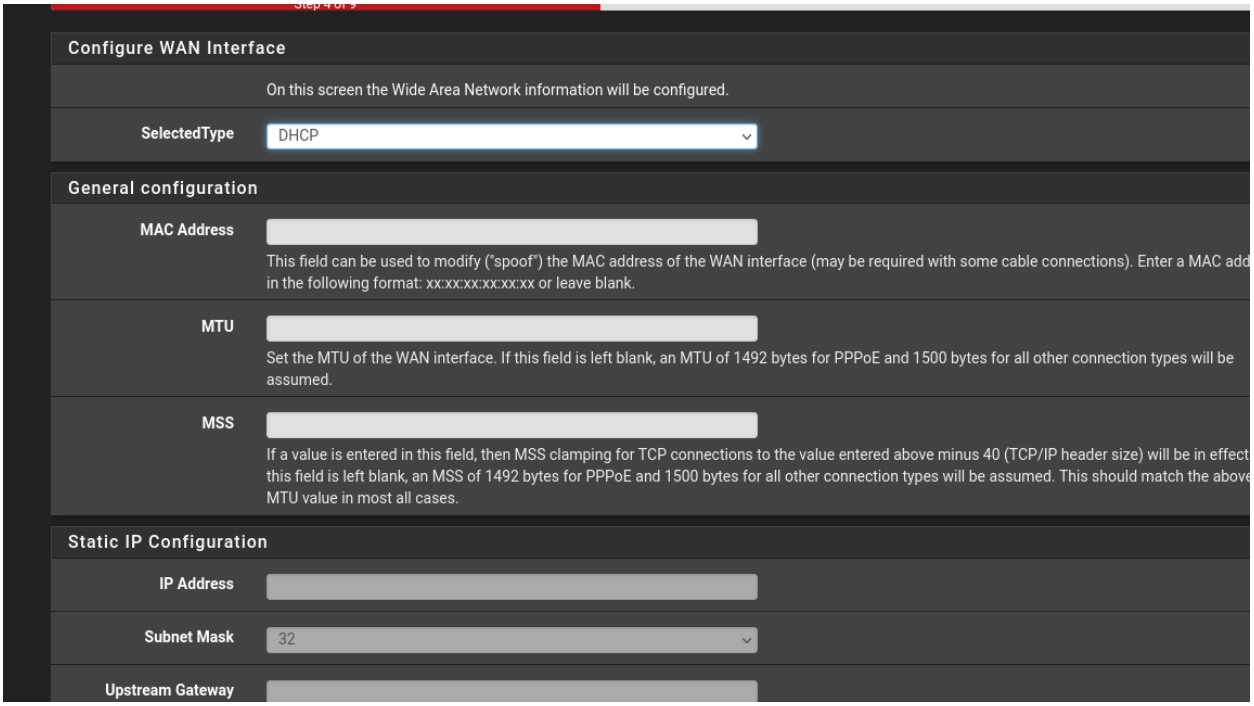
On this page, you can give your hostname and domain name



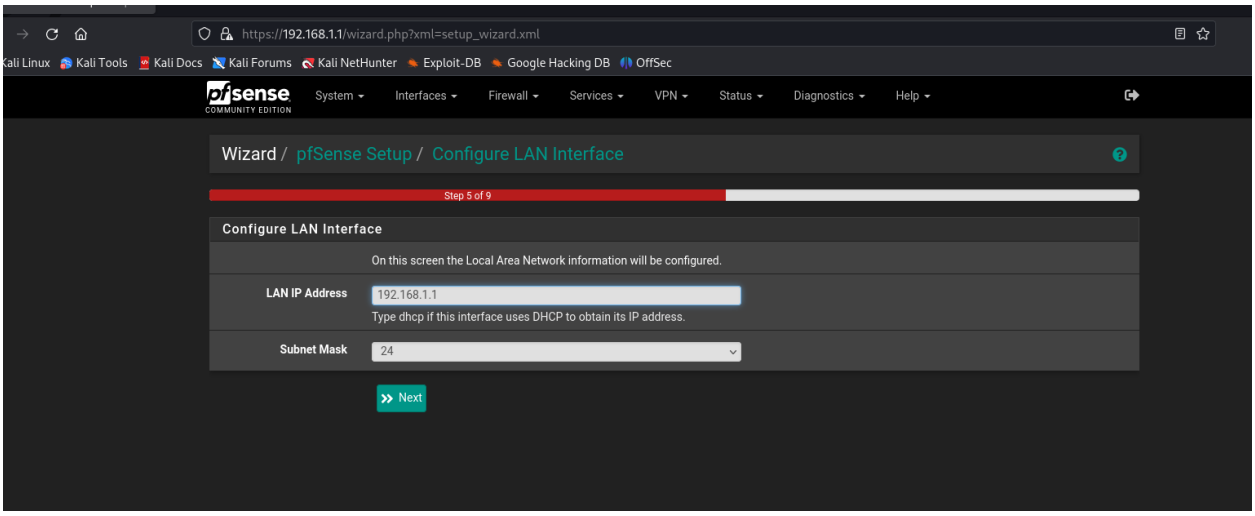
Click on next



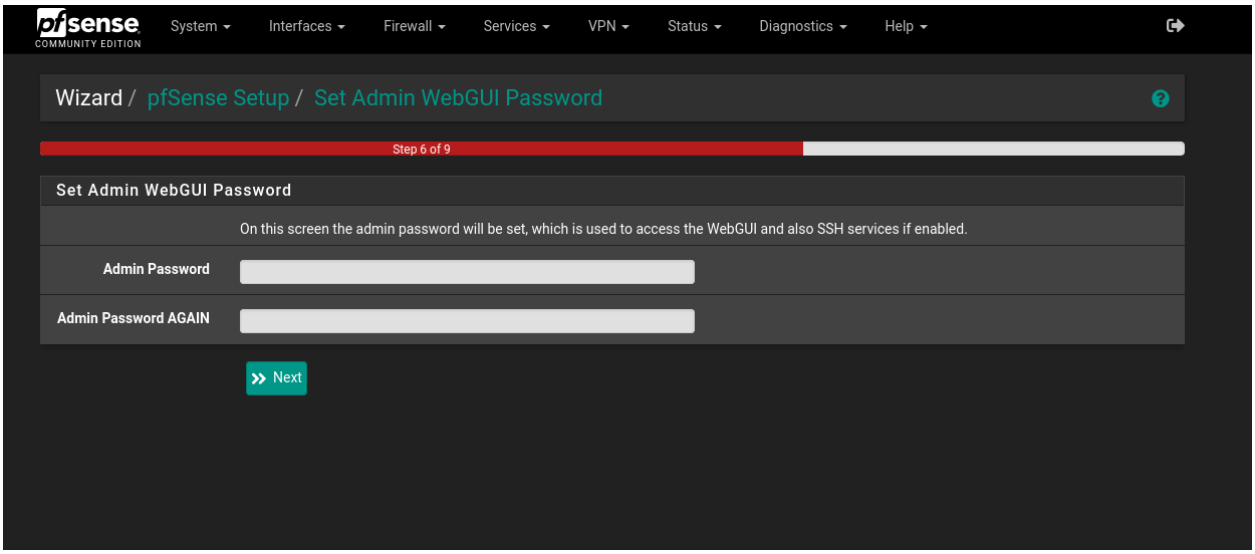
Click on next



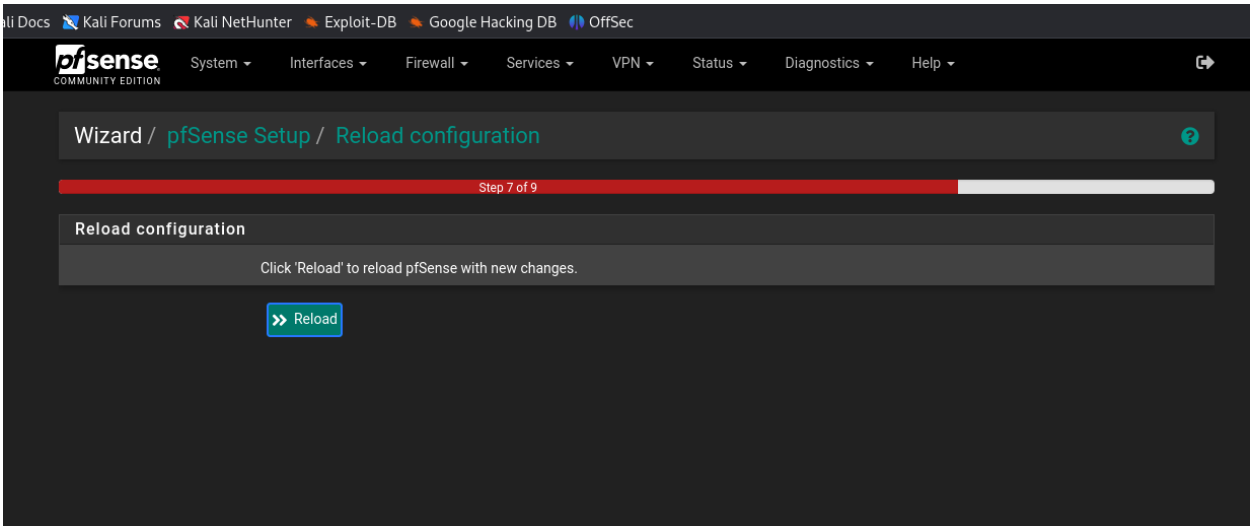
This page shows your LAN Ip address you can configure t your preference but I will leave my default.



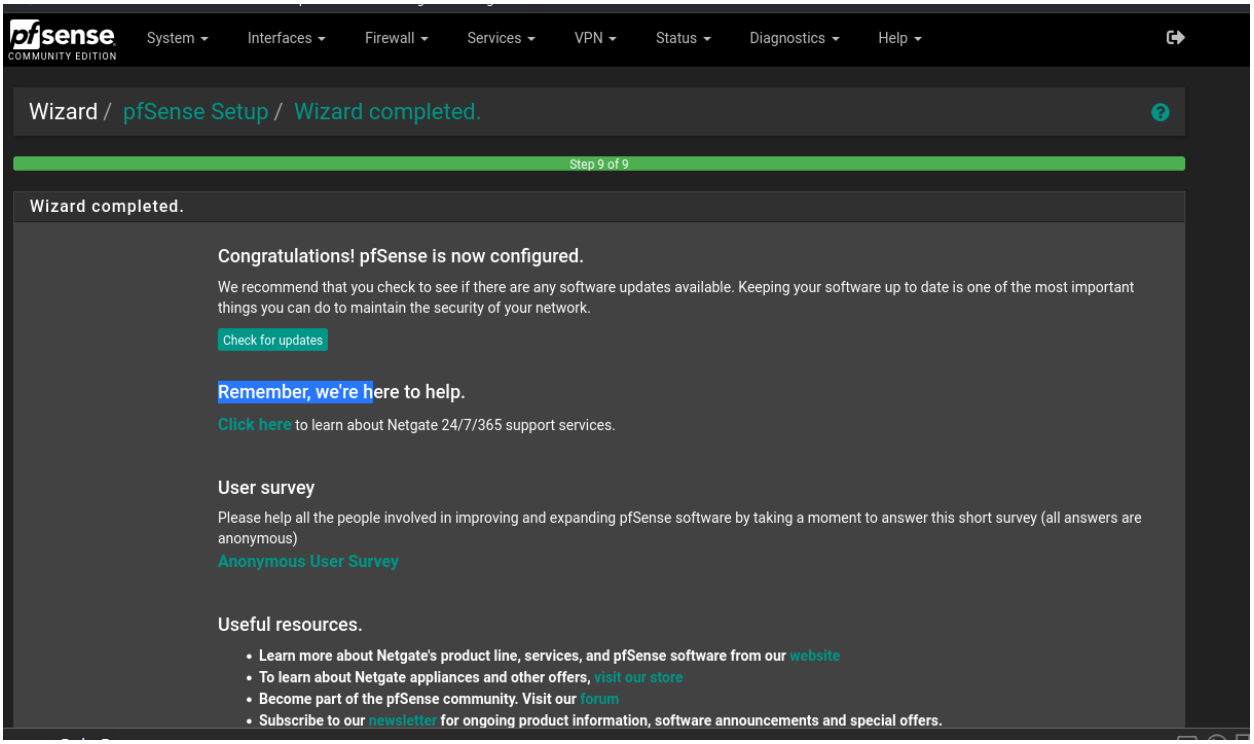
Click on Next,



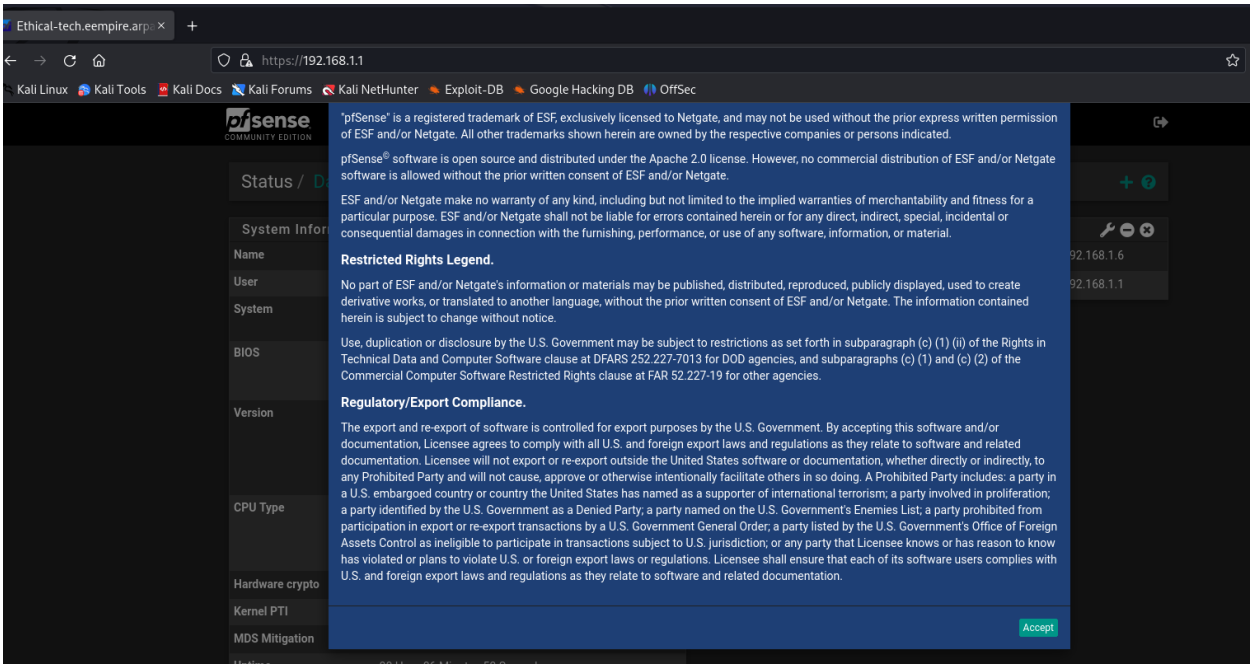
This above page allows you to set password to your preference for security measures.



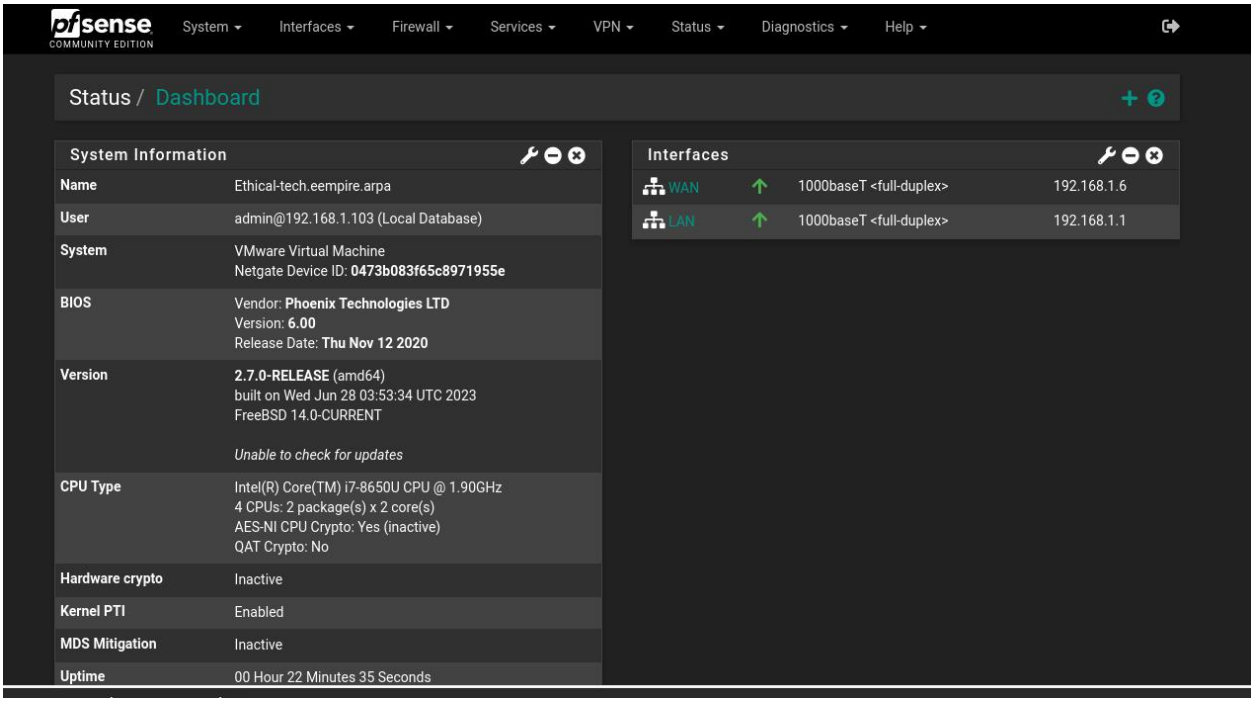
Click on Reload



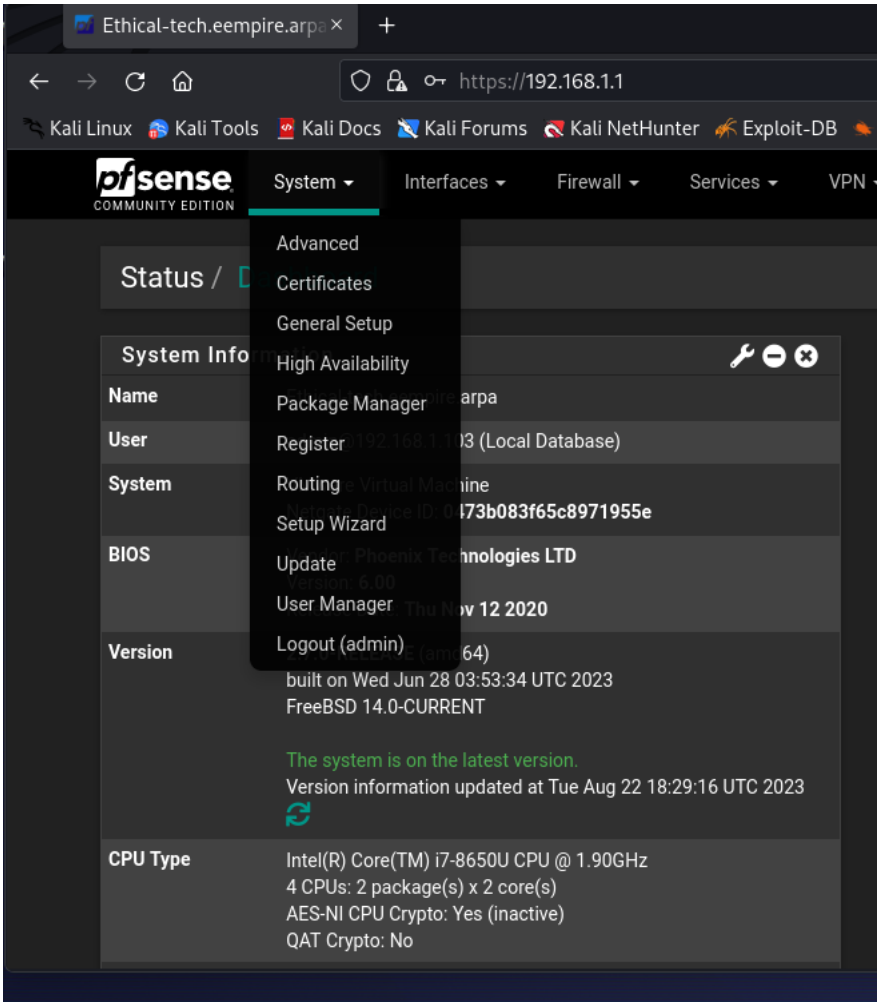
Now you scroll down and you click on finish, it will take you pfsense dashboard and then we can start our configuration



Click on accept



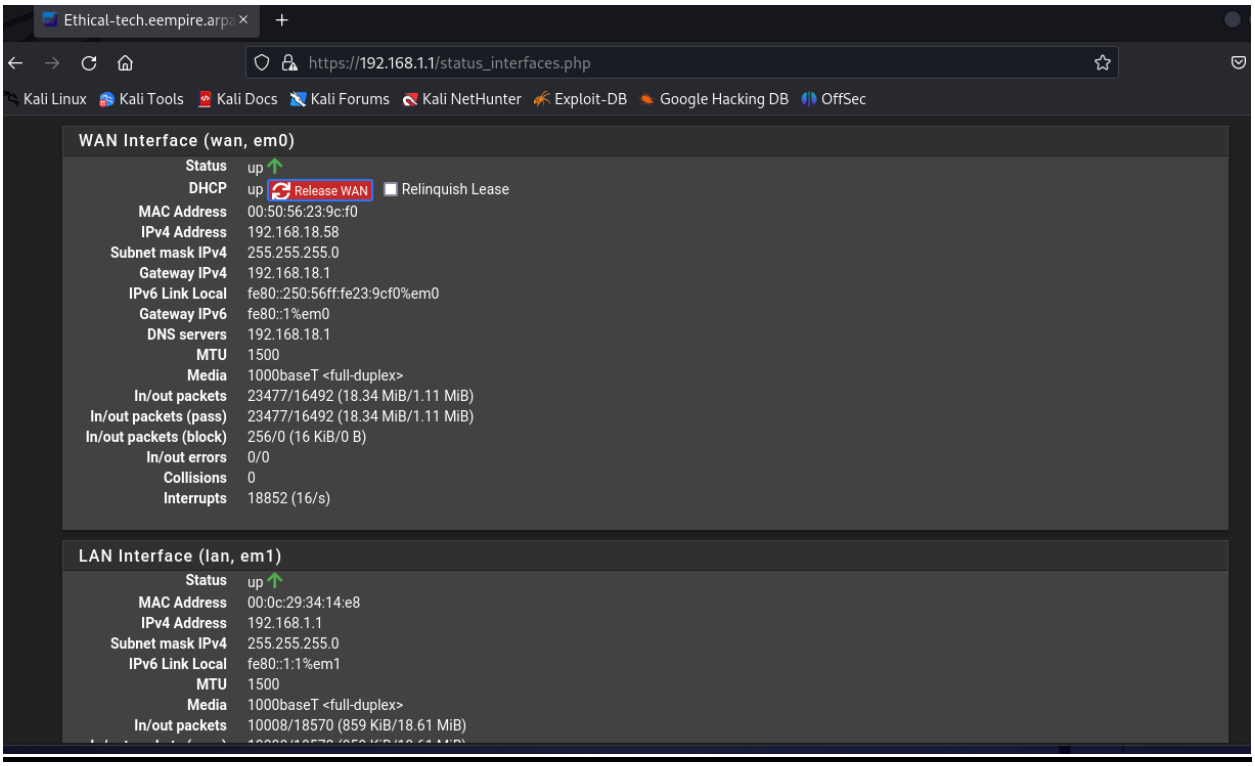
Now we can navigate and see what pfsense contains.



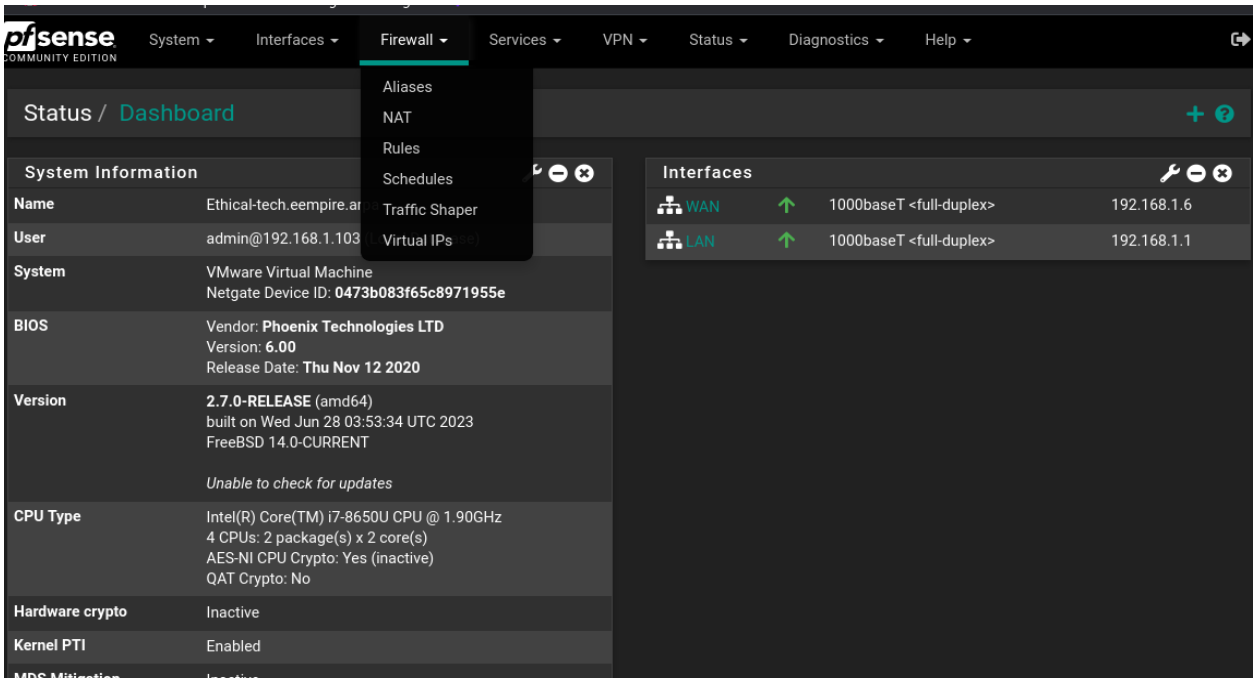
On the above interface you can you make any changes to your preference and also add packages from Package Manager, add new user and disable the admin user and many more.

Let gets on to our main aim of this project.
Now we set the firewalls on the various interface (LAN and WAN) to control both ingression and egression of traffic.

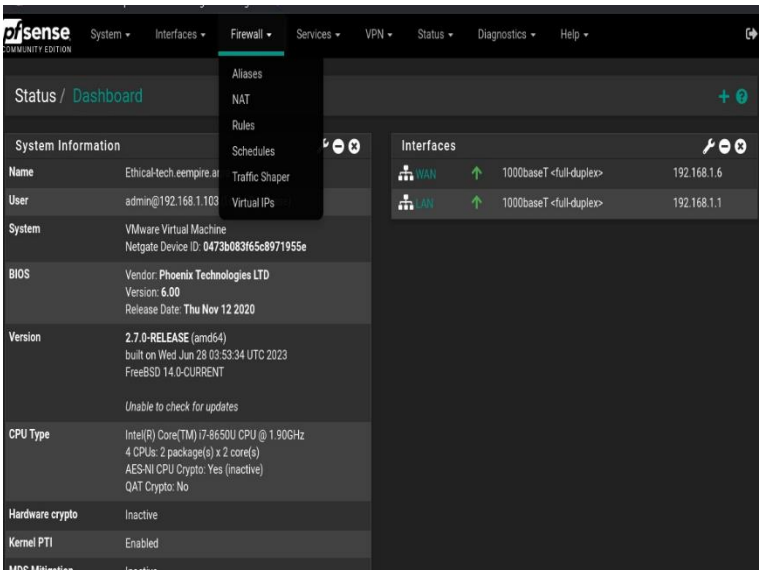
If you want to know your interface navigate to Interface and look at the various interface you have available.

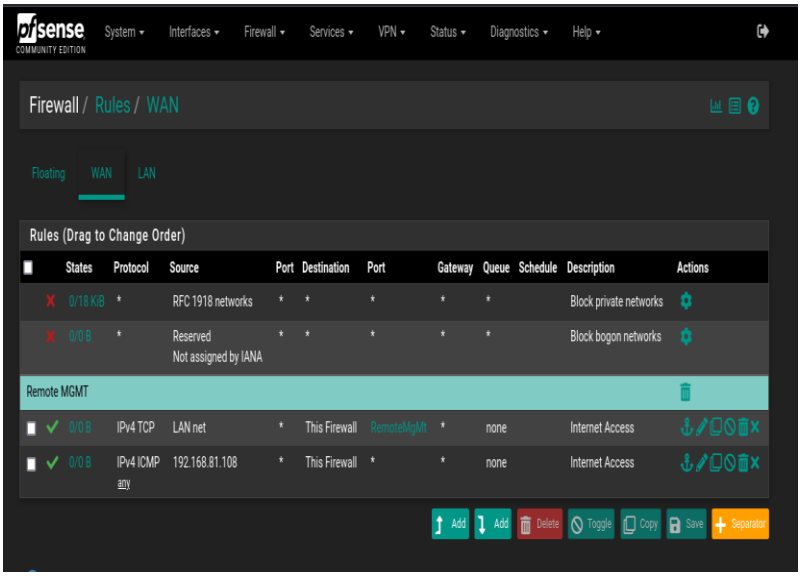


Now we can see all our interface active showing up
Let navigate to the firewall drop and see what is there.



You choose rules to apply instructions to execute the flow of traffic in your local network. Now to do this, go to firewall, select rules from the drop down. This will open interface as shown in fig below.





Machine: Ubuntu 64 bit
IP address: 192.168.62.103
Host

Machine: Windows OS
IP address:192.168.2.100
Guest

Case study: Allowing Host machine to access anything using super user privileges. The Guest machine can access the GUI of the pfsense but cannot get ICMP response.

Machines in the LAN net can access anywhere on the internet but Guest machine is restricted on the WAN interface

So now we start implementing our rules.

But how does pfsense apply these rules?
Pfsense has three actions that are used to execute operations. They are “pass, block, reject”.

The pass action allows a specified domain such as ip, port, traffic to go through.

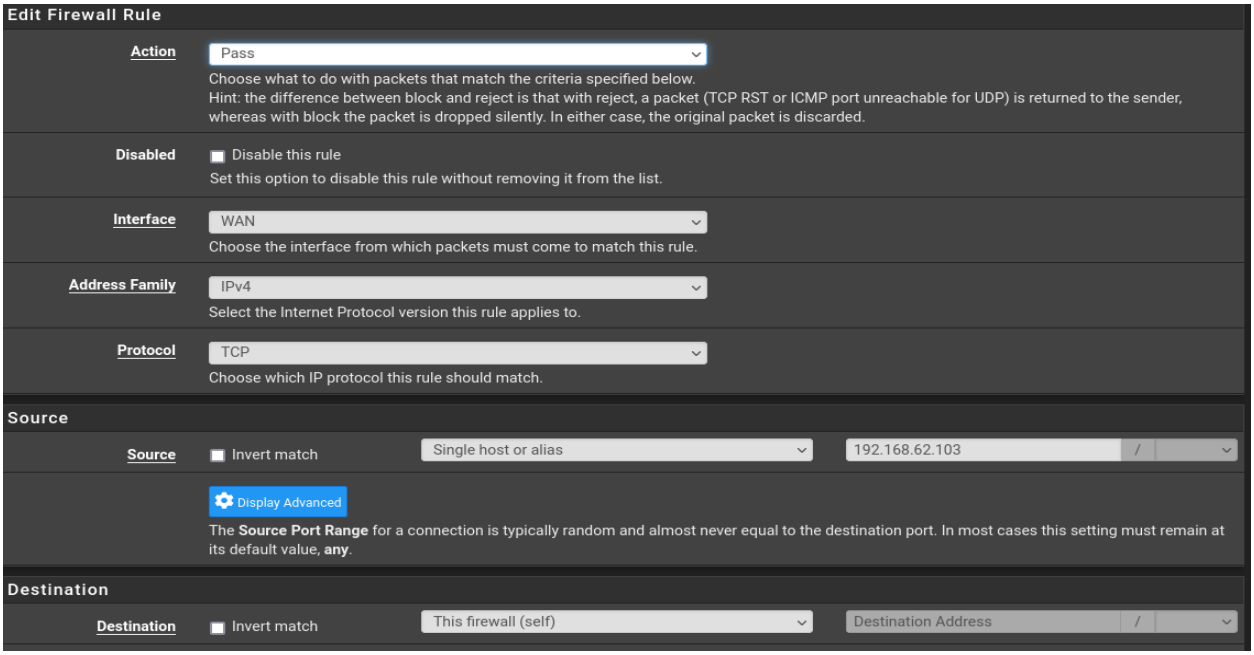
This with block the packet is dropped silently.

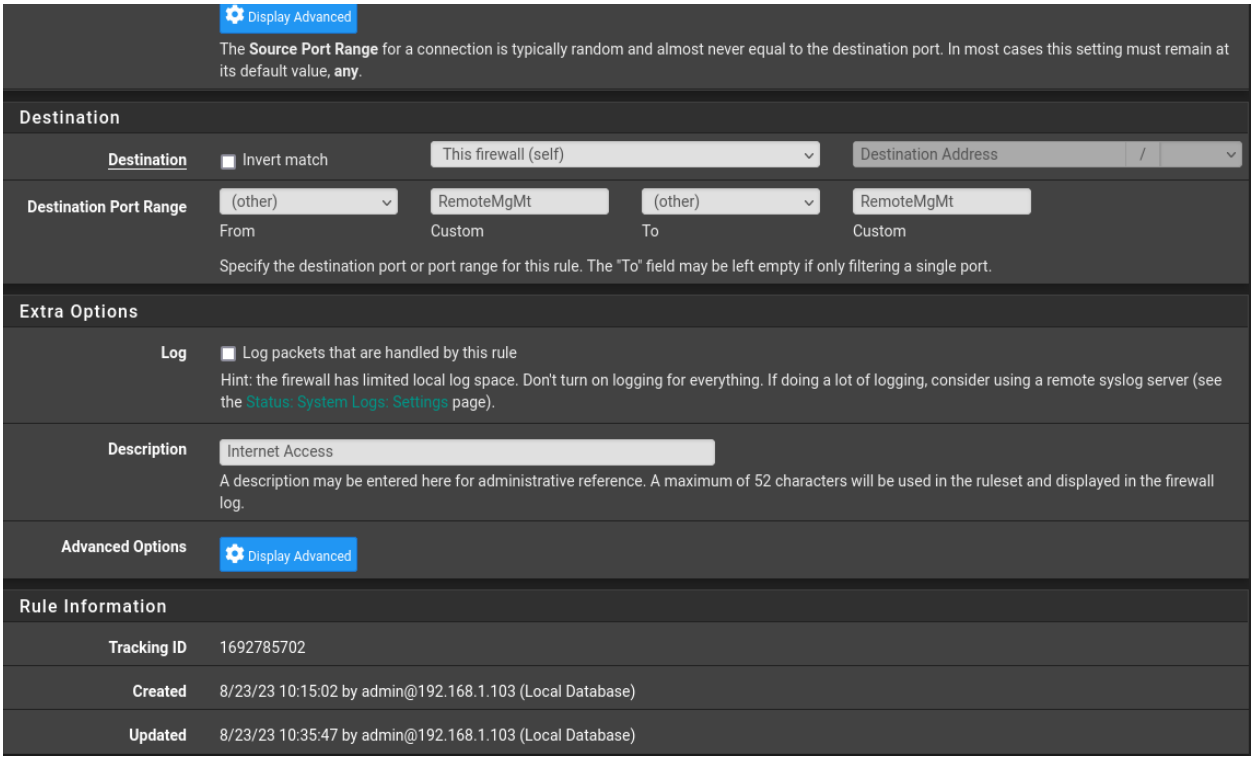
With the reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender.

Let open Firewall/rules/WAN

NB: Rules are applied in hierarchical manner; we use separator to give comment and differentiate various rules.

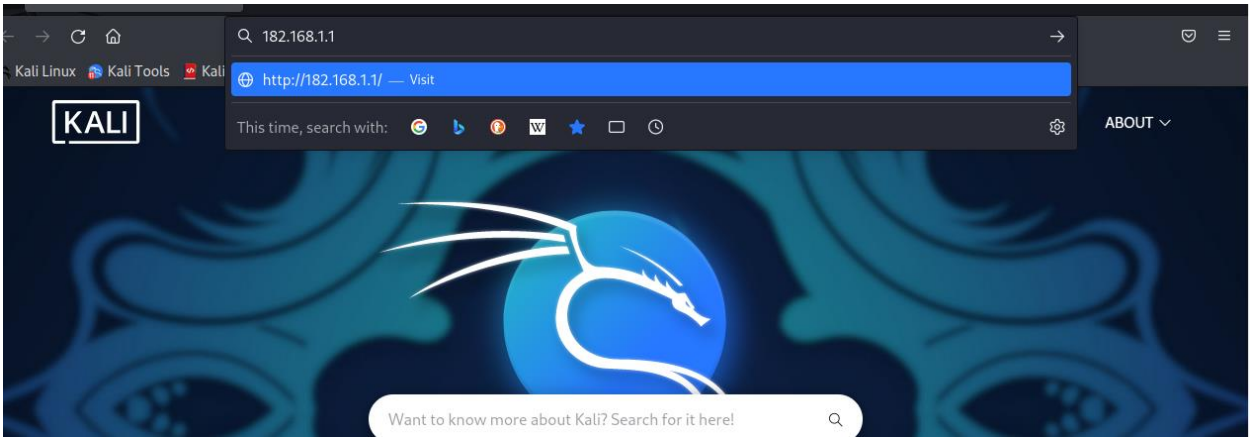
So, now am adding a rule says anything coming my WAN interface on Management port won’t be allowed.





Now let go on to the Ubuntu Os and check if we can access Management control.

On my Ubuntu os



We search for the ip 192.168.1.1 which is our LAN IP of pfsense

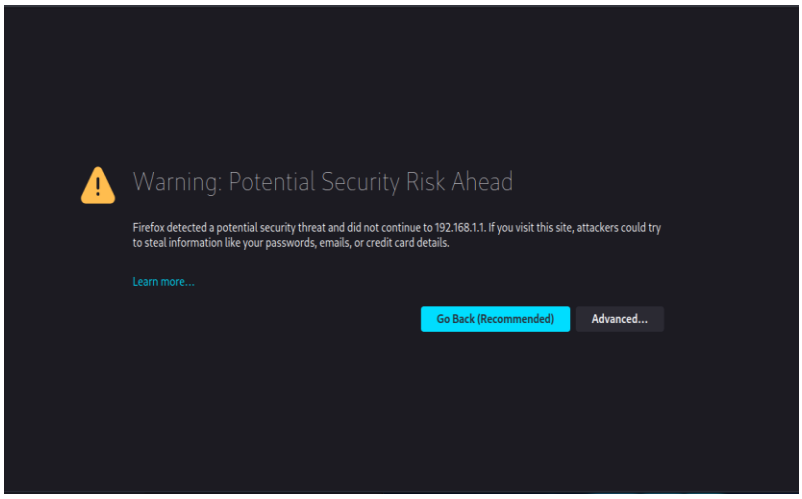
Accessible

click on **Advance**

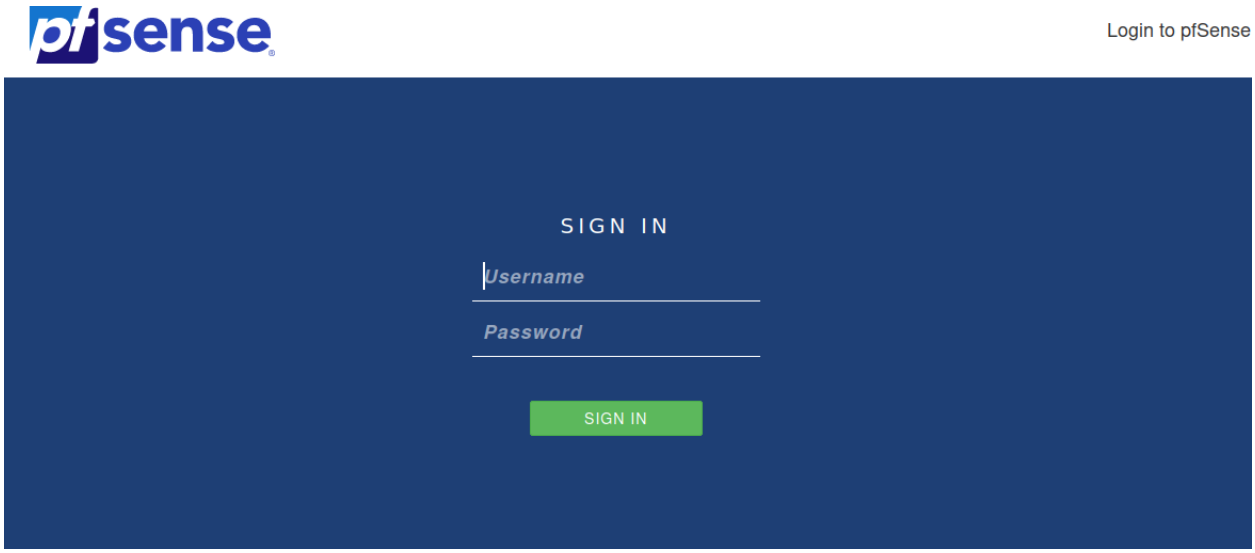
to **accept the risk**

and this will take you

to pfsense log in page.



Pfsense log in interface



So now let try to see if we will be able to ping it, the answer will let us see what we need to do.

```
File  Actions  Edit  View  Help
┌──(bworld㉿Ethical)-[~]
└─$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.685 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.25 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.519 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.15 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=1.21 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=1.39 ms
```

Yes, it ping it and this is not a good practice but let see what caused this.

On the destination port it might be set to ‘any’ or a rule is set to allow.

Let disable this permission.

Go to Firewall/rules/wan

Set action = pass

Interface = WAN

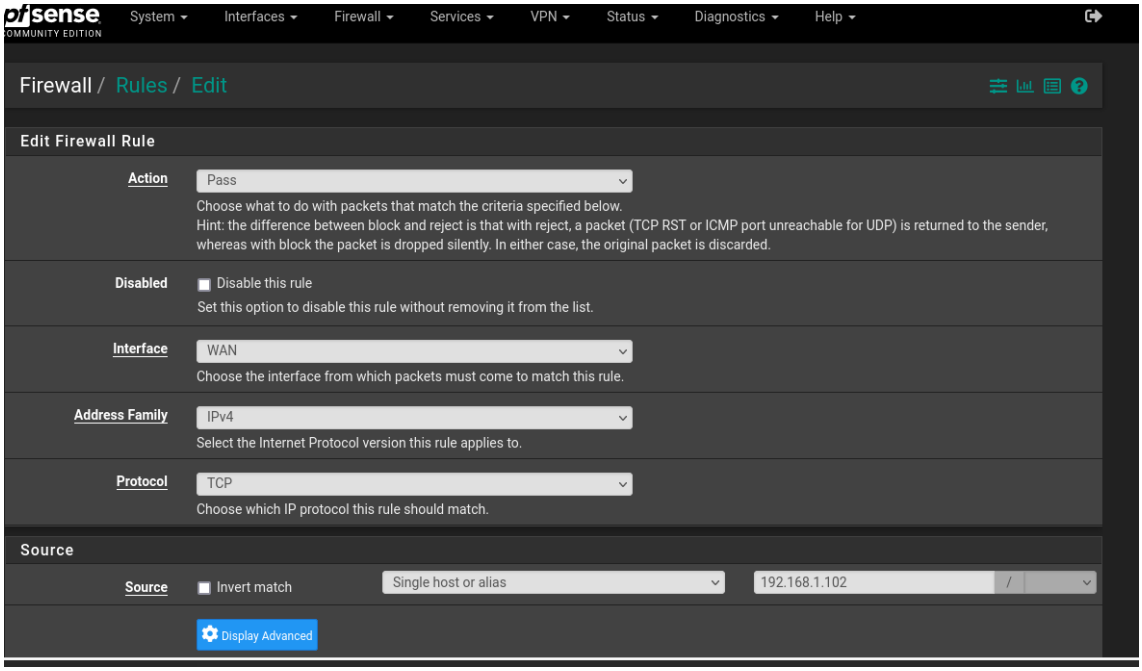
Port = TCP

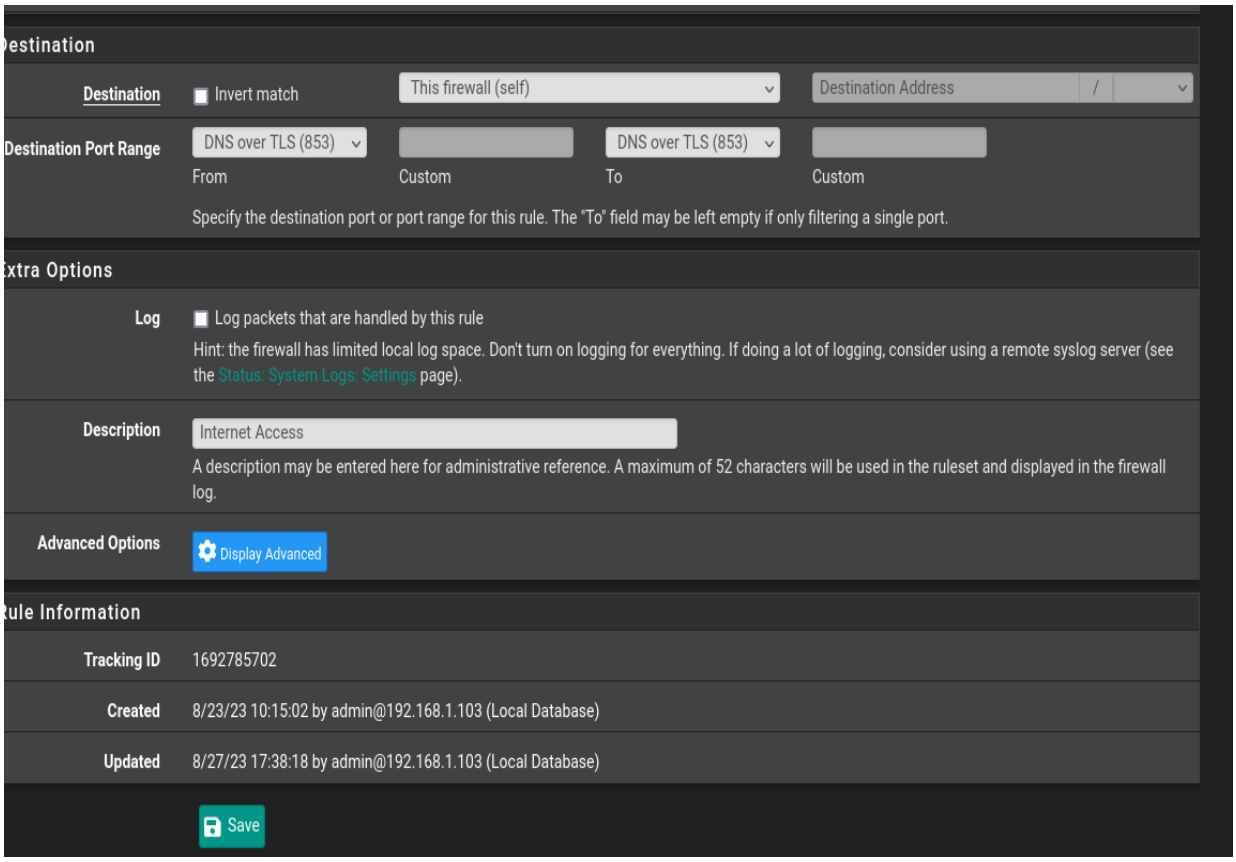
Source = 192.168.1.102

Destination port = DNS with TLS

This will allow it access dns servers

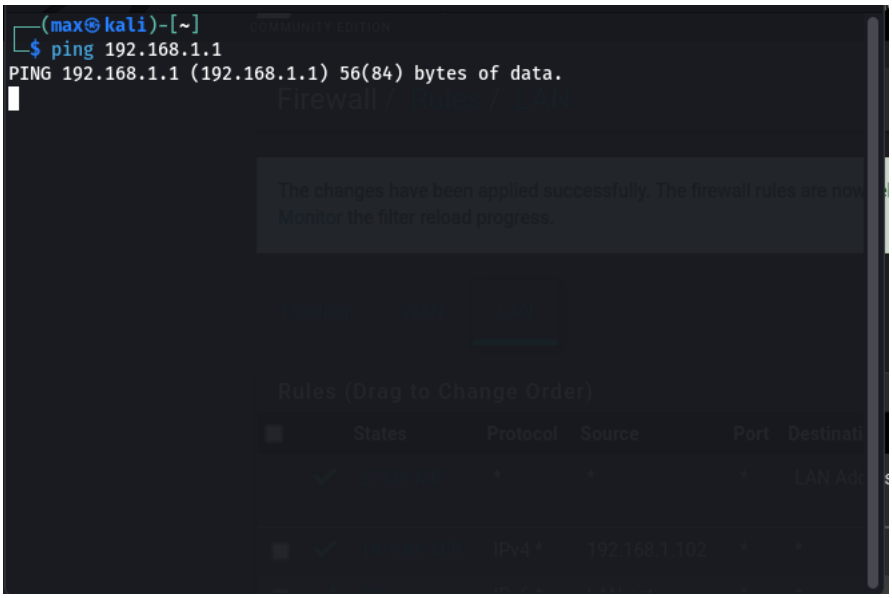
Fig Demonstrate





Now let try to see if we can ping it again

On our ubuntu server



Yeah now Ubuntu server can access TCP port but cannot get ICMP acknowledgement.

REFERENCE

Pfsense: pfSense® - World's Most Trusted Open Source Firewall

Kali Linux: Get Kali | Kali Linux

Network Berg: pfSense Firewall (totally) Rules! Basic rule setup... 😮 - YouTube