CY3001-Networks and Cyber Security-II

Course Instructor: Sir Shoaib Raza

PFsense Implementation

Group Members:

Ayan Mohammad Zakriya K224728

Sami-Ur-Rehman K224673

Table of Contents

1. Abstract

This project demonstrates the setup and configuration of PFsense, a free and open-source firewall/router software distribution based on FreeBSD. The aim is to simulate and secure network traffic within a virtualized environment using Windows 11 and VirtualBox. Key components include IP assignment for LAN/WAN interfaces, DHCP configuration, firewall rule implementation, SSH access, and package installations like ARPing. The project highlights a hands-on approach to network policy enforcement and system monitoring.

2. Introduction

PFsense is a powerful open-source platform for firewall and routing solutions. This project uses a Windows 11 VM environment with NAT adapters to simulate real-world network configurations. By leveraging PFsense, the goal is to secure virtual network communications, monitor system health, and enforce customizable policies for better network hygiene and access control.

3. Policy Implementation

In this project, several security and access control policies were enforced using PFsense:

1. Static IP configuration was applied to both LAN and WAN interfaces for consistent routing. The PFsense interface was accessed through the terminal and LAN IP was updated to 192.168.88.100/24 using option 2 in the interface configuration menu (**Figure 11**).
2. A DHCP service was enabled on the LAN side to assign dynamic IP addresses within a controlled range, specifically from 192.168.88.151 to 192.168.88.200 (**Figure 14**). This allowed client devices within the LAN to communicate without requiring static IP assignment.
3. Firewall rules were implemented through the PFsense GUI to filter traffic. Custom rules were added to control access between interfaces and manage port forwarding (**Figure 27**).
4. SSH access was enabled through the GUI to allow secure terminal access to the PFsense system (**Figure 25**). The GUI was further customized by assigning a non-standard port (11443) for HTTPS access (**Figure 24**).
5. To simulate user access control, a non-administrative user named *Ayan* was created via the user manager (**Figure 31**), and SSH of admin login was tested from the Windows host (**Figure 32**).
6. System monitoring tools like ARPing were installed to support ARP-level diagnostics and monitor connectivity within the LAN (**Figure 30**). Corresponding logs were inspected using the PFsense terminal to ensure policies were being enforced as expected (**Figure 33**).

4. Configuration

4.1 Installation of PFsense

The installation used the guided UFS method with GPT partitioning. Once completed, PFsense was rebooted and the interfaces (WAN and LAN) were configured automatically. At this point, PFsense displayed its default WAN IP (192.168.191.132) and LAN IP (192.168.1.1) (**Figure 8**).

4.2 Network Setup (LAN/WAN)

The VM was configured with NAT (for WAN) and internal network (for LAN) adapters (see **Figure 1**). The LAN IP was changed manually to 192.168.88.100/24 to enable proper communication (see **Figure 11**). A DHCP pool was configured (see **Figure 14**), and the Windows VM received IP 192.168.88.129 (see **Figure 16**). Successful ping and web login tests validated the setup (see **Figure 17**, **Figure 18**).

4.3 Web Access and Dashboard Customization

Accessed the GUI via browser at 192.168.88.100:11443. The setup wizard was completed (see **Figure 21**), and widgets were added to the dashboard showing gateway status and traffic flow (see **Figure 22**, **Figure 23**).

4.4 Firewall Rules and Routing

Custom rules were added to restrict or allow specific traffic (see **Figure 27**). The routing table and ARP table were reviewed for correct packet forwarding (see **Figure 26**, **Figure 28**).

4.5 SSH and Port Configuration

To ensure secure remote access, SSH was enabled from the PFsense GUI (**Figure 25**). Additionally, the web GUI port was changed from default 443 to 11443 (**Figure 24**) to demonstrate port redirection and reduce attack surface (**Figure 42 & 43**).

4.6 Package Installation

The ARPing package was installed to allow sending ARP packets and diagnosing Layer 2 connectivity issues between devices (**Figure 30**).

4.7 User Management

To enforce user privilege policies, a new user named *Ayan* was created without administrative rights (**Figure 19**). SSH login was successfully performed using this account from a Windows command prompt (**Figure 20**), and corresponding activity was visible in the PFsense system logs (**Figure 21**).

Conclusion

This project successfully demonstrated the deployment and secure configuration of PFsense in a virtualized environment. Through LAN/WAN IP assignment, firewall policy implementation, service configuration, and user access control, PFsense proved to be a flexible and powerful tool for managing network security. Future work can include VPN setup, traffic shaping, and integration with external monitoring systems.

References

- PFsense Documentation
- VirtualBox Networking Guide
- https://www.youtube.com/watch?v=Ayr_av2EX_U&t=296s

Figure References

- Getting started with windows 11 and adding and additional Nat Adapter to config Wan & Lan

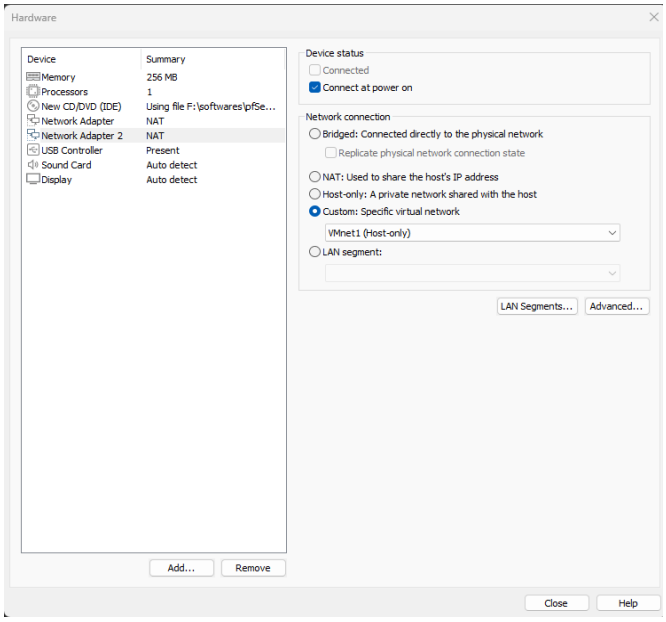

Figure 1

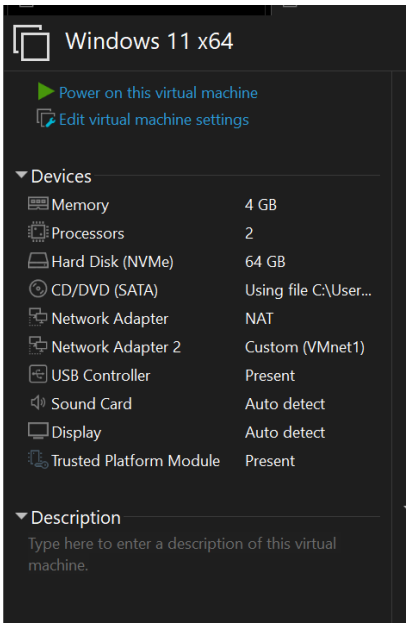

Figure 2

- Now with PFsense and adding and additional Nat Adapter to config Wan & Lan

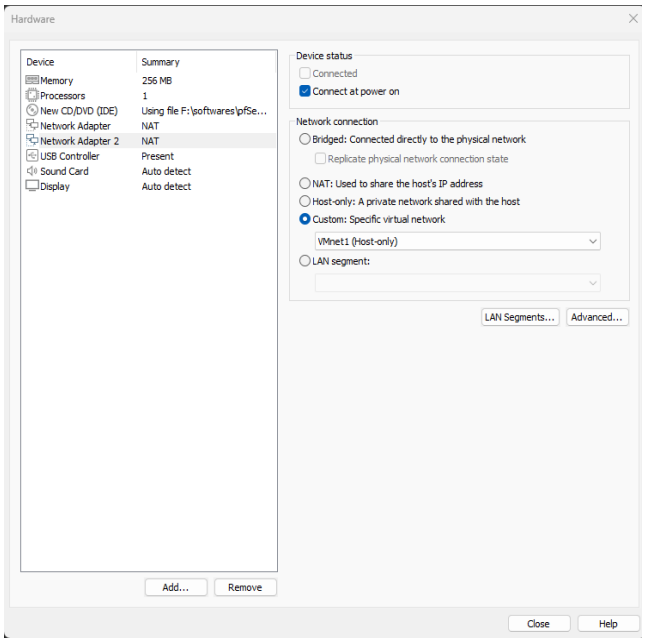

Figure 3

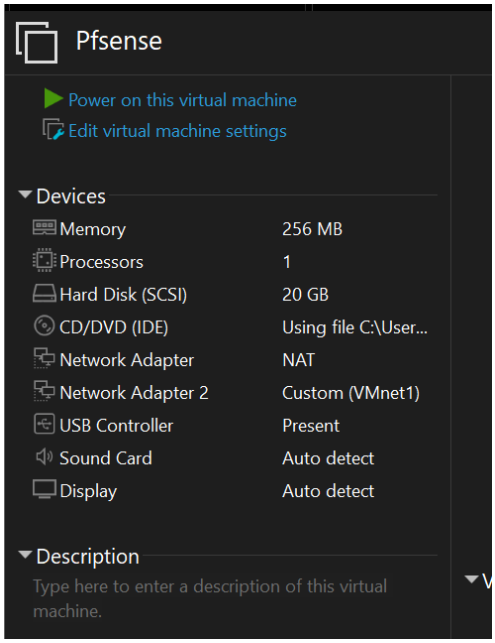

Figure 4

- Network address of Lan 192.168.88.0 and Wan 192.168.191.0

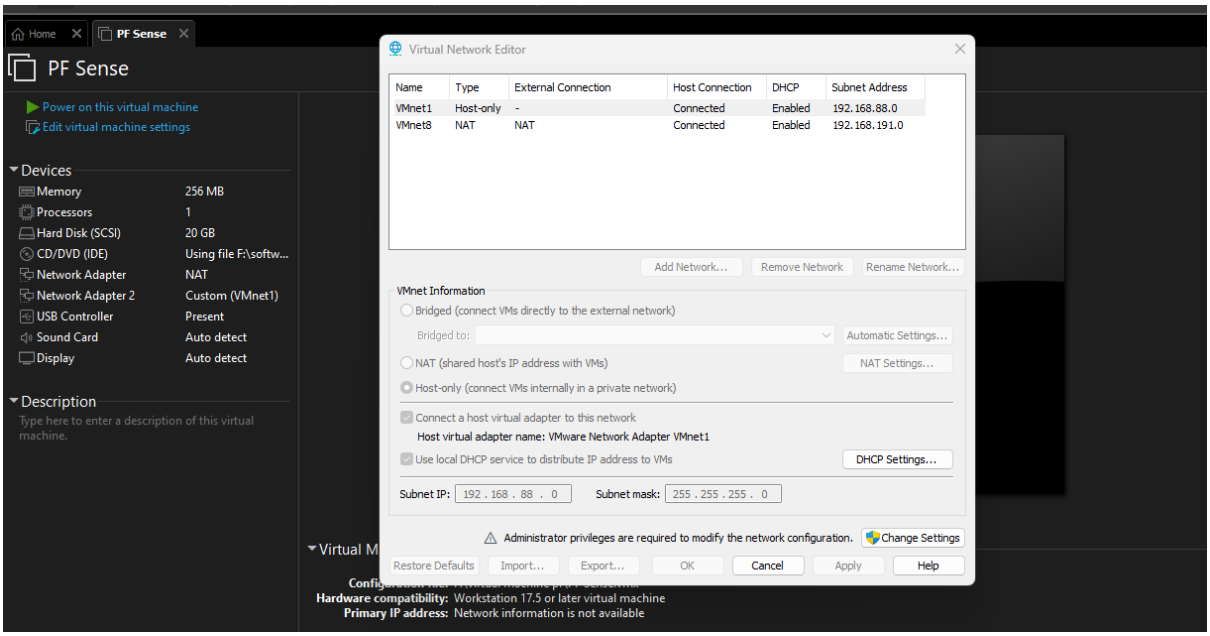

Figure 5

Installation Process of PFsense

- we'll go for Guided UFS Disk Setup

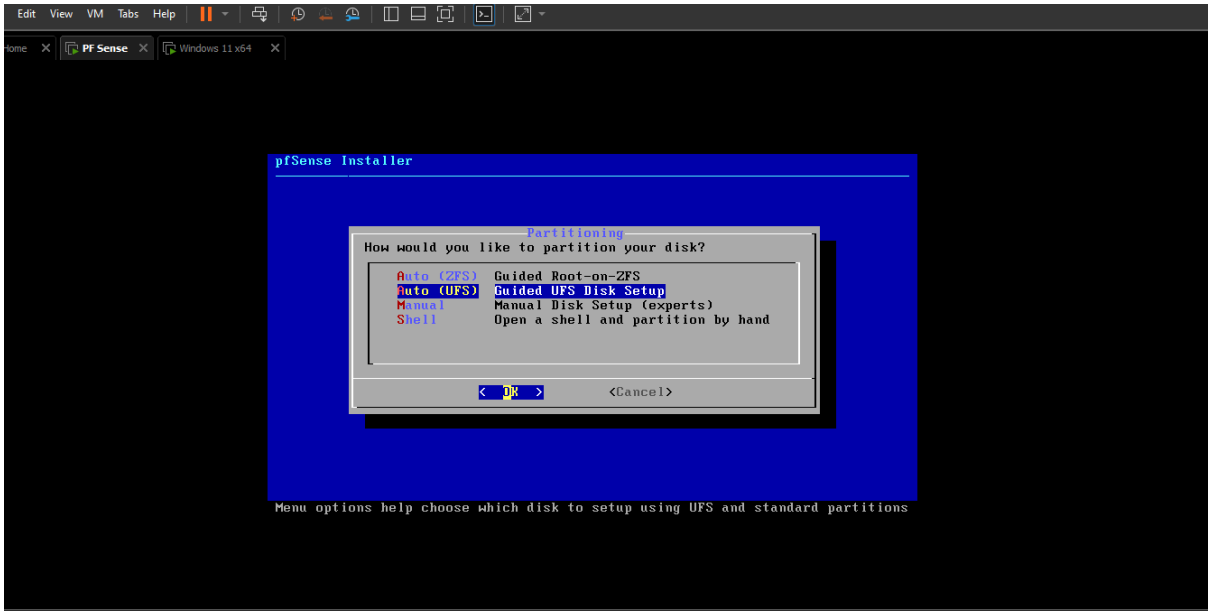

Figure 6

- Then we'll go for GUID Partion Tables

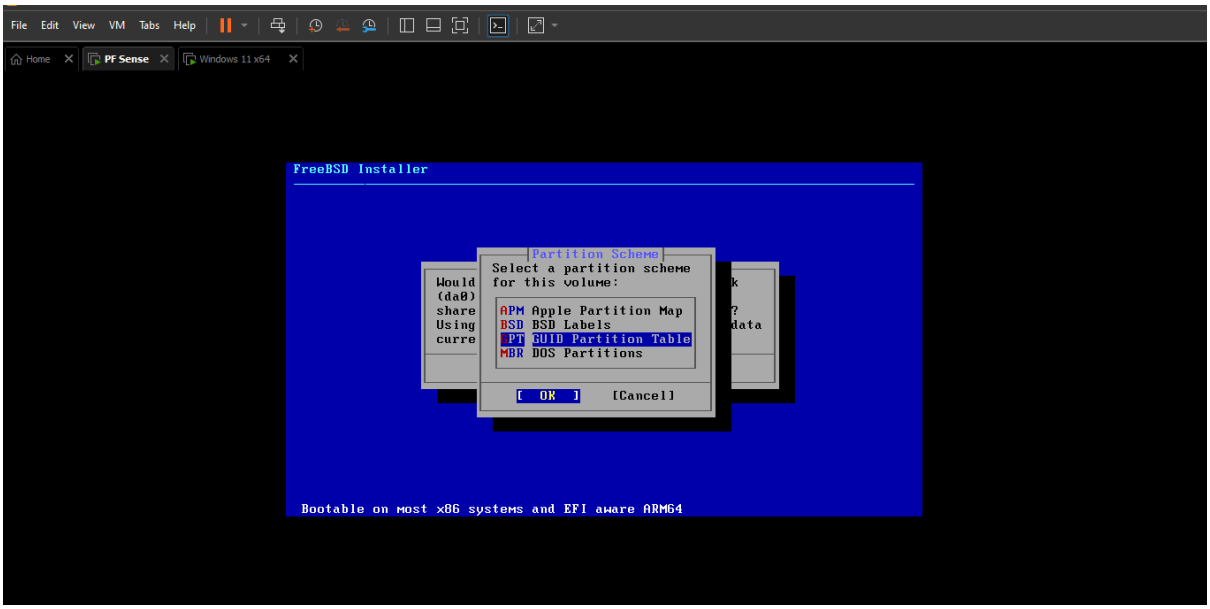

Figure 7

- And Finalise the setup click on finish ->commit then it'll be rebooted automatically

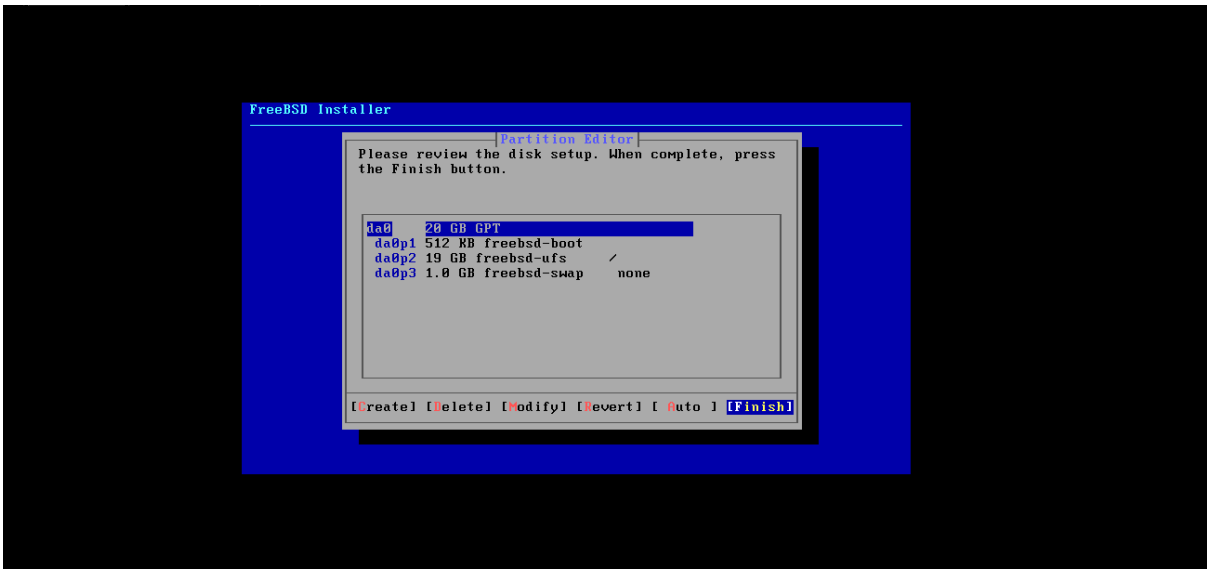

Figure 8

This is the main interface of PFsense and you can see the Ip address of Lan and Wan

- Lan has an ip address of 192.168.1.1/24(which is not correct in Our case) then we have the wan Ip address it states 192.168.191.132/24

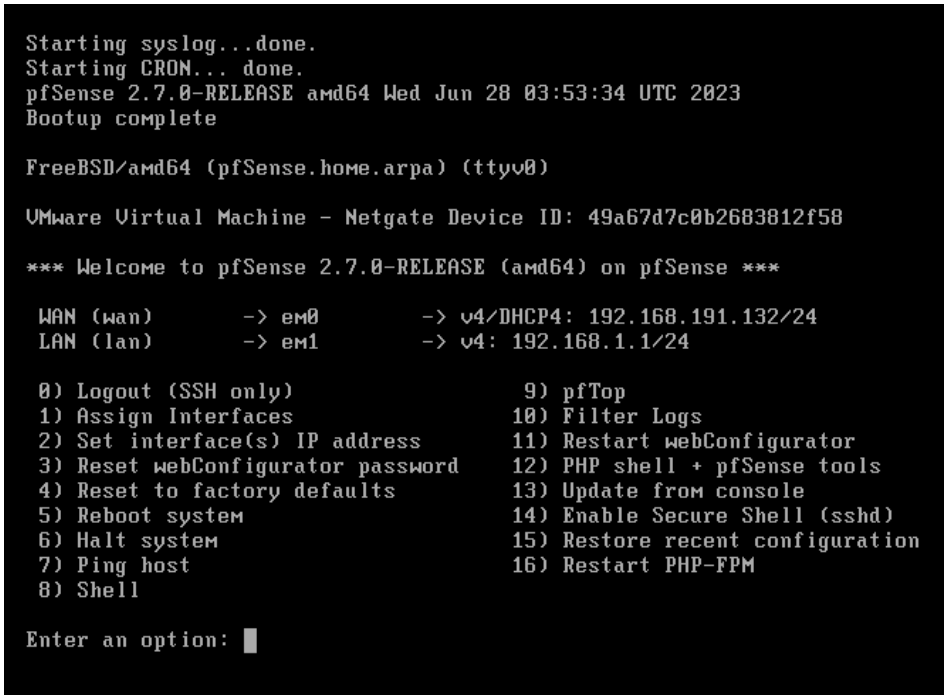

Figure 9

- As we are performing our project in windows 11 virtual machine so this is the main interface of it

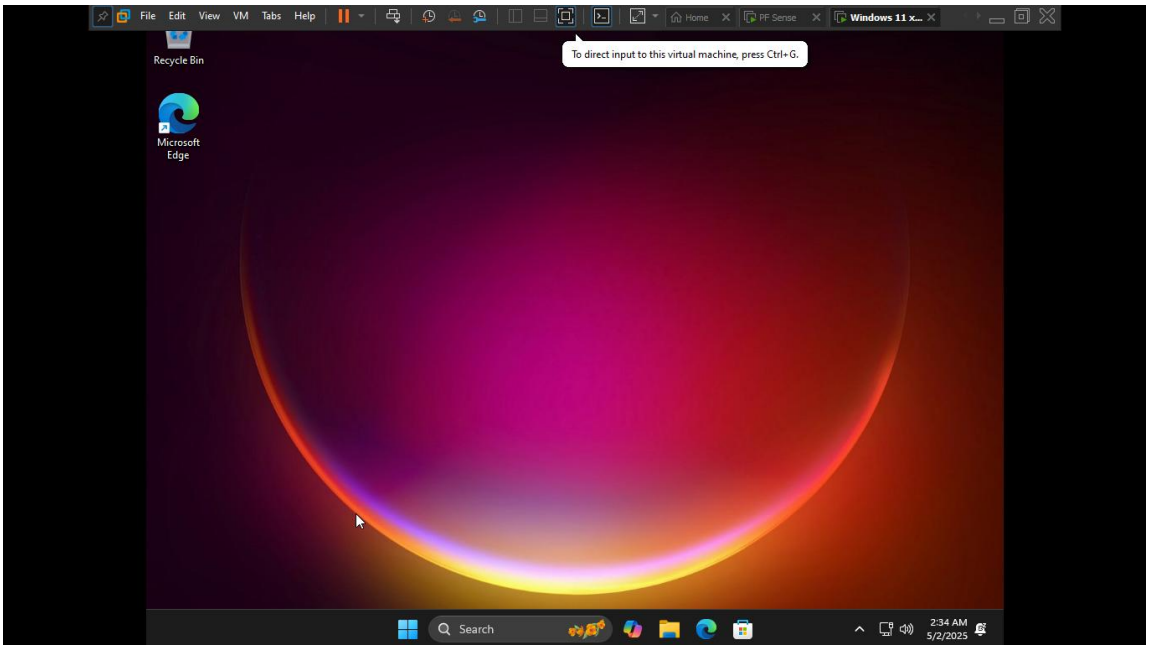

Figure 10

- Now see the connection between my pfsense machine and this windows machine is connected via Lan and the la nip address is 192.168.88.129 which is perfectly fine and wan address is 192.168.191.133 and I tried to ping the PFsense machine since that doesn't have the correct Lan address mention earlier so the ping failed You would be wondering that I've pinged the wan address so thats because PFsense doesn't have the valid address

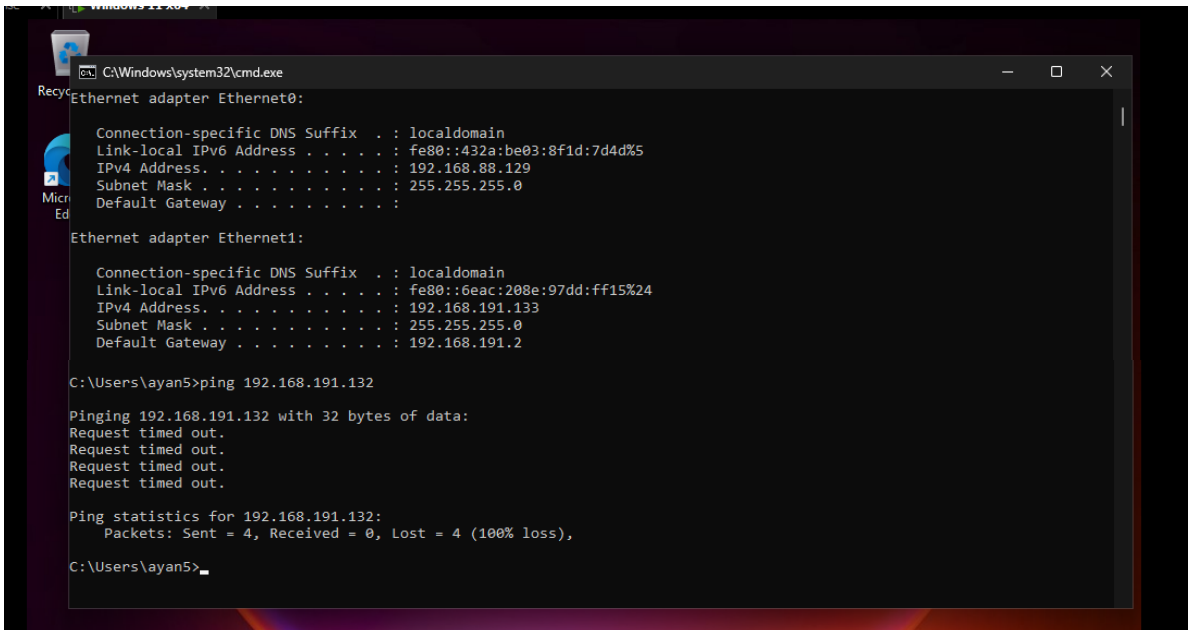

Figure 11

- Now we'll configure the correct Ip address in the lan and for that we have to be in PFsense machine and press the option 2 set interface ip address and then select 2 for lan and press no cause we don't the ip address to be set with dhcp and I entered the ip address 192.168.88.100 with subnet mask of 24 and then enable the dhcp for lan(so that my windows virtual machine can get the ip address) so I started the range from 192.168.88.151-192.168.88.200

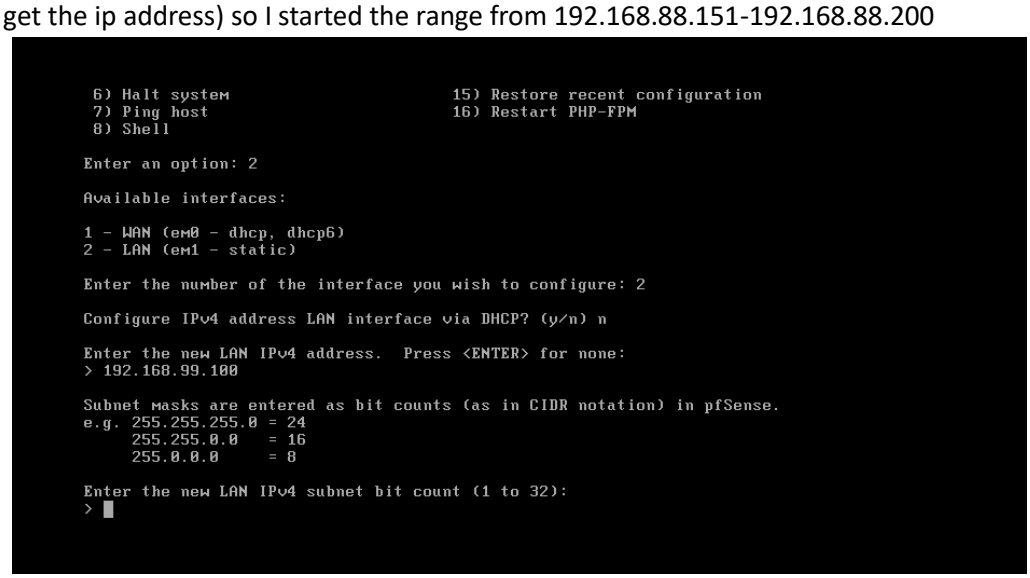

Figure 12

```
2 - LAN (em1 - static)

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:
> 192.168.88.100

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

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

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.88.151
```

Figure 13

```
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

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

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.88.151
Enter the end address of the IPv4 client address range: 192.168.88.200
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...
```

Figure 14

- Now see the ip address of lan has been updated to 192.168.88.100

```
The IPv4 LAN address has been set to 192.168.88.100/24


The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 49a67d7c0b2683812f58

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

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.191.132/24
 LAN (lan)       -> em1        -> v4: 192.168.88.100/24

 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:
```

Figure 15

- Now in the windows machine we'll release the ip address first and than renew the ip address

```
C:\Users\samia>ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::954b:36b7:f56c:7687%6
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::336d:7a1e:5ed9:34d5%10
   Default Gateway . . . . . . . . . :

C:\Users\samia>ipconfig /renew

Windows IP Configuration
```

Figure 16

- Now the ip of the wan is 192.168.191.133 and lan is192.168.88.129
- And see we pinged with the PFsense machine as well and it is responding properly

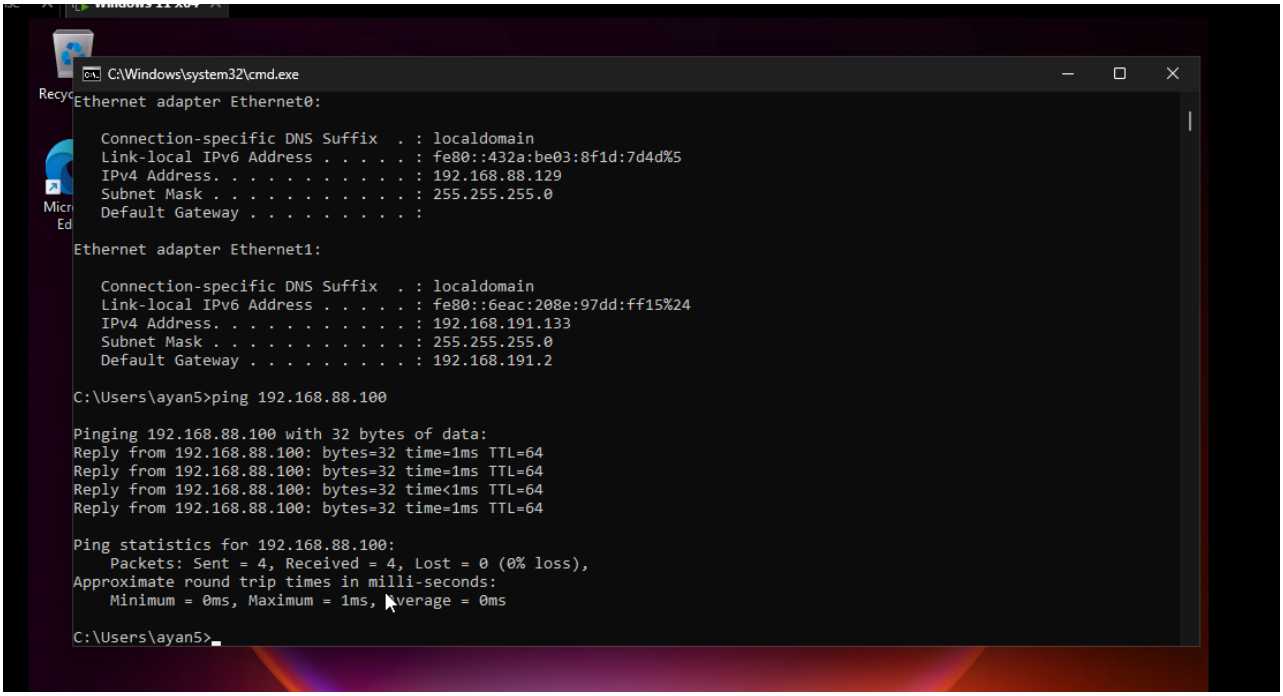

Figure 17

- We went on our web Browser and access the Ip 192.168.88.100(ip of PFsense machine)
- And see the page is loaded successfully

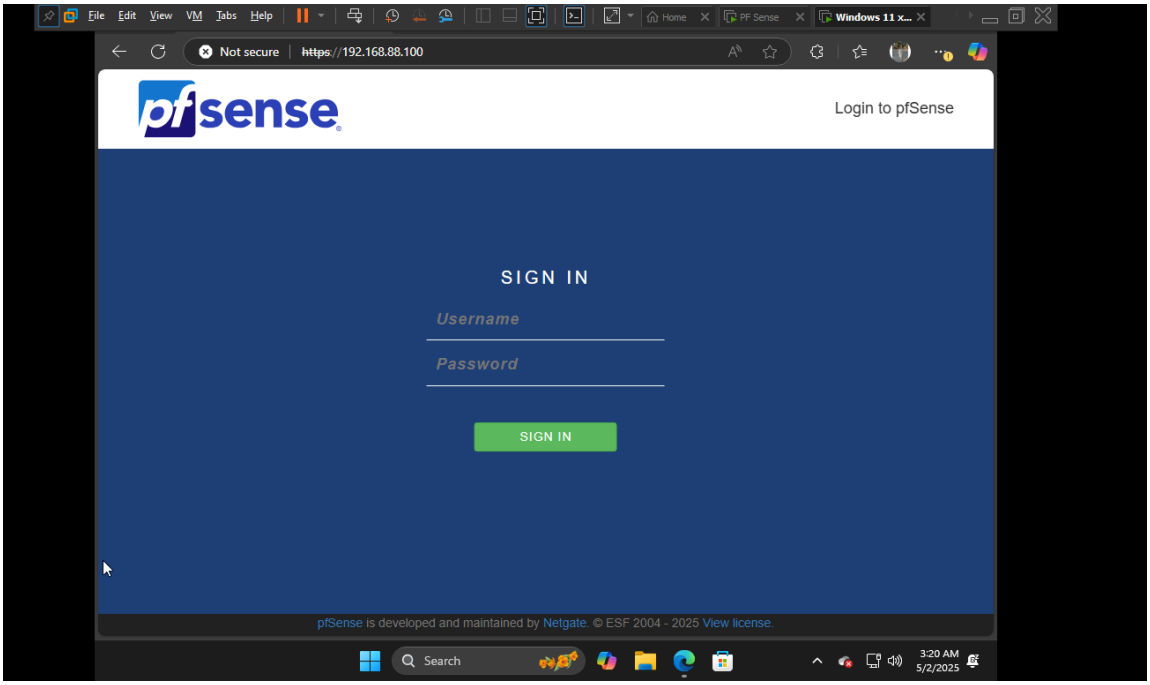

Figure 18

Now we'll setup the PFsense

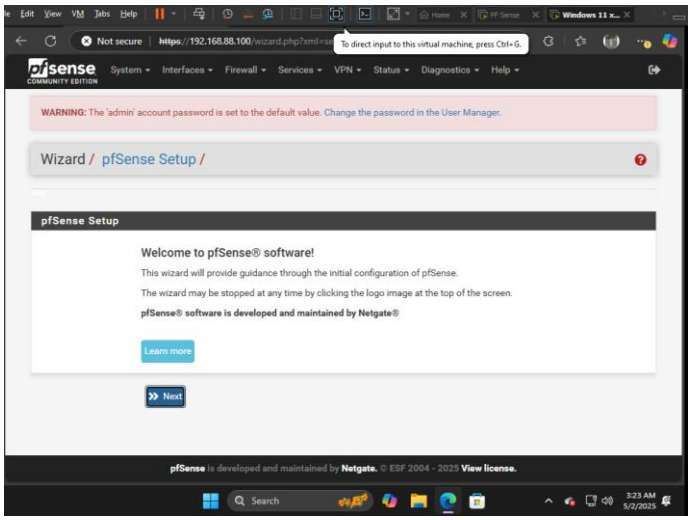

Figure 19

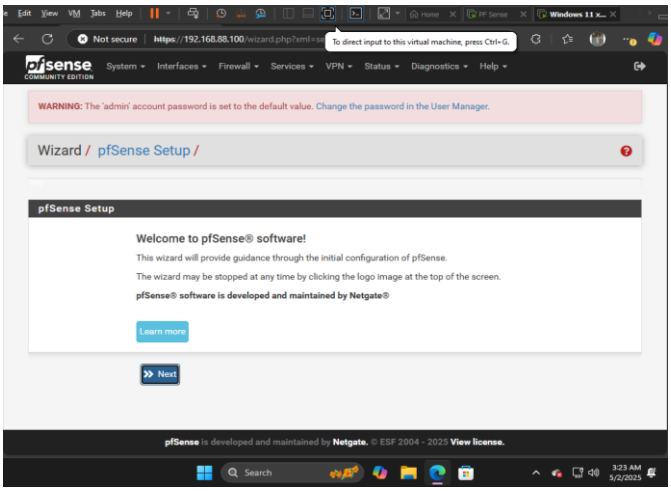

Figure 20

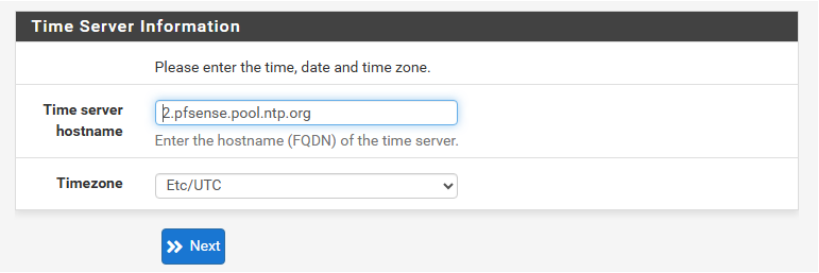

Figure 21

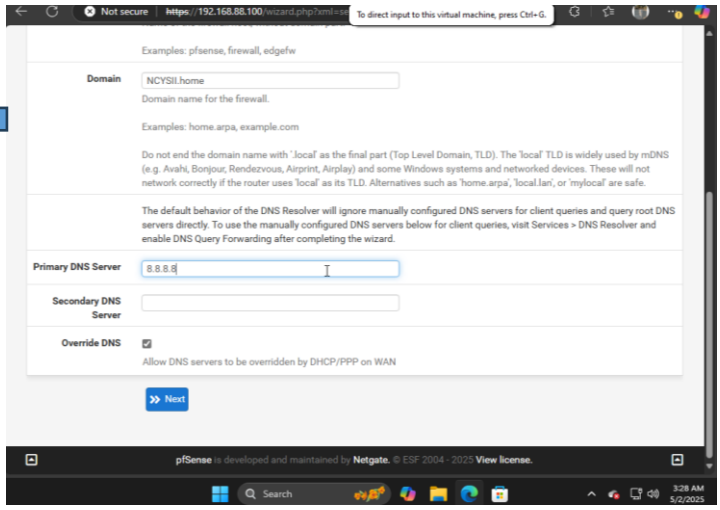

Figure 22

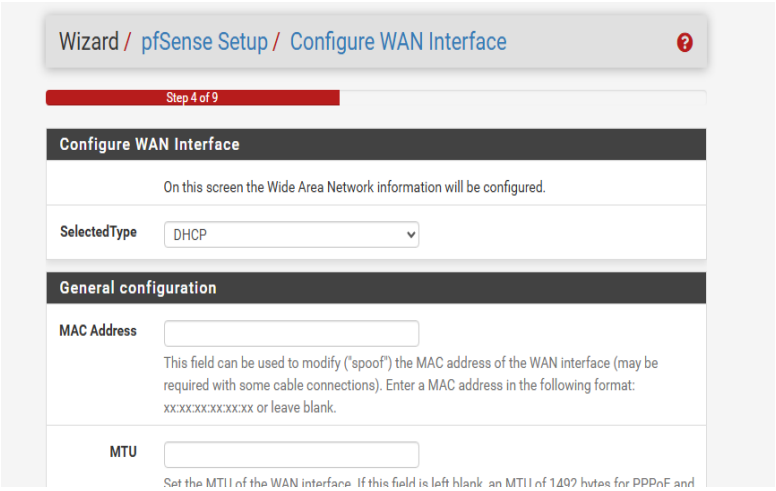

Figure 23

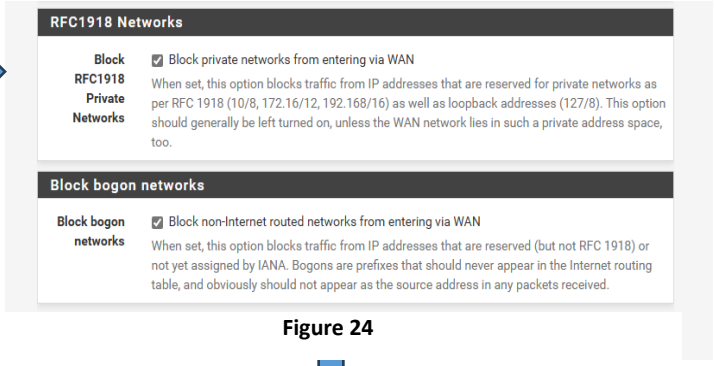

Figure 24

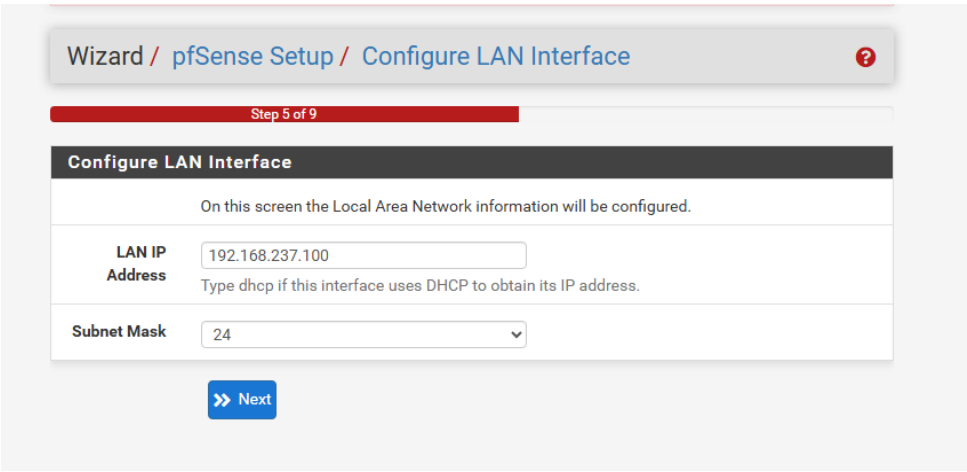

Figure 25

- After this it'll reboot automatically

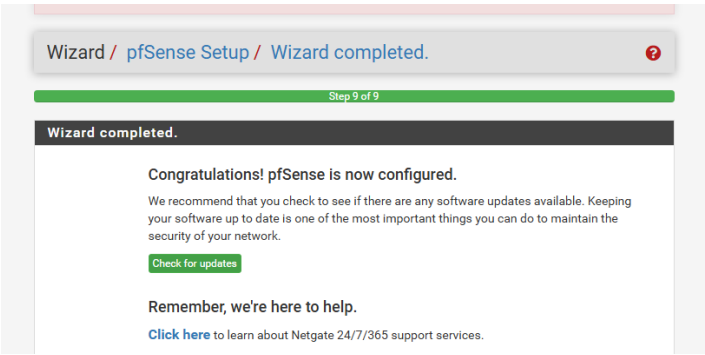

Figure 26

- These are the addon options that we can add on our dashboard

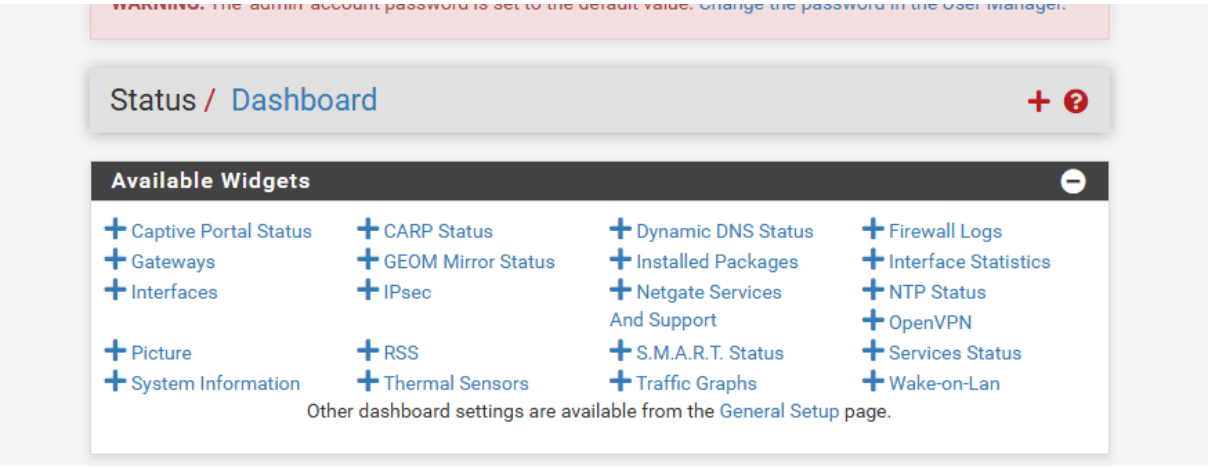

Figure 27

- My personalised Dashboard view in this you can easily view the System Information, Firewall logs, Interfaces (in our case we have Lan and Wan) then it'll also show you Disks, gateways (in my case I'm using the wan gateway) and also we can see the services status

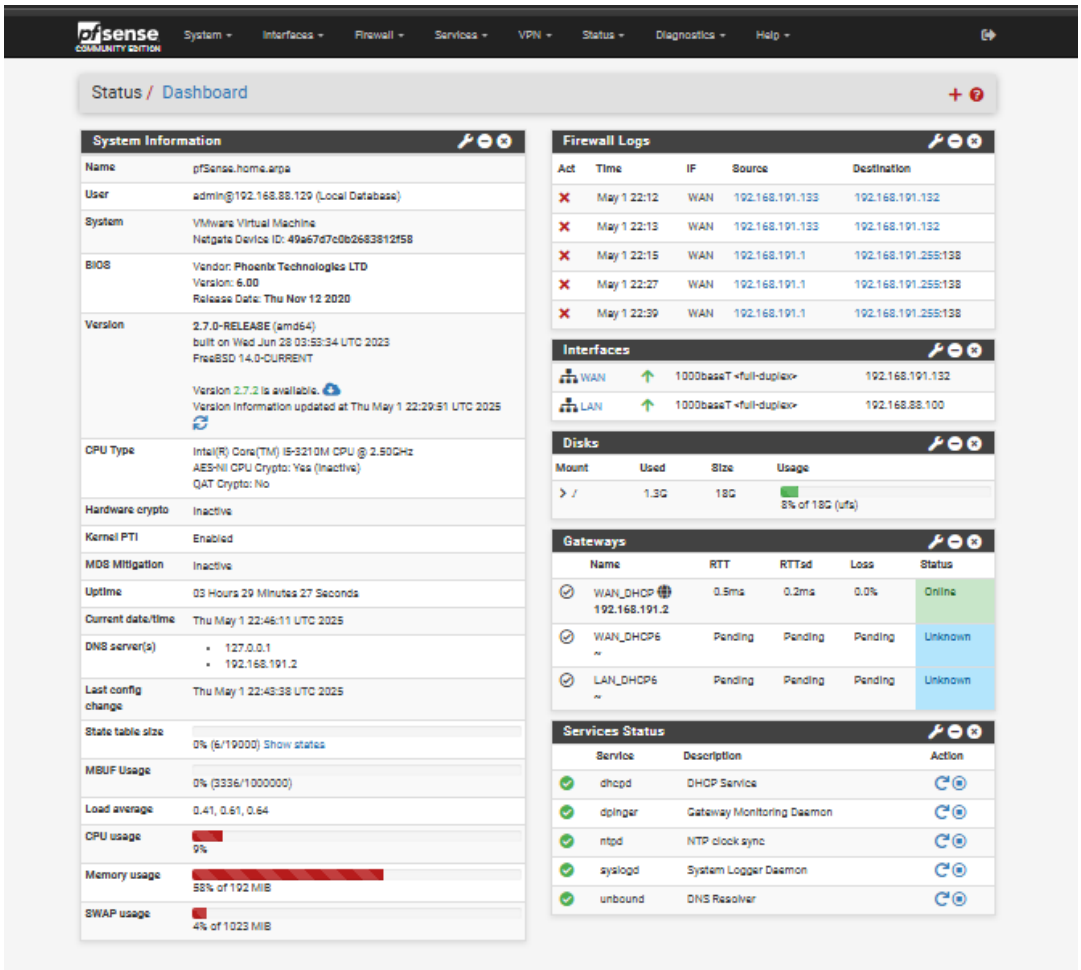

Figure 28

- Now iam assigning the tcp custom port its not mandatory but once I've assigned it my PFsense home page would be accessed via https://192.168.88.100:11443

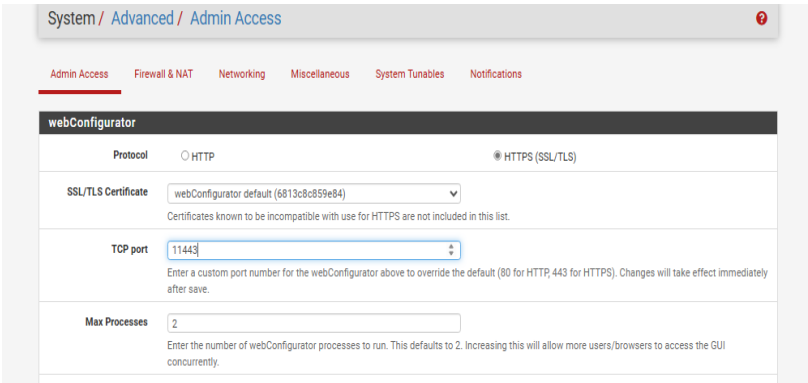

Figure 29

- Also I've enable the Secure Shell Server (SSH) with by default port of 22 to access PFsense from my command prompt

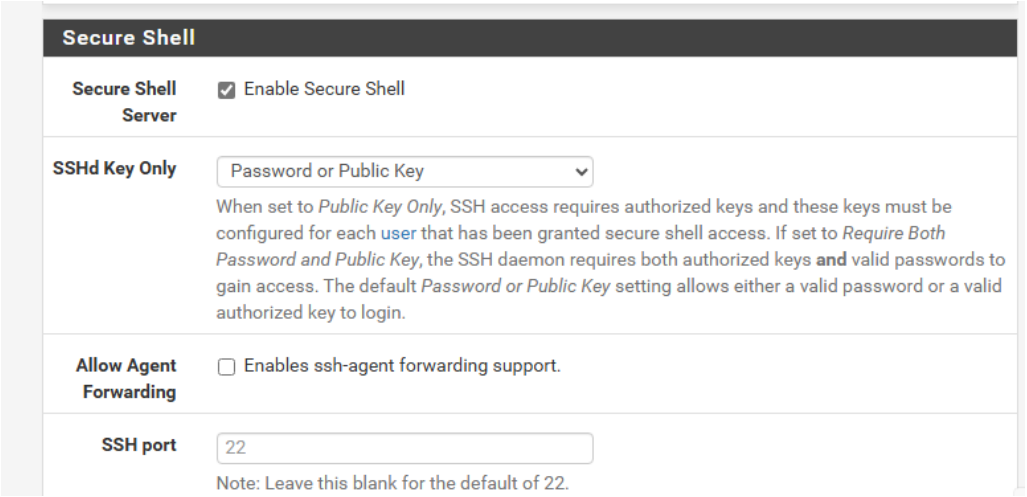

Figure 30

- And saving all the changes and it would take 20 sec(s) to apply the changes

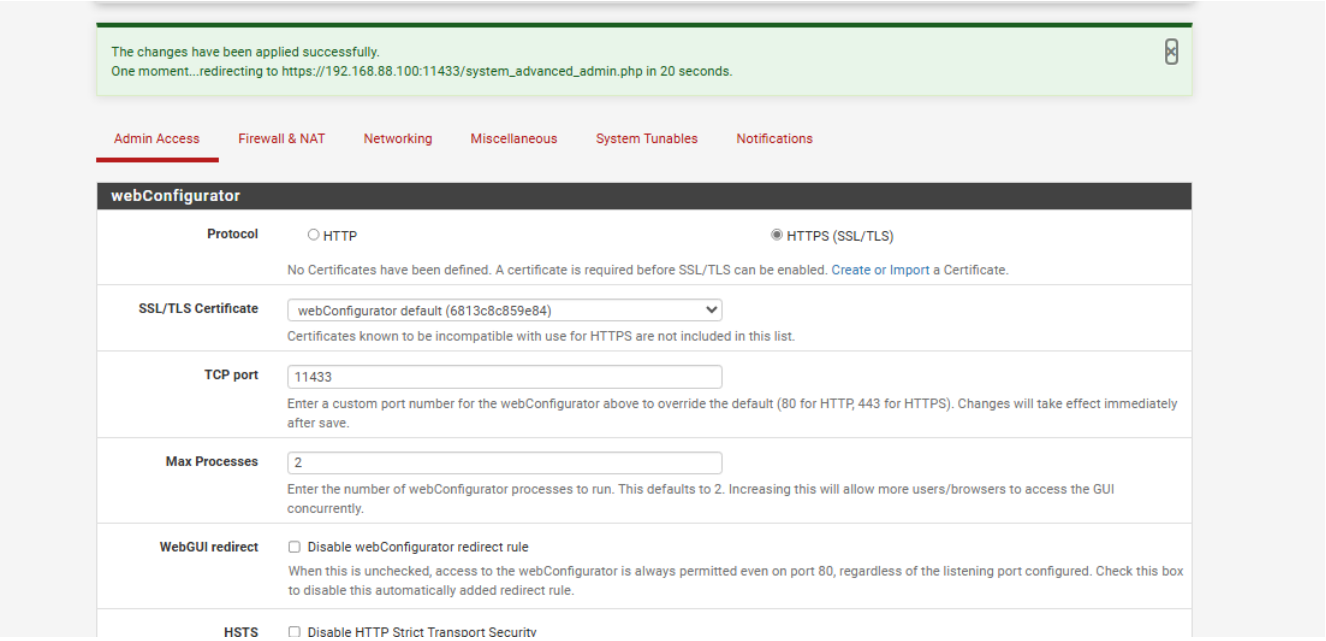

Figure 31

- These are all the Ipv4 routes

IPv4 Routes

Destination	Gateway	Flags	Uses	MTU	Interface	Expire
default	192.168.247.2	UGS	8	1500	em0	
127.0.0.1	link#4	UH	2	16384	lo0	
192.168.237.0/24	link#2	U	4	1500	em1	
192.168.237.100	link#4	UHS	7	16384	lo0	
192.168.247.0/24	link#1	U	5	1500	em0	
192.168.247.2	link#1	UHS	1	1500	em0	
192.168.247.131	link#4	UHS	6	16384	lo0	

Figure 32

- Firewall Rules implemented via PFsense

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	2/2.45 MiB	*	*	*	LAN Address	11433 80	*	*		Anti-Lockout Rule	
	0/5 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Figure 33

- ARP Table being displayed via PFsense

Diagnostics / ARP Table

Search

Search term All Search Clear

Enter a search string or *nix regular expression to filter entries.

ARP Table

Interface	IP address	MAC address	Hostname	Status	Link Type	Actions
LAN	192.168.237.128	00:0c:29:bb:8a:92		Expires in 832 seconds	ethernet	
WAN	192.168.247.131	00:0c:29:80:6e:1e		Permanent	ethernet	
WAN	192.168.247.2	00:50:56:e2:51:b3		Expires in 1119 seconds	ethernet	
LAN	192.168.237.100	00:0c:29:80:6e:28	pfSense.home.arpa	Permanent	ethernet	

Figure 34

- You can implement many more things via PFsense for e.g. Firewall, OpenVPN, Packages Authentication and many more

Figure 35

- This is the display of monitoring the PFsense it will display all the utilities with an interactive graph

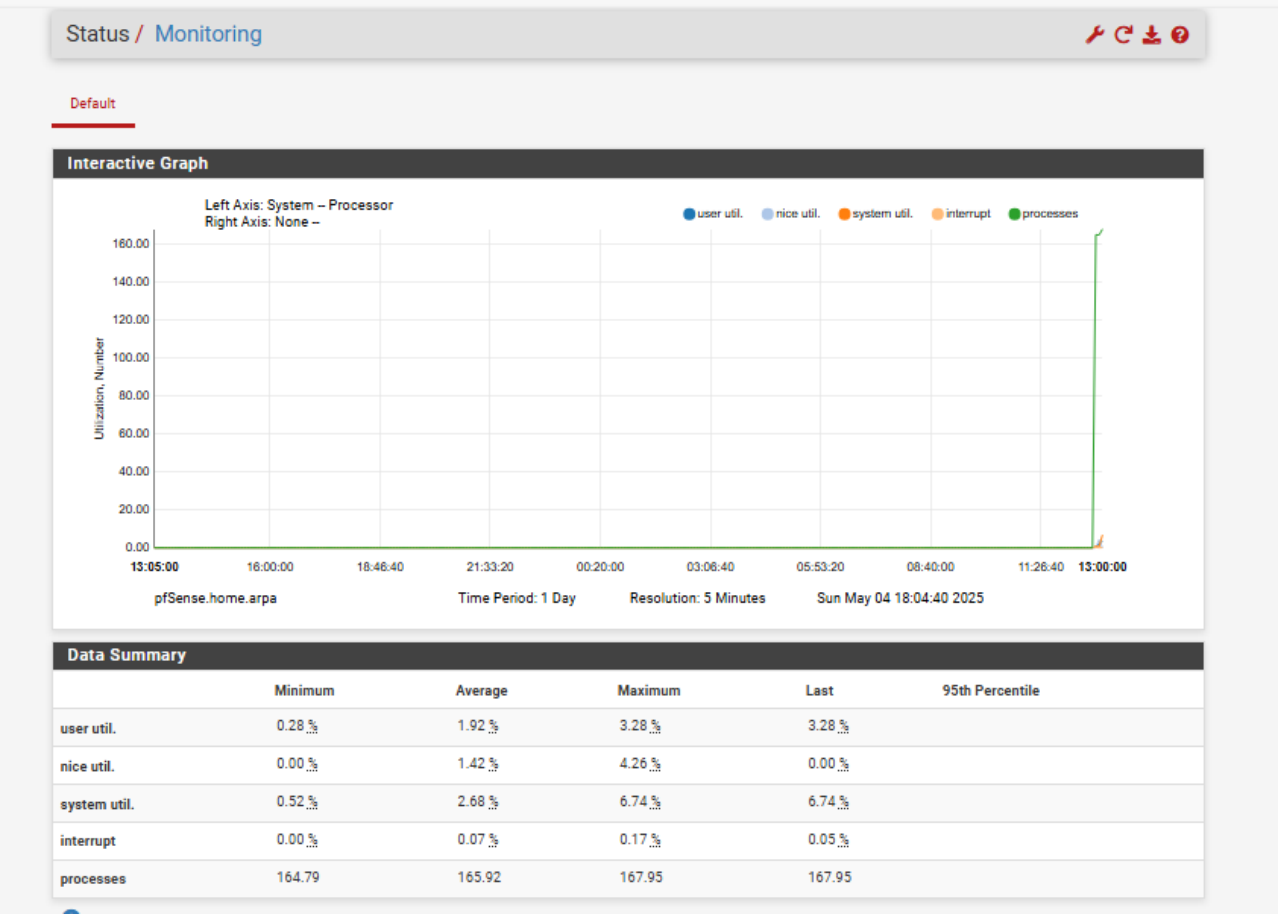

Figure 36

Package Installation

- I've Installed the package of ARPing this will help in broadcasting a who-has ARP packet on the network and display the answer

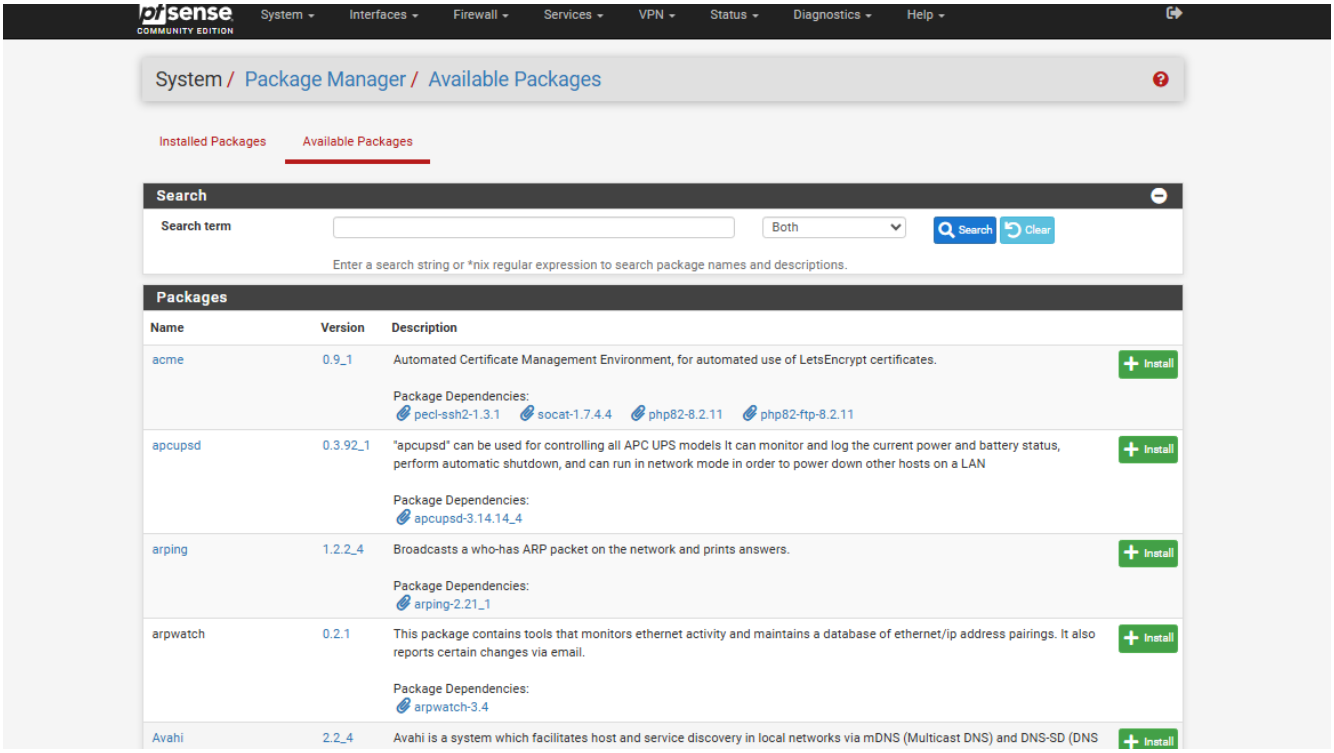

Figure 37

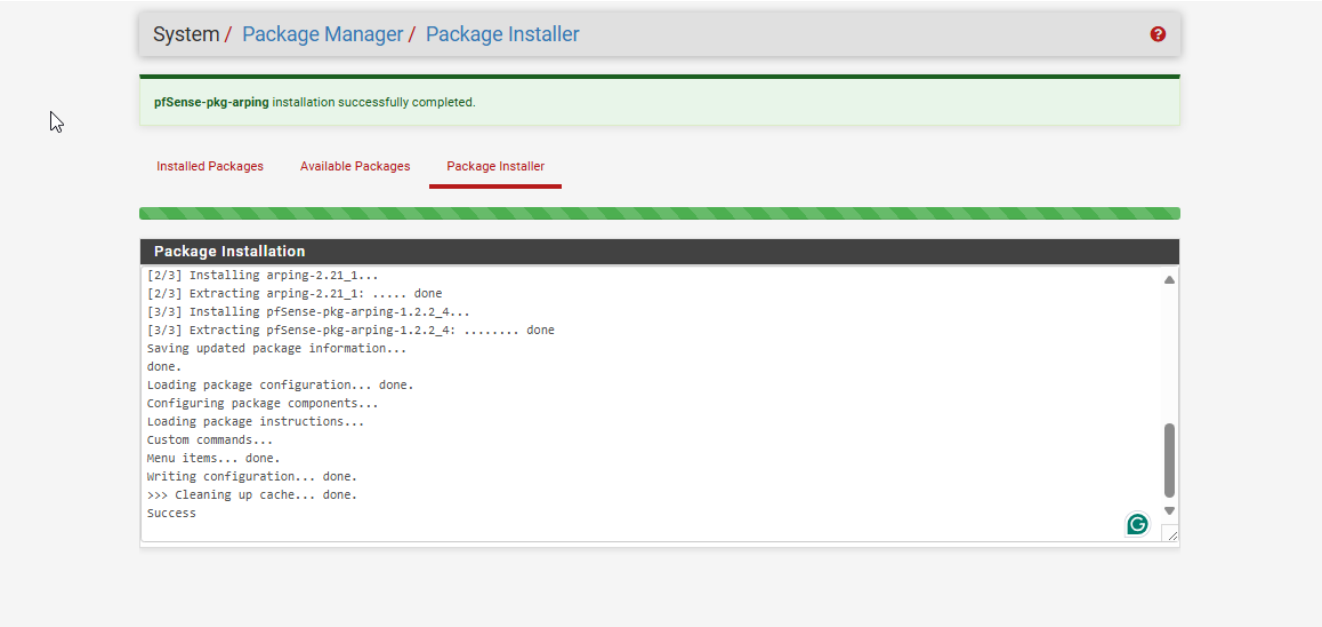

Figure 38

- Creating a new user named as Ayan so to create it you have to fill the information and you can also add the user in the admin group but in this case we are not adding Ayan in the admin Group

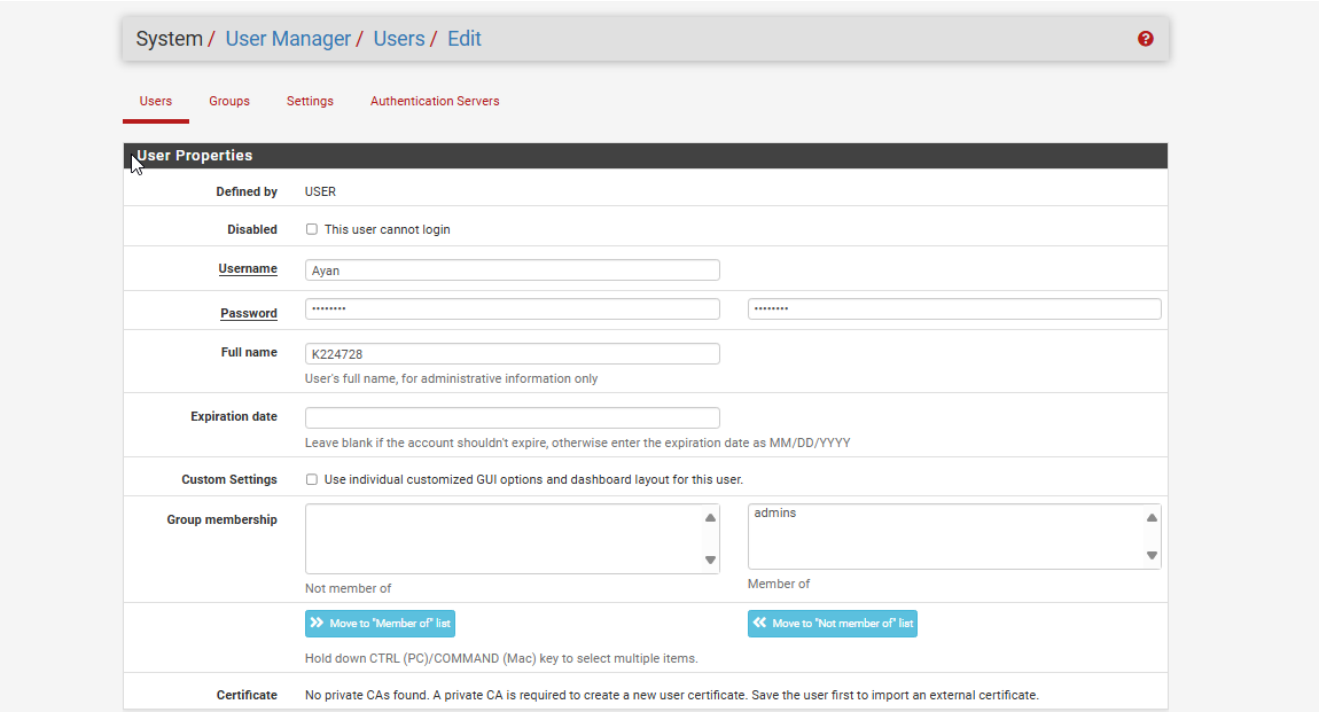

Figure 39

- See the user have been successfully created

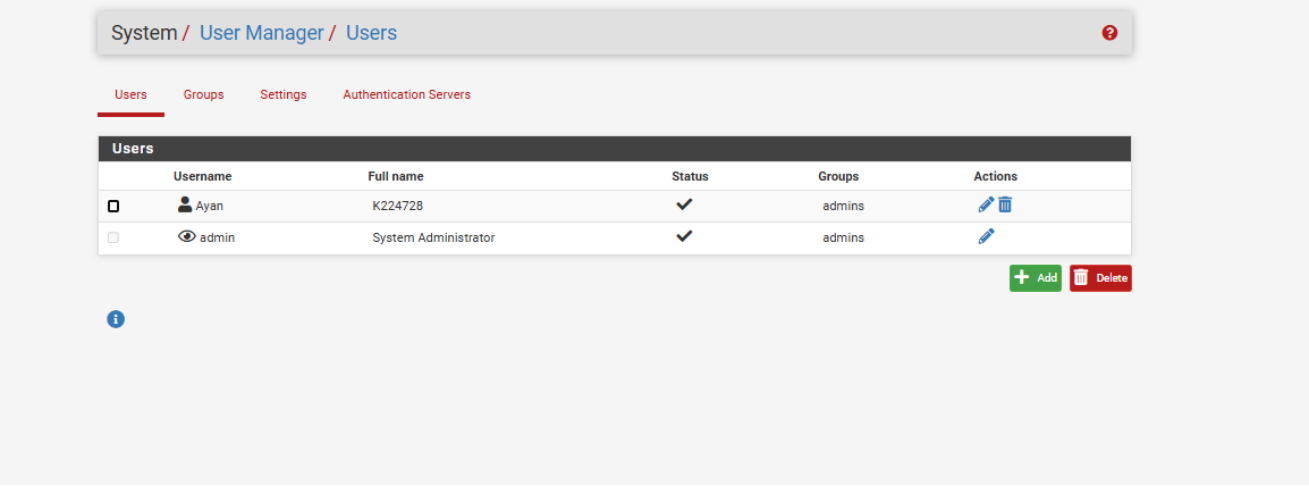

Figure 40

- Now we'll try to access the PFsense via ssh as we allow the ssh while configuration so to access it first open the command prompt and write the command
- ssh username@<ip-address of PFsense lan >

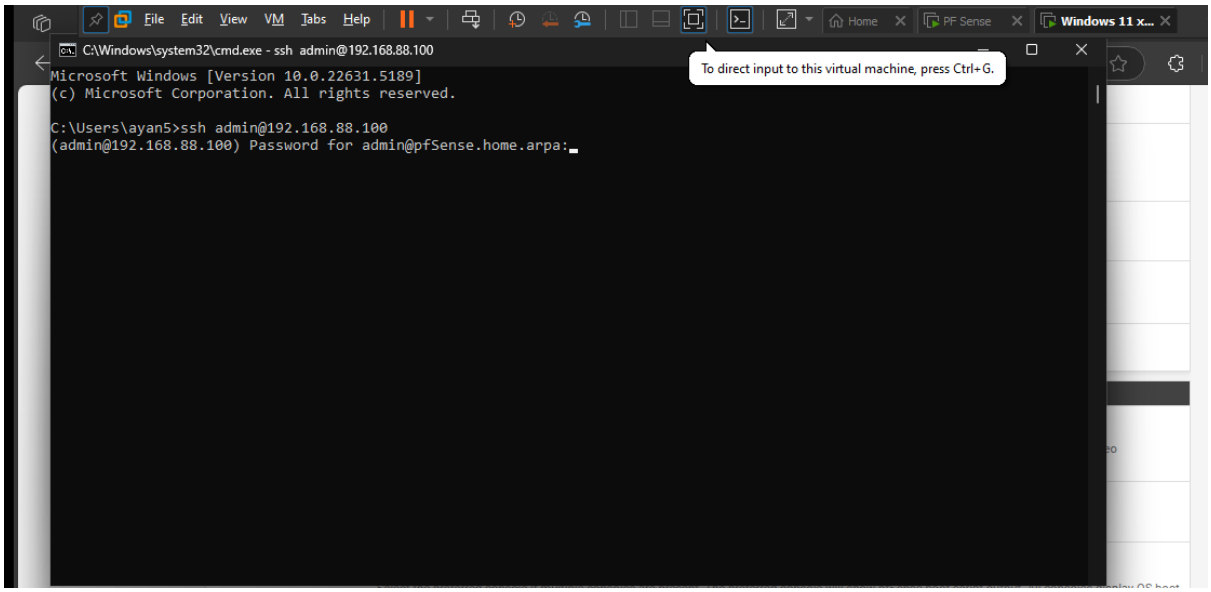

Figure 41

- Enter the password and once authenticated now you'll be allowed to enter in the PFsense terminal which actually same with the PFsense virtual machine
- And for the demo I've tried to accessthe firewall logs as well

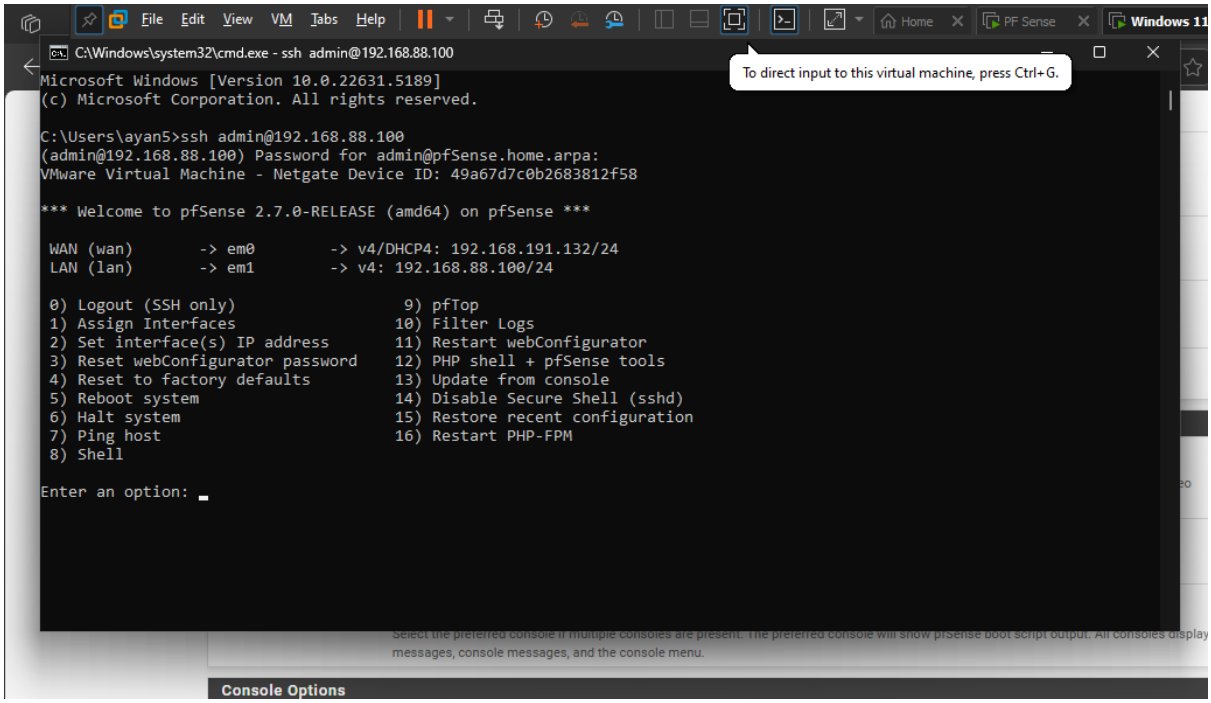

Figure 42

- See this the output of the firewall accessed via command Prompt

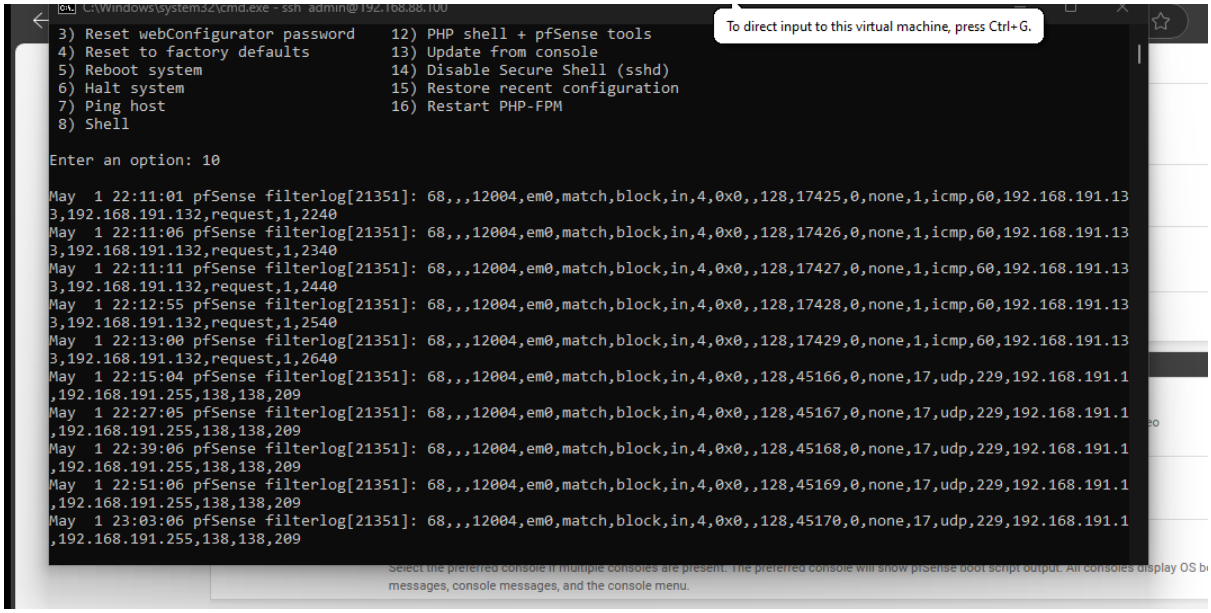

Figure 43