

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

| | |
|--|------|
| Subject of the Project | I |
| Aims and Objectives | II |
| Introduction | III |
| Acknowledgment..... | IV |
| Company profile..... | V |
| 1. Global presence..... | VI |
| 2. Products and services..... | VII |
| Technology..... | VIII |
| Training..... | IX |
| 1. Environment: VMware Workstation..... | X |
| 2. PfSense: Downloading & Installing..... | XI |
| 3. Virtual Host: Kali Linux OS | XII |
| 4. Configuration: Virtual Network Editor | XIII |
| Screenshots..... | XIV |
| Screenshots of tools..... | XV |
| Reference..... | XVI |

Firewall Configuration using pfsense Technology

What is pfsense?

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

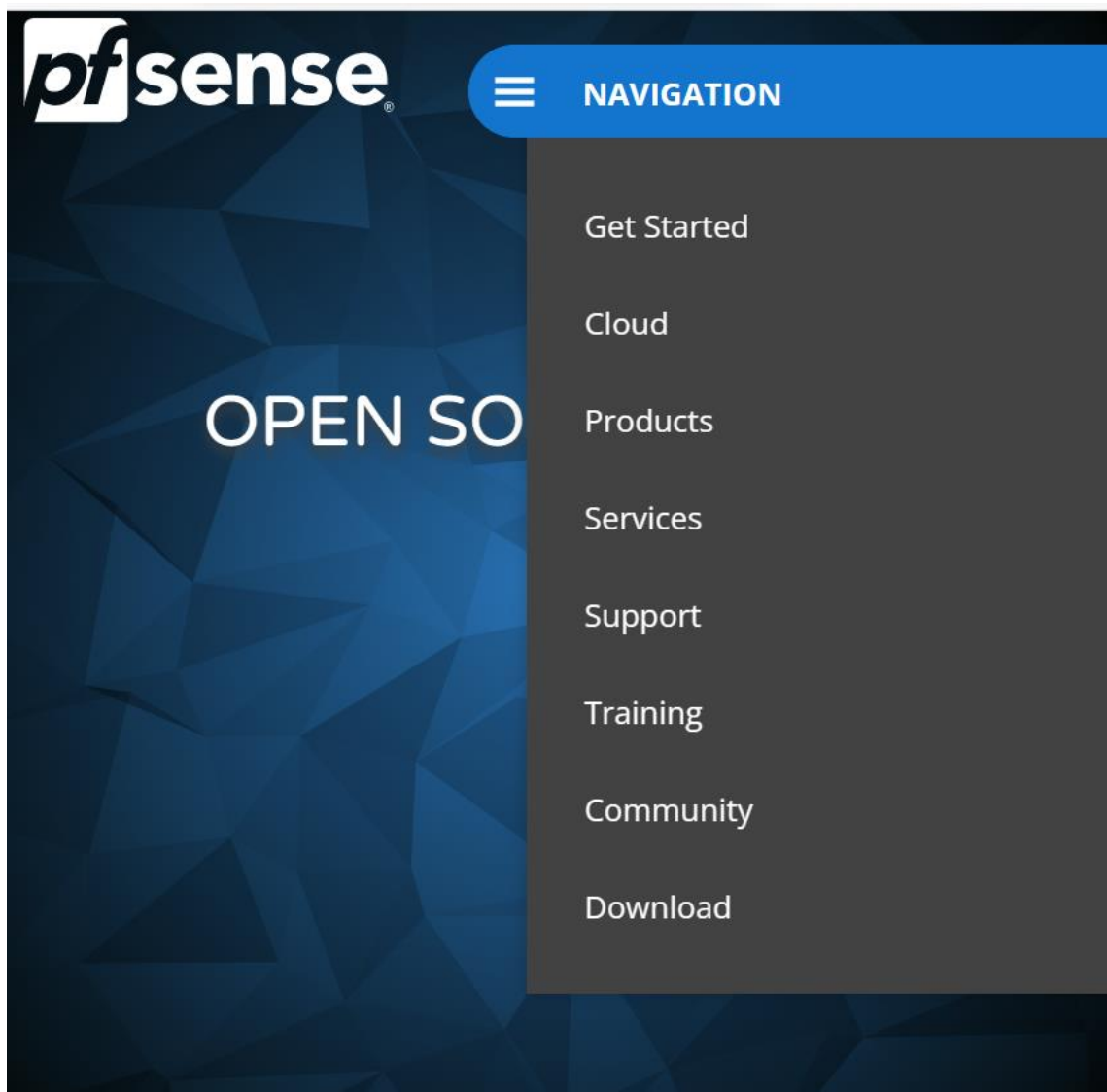
1. VMware workstation
2. pfsense
3. Win 10 OS
4. Ubuntu 64 11

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

Select Image To Download

Version:

2.7.0

Architecture:

AMD64 (64-bit) ?


Installer:


DVD Image (ISO) Installer ?

Mirror:

Austin, TX USA ?

Supported by



 **DOWNLOAD**

[SHA256 Checksum](#) for compressed (.gz) file:
98a14db2746327ab4665610679c9ed7a78091687ee3097036ee9090ee8e33470

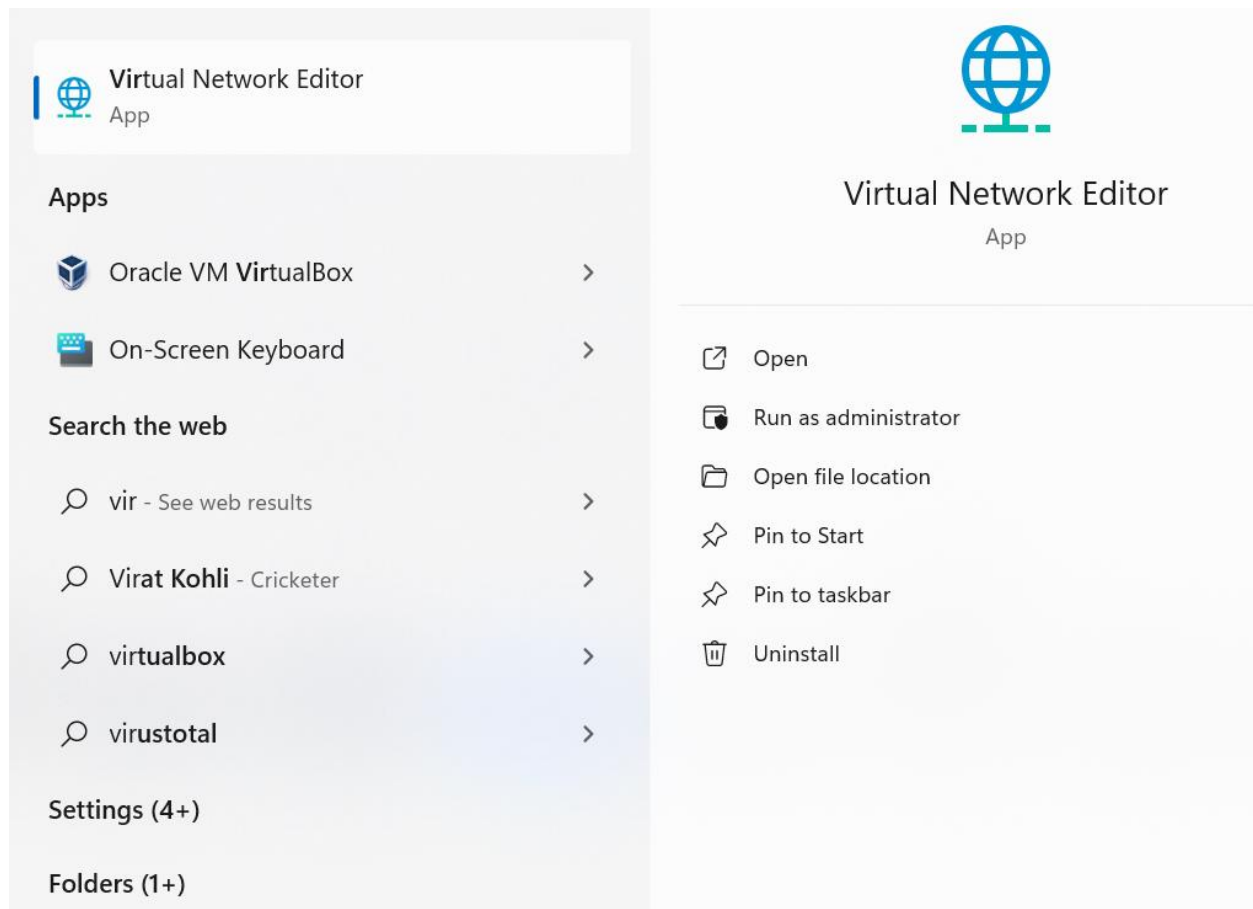
Pfsense will automatically start downloading.

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.

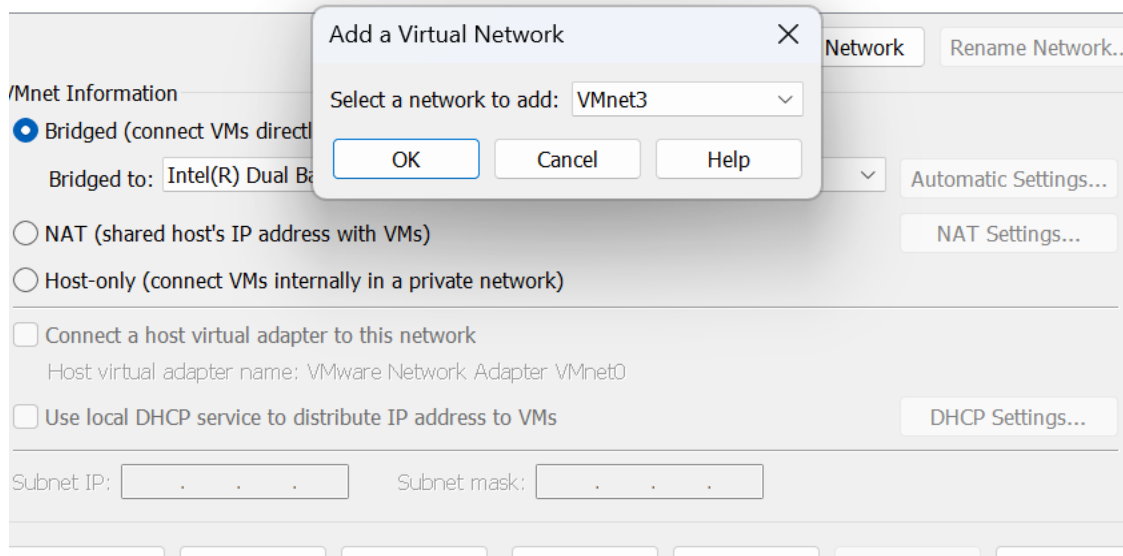
Go to search bar on your taskbar, search Virtual Network Editor

Run as administrator



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

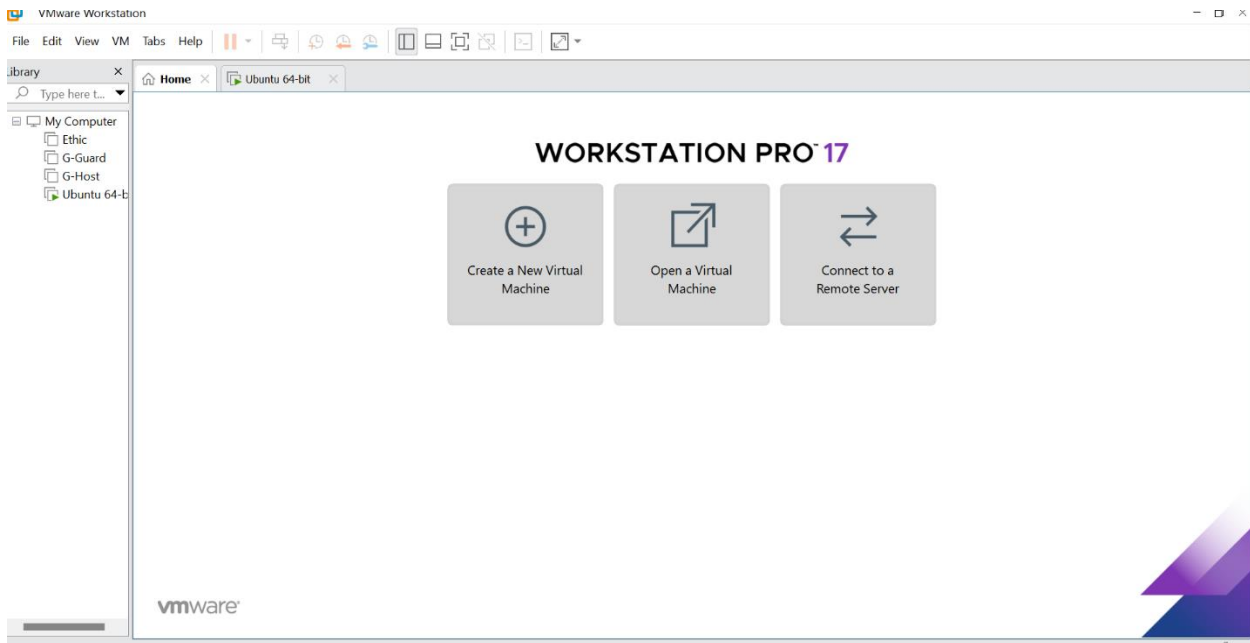
| Name | Type | External Connection | Host Connection | DHCP | Subnet Address |
|--------|-----------|----------------------------------|-----------------|---------|----------------|
| VMnet0 | Bridged | Intel(R) Dual Band Wireless-A... | - | - | - |
| VMnet1 | Host-only | - | Connected | Enabled | 192.168.5.0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



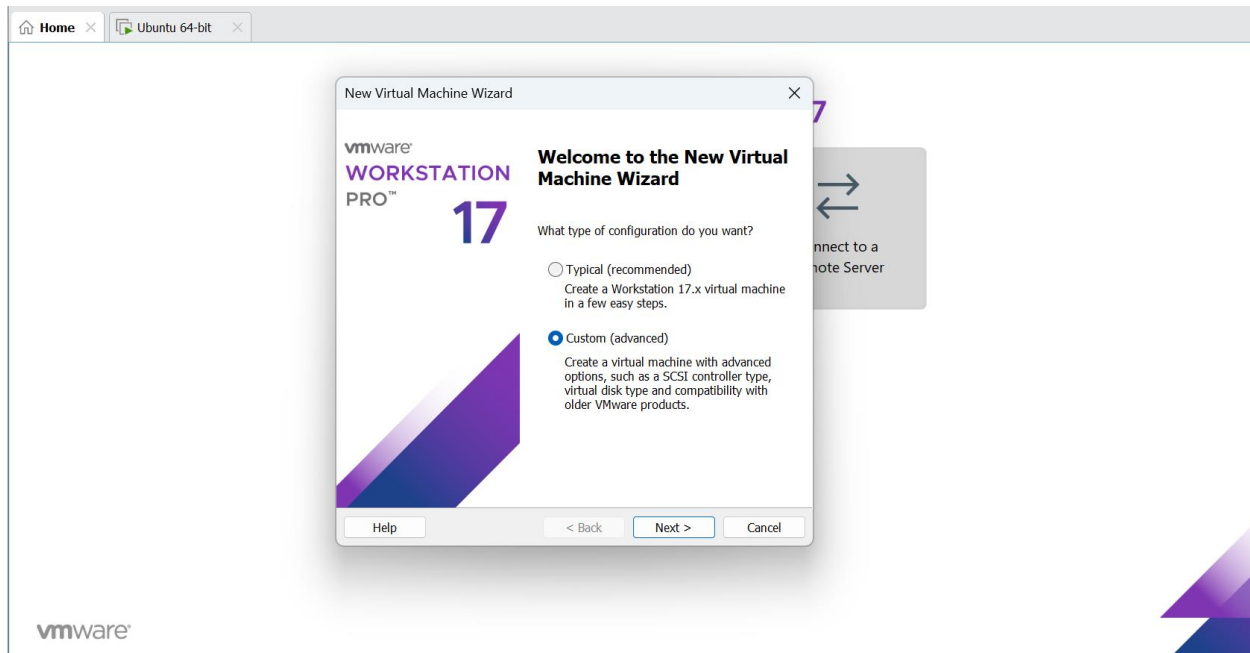
Now make sure you disable local dhcp server then click on apply

Let's get started

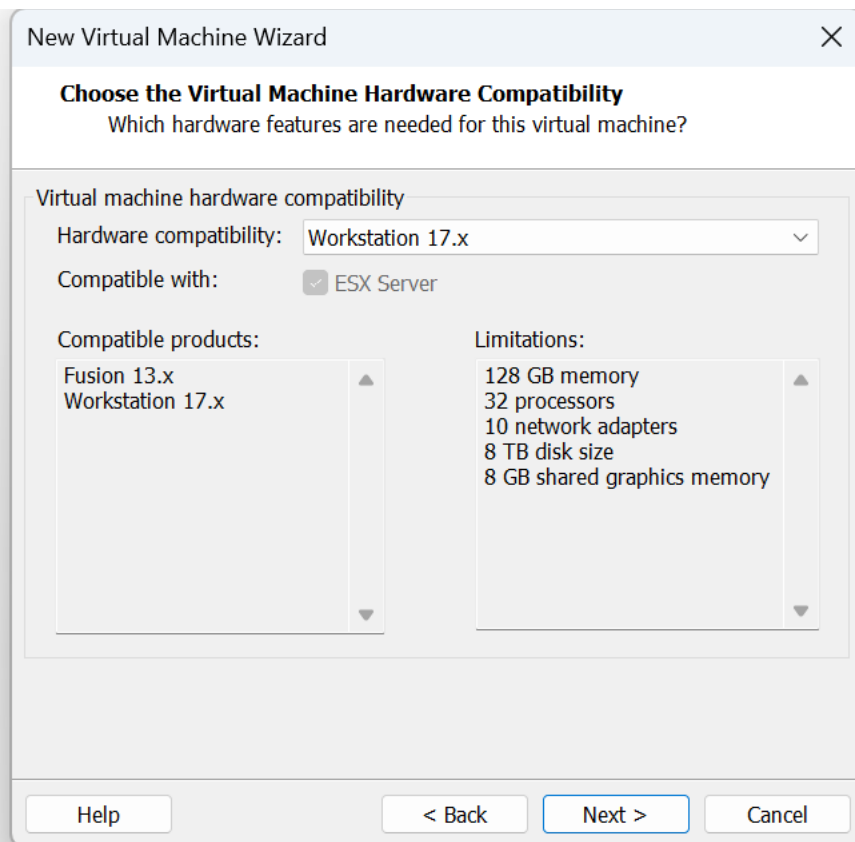
Open VMware workstation



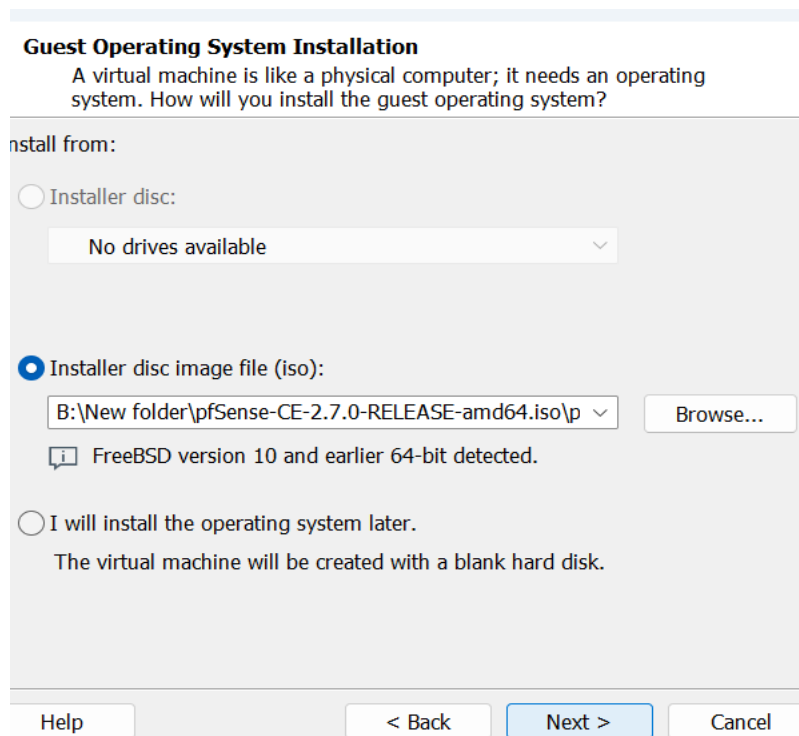
Click on create a New virtual machine



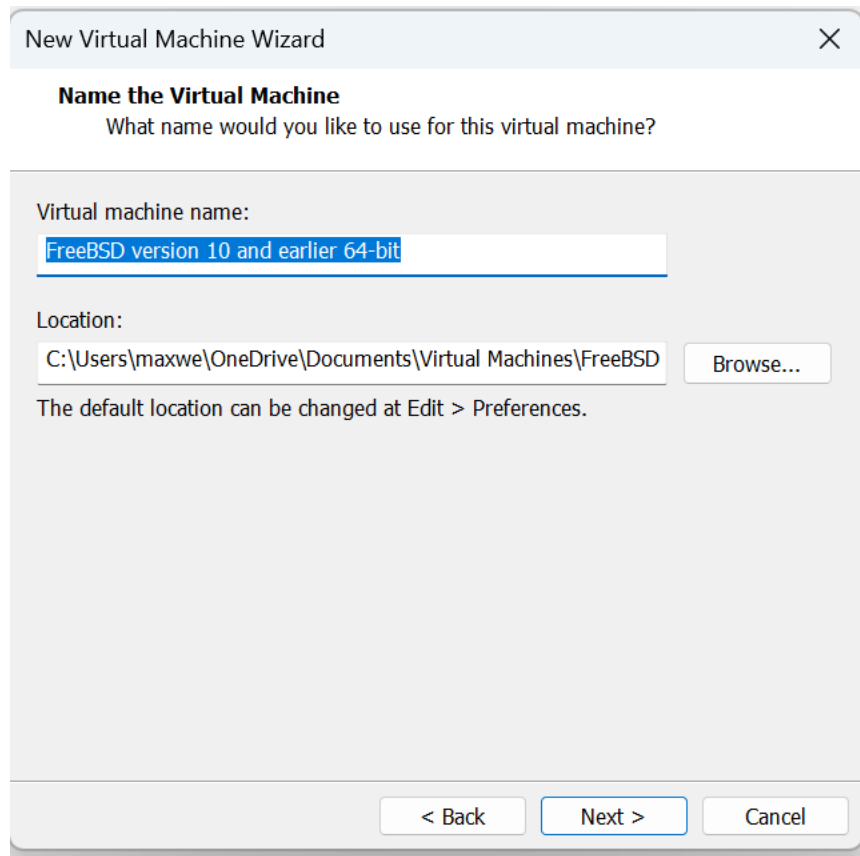
Click on Next



Click on Next

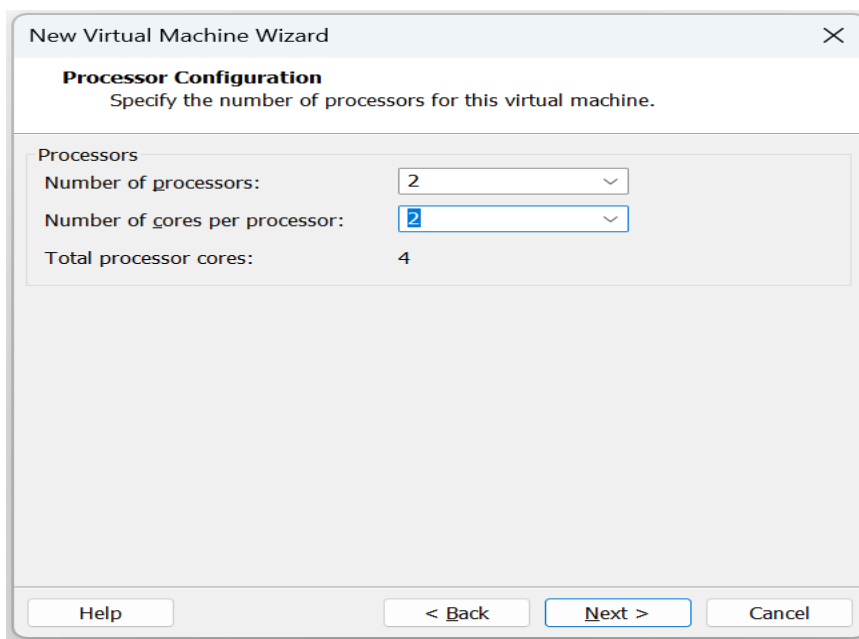


You click on browse to location of the iso file, select the file
Click on Next,



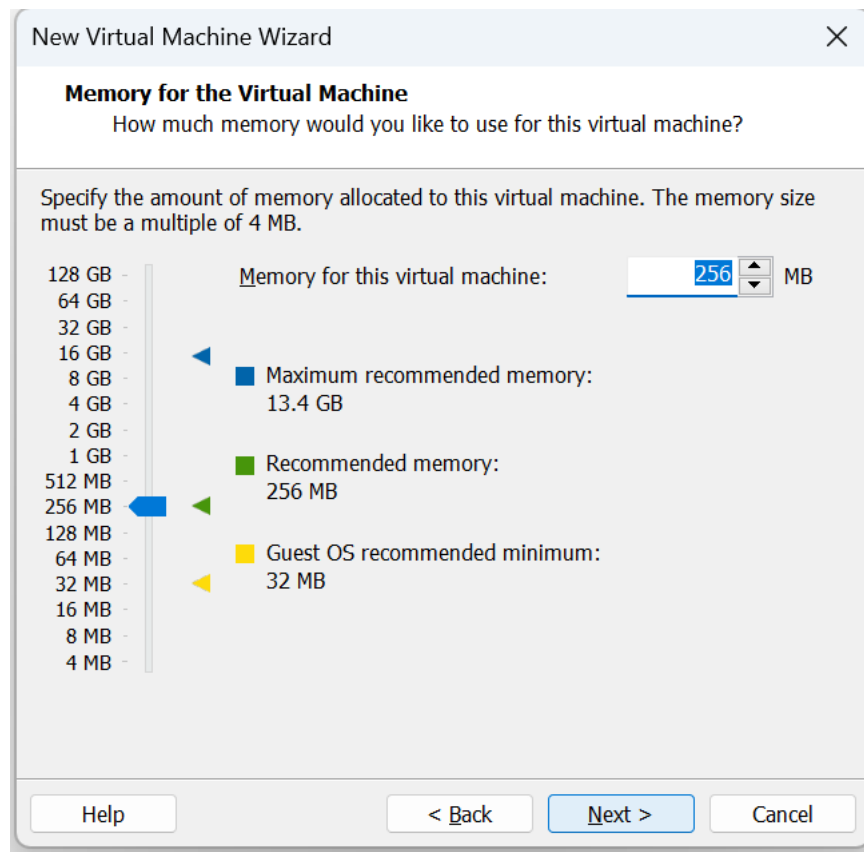
The screenshot shows the 'New Virtual Machine Wizard' dialog box. The title bar says 'New Virtual Machine Wizard' with a close button. The main heading is 'Name the Virtual Machine' with the subtitle 'What name would you like to use for this virtual machine?'. Below this, there is a text field for 'Virtual machine name:' containing 'FreeBSD version 10 and earlier 64-bit'. Below that is a 'Location:' section with a text field showing 'C:\Users\maxwe\OneDrive\Documents\Virtual Machines\FreeBSD' and a 'Browse...' button. A note below the location field states: 'The default location can be changed at Edit > Preferences.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Click on Next,

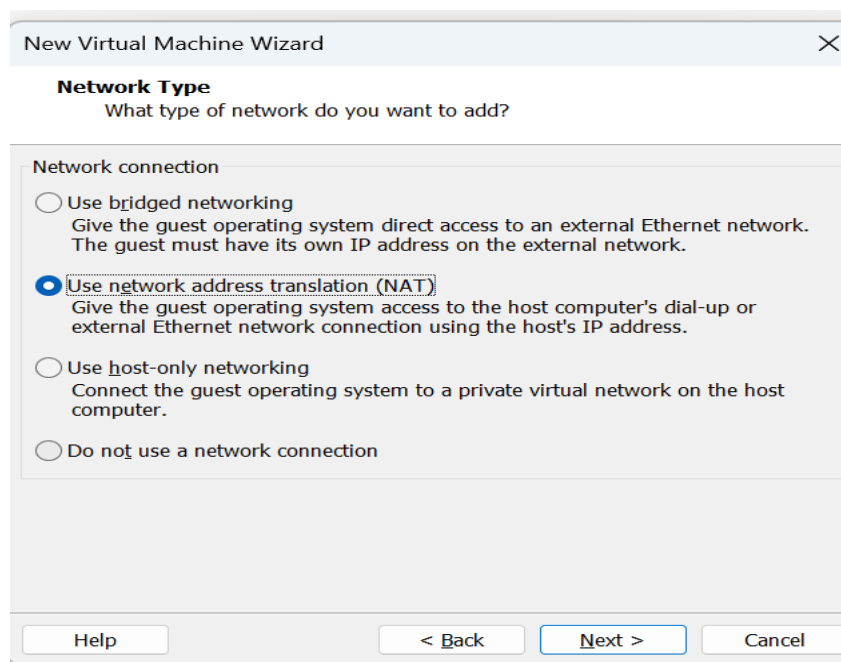


The screenshot shows the 'New Virtual Machine Wizard' dialog box at the 'Processor Configuration' step. The title bar says 'New Virtual Machine Wizard' with a close button. The main heading is 'Processor Configuration' with the subtitle 'Specify the number of processors for this virtual machine.' Below this, there is a 'Processors' section with two dropdown menus: 'Number of processors:' set to '2' and 'Number of cores per processor:' set to '2'. Below these, it shows 'Total processor cores: 4'. At the bottom, there are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

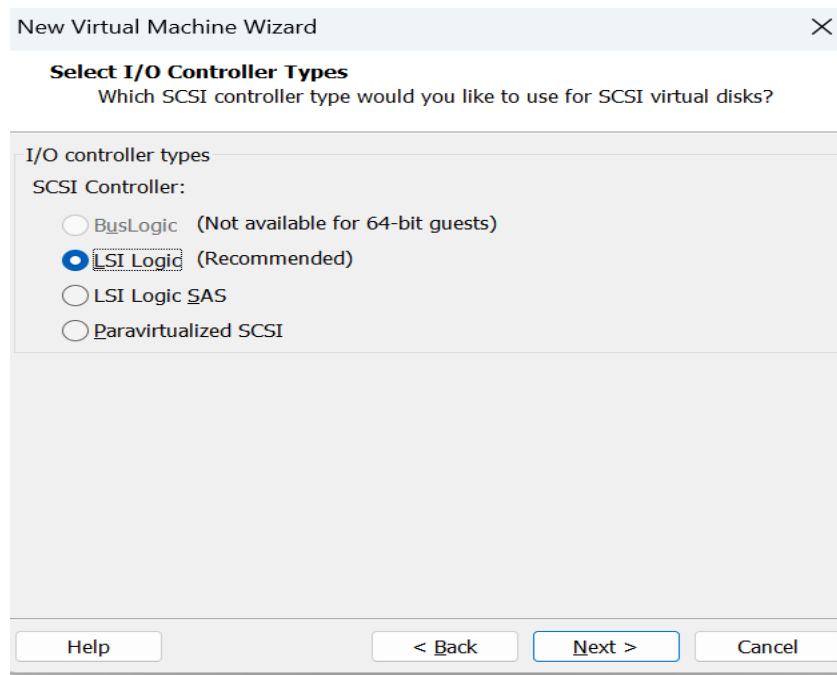
You configure your processor and click Next.



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



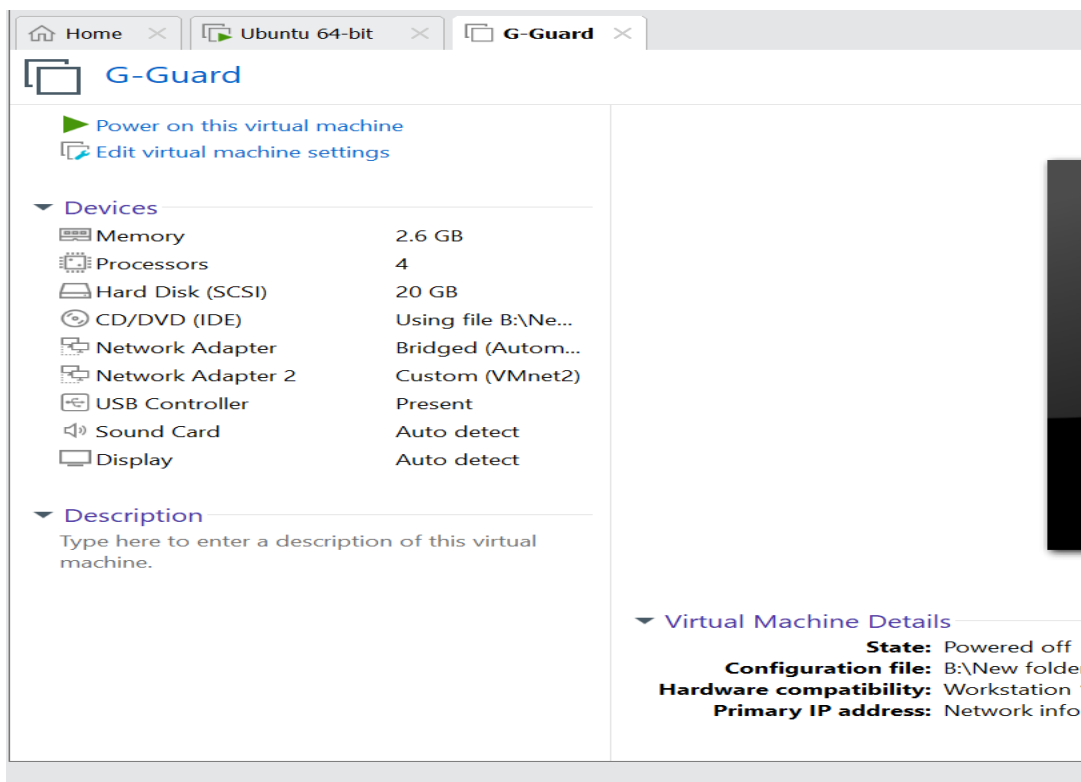
Click on next



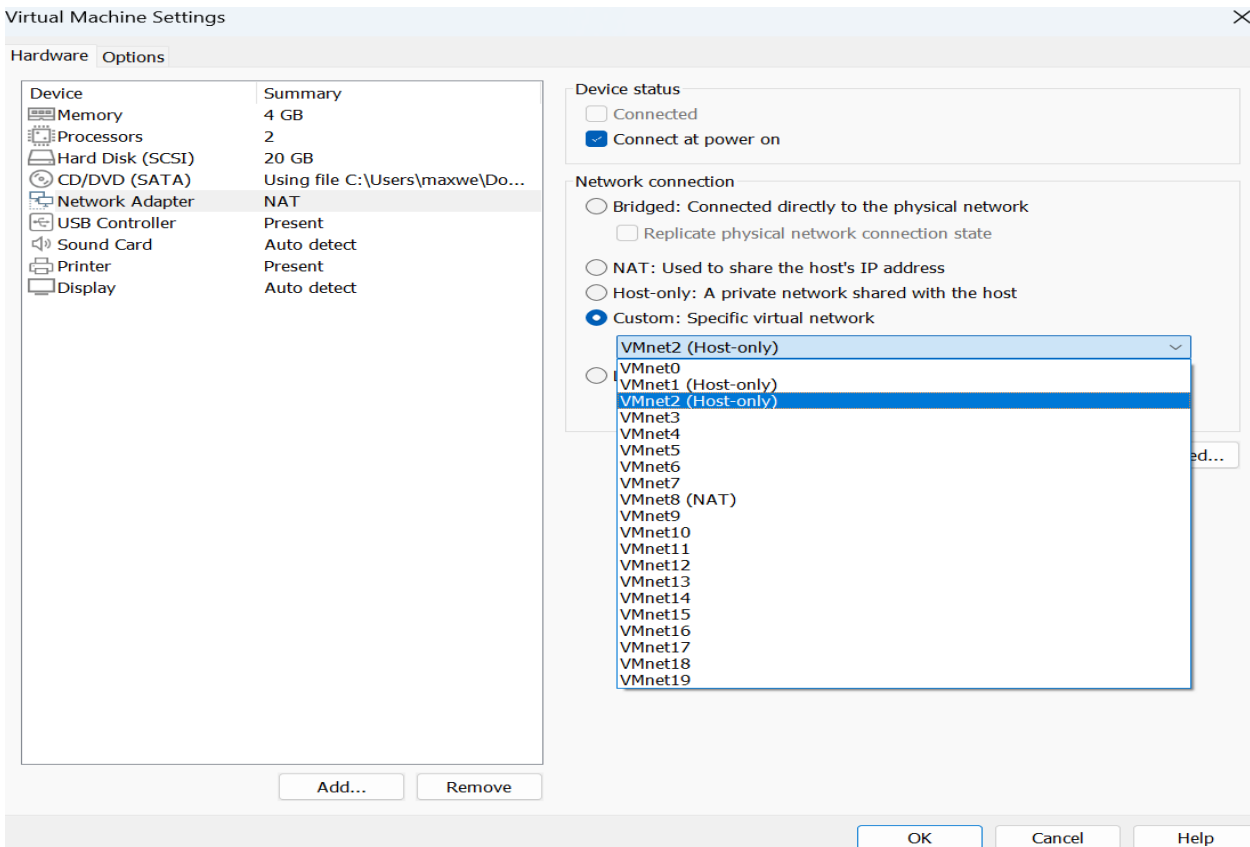
Click on next to all next pages

After pfsense will boot to start running,

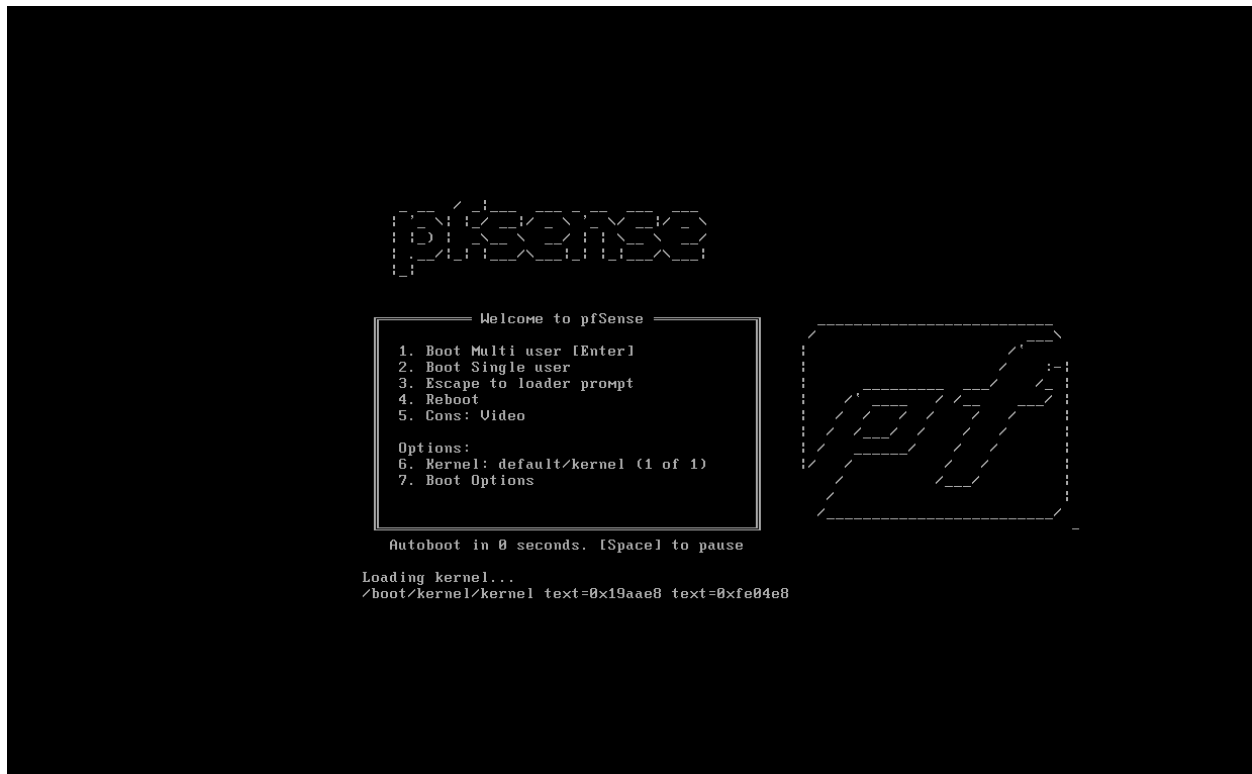
power off the pfsense and click on edit virtual machine settings



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

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (Ethical-tech.eempire.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 0473b083f65c8971955e

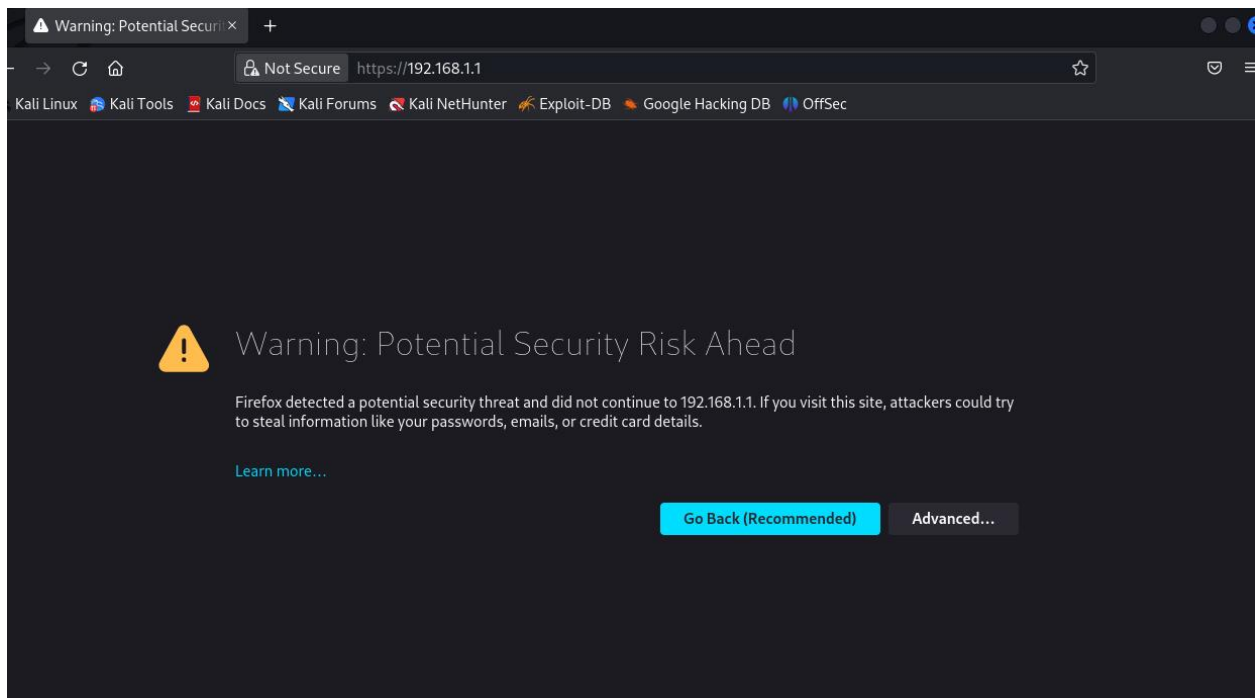
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on Ethical-tech ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.18.58/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

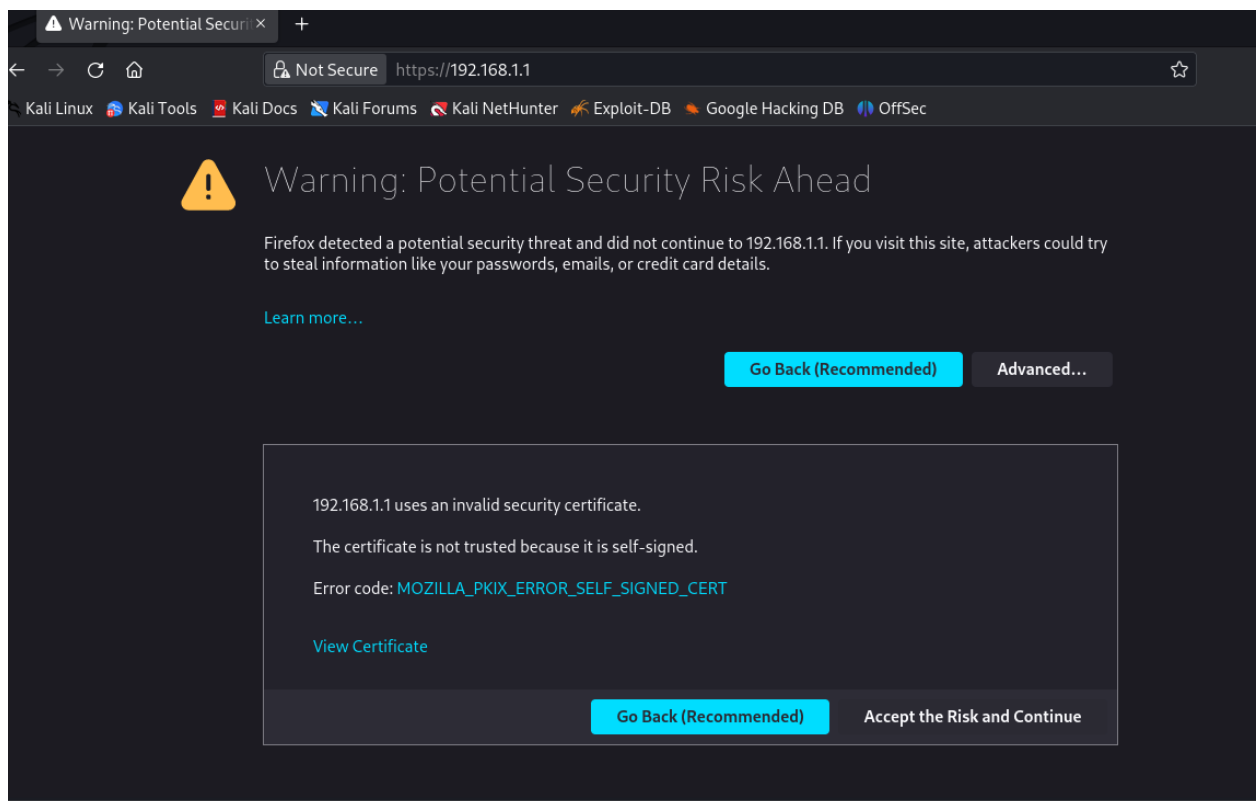
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable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

Enter an option: █
```

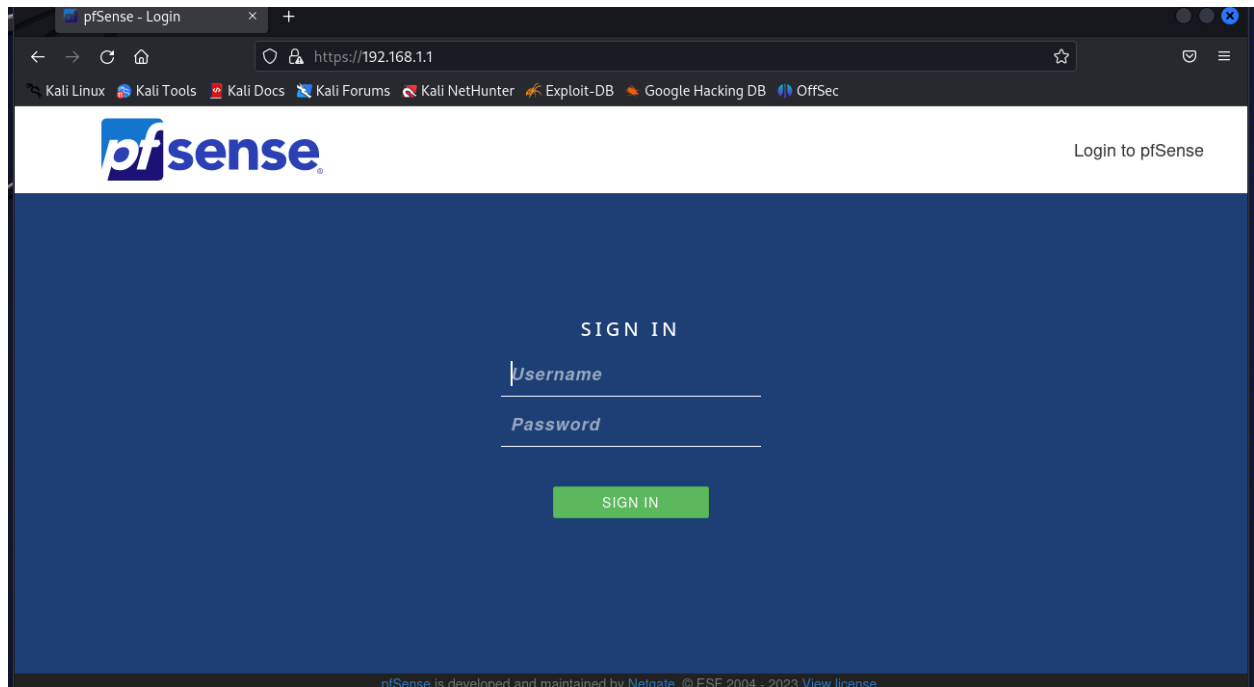

Now go to your browser on your OS configured with specific virtual network (custom) and input the LAN ip address(mine is 192.168.1.1) as shown above



Click on advance



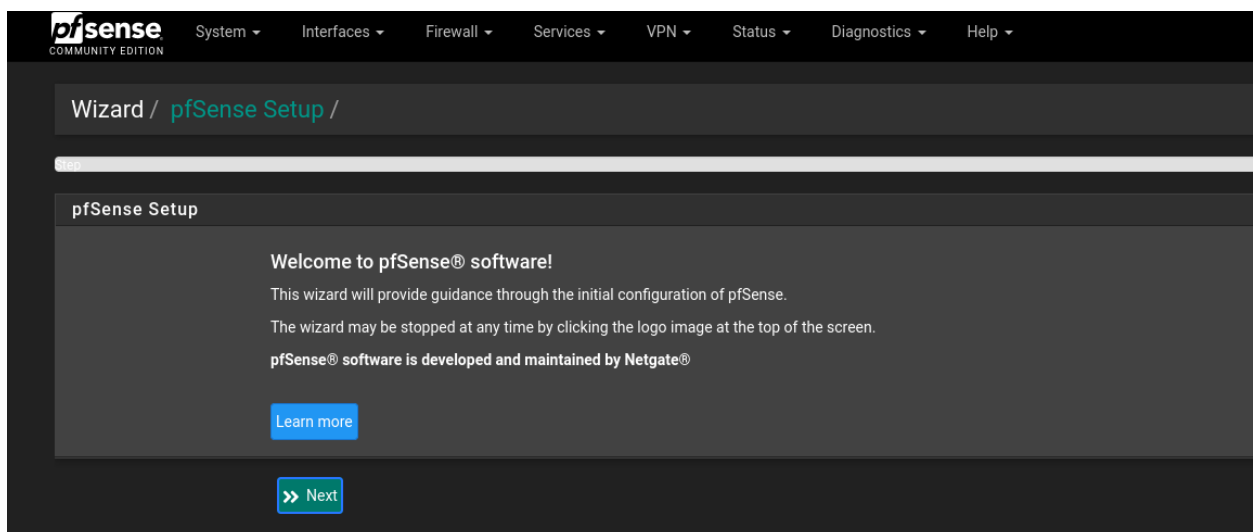
Click on accept the Risk and Continue,



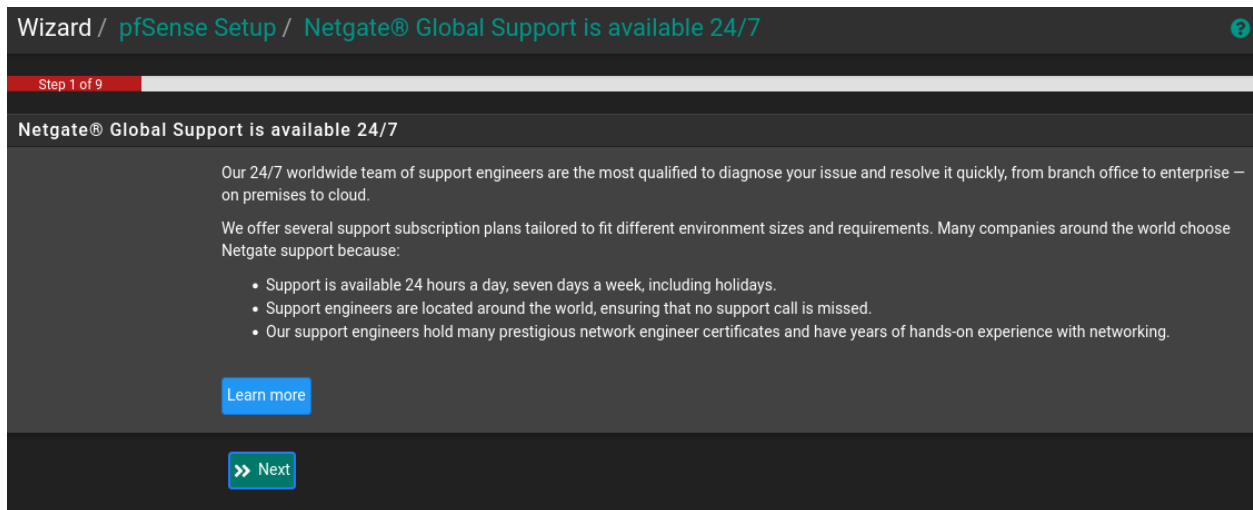
Default log in credentials

Username: admin

Password: pfsense



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



Wizard / pfSense Setup / Netgate® Global Support is available 24/7

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

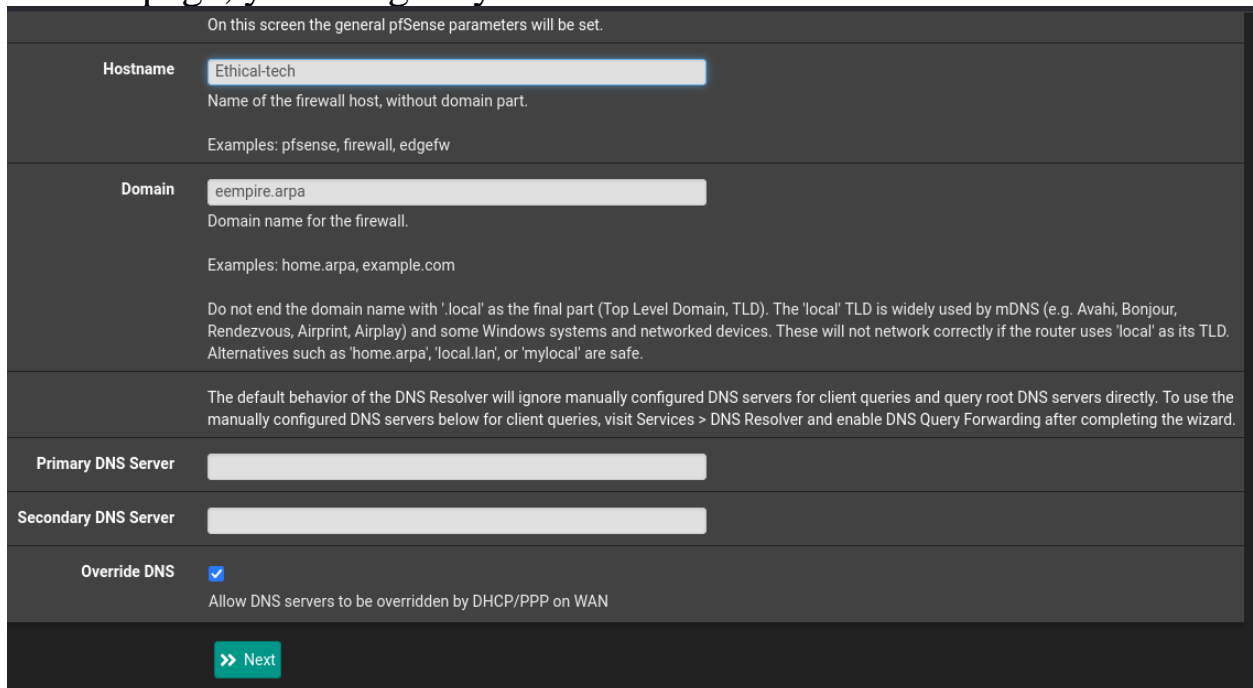
We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

[>> Next](#)

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



On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
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](#)

Click on next

[Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [0wnSec](#)

pfSense
COMMUNITY EDITION

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

Wizard / **pfSense Setup** / Time Server Information ?

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

>> Next

Click on next

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

General configuration

MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

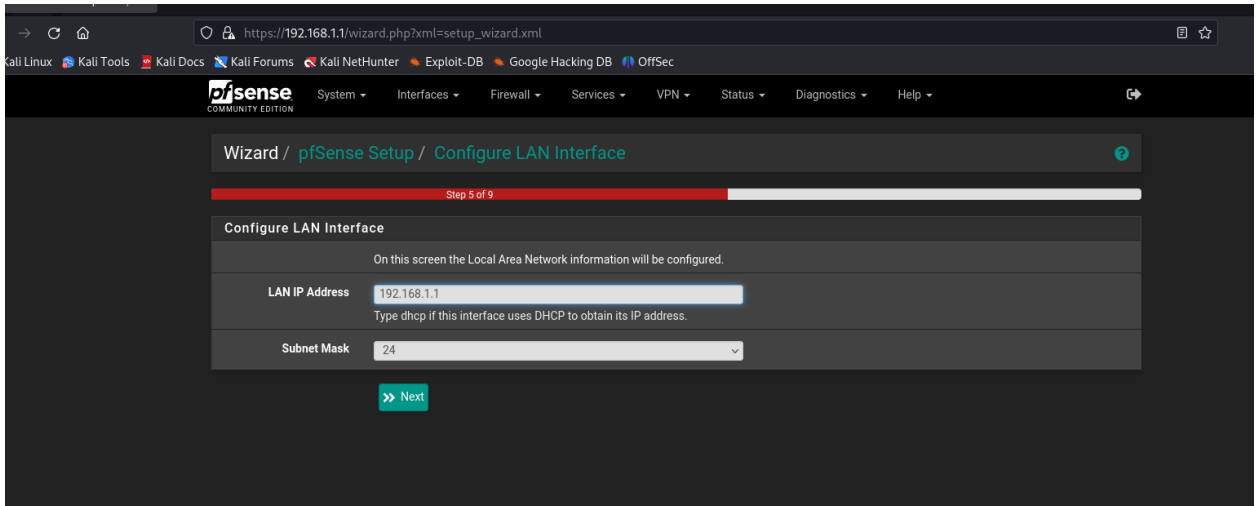
Static IP Configuration

IP Address

Subnet Mask

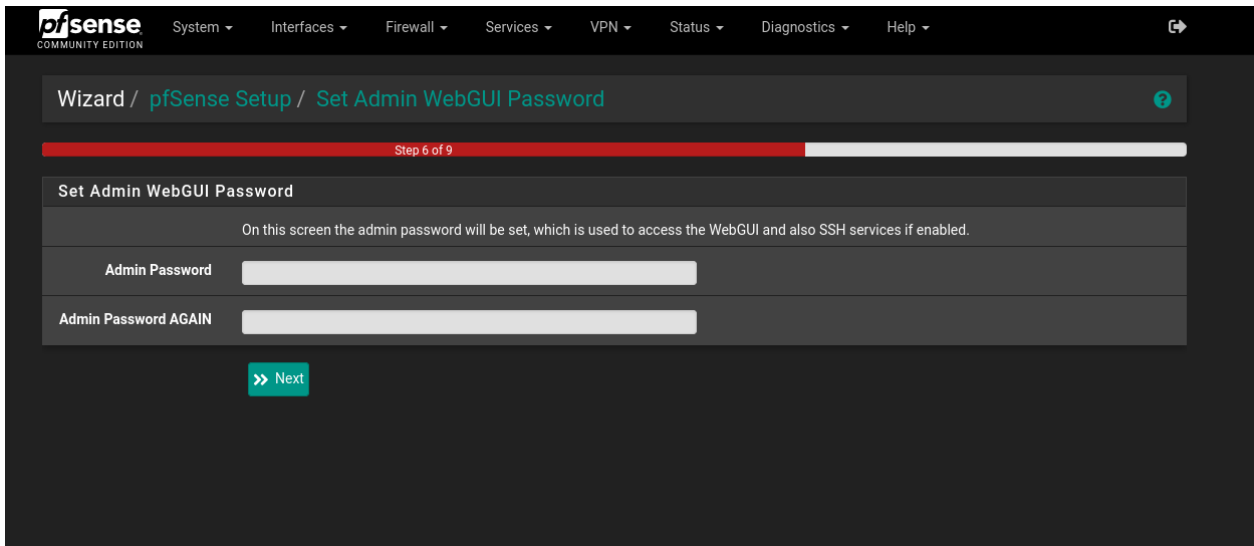
Upstream Gateway

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



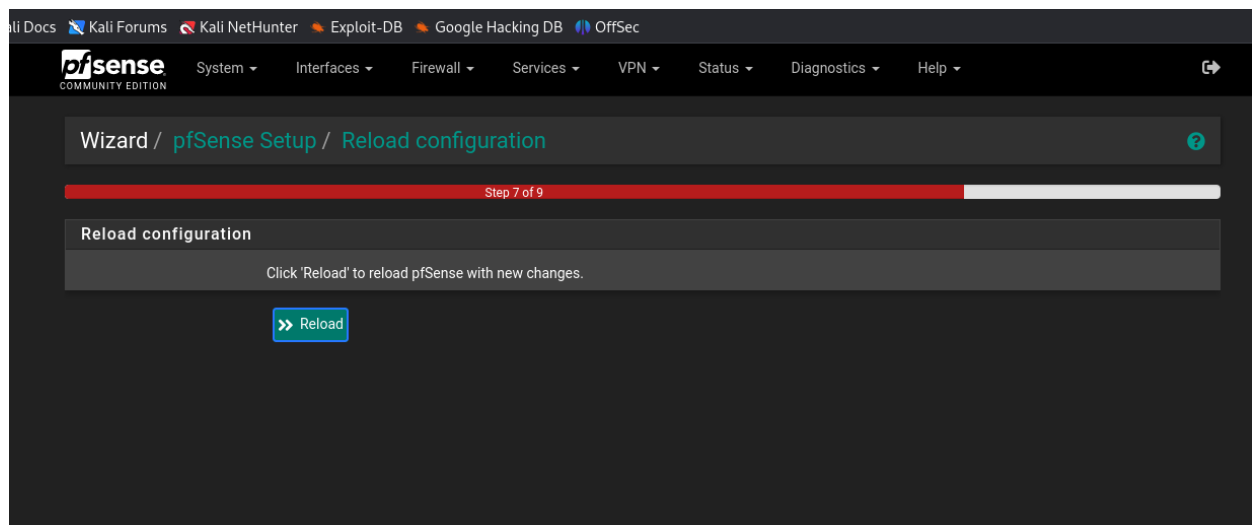
The screenshot shows the pfSense Setup Wizard at Step 5 of 9, titled "Configure LAN Interface". The breadcrumb trail is "Wizard / pfSense Setup / Configure LAN Interface". A progress bar indicates the current step. The main heading is "Configure LAN Interface", followed by the instruction: "On this screen the Local Area Network information will be configured." Below this, there are two input fields: "LAN IP Address" with the value "192.168.1.1" and a subtext "Type dhcp if this interface uses DHCP to obtain its IP address.", and "Subnet Mask" with the value "24". A green "Next" button is at the bottom.

Click on Next,

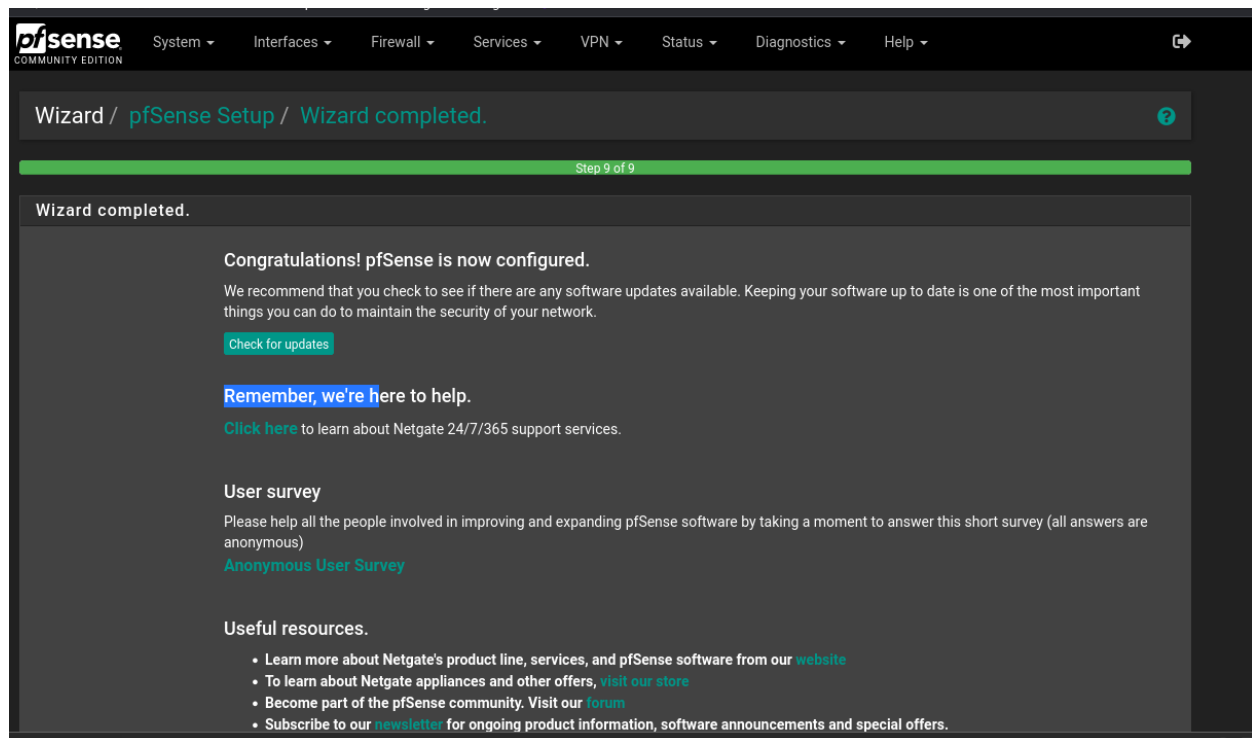


The screenshot shows the pfSense Setup Wizard at Step 6 of 9, titled "Set Admin WebGUI Password". The breadcrumb trail is "Wizard / pfSense Setup / Set Admin WebGUI Password". A progress bar indicates the current step. The main heading is "Set Admin WebGUI Password", followed by the instruction: "On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled." Below this, there are two input fields: "Admin Password" and "Admin Password AGAIN". A green "Next" button is at the bottom.

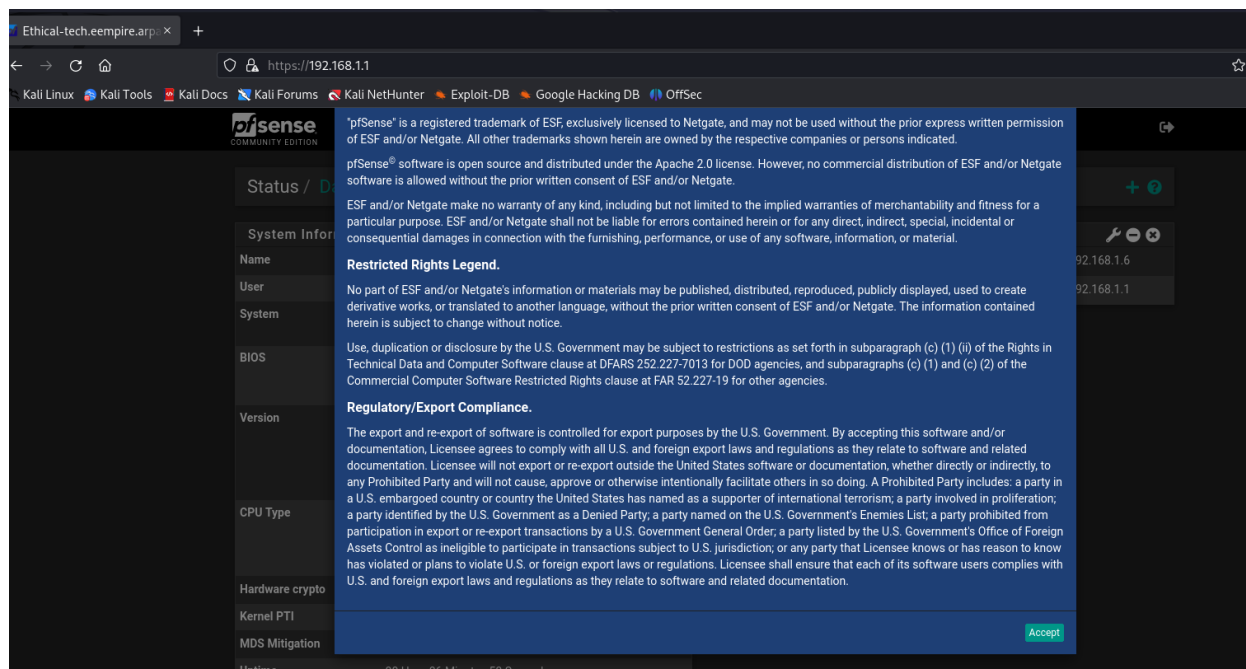
This above page allows you to set password to your preference for security measures.



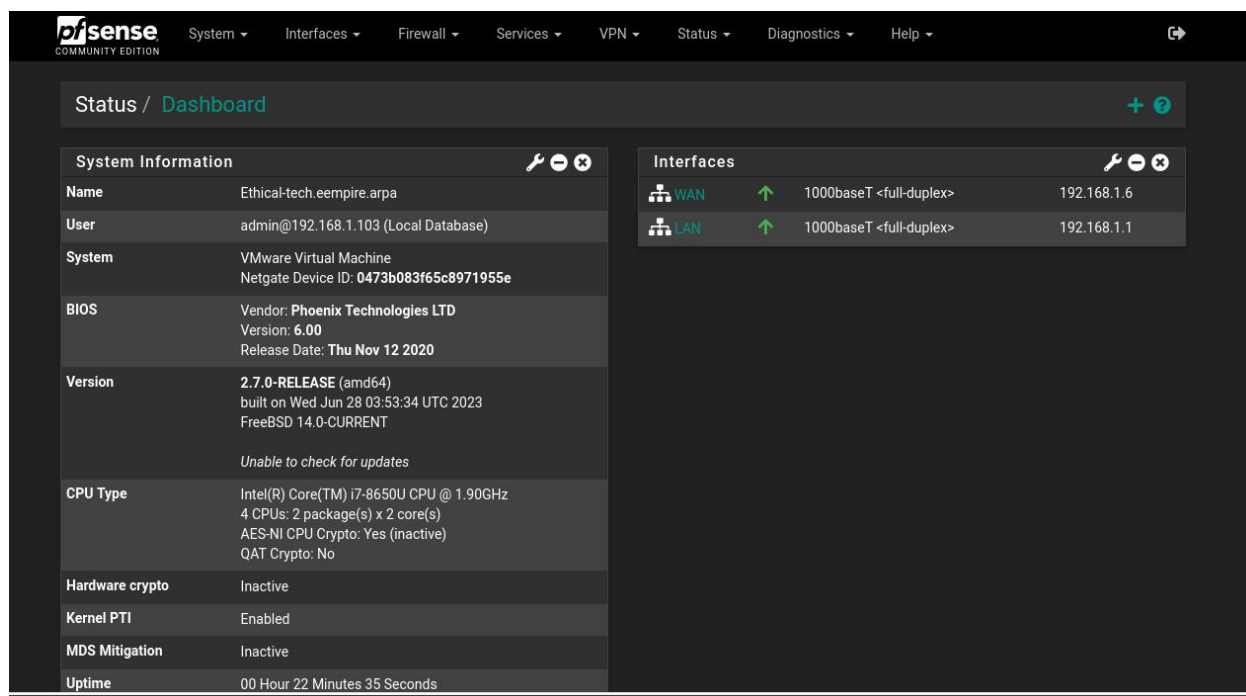
Click on Reload



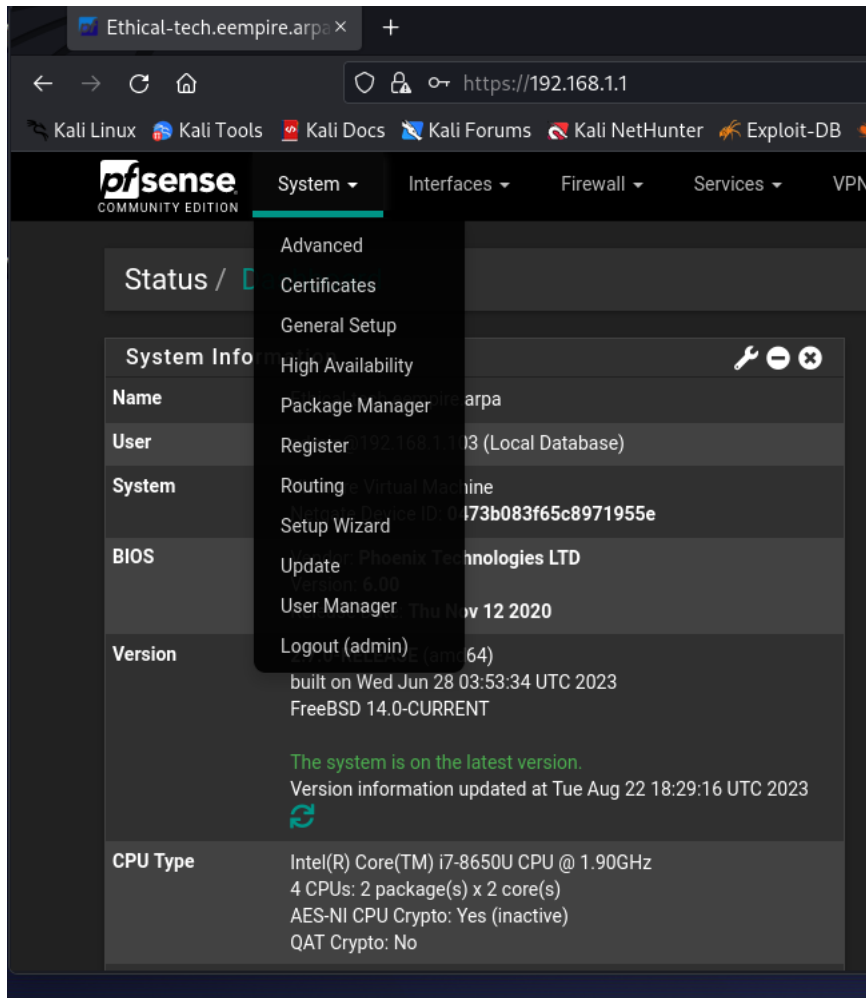
Now you scroll down and you click on finish, it will take you pfSense dashboard and then we can start our configuration



Click on accept



Now we can navigate and see what pfSense contains.

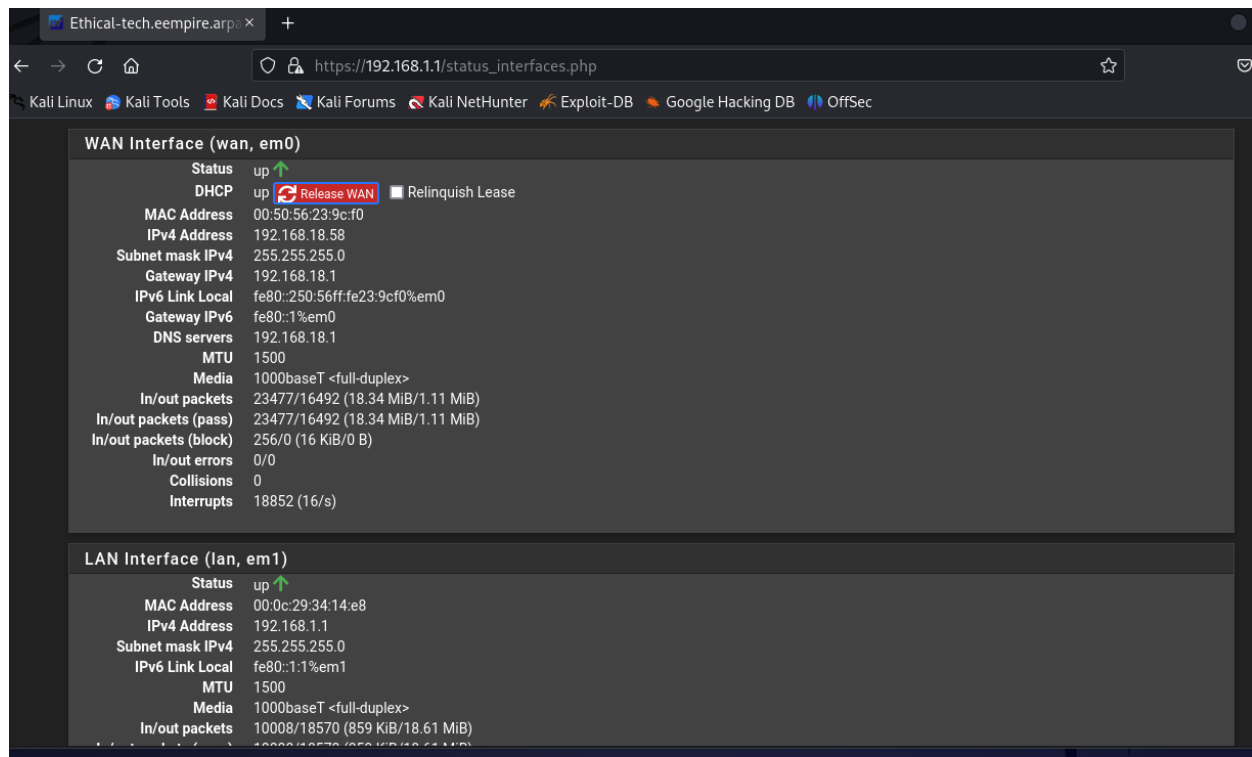


On the above interface you can make any changes to your preference and also add packages from Package Manager, add new user and disable the admin user and many more.

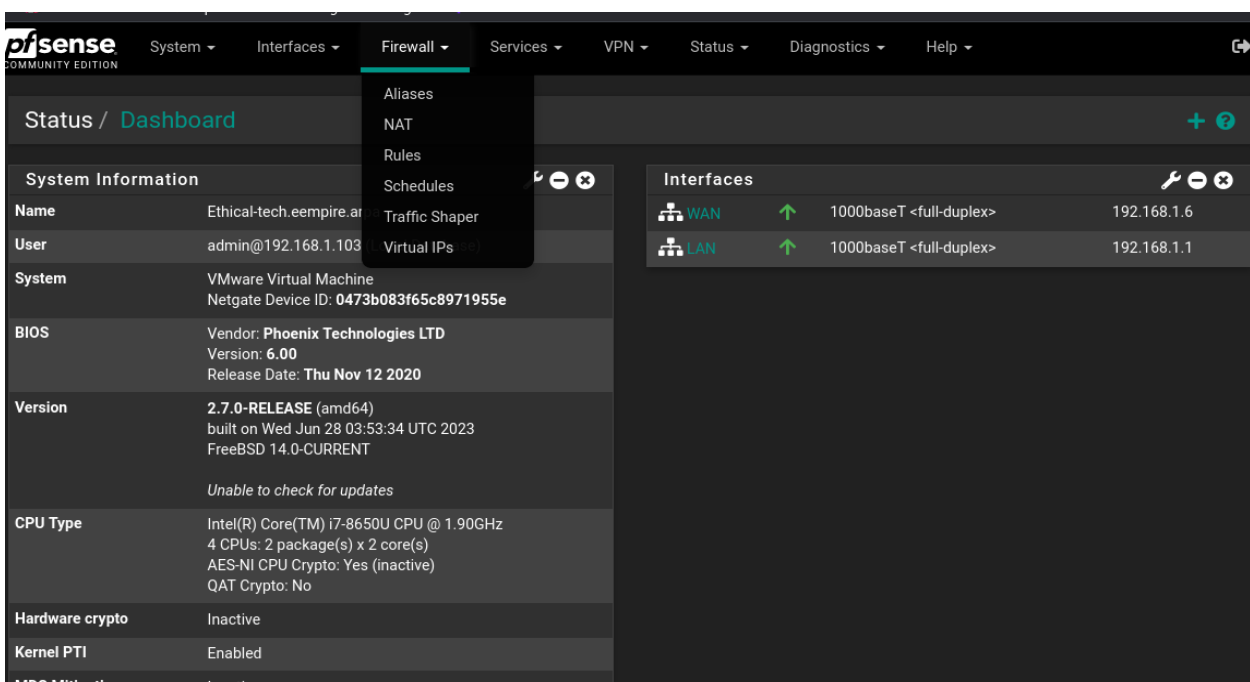
Let gets on to our main aim of this project.

Now we set the firewalls on the various interface (LAN and WAN) to control both ingression and egression of traffic.

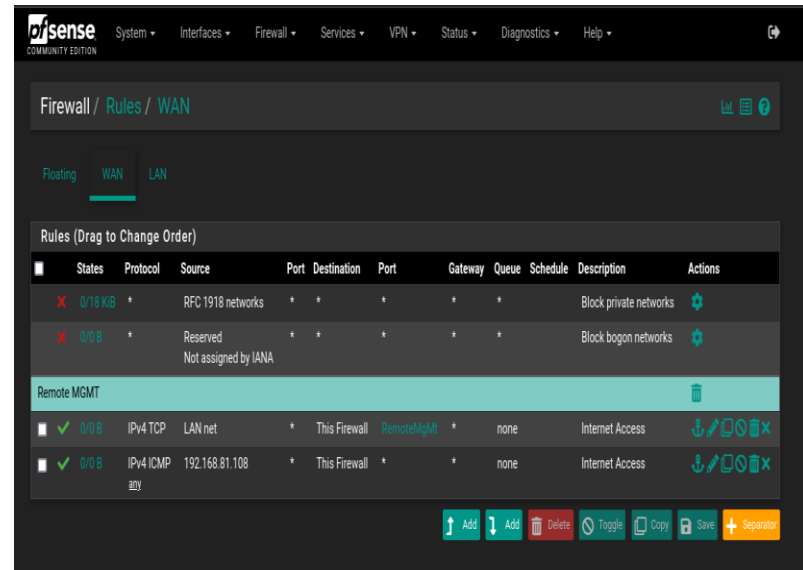
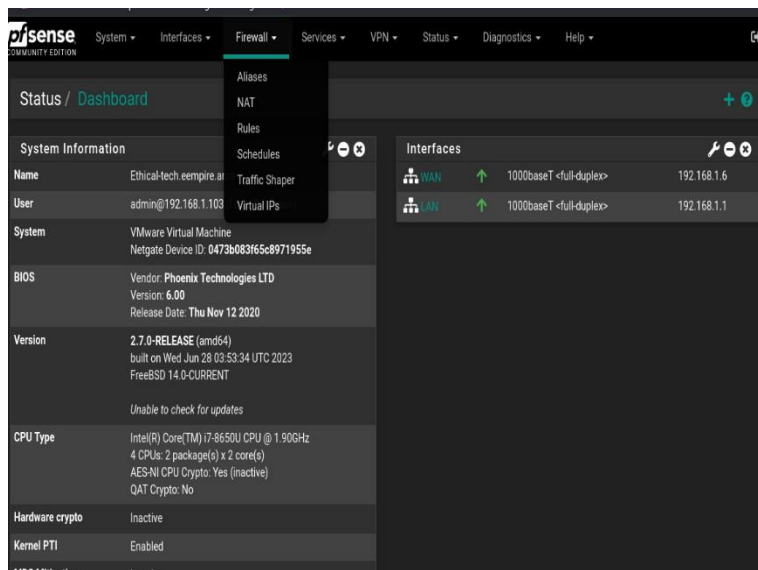
If you want to know your interface navigate to Interface and look at the various interface you have available.



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.

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 WAN
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 TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Single host or alias 192.168.62.103 /

[Display Advanced](#)
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match This firewall (self) Destination Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match This firewall (self) Destination Address /

Destination Port Range (other) RemoteMgMt (other) RemoteMgMt

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

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 Internet Access

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.

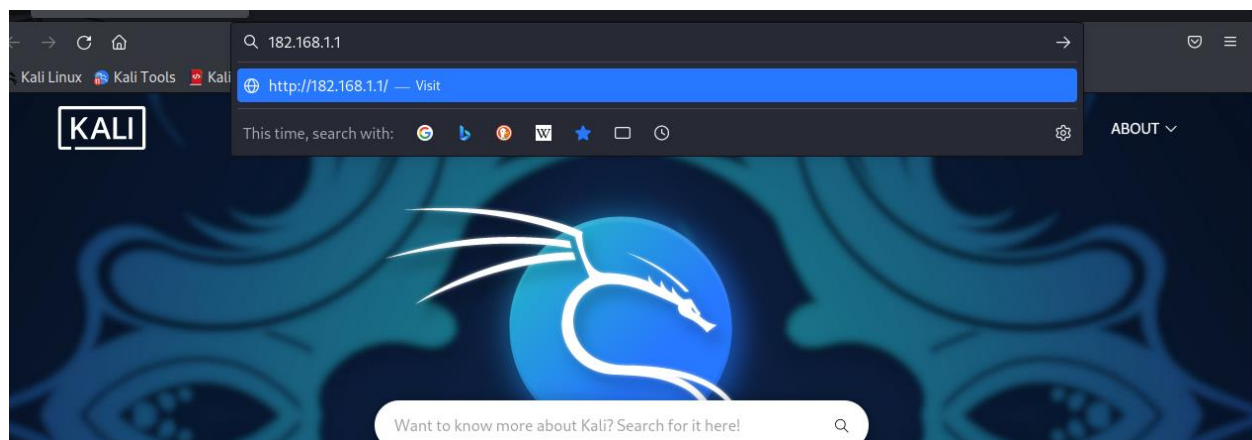
Advanced Options [Display Advanced](#)

Rule Information

| | |
|--------------------|--|
| Tracking ID | 1692785702 |
| Created | 8/23/23 10:15:02 by admin@192.168.1.103 (Local Database) |
| Updated | 8/23/23 10:35:47 by admin@192.168.1.103 (Local Database) |

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

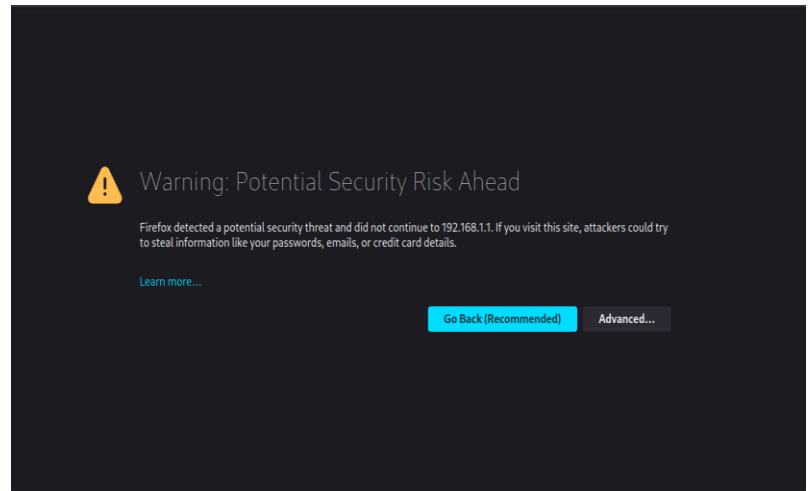
Accessible

click on **Advance**

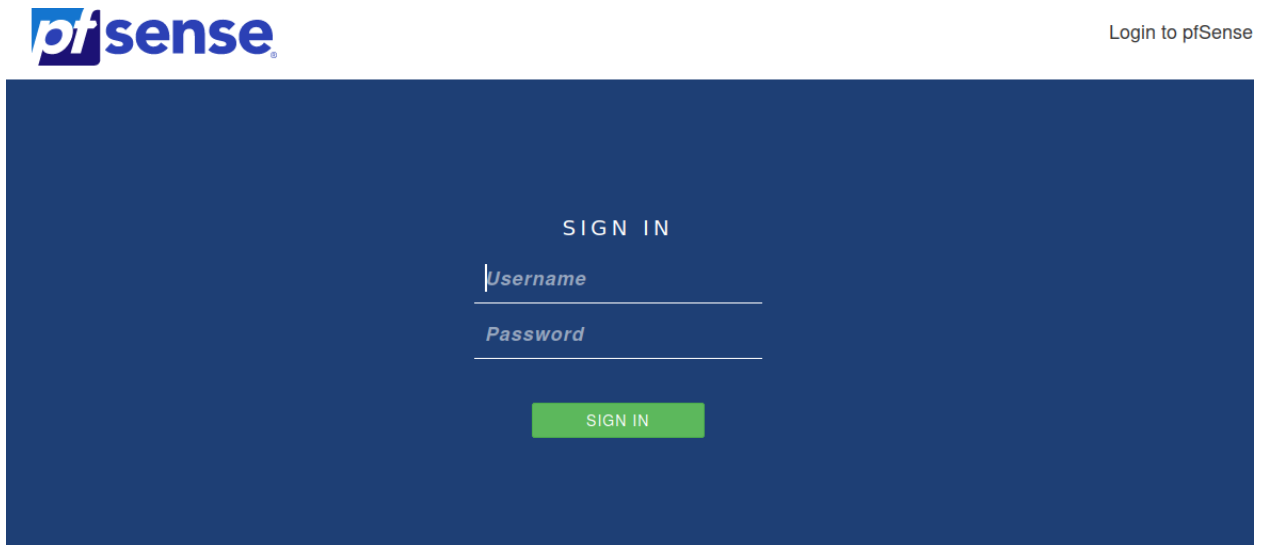
to **accept the risk**

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

Pfsense COMMUNITY EDITION

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

Firewall / Rules / Edit

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 WAN ▾
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 TCP ▾
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Single host or alias ▾ 192.168.1.102 / ▾

[Display Advanced](#)

Destination

Destination ☐ Invert match This firewall (self) ▾ Destination Address / ▾

Destination Port Range DNS over TLS (853) ▾ From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

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 Internet Access
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.

Advanced Options [Display Advanced](#)

Rule Information

| | |
|-------------|--|
| Tracking ID | 1692785702 |
| Created | 8/23/23 10:15:02 by admin@192.168.1.103 (Local Database) |
| Updated | 8/27/23 17:38:18 by admin@192.168.1.103 (Local Database) |

[Save](#)

Now let try to see if we can ping it again

On our ubuntu server

```
(max@kali)~]$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.

```

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](#)