PfSense Firewall Setup and Configuration -Documentation

Nithin Ragesh V

22 September 2024

Table of Contents

Introduction 3

What is Virtualization? 3

What is PfSense? 3

Downloading Vmware 4

Downloading PfSense 4

Making a new VM in Vmware 5

Configuring Interfaces 9

Accessing the web portal 11

Security 13

Basic Configuration 16

Setting up a firewall rule 17

Conclusion 19

INTRODUCTION

I'm Nithin, as a Computer Science undergrad, I am driven by my passion for cybersecurity. Throughout my academic journey, I have learned programming languages and concepts of operating systems, software, hardware, and networks. One of my proudest accomplishments is obtaining an internship in Vulnerability Assessment and Penetration Testing. This experience allowed me to gain various aspects of knowledge in web penetration testing.

On this Documentation, I will be showing about the basic firewall setup and configuration using PfSense on the Vmware workstation.

What is Virtualzation?

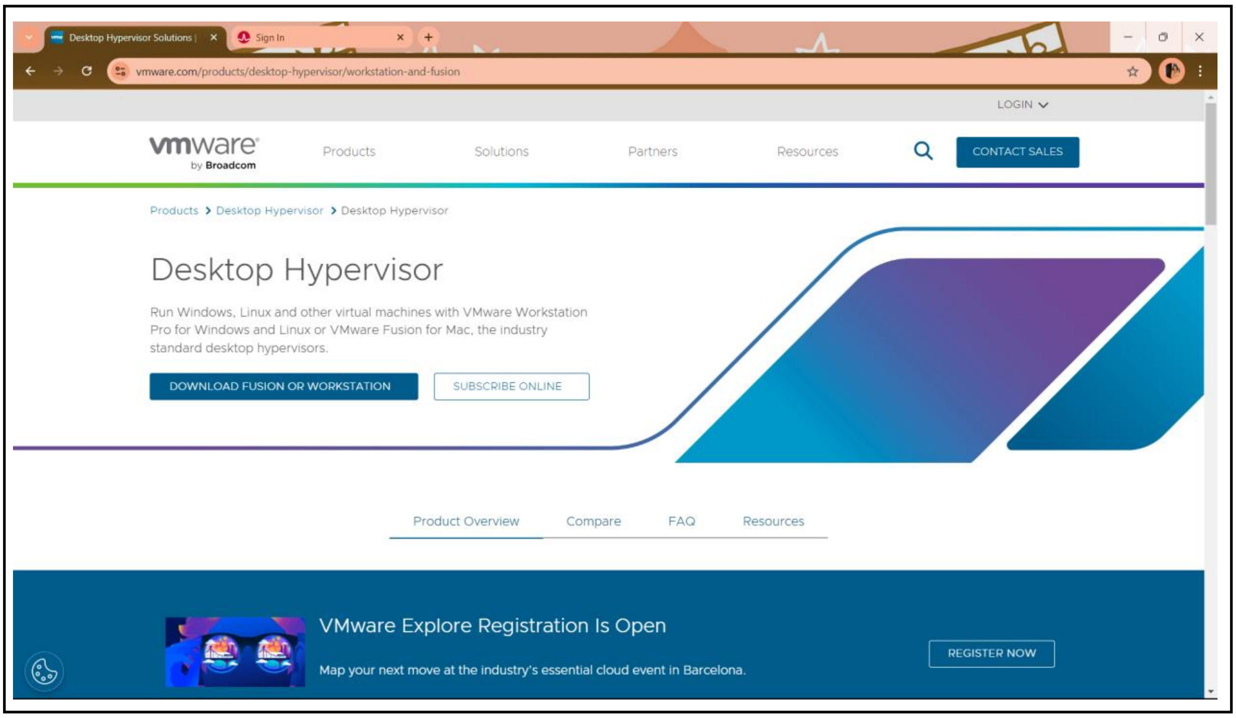
Virtualization is a method of creating virtual versions of physical resources like servers or networks. It uses software to mimic hardware, allowing multiple operating systems and applications to run on one machine. This approach boosts efficiency and reduces costs. It started with mainframes, where it helped save expensive processing power by running several systems on one physical machine. There are various software which support the concept, for example Virtual box, Vmware etc. In simple terms, Virtualization helps make various operating system inside a host operating system. Running a Windows host and using virtualization running linux distros.

What is PfSense?

PfSense is an open-source firewall and router software that runs on physical or virtual machines. It is used to secure and manage network traffic, offering features like firewall rules, VPNs, load balancing, and traffic monitoring. Designed for ease of use, PfSense can turn a regular computer into a powerful firewall, allowing you to customize and control network security. It's popular in both home and business environments for managing networks efficiently without expensive hardware.

Downloading Vmware

Go to www.vmware.com and download the vmware workstation player for the preferred operating system. After downloading the .exe file, install it.



Desktop Hypervisor Solutions |
Sign In
vmware.com/products/desktop-hypervisor/workstation-and-fusion
LOGIN
vmware by Broadcom
Products
Solutions
Partners
Resources
CONTACT SALES
Products > Desktop Hypervisor > Desktop Hypervisor

Desktop Hypervisor

Run Windows, Linux and other virtual machines with VMware Workstation Pro for Windows and Linux or VMware Fusion for Mac, the industry standard desktop hypervisors.

DOWNLOAD FUSION OR WORKSTATION
SUBSCRIBE ONLINE
Product Overview
Compare
FAQ
Resources

VMware Explore Registration Is Open

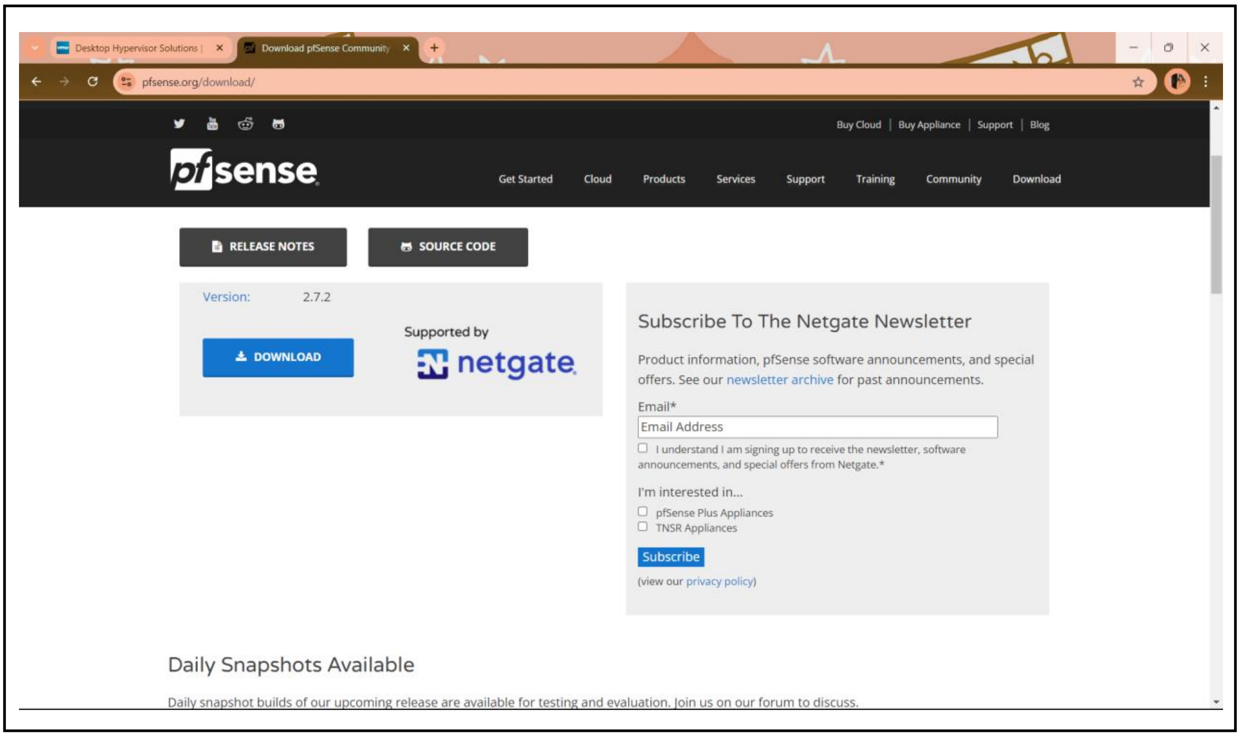
Map your next move at the industry's essential cloud event in Barcelona.

Downloading PfSense

By going to the www.pfSense.org/downloads page we can get the PfSense latest stable version of ISO image which is provided by the Netgate. (Netgate is an open-source driven secure networking company that provides appliance and software-based firewall, VPN and routing solutions including PfSense.)

The website wants you to fill out the basic information about you and deliver the iso link on your email. After getting the email you can download the compressed file to your machine.

Extracting the zip file gives you the PfSense ISO.



Desktop Hypervisor Solutions | ✕ Download pfSense Community ✕ +

pfsense.org/download/

Buy Cloud | Buy Appliance | Support | Blog

pfsense

Get Started Cloud Products Services Support Training Community Download

RELEASE NOTES SOURCE CODE

Version: 2.7.2

DOWNLOAD

Supported by netgate

Subscribe To The Netgate Newsletter

Product information, pfSense software announcements, and special offers. See our newsletter archive for past announcements.

Email*

Email Address

□ I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.*

I'm interested in...

□ pfSense Plus Appliances

□ TNSR Appliances

Subscribe

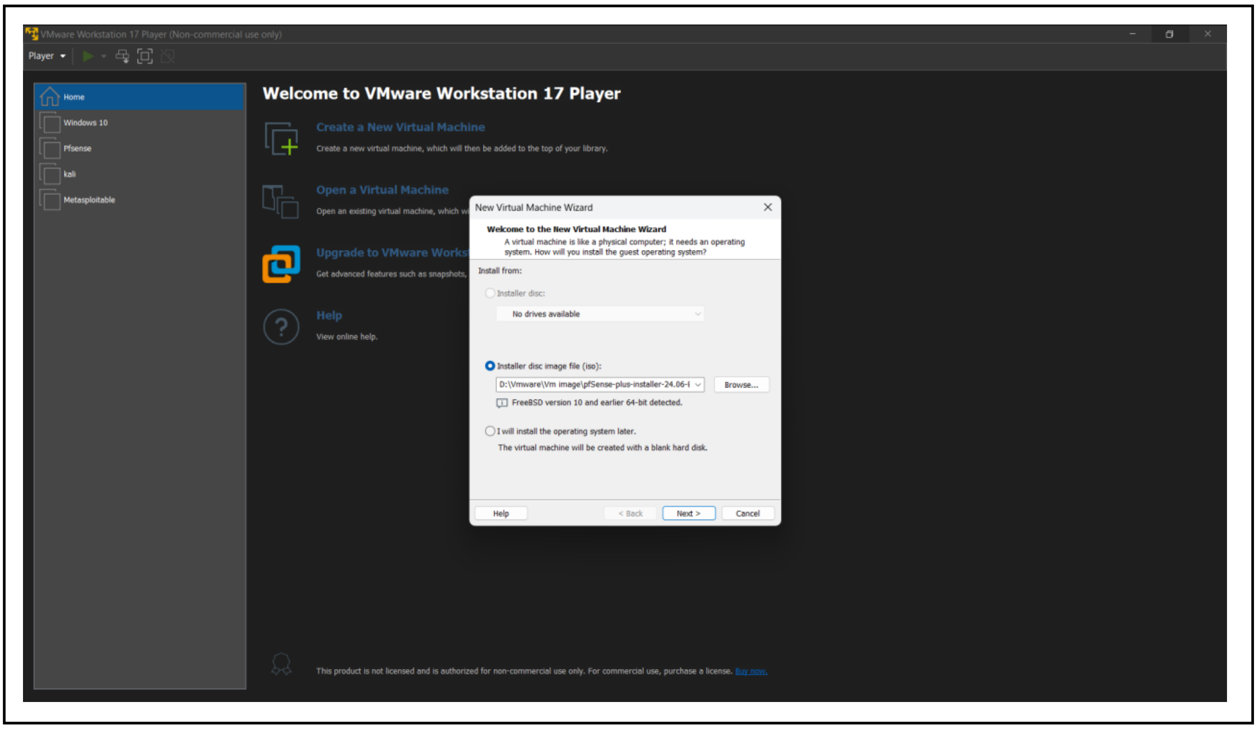
(view our privacy policy)

Daily Snapshots Available

Daily snapshot builds of our upcoming release are available for testing and evaluation. Join us on our forum to discuss.

Making a New VM on Vmware

Open the Vmware software and click the "Create a new Virtual machine" option on the right side.



VMware Workstation 17 Player (Non-commercial use only)

Player

Home

Windows 10

Pfsense

kali

Metasploitable

Welcome to VMware Workstation 17 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine

Open an existing virtual machine, which wi

Upgrade to VMware Works

Get advanced features such as snapshots,

Help

View online help.

New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

D:\Vmware\Vm image\pfSense-plus-installer-24.06-I Browse...

FreeBSD version 10 and earlier 64-bit detected.

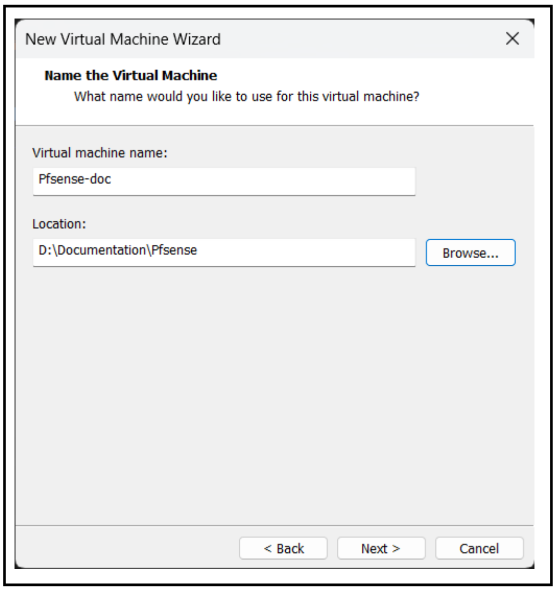
○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

On the "Install disk image file (ISO)" option, browse the extracted PfSense ISO file and click next.



New Virtual Machine Wizard

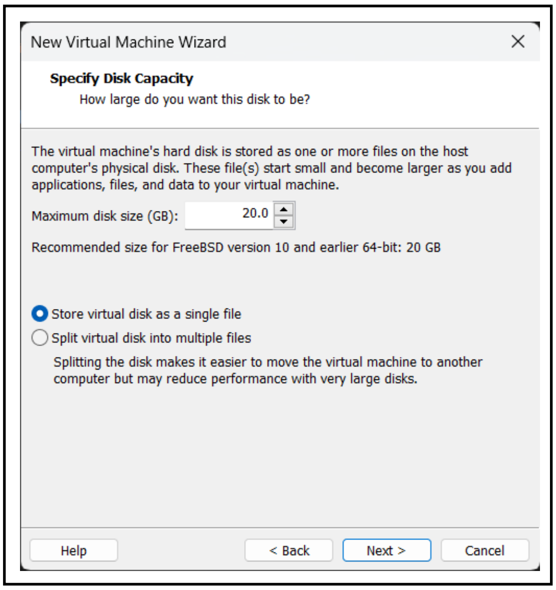
Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name: Pfsense-doc

Location: D:\Documentation\Pfsense

Give Virtual machine a name and browse the storage location for the PfSense VM.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 20.0

Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

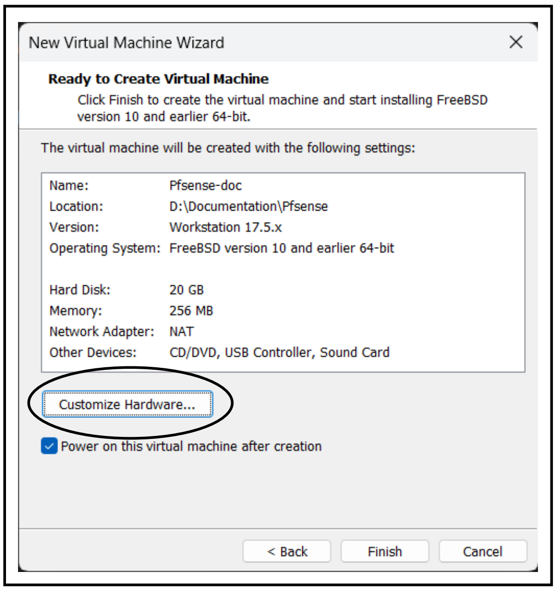
● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Give the Virtual machine a required size and select the "Store virtual disk as singe file".

On the next step the Vmware gives us the summary of the VM. We are not finished yet, on the panel click "Customize Hardware" option.



New Virtual Machine Wizard

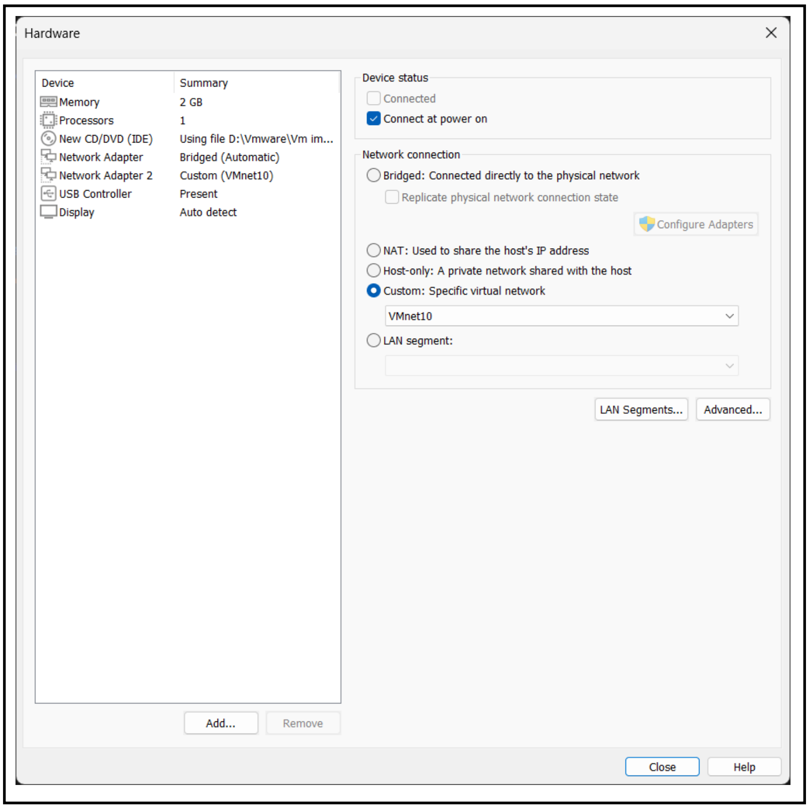
Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing FreeBSD version 10 and earlier 64-bit.

The virtual machine will be created with the following settings:

Name:	Pfsense-doc
Location:	D:\Documentation\Pfsense
Version:	Workstation 17.5.x
Operating System:	FreeBSD version 10 and earlier 64-bit
Hard Disk:	20 GB
Memory:	256 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Sound Card

☑ Power on this virtual machine after creation



Hardware

Device	Summary
Memory	2 GB
Processors	1
New CD/DVD (IDE)	Using file D:\Vmware\Vm im...
Network Adapter	Bridged (Automatic)
Network Adapter 2	Custom (VMnet10)
USB Controller	Present
Display	Auto detect

Device status

□ Connected
☑ Connect at power on

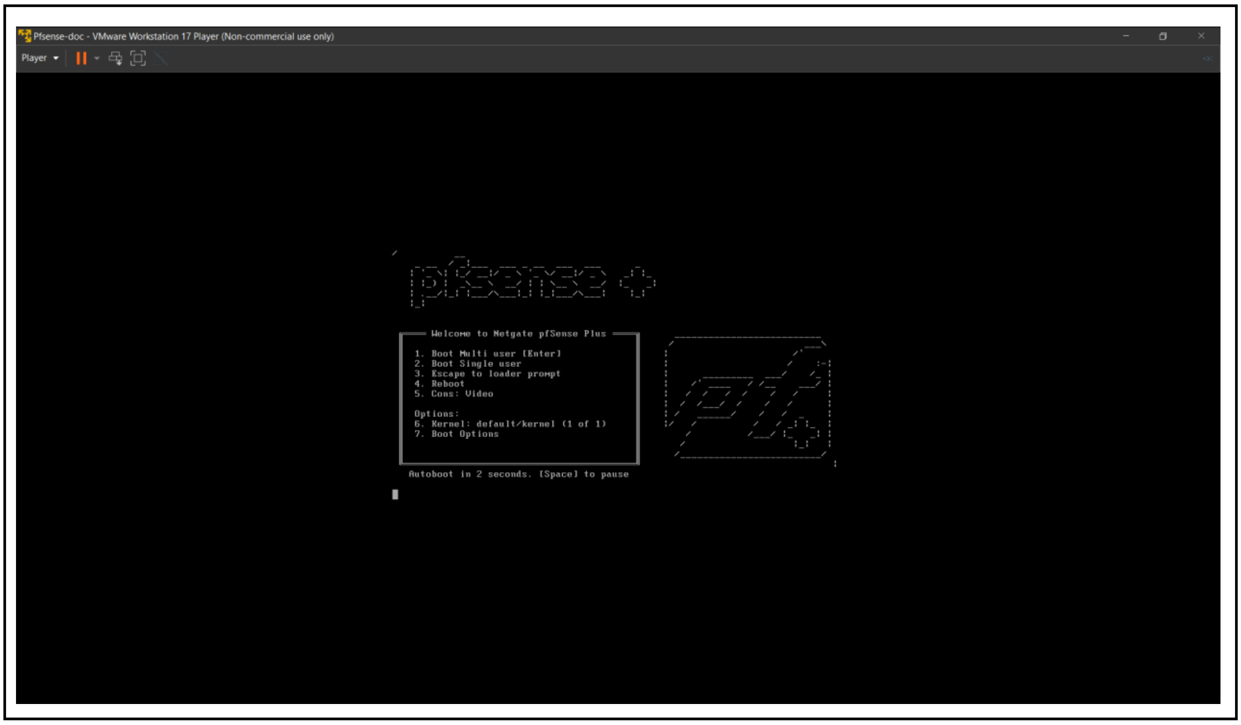
Network connection

○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet10
○ LAN segment:

On the screen we have the options to customize hardware, change the memory to 2gb. We need at least two network adapters for setting up a firewall on pfSense, on the first attempt you don’t see two network adapters, for this you should click on the add option below to add a new network adapter.

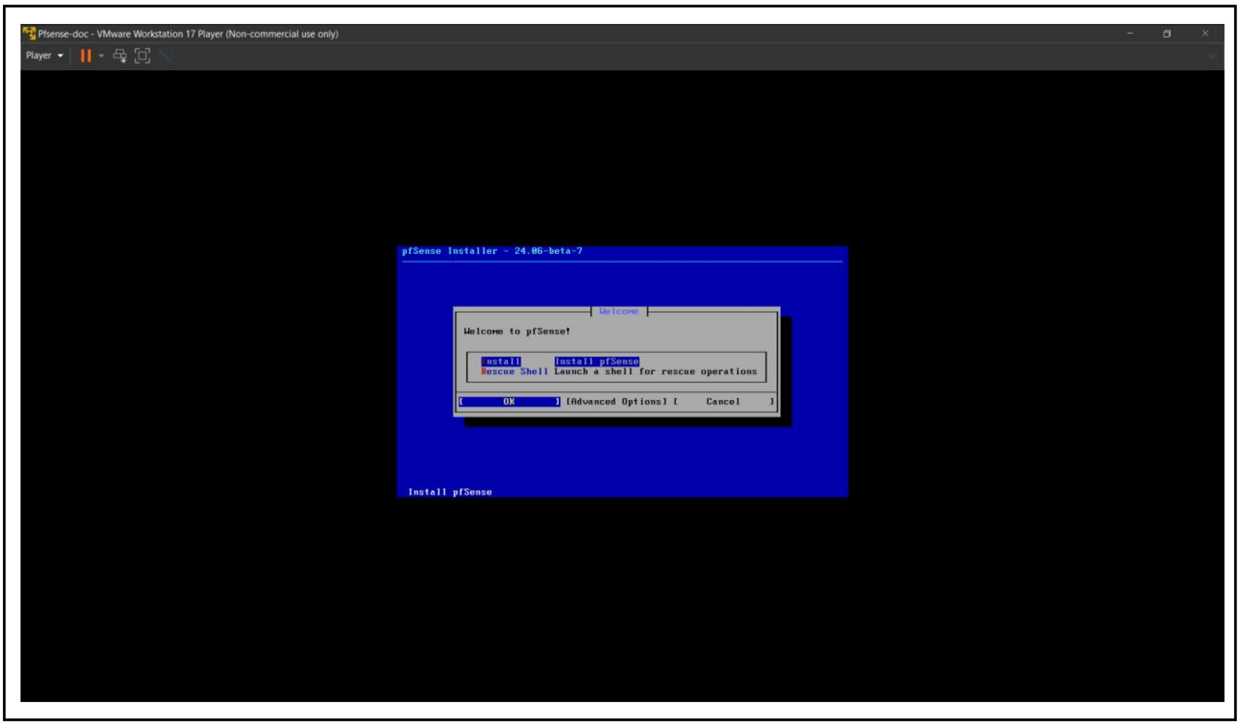
The first network adapter should be set to bridged (Automatic) which acts as WAN to PfSense and the next network adapter should be kept on custom: Specific virtual network and set to the VMnet10.

Then we are ready to fire the VM. On starting the PfSense installer..


Pfsense-doc - VMware Workstation 17 Player (Non-commercial use only)
Player

```
Welcome to Netgate pfSense Plus

 1. Boot Multi user [Enter]
 2. Boot Single user
 3. Escape to loader prompt
 4. Reboot
 5. Cons: Video

 Options:
 6. Kernel: default/kernel (1 of 1)
 7. Boot Options

Autoboot in 2 seconds. [Space] to pause
```

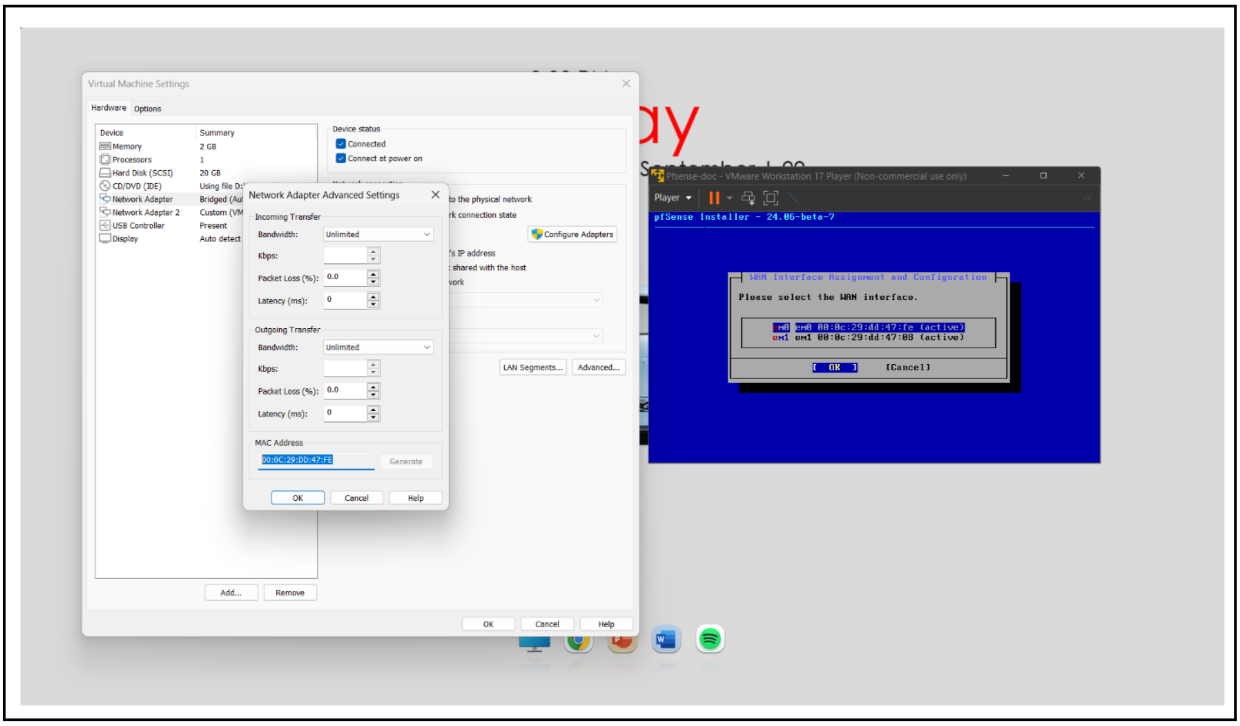
On the next screen..


Pfsense-doc - VMware Workstation 17 Player (Non-commercial use only)
Player

```
pfSense Installer - 24.06-beta-7

Welcome

Welcome to pfSense!

 Install       Install pfSense
 Rescue Shell  Launch a shell for rescue operations

[      OK      ] [Advanced Options] [     Cancel     ]

Install pfSense
```

Configuring Interfaces

By selecting the option "Install pfSense", need to configure the WAN and LAN interfaces to the pfSense this is crucial.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file D:
Network Adapter	Bridged (Au
Network Adapter 2	Custom (VM
USB Controller	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network Adapter Advanced Settings

Incoming Transfer

Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

Latency (ms): 0

Outgoing Transfer

Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

Latency (ms): 0

MAC Address

00:0C:29:DD:47:FE

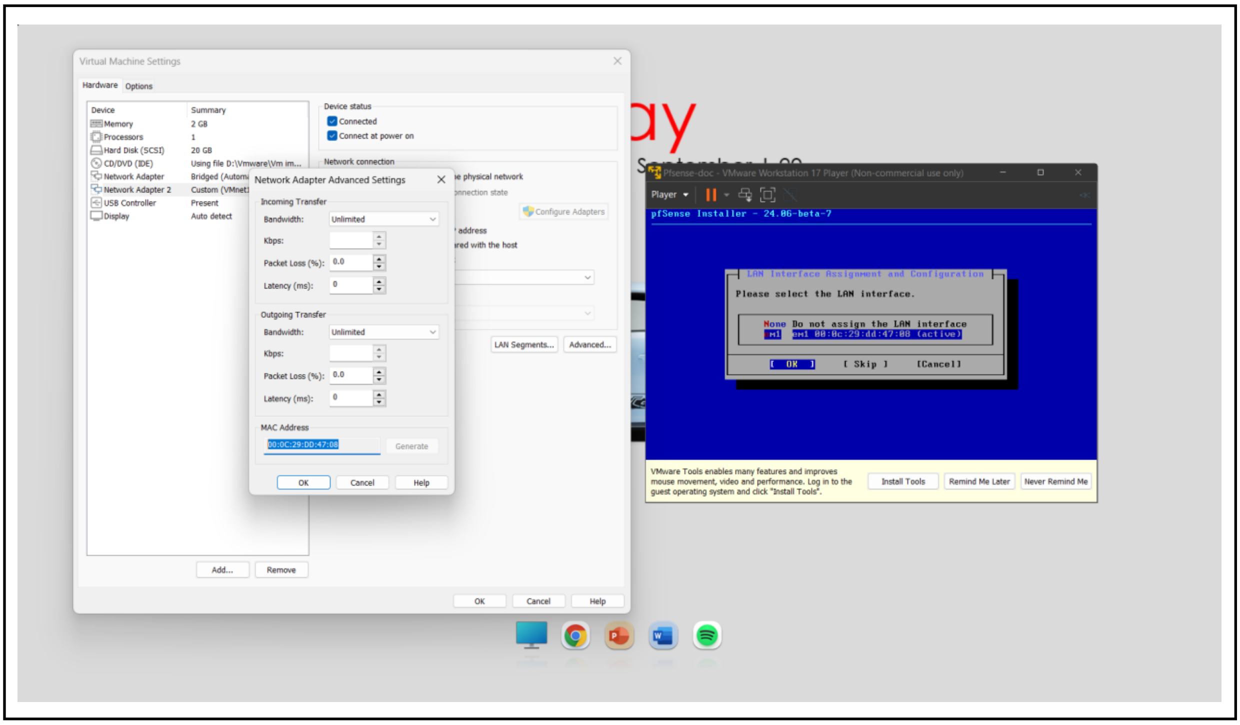
Pfsense-doc - VMware Workstation 17 Player (Non-commercial use only)

```
pfSense Installer - 24.06-beta-7

WAN Interface Assignment and Configuration

Please select the WAN interface.

   em0  em0 00:0c:29:dd:47:fe (active)
   em1  em1 00:0c:29:dd:47:08 (active)

        [  OK  ]      [Cancel]
```

On the next screen there are two adapters eM0 and eM1 with MAC addresses respectively. Let's take a glance at the vm settings and locate to the bridged network adapter's advanced tab. We see the MAC address of the adapter, same can be checked for the second adapter which is VMnet0. According to eM0 the bridged adapter is assigned and the eM1 is the VMnet0 adapter we configured when creating the VM. The eM0 should be assigned as WAN interface.

After configuring the eM0 which has MAC address of "00:0C:29:DD:47:FE", the WAN interface is assigned to the eM0 which is the bridged adapter in the VM settings.

Then in the next step the installer ask us to configure the LAN interface for this the next adapter should be assigned. The eM1 in the installer signifies the VMnet10 in the VM settings of the next network adapter and LAN interface is configured to this eM1 interface which has a MAC address of "00:0C:29:DD:47:08". This is configured to be our LAN interface for pfSense.



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file D:\Vmware\Vm im...
Network Adapter	Bridged (Automa
Network Adapter 2	Custom (VMnet1
USB Controller	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

Network Adapter Advanced Settings

Incoming Transfer

Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

Latency (ms): 0

Outgoing Transfer

Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

Latency (ms): 0

MAC Address

00:0C:29:DD:47:08

Pfsense-doc - VMware Workstation 17 Player (Non-commercial use only)

```
pfSense Installer - 24.06-beta-7

LAN Interface Assignment and Configuration
Please select the LAN interface.

None  Do not assign the LAN interface
em1   em1 00:0c:29:dd:47:08 (active)

[  OK  ]     [ Skip ]     [Cancel]
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

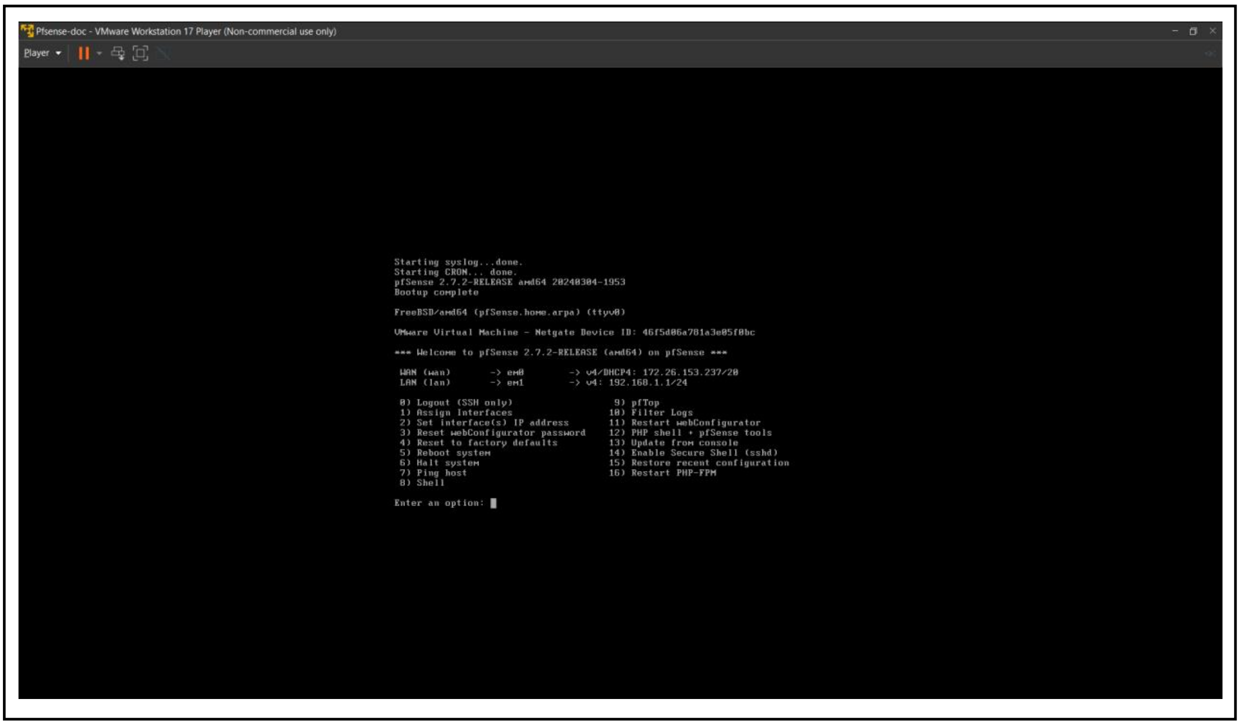
After configuring we can proceed with the installation by checking the option “Proceed with the Installation”. Then the pfSense will try to reach its backend server and proceed us with the next step of “Install CE”. By checking the option the installation of pfSense starts. On installation completion the VM restarts and gives us the LAN IP of pfSense that can be entered in a web browser and we can access the web portal for pfSense.

For obtaining the web portal, we cannot put the IP in the browser which is on the host. We should create a windows or a Linux distro with the network adapter setting configured to be set as VMnet10.

We need to run the pfSense and the Windows VM at a stretch to make this possible.

NOTE: Running more than one VM on a host machine simultaneously can drain out memory and processor from the host machine which in terms slows down the host machine and can cause errors.

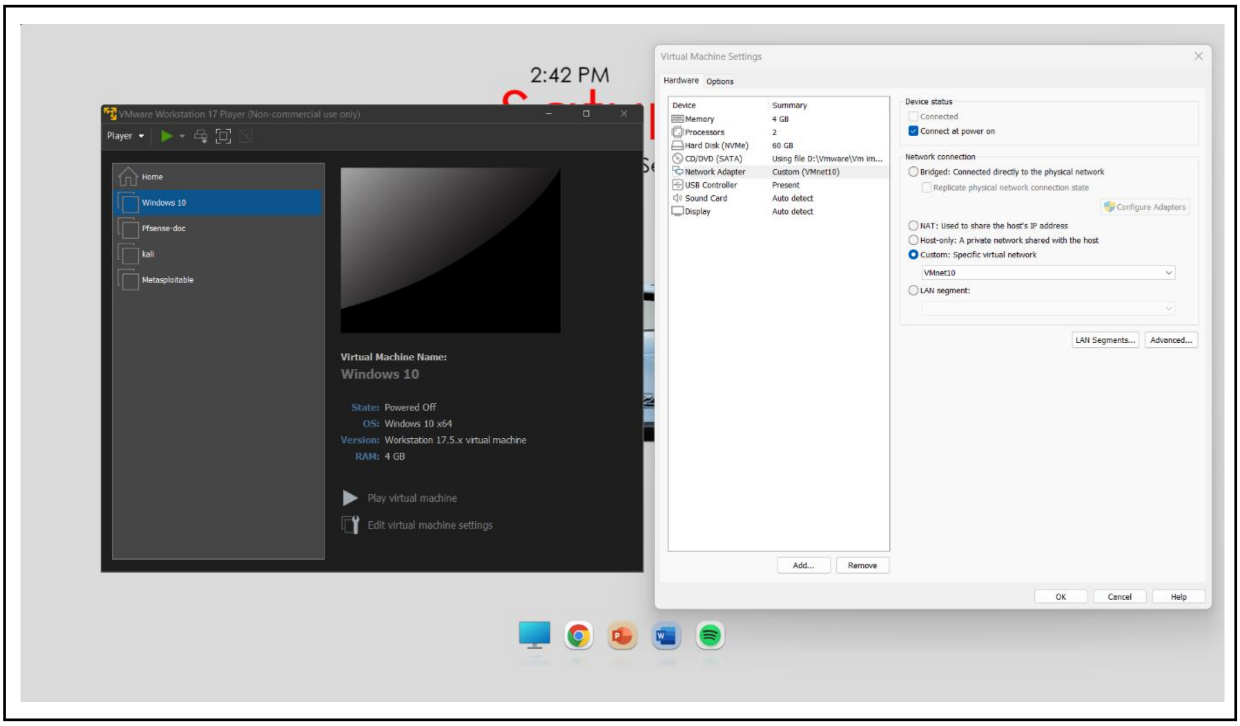
Accessing the web portal


Pfsense-doc - VMware Workstation 17 Player (Non-commercial use only)
Player

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: 46f5d06a781a3e05f0bc

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

 WAN (wan)       -> em0        -> v4/DHCP4: 172.26.153.237/20
 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: █
```

After complete installation the console shows us the WAN and LAN interface IP. The default IP address for the pfSense web portal is shown as 192.168.1.1/24.

For accessing the web portal create a new windows VM and set the network adapter of windows machine to VMnet0 which is our pfSense eM1 which is LAN.



Virtual Machine Name: Windows 10

State: Powered Off
OS: Windows 10 x64
Version: Workstation 17.5.x virtual machine
RAM: 4 GB

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Using file D:\Vmware\Vm im...
Network Adapter	Custom (VMnet10)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

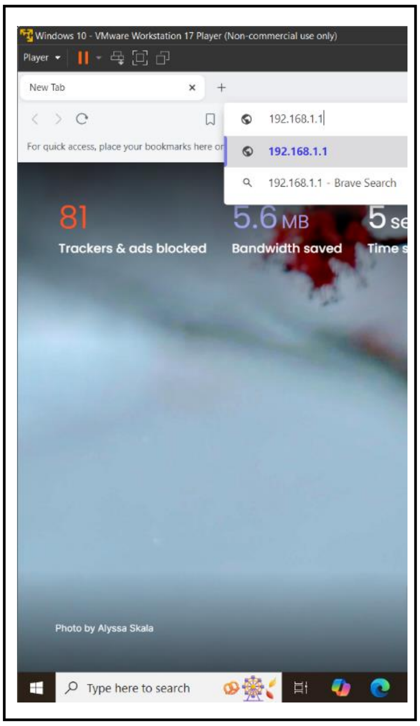
Device status

□ Connected
☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet10
○ LAN segment:

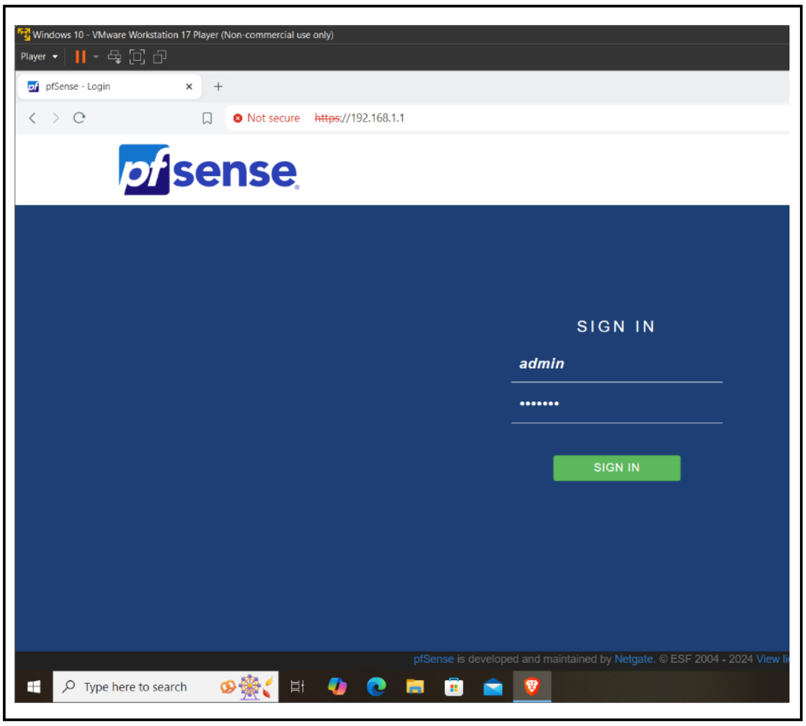
After changing the network settings on the windows VM we are ready to fire up the VM. On the browser of the windows VM type the default LAN IP which we found on the pfSense (192.168.1.1).


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
New Tab
For quick access, place your bookmarks here on
81
Trackers & ads blocked
5.6 MB
Bandwidth saved
Photo by Alyssa Skala
Type here to search

192.168.1.1

192.168.1.1

192.168.1.1 - Brave Search


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
pfSense - Login
Not secure
https://192.168.1.1
pfsense
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View li
Type here to search

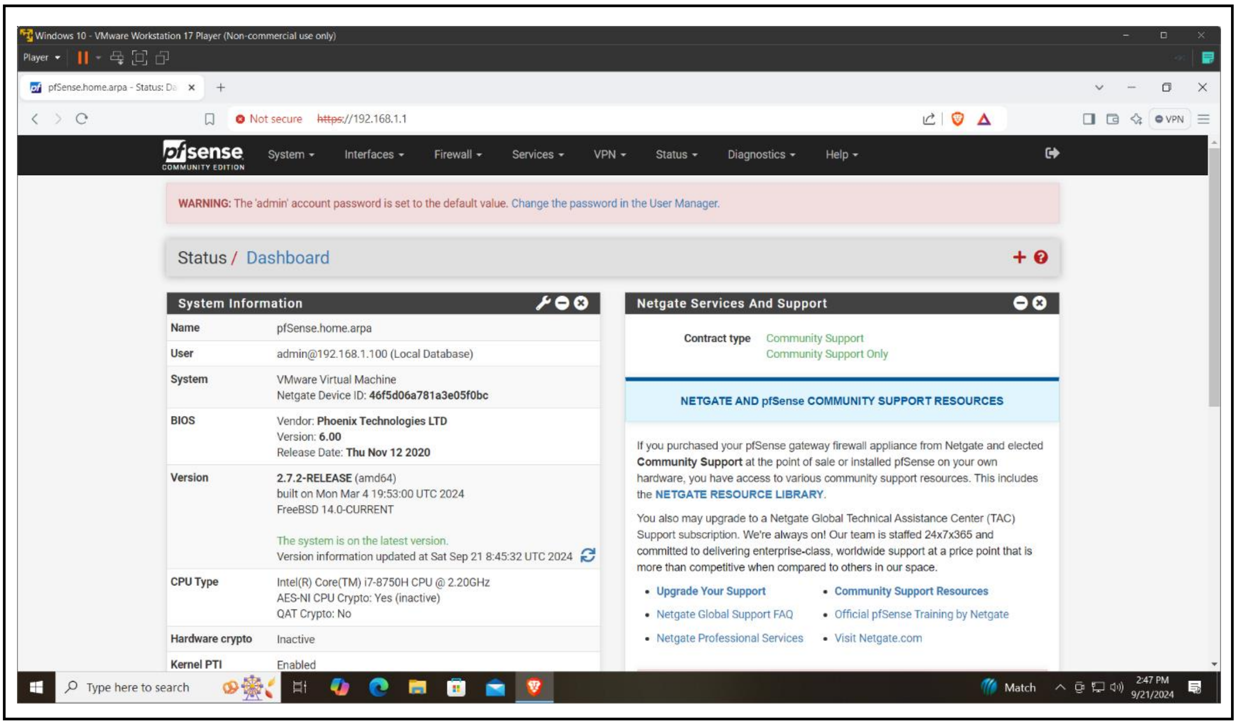
SIGN IN

admin

•••••••

SIGN IN

The default username and password is “admin” and “pfsense” respectively.



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

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.1.100 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **46f5d06a781a3e05f0bc**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Thu Nov 12 2020**
Version	**2.7.2-RELEASE** (amd64) built on Mon Mar 4 19:53:00 UTC 2024 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Sat Sep 21 8:45:32 UTC 2024
CPU Type	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled

Netgate Services And Support

Contract type	Community Support Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

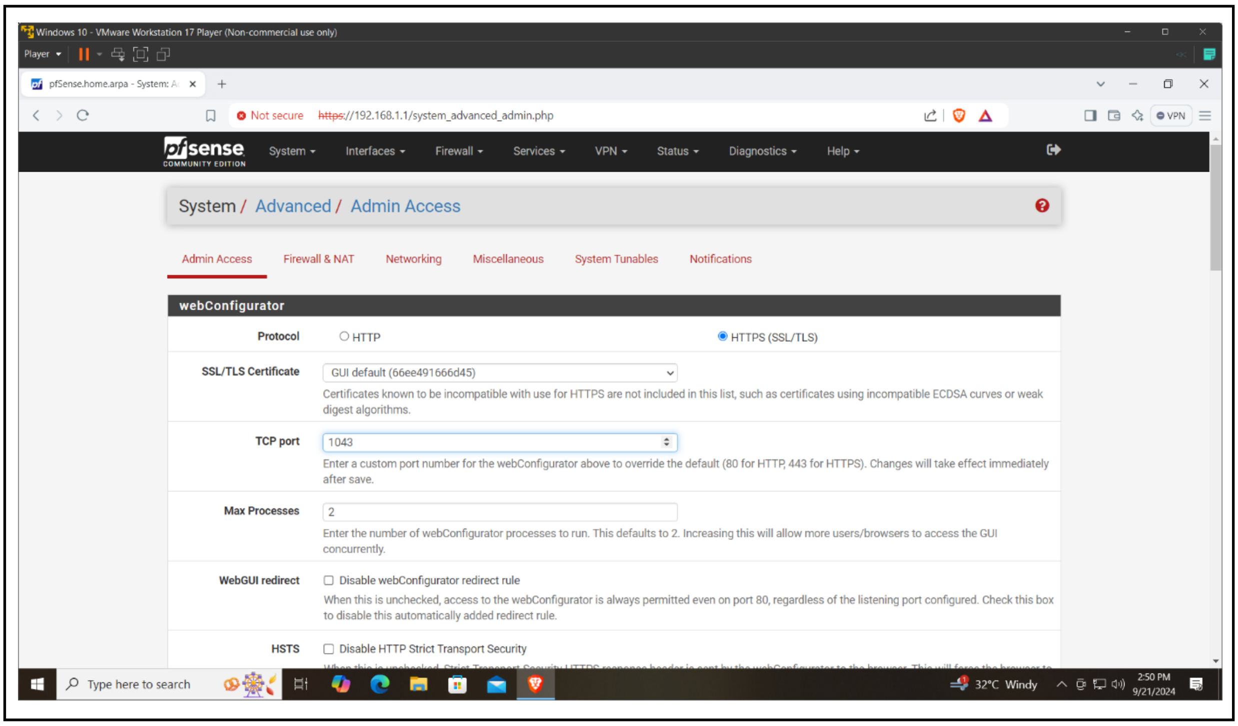
- **Upgrade Your Support**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

Security

I recommend to change the default login credentials and the default LAN IP which gives us more security by not logging in the unauthorized people.

After changing the default password, set a TCP port number for the webConfigurator to override the default 80 for HTTP, 443 for HTTPS.

Go to System>Advanced>TCP port to set a new port number.

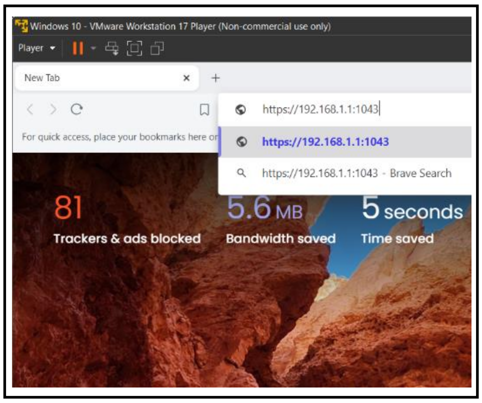


System / Advanced / Admin Access

webConfigurator

Protocol	○ HTTP ● HTTPS (SSL/TLS)
SSL/TLS Certificate	GUI default (66ee491666d45) Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
TCP port	1043 Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
Max Processes	2 Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.
WebGUI redirect	□ Disable webConfigurator redirect rule When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.
HSTS	□ Disable HTTP Strict Transport Security

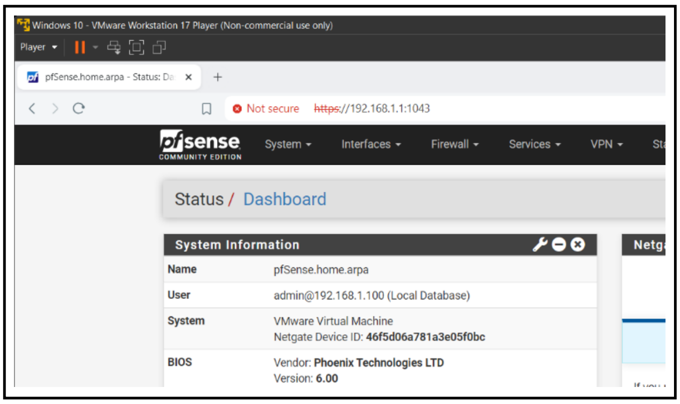
Now without typing the full IP address without the port number in the browser, will not see the web portal.


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
New Tab
For quick access, place your bookmarks here or
81
Trackers & ads blocked
5.6 MB
Bandwidth saved
5 seconds
Time saved

https://192.168.1.1:1043

https://192.168.1.1:1043

https://192.168.1.1:1043 - Brave Search


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
pfSense.home.arpa - Status: Da
Not secure
https://192.168.1.1:1043
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Netg

Status / Dashboard

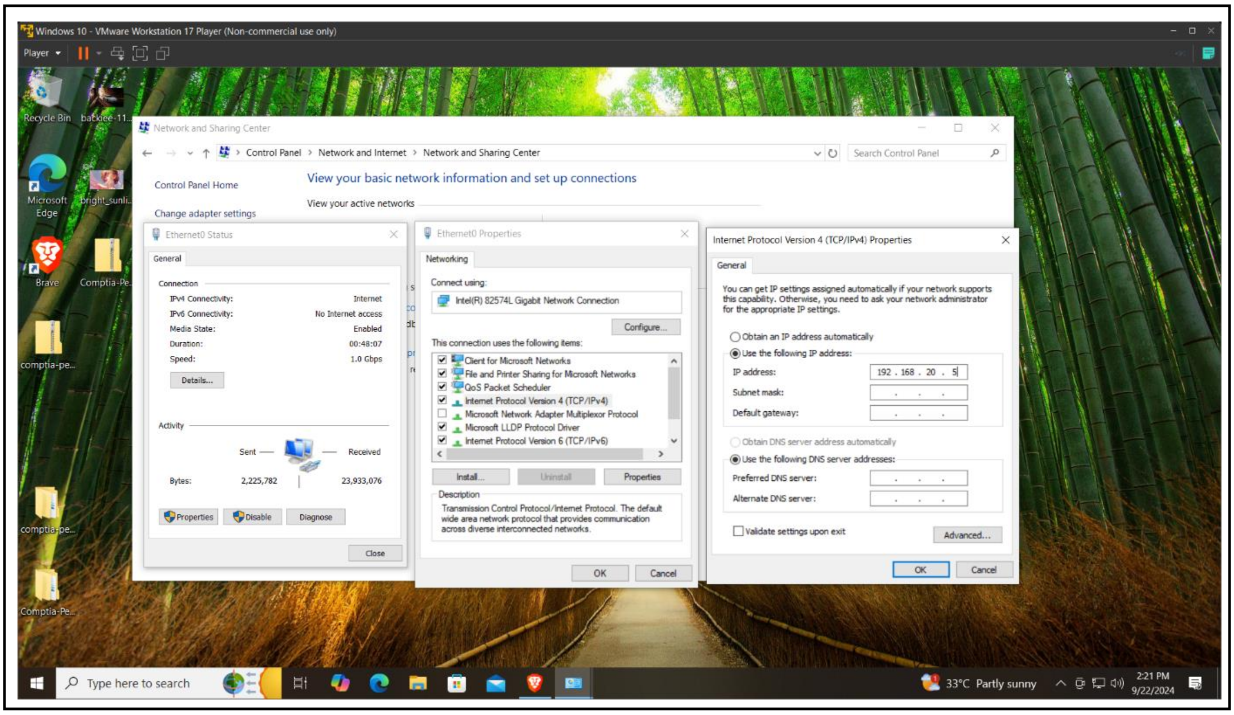
System Information

Name	pfSense.home.arpa
User	admin@192.168.1.100 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 46f5d06a781a3e05f0bc
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00

For security measures the LAN IP should be changed for the pfSense and new DHCP range should be configured.

By going to Interfaces>LAN>IPV4 address, set a new IP address. In my case it is 192.168.20.1. After setting the address click on save and scroll top, there will be a option to apply changes click there. After clicking there your Windows VM will not receive internet. This is because the new IP you changed affects the DHCP range of IP. By forcing the windows network settings to use the new changed IP will bring back the the web portal.

Go to control panel>Network and sharing centre>your adapter>properties>Internet protocol version 4(TCP/IPv4)>Use the following IP address and enter the changed LAN IP and just tap on the Subnet to auto set it.


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)

Control Panel > Network and Internet > Network and Sharing Center

View your basic network information and set up connections

Ethernet0 Status

- IPv4 Connectivity: Internet
- IPv6 Connectivity: No Internet access
- Media State: Enabled
- Duration: 00:48:07
- Speed: 1.0 Gbps
- Bytes: Sent 2,225,782 Received 23,933,076

Ethernet0 Properties

Connect using: Intel(R) 82574L Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

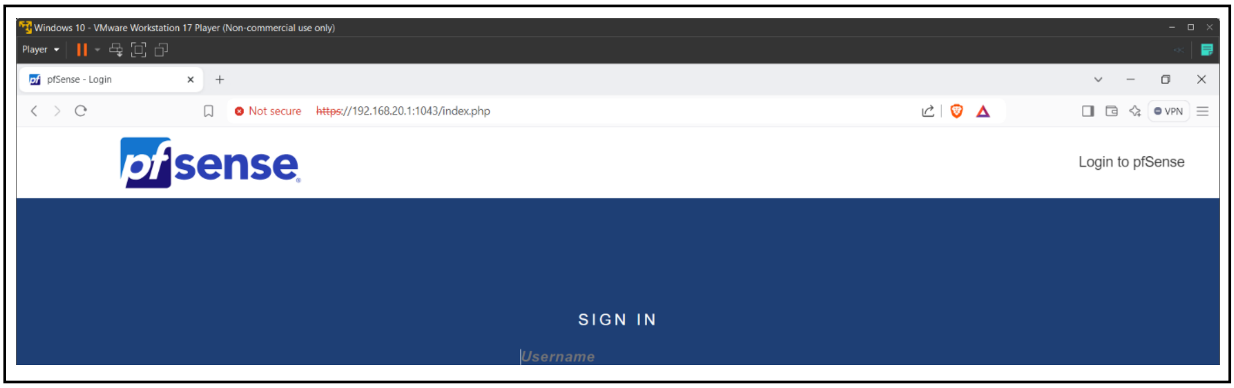
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 20 . 5
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Now entering the new changed IP on the browser will give the web portal.


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)

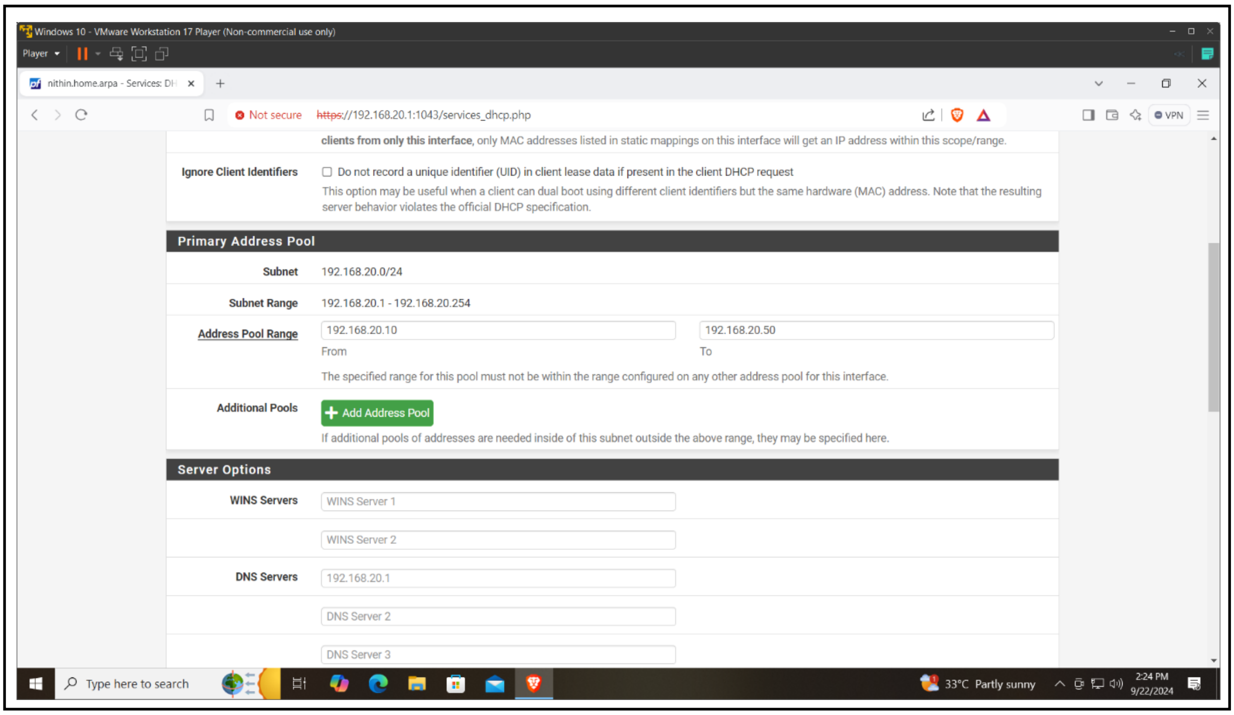
pfSense - Login

Not secure ~~https~~://192.168.20.1:1043/index.php

Login to pfSense

SIGN IN

After login go to Services>DHCP server and change the DHCP range. This change will allow the pfsense to automatically give IP address to the connecting client from the DHCP pool range which you will provide.



Windows 10 - VMware Workstation 17 Player (Non-commercial use only)

nithin.home.arpa - Services: DHCP

Not secure https://192.168.20.1:1043/services_dhcp.php

clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore Client Identifiers: □ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet: 192.168.20.0/24

Subnet Range: 192.168.20.1 - 192.168.20.254

Address Pool Range: From 192.168.20.10 To 192.168.20.50

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools: + Add Address Pool

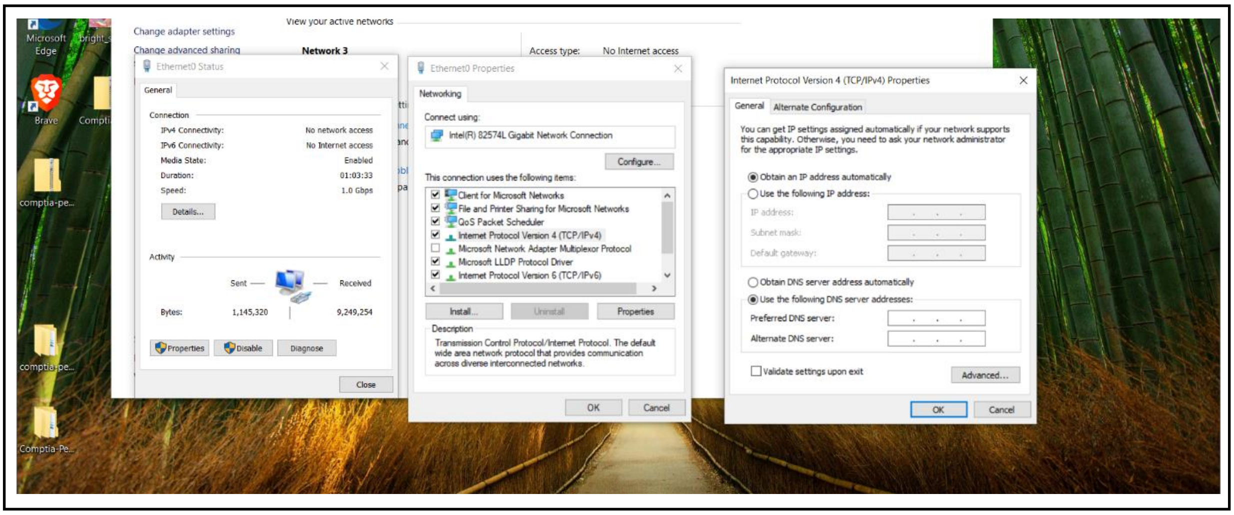
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers: WINS Server 1, WINS Server 2

DNS Servers: 192.168.20.1, DNS Server 2, DNS Server 3

After setting the DHCP you can change the network setting on the Network sharing center which in terms makes the pfsense to give IP from its DHCP pool to its client. Once again going to control panel>Network and sharing centre>your adapter>properties>Internet protocol version 4(TCP/IPv4) and set to the defaults "Obtain the IP address automatically"



View your active networks

Network 3 — Access type: No Internet access

Ethernet0 Status — General

Connection

IPv4 Connectivity: No network access
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 01:03:33
Speed: 1.0 Gbps

Activity

Bytes: Sent 1,145,320 | Received 9,249,254

Ethernet0 Properties — Networking

Connect using: Intel(R) 82574L Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description: Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties — General | Alternate Configuration

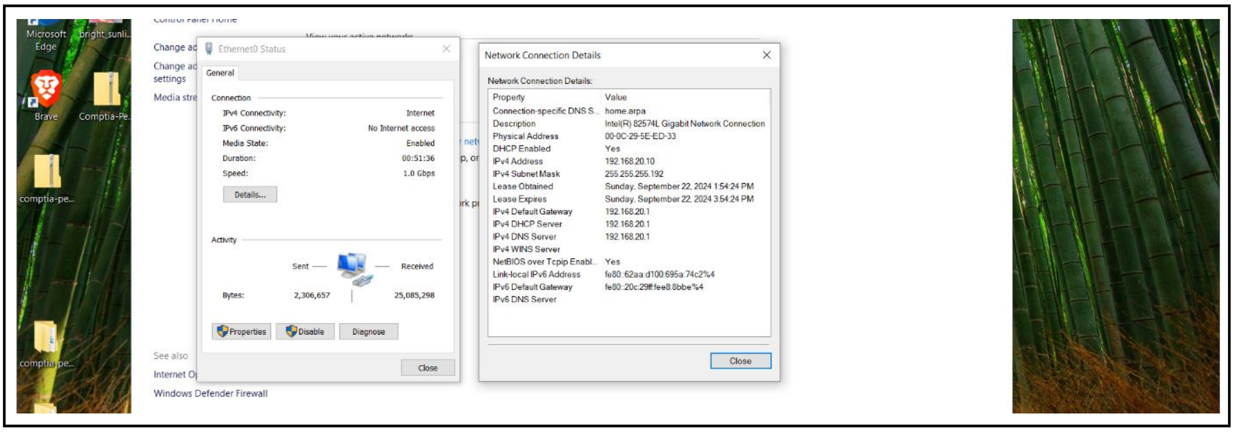
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

□ Validate settings upon exit

Now we can see the details of the IP which is allocated from the available pool of address from pfsense DHCP server.



Connection

IPv4 Connectivity: Internet
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 00:51:36
Speed: 1.0 Gbps

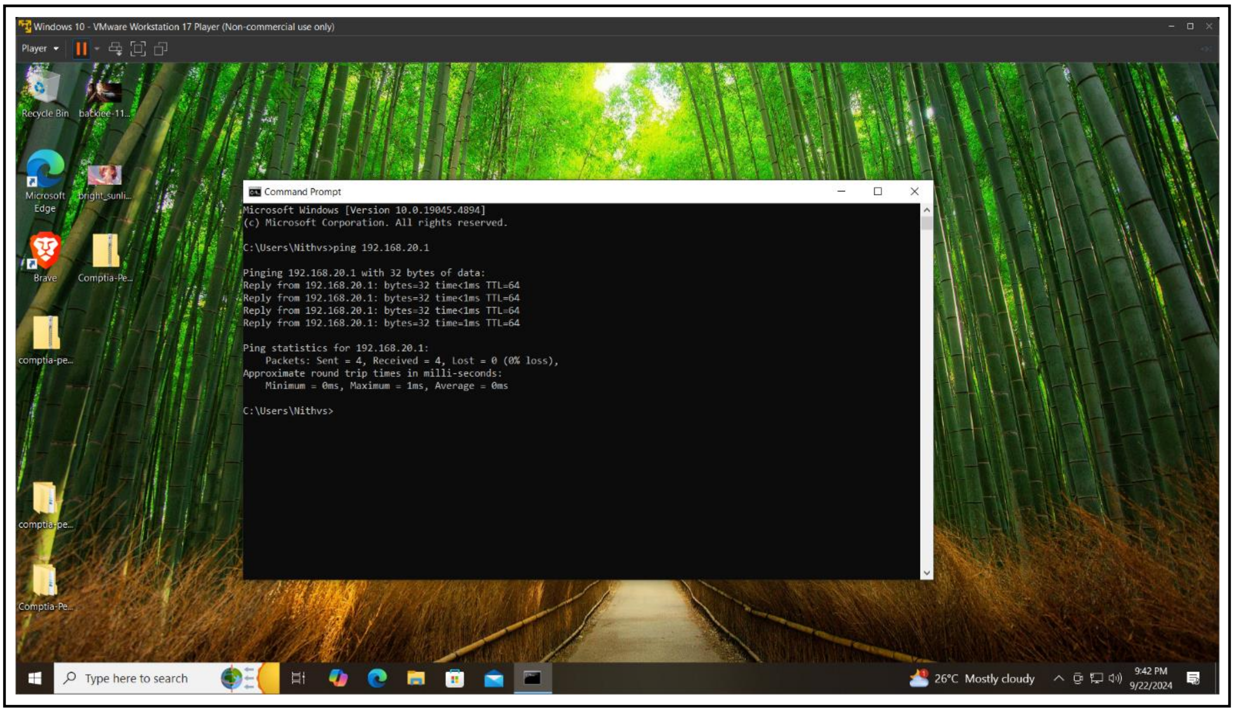
Bytes: 2,306,657 | 25,085,298

Network Connection Details:

Property	Value
Connection-specific DNS S...	home.arpa
Description	Intel(R) 82574L Gigabit Network Connection
Physical Address	00-0C-29-5E-ED-33
DHCP Enabled	Yes
IPv4 Address	192.168.20.10
IPv4 Subnet Mask	255.255.255.192
Lease Obtained	Sunday, September 22, 2024 1:54:24 PM
Lease Expires	Sunday, September 22, 2024 3:54:24 PM
IPv4 Default Gateway	192.168.20.1
IPv4 DHCP Server	192.168.20.1
IPv4 DNS Server	192.168.20.1
IPv4 WINS Server	
NetBIOS over Tcpip Enabl...	Yes
Link-local IPv6 Address	fe80::62aa:d100:695a:74c2%4
IPv6 Default Gateway	fe80::20c:29ff:fee8:8bbe%4
IPv6 DNS Server	

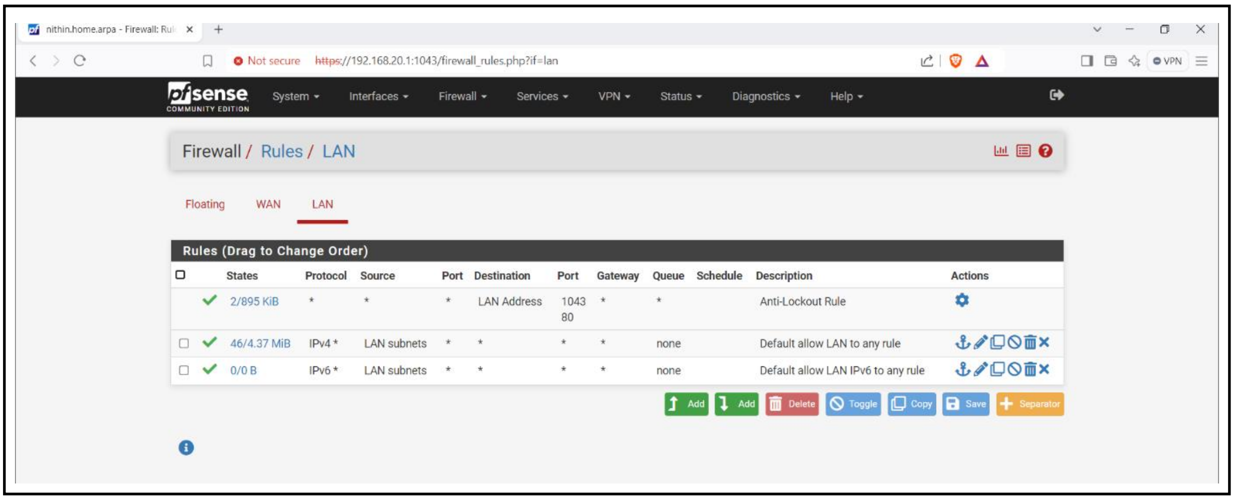
Basic Configuration

By changing the default LAN IP and configuring the new DHCP range of IP and by checking the pfsense firewall is alive or not by pinging the pfsense using its IP on the Windows VM confirms that the pfsense is automatically assigning the IP to the windows VM and the Windows VM is accessing the internet.



```
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Nithvs>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time<1ms TTL=64
Reply from 192.168.20.1: bytes=32 time<1ms TTL=64
Reply from 192.168.20.1: bytes=32 time<1ms TTL=64
Reply from 192.168.20.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Nithvs>
```

The default LAN firewall rules are shown in the pfsense Web interface, going to Firewall>Rules>LAN.



Firewall / Rules / LAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	2/895 KiB	*	*	*	LAN Address	1043 80	*	*		Anti-Lockout Rule	⚙
□	✓	46/4.37 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	⚓✎❐⊘🗑✕

My basic Configuration of the pfsense firewall is configured and the windows VM is receiving the internet. But this basic rule allows all the network traffic to the LAN.

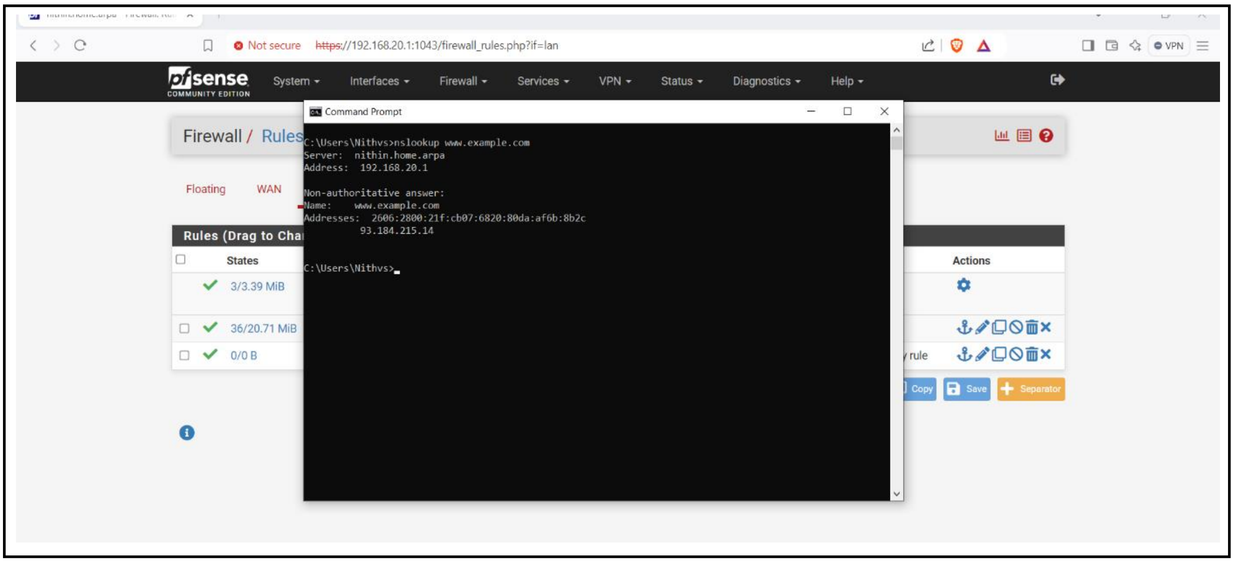
Now as a beginner I want to block some basic website that the windows VM should not access.

Setting up a new firewall Rule

Let's block a website which is www.example.com.

In command prompt of the windows VM type the command

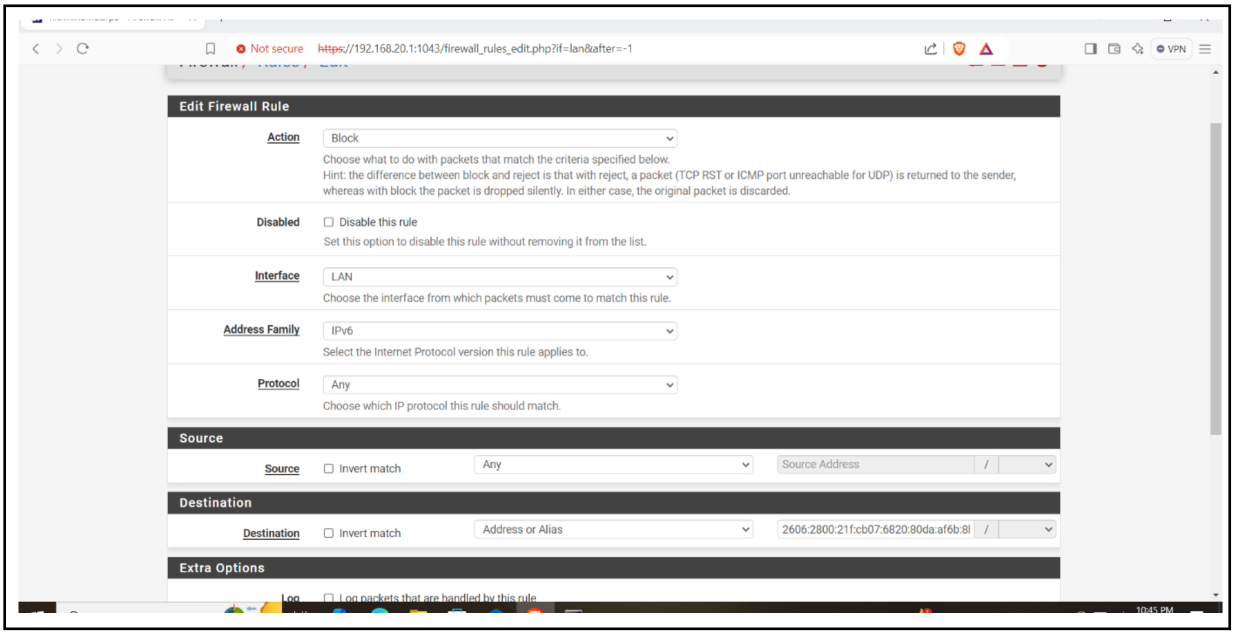
nslookup www.example.com to view the website IP address. In my case there is a output of both IPv4 and IPv6 address.



```
C:\Users\Nithvs>nslookup www.example.com
Server:  nithin.home.arpa
Address:  192.168.20.1

Non-authoritative answer:
Name:    www.example.com
Addresses:  2606:2800:21f:cb07:6820:80da:af6b:8b2c
          93.184.215.14


C:\Users\Nithvs>
```

Now the both IP address should be added to the LAN rules as separate rules.

Copy the IPv6 address and go to the web portal, go to Firewall>Rules>LAN and add (up arrow) option. Adding the rule as mentioned below.



Not secure https://192.168.20.1:1043/firewall_rules_edit.php?if=lan&after=-1

Edit Firewall Rule

Action: Block

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

Disabled: □ Disable this rule

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

Interface: LAN

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

Address Family: IPv6

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Any | Source Address /

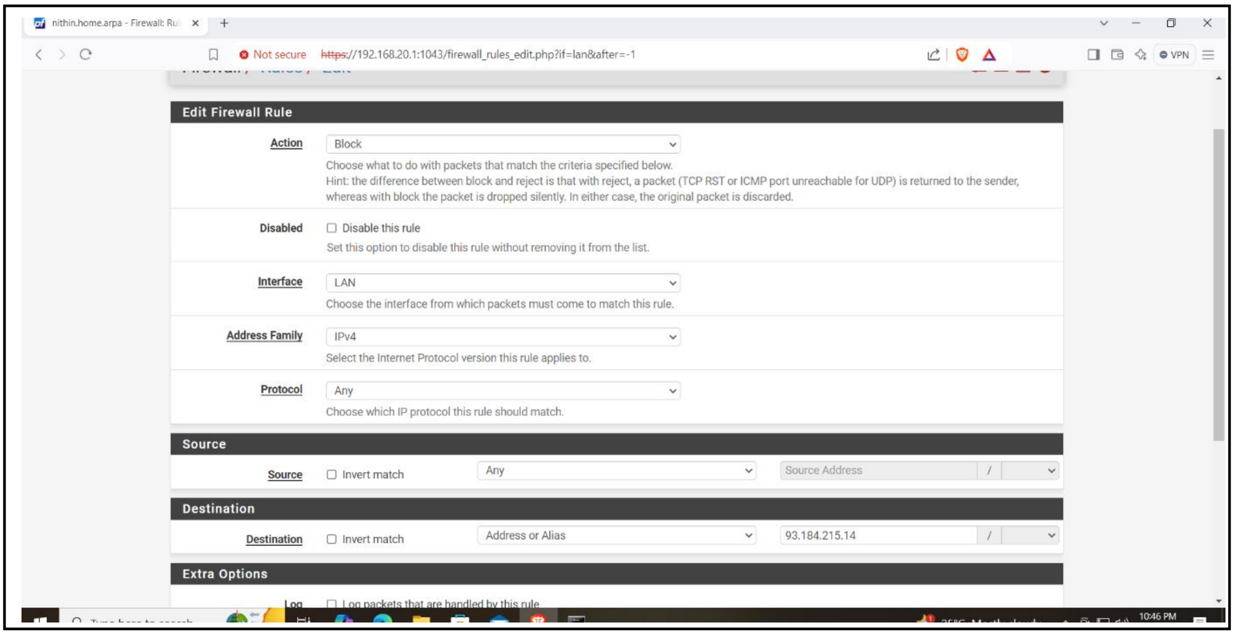
Destination

Destination: □ Invert match | Address or Alias | 2606:2800:21f:cb07:6820:80da:af6b:8l /

Extra Options

Log: □ Log packets that are handled by this rule

Copy the IPv4 address and go to the web portal, go to Firewall>Rules>LAN and add (up arrow) option. Adding the rule as mentioned below.



nithin.home.arpa - Firewall: Ru

Not secure https://192.168.20.1:1043/firewall_rules_edit.php?if=lan&after=-1

Edit Firewall Rule

Action: Block

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

Disabled: □ Disable this rule

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

Interface: LAN

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

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Any | Source Address /

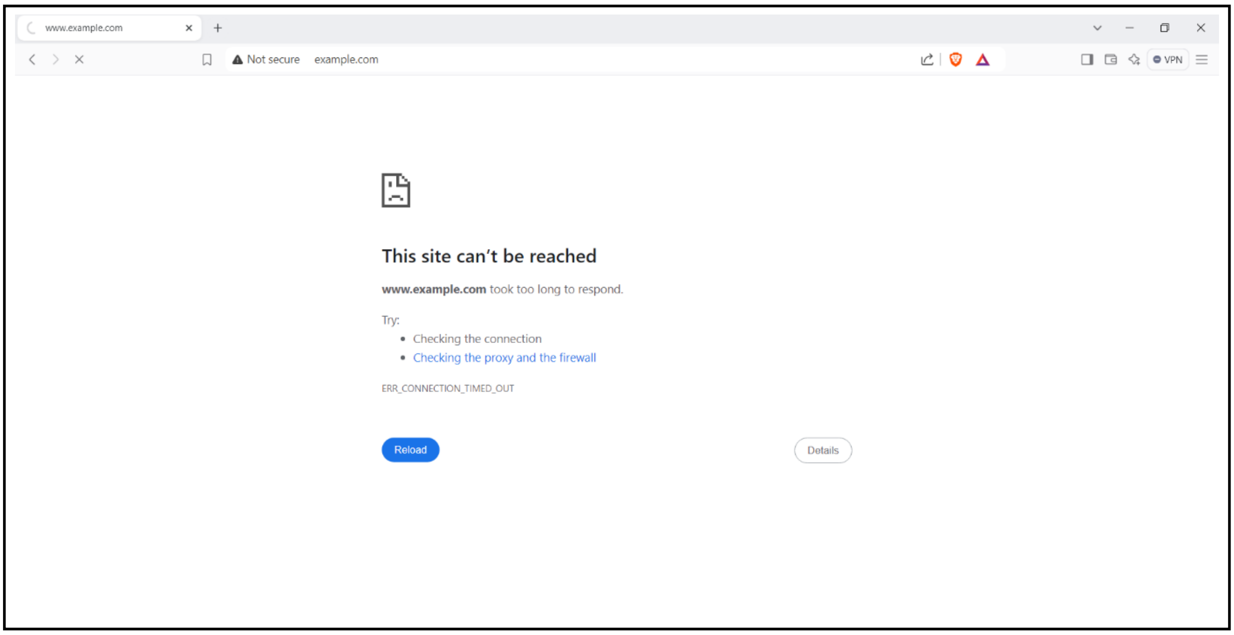
Destination

Destination: □ Invert match | Address or Alias | 93.184.215.14 /

Extra Options

Log: □ Log packets that are handled by this rule

By this configuration, clearing all the browsing data and cache, searching for the website www.example.com, the firewall now blocks the website and it is inaccessible.



This site can't be reached

www.example.com took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

Conclusion

In this project, I explored the process of setting up a pfSense firewall within a virtual machine (VM) environment, which significantly enhanced my understanding of both firewall technology and virtualization.

Key Learnings:

- Understanding firewall
- Hands-on experience with pfsense
- Virtualization skills
- Importance of documentation

Overall, this project has been an invaluable learning experience, enhancing my technical abilities and preparing me for future endeavors in network security and administration.