# pfSense Installation

Lab Goal:

Creatting and installing pfSense VM.

Lab Requrenments:

1. Host OS (Wndows or Unix/Linux)
2. VMWare workstation Pro or Fusion
3. Internet Connection



Contents

[pfSense Installation 1](#_Toc169531244)

[PfSense 3](#_Toc169531245)

[Netgate 5](#_Toc169531246)

[Task 1: Download pfSense ISO 6](#_Toc169531247)

[Step 1: Create an Account 6](#_Toc169531248)

[Step 2: “Purchase” pfSense 6](#_Toc169531249)

[Step 3: Unpack pfSense Archive 8](#_Toc169531250)

[Task 2: Creating a pfSense VM in VMWare Workstation: 9](#_Toc169531251)

[Step:1 New Virtual Machine Wizard: 9](#_Toc169531252)

[Step 2: Customize Hardware 16](#_Toc169531253)

[Task 3: pfSense installation 21](#_Toc169531254)

[Step 1: Power on the Virtual Machine 22](#_Toc169531255)

[Step 2: Installation Process 22](#_Toc169531256)

[Step 3: pfSense menu 32](#_Toc169531257)

[Step 4: Unmount ISO 33](#_Toc169531258)

[Task 4 – Connecting to Web Interface of pfSense 34](#_Toc169531259)

[Step 1. Connect your Debian VM to LAN Internal Network 34](#_Toc169531260)

[Step 2: Connect to pfSense WebGUI 35](#_Toc169531261)

[Step 3 – pfSense Configuration Wizard 37](#_Toc169531262)

[Task 5 – Create a new user 45](#_Toc169531263)

[Step 1: Create a new Administrator account 45](#_Toc169531264)

[Step 2: Disable Admin login 52](#_Toc169531265)



## PfSense

pfSense is a highly configurable, secure, and feature-rich firewall and routing platform suitable for both small and large network environments. It leverages the robustness of FreeBSD and the powerful pf firewall to provide advanced networking capabilities. By combining these with extensive VPN support, high availability, traffic shaping, and security services, pfSense is a go-to solution for network administrators seeking to build and maintain secure and efficient networks.

Overview of pfSense

1. Firewall and Packet Filtering

Stateful Inspection: pfSense uses a stateful packet inspection engine, pf, from OpenBSD, which tracks the state of active connections and makes decisions based on the context of traffic.

Rules Configuration: Rules can be defined based on IP address, protocol, port, and interface. pfSense allows for complex rule sets with granular control.

Aliases: Users can create aliases for IP addresses, networks, and ports to simplify the management of firewall rules.

2. Network Address Translation (NAT)

* Port Forwarding: Easily set up port forwarding rules to direct traffic from one port to another or to an internal network address.
* 1:1 NAT: Maps one external IP address to one internal IP address.
* Outbound NAT: Configures how internal IP addresses are translated to the external IP address range.

3. Virtual Private Network (VPN)

* OpenVPN: Fully supports OpenVPN, offering both site-to-site and remote access VPNs. It includes options for encryption algorithms, authentication methods, and multi-factor authentication (MFA).
* IPsec: Supports IPsec VPNs with various encryption and hashing algorithms. Advanced features include mobile IPsec for VPN clients and VTI (Virtual Tunnel Interface) support.
* PPTP: Although less secure, PPTP is available for legacy support and simple configurations.

4. High Availability and Redundancy

* CARP: Implements the Common Address Redundancy Protocol, allowing multiple pfSense systems to share a virtual IP address, providing failover capabilities.
* pfSync: Synchronizes states between primary and backup firewalls, ensuring seamless failover.
* XMLRPC: Synchronizes configuration settings between pfSense nodes in a high-availability setup.

5. Load Balancing and Failover

* Multi-WAN: Supports multiple WAN connections, allowing for load balancing and failover. Traffic can be balanced based on round-robin, weighted round-robin, or failover.
* Server Load Balancing: Distributes incoming connections across multiple backend servers to balance the load and improve redundancy.

6. Advanced Networking Features

* VLANs: pfSense supports IEEE 802.1Q VLAN tagging, allowing for the segmentation of network traffic.
* DHCP Services: Integrated DHCP server and relay capabilities.
* Dynamic DNS: Keeps your dynamic IP address mapped to a hostname.
* DNS Resolver: Unbound DNS resolver can operate in resolver or forwarder mode.

7. Traffic Shaping and QoS

* Traffic Shaping: Implements various traffic shaping techniques to manage bandwidth, including HFSC (Hierarchical Fair Service Curve) and CBQ (Class-Based Queuing).
* Limiter: Allows rate-limiting of traffic based on IP, protocol, and port.

8. Security Services

* Snort and Suricata: pfSense integrates with these popular IDS/IPS systems to provide real-time traffic analysis and blocking of threats.
* pfBlockerNG: Enhances firewall capabilities by providing geo-blocking and IP reputation filtering.
* TLS/SSL Inspection: Allows for deep packet inspection of encrypted traffic to identify threats.

9. Monitoring and Reporting

* Real-Time Graphs: Provides visual representation of bandwidth usage, interface statistics, and system performance.
* Logging: Detailed logs for firewall events, system events, and VPN connections. Supports remote logging to a syslog server.
* Package Manager: Offers additional functionalities such as ntopng for network traffic analysis, BandwidthD for bandwidth monitoring, and many others.

10. Management and Interfaces

* Web-Based GUI: Provides a user-friendly interface for configuration and management. Built using PHP and Bootstrap.
* CLI Access: Provides advanced management capabilities through SSH or console access.
* Backup and Restore: Supports configuration backups and restores, ensuring quick recovery from failures.



## Netgate

**Netgate** is the company behind **pfSense**, an open-source firewall and router software based on FreeBSD. Netgate develops, maintains, and supports pfSense, offering both software and hardware solutions for network security.

pfSense: Provides advanced firewall, router, VPN, NAT, traffic shaping, and monitoring capabilities.

Netgate Hardware: Produces optimized appliances (e.g., SG-1100, SG-5100) for running pfSense, ensuring high performance and reliability.

TNSR: A high-performance router software by Netgate, using Vector Packet Processing (VPP) and DPDK for data centers and ISPs.

Professional Services: Netgate offers support, consulting, and training for pfSense users.

Community and Ecosystem: pfSense benefits from a large, active user community, extensive documentation, and a commitment to open-source principles.

# Task 1: Download pfSense ISO

For the purposes of this lab, you will be provided an ISO, but the account creation and purchase process is included below for reference.

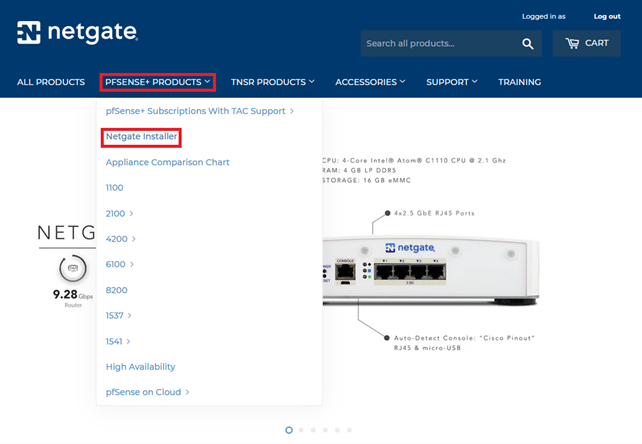
pfSense used to be free to download, but as of 2024 requires a “purchase” of AUD $0.00 to be made using a netgate account.

### Step 1: Create an Account

Link: Create an [account](https://shop.netgate.com/account/register).

### Step 2: “Purchase” pfSense

1. Select “Negate Installer” under the PFSESE+ Products tab.



1. Select the Installation Image. Open the dropdown menu and select the “AMD64 ISO IPMI/Virtual Machines” as the Image Type.
2. Add your select Image Type to the cart.

A screenshot of a computer

Description automatically generated

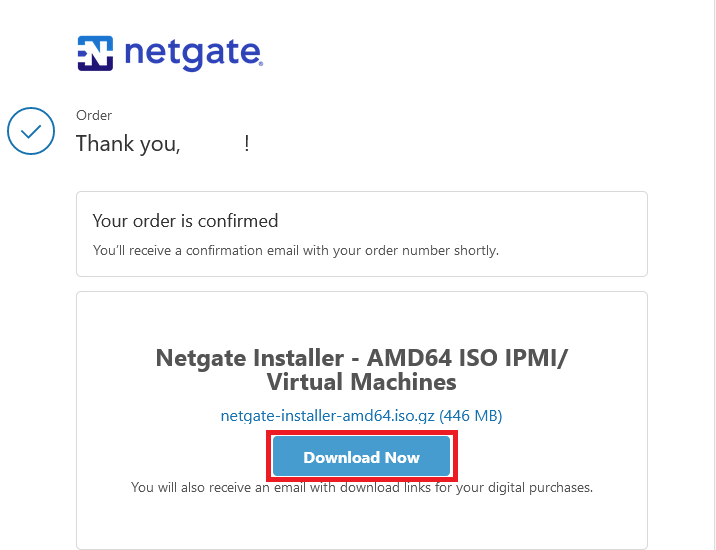
1. Enter your Cart and select checkout.
2. Fill in the billing address, agree to the terms and conditions, and complete the purchase with the Complete Order button.

**NOTE: Use your private details and private email address as you will be keeping this account after you finish TAFE course, and you will lose access to TAFE email.**

A screenshot of a computer

Description automatically generated

1. Once the order has been completed, click Download Now to download the pfSense archive.



### Step 3: Unpack pfSense Archive.

The downloaded pfSense file needs to be decompressed before it can be used.

1. Use 7ZIP to unpack the archive. Right click on the netgate-installer-amd64.ios.gz archive, select 7ZIP, and Extract

A screenshot of a computer

Description automatically generated

1. The ISO file is now ready to be used with our Virtual Machine



Additional documentation for pfSense can be found on official website: [pfSense Documentation](https://docs.netgate.com/pfsense/en/latest/)

Keep in mind that releases change, so ensure that you are using documentation that is for your specific version as requirements and features might change.

# Task 2: Creating a pfSense VM in VMWare Workstation:

Create a new Virtual Machine to install pfSense.

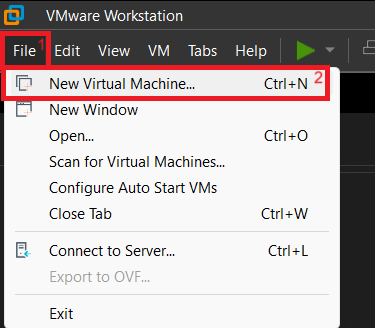
VM Specifications:

* CPU Cores: 2
* Memory: 1024MB
* HDD: 10GB
* Network adapter: NAT
* Network Adapter 2: VMnet1 (Host Only)

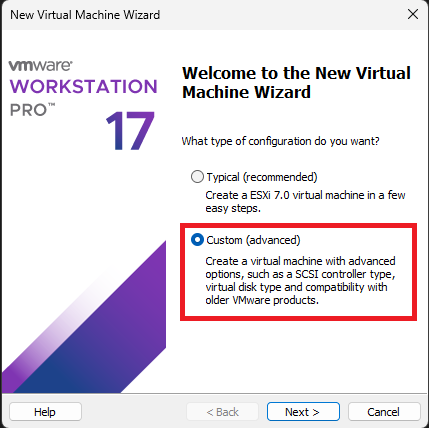
To accomplish this task, you will use the Custom (advanced) option in the New Virtual Machine Wizard.

### Step:1 New Virtual Machine Wizard:

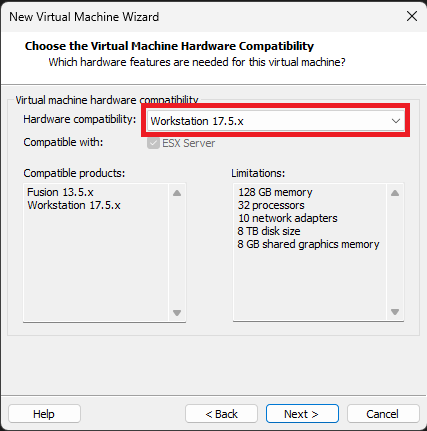
1. Open the New Virtual Machine Wizard by clicking File and selecting New Virtual Machine



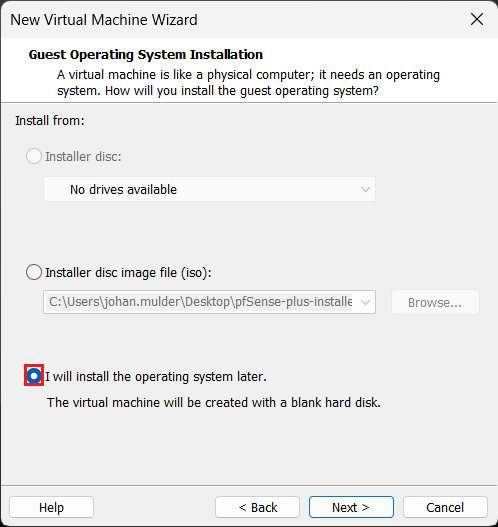
1. Select Custom (advanced) and click next.



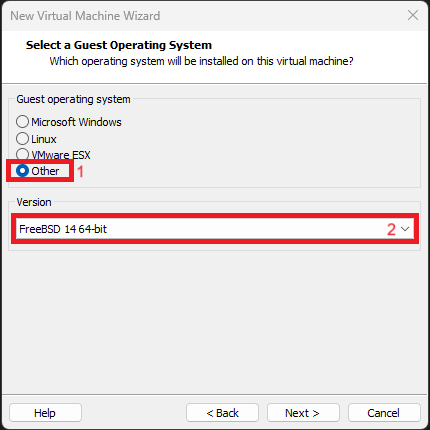
1. Use the dropdown to select the hardware compatibility. The latest version of Workstation is recommended (17.5.x at time of writing). Click next.



1. Select I will install the operating system later. Click next.



1. For the Guest OS, use “Other”, and for the version use “FreeBSD 14 64-bit”. Click next.



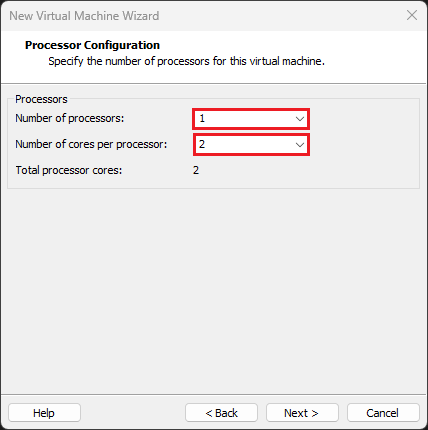
* + If you are using older versions of pfSense, you can find the required version of FreeBSD to use in the “Version of pfSense software and FreeBSD” [Document](https://docs.netgate.com/pfsense/en/latest/releases/versions.html)

1. Name your VM “pfSense Lab”, and select the location for the VM files to be saved. Click next.

A screenshot of a computer

Description automatically generated

1. Allocate one (1) Processor and two (2) Cores. Click next.

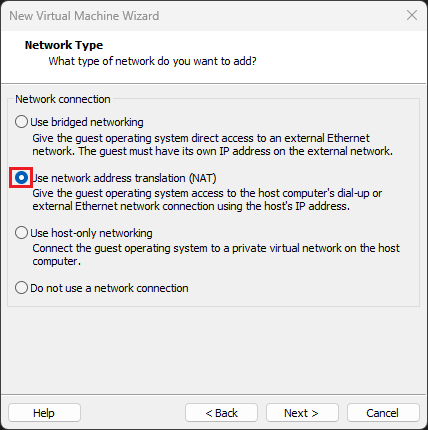


1. Allocate 1024MB (1GB) memory. Click next.

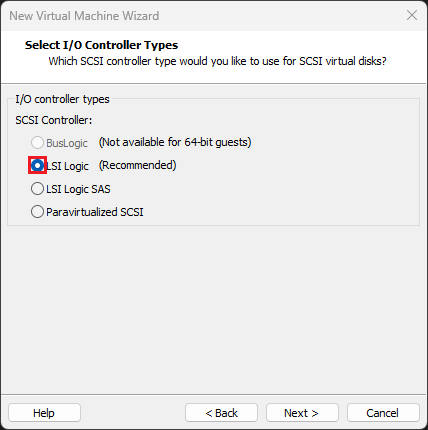
A screenshot of a computer

Description automatically generated

1. For the Network Type, select “Use network address translation (NAT). Click next



1. For the I/O Controller type, leave as the default Recommended option. Click next



1. For the Disk Type, leave as the default Recommend option. Click next.



1. For Select a Disk, use the first option, “Create a new virtual disk”. Click next.

A screenshot of a computer

Description automatically generated

1. Change the disk capacity to 30.0 GB. Either the single or multiple file/s option can be used. If unsure which one to use, leave as default. Click next.

A screenshot of a computer

Description automatically generated

1. The disk file name will be the Virtual machine name (as created in Step 2 f). There’s no need to change it. Click next.

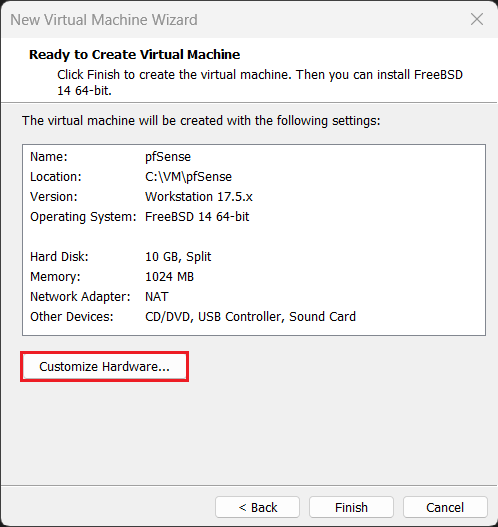
A screenshot of a computer

Description automatically generated

### Step 2: Customize Hardware

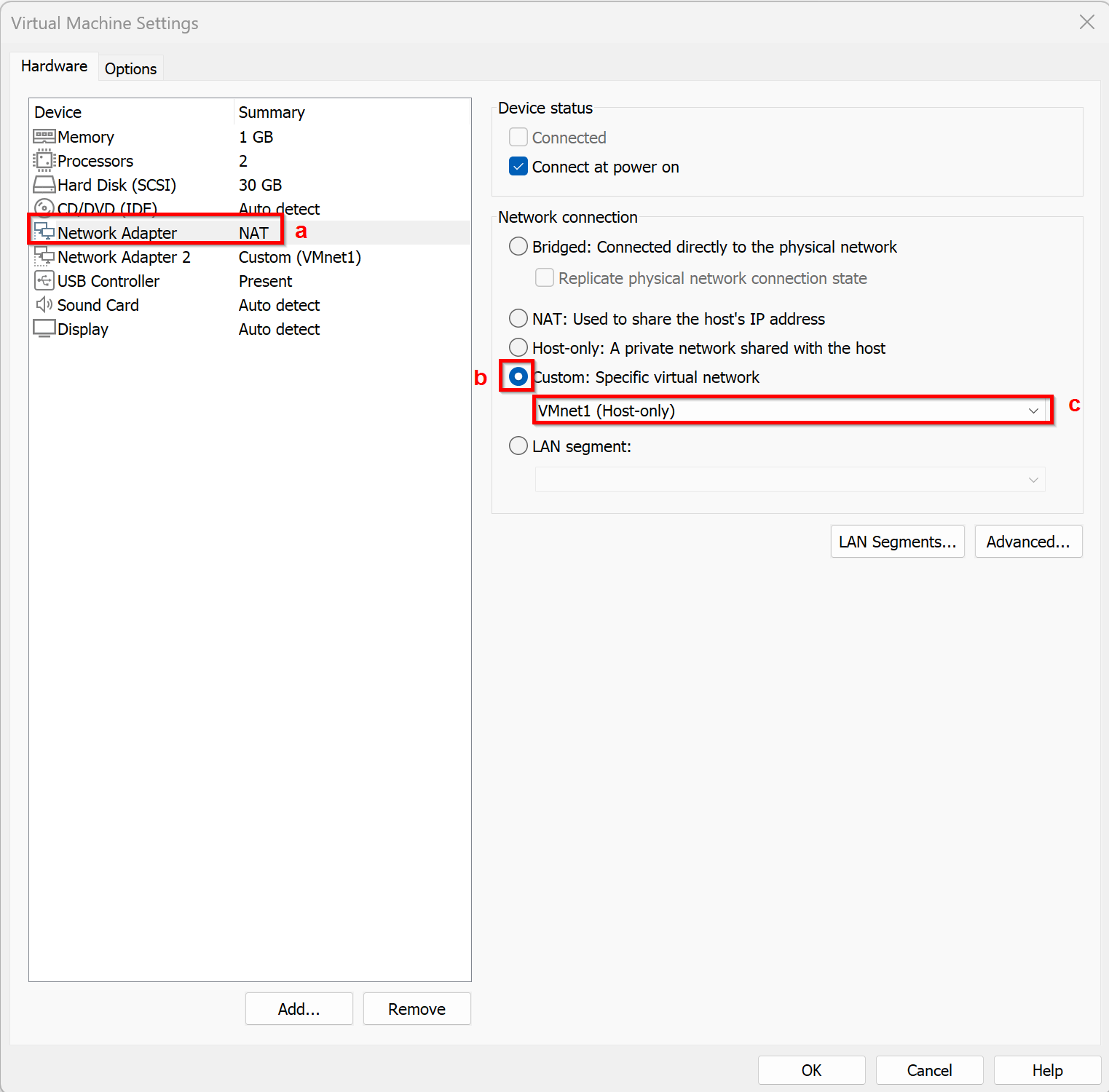
The basic hardware and specifications of the VM have now been configured. But there are a few additional options we need to add using the “Customize Hardware…” screen.

1. On the final page of the creation wizard, select “Customize Hardware”.

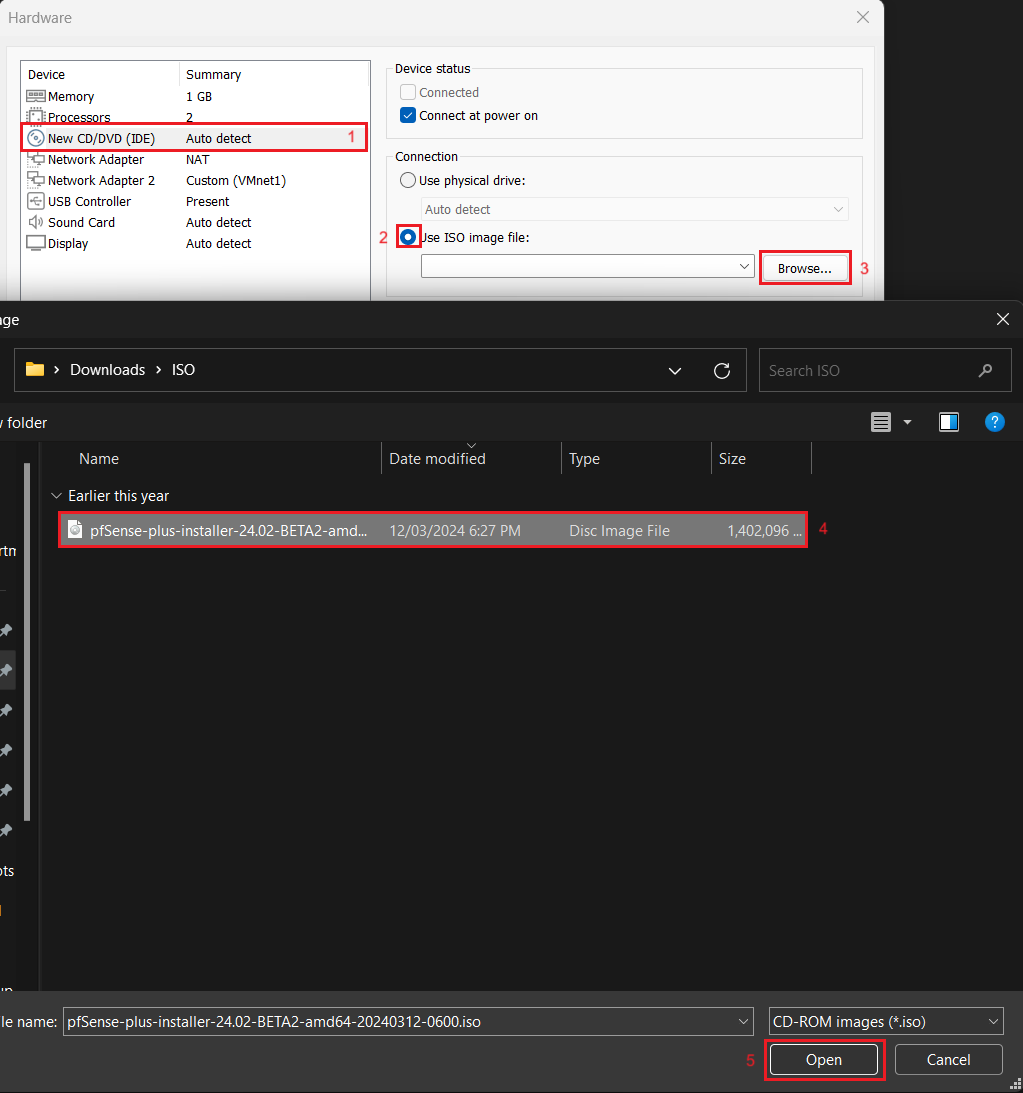


1. Click the Add button (a) and add a network adapter (b). Click finish (c). A screenshot of a computer

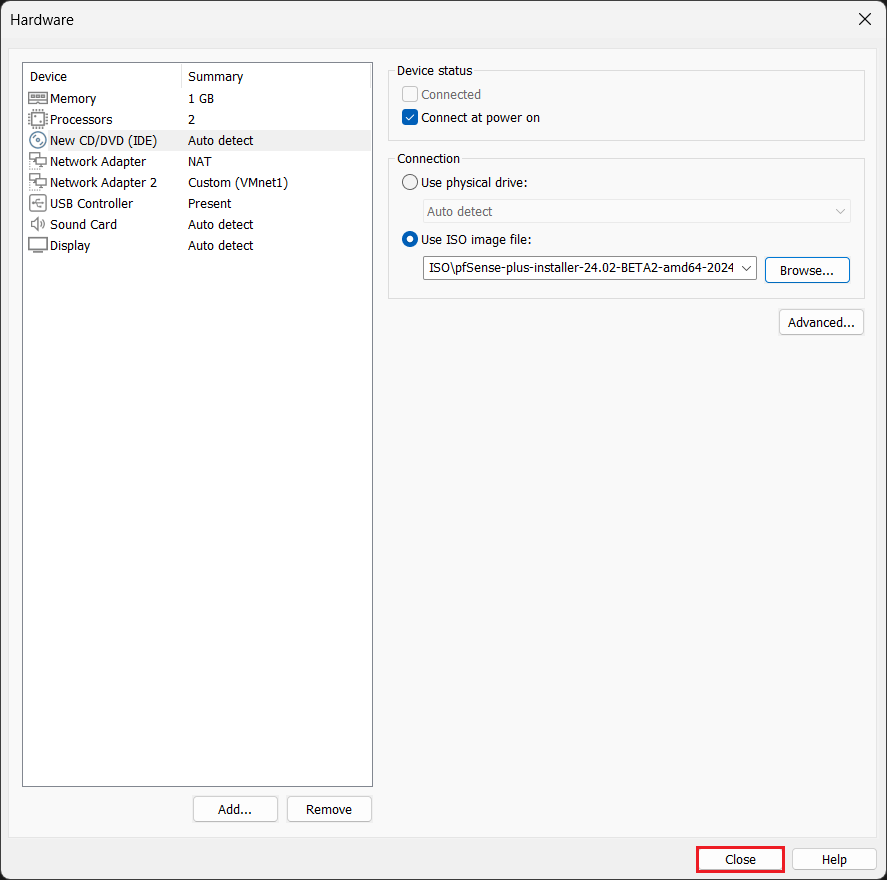
   Description automatically generated
2. Select the new adapter, named Network Adapter 2 (a) and change the Network connection to Custom (b). From the drop-down menu, select VMnet1 (c).



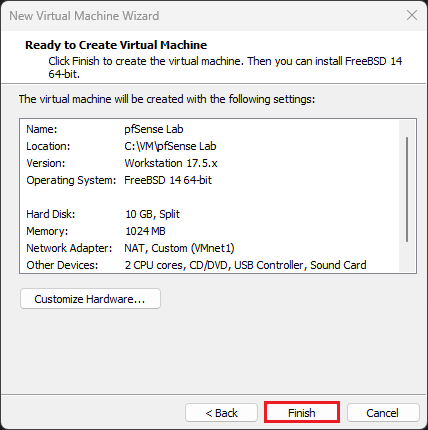
1. Attach ISO image that was downloaded and extracted. Select New CD/DVD (1) and change the Connection to Use ISO image file (2). Click Browse to open file explorer and navigate to where the ISO image file was extracted in Task 1 Step 3. Select the ISO, and click Open (3)



1. Close the customize menu via the Close button.



1. Double check the configuration of the VM, it should match with the below image (your Location might be different). If everything matches, click Finish.

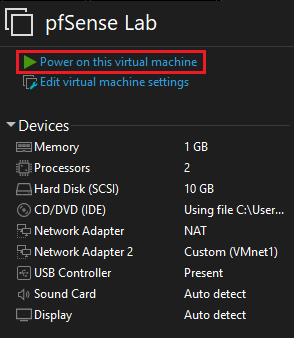


The VM should now be ready to use.

# Task 3: pfSense installation

Install pfSense from the ISO file.

### Step 1: Power on the Virtual Machine

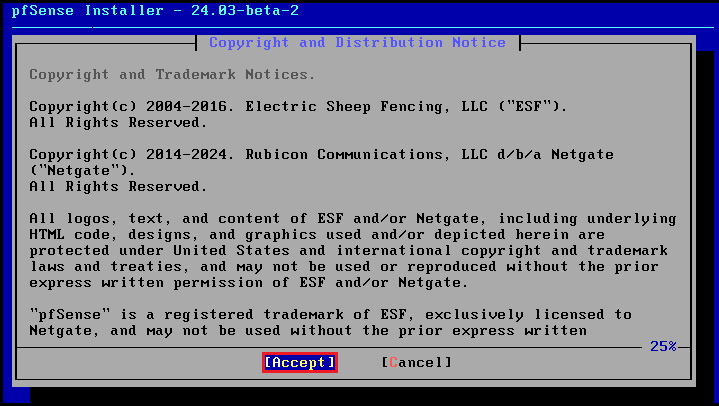


### Step 2: Installation Process

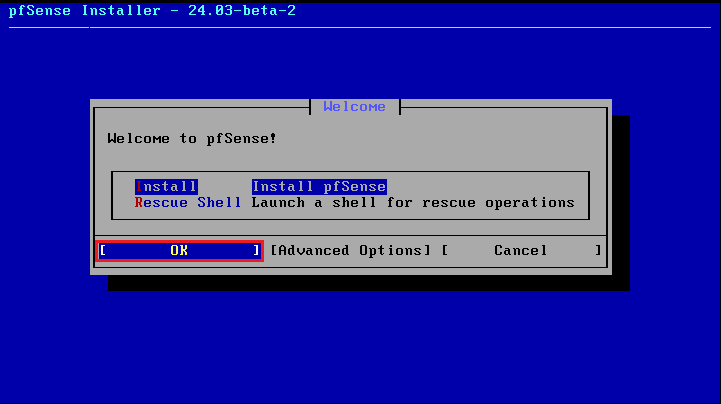
The VM will automatically boot the ISO file, leading to a selection screen. This screen will time out and automatically start the Installer.

Use the arrow keys to navigate and Enter to select.

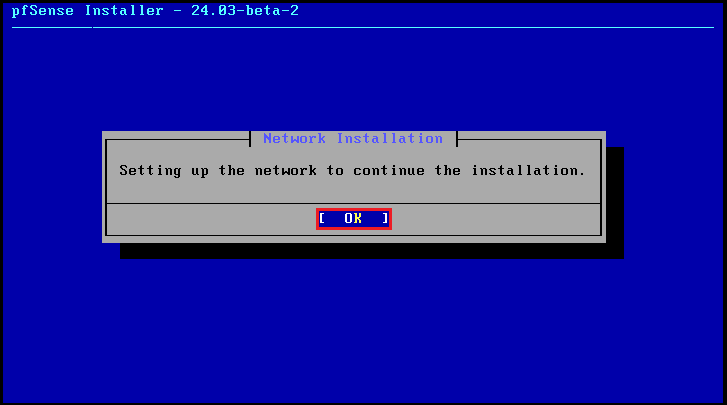
1. Read and accept the EULA.



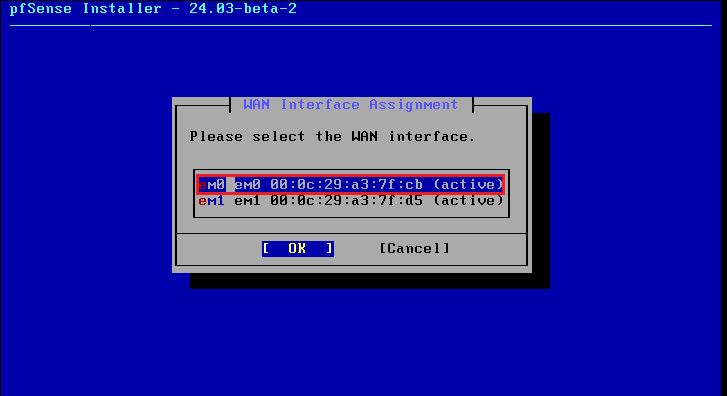
1. Here you can also lunch rescue shell if you need to fix already existing pfSense or you can recover configuration from previous install. You will continue with new installation. Press Enter.



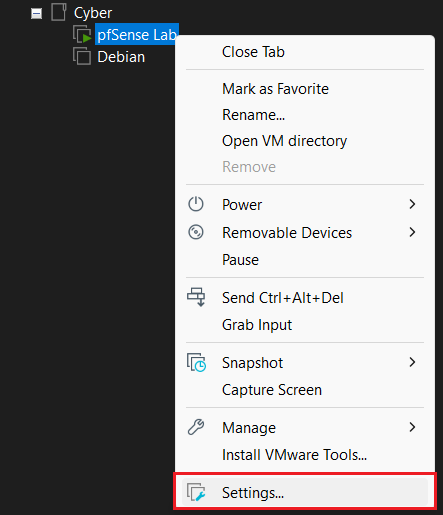
1. The network needs to be configured before installation. Press OK.



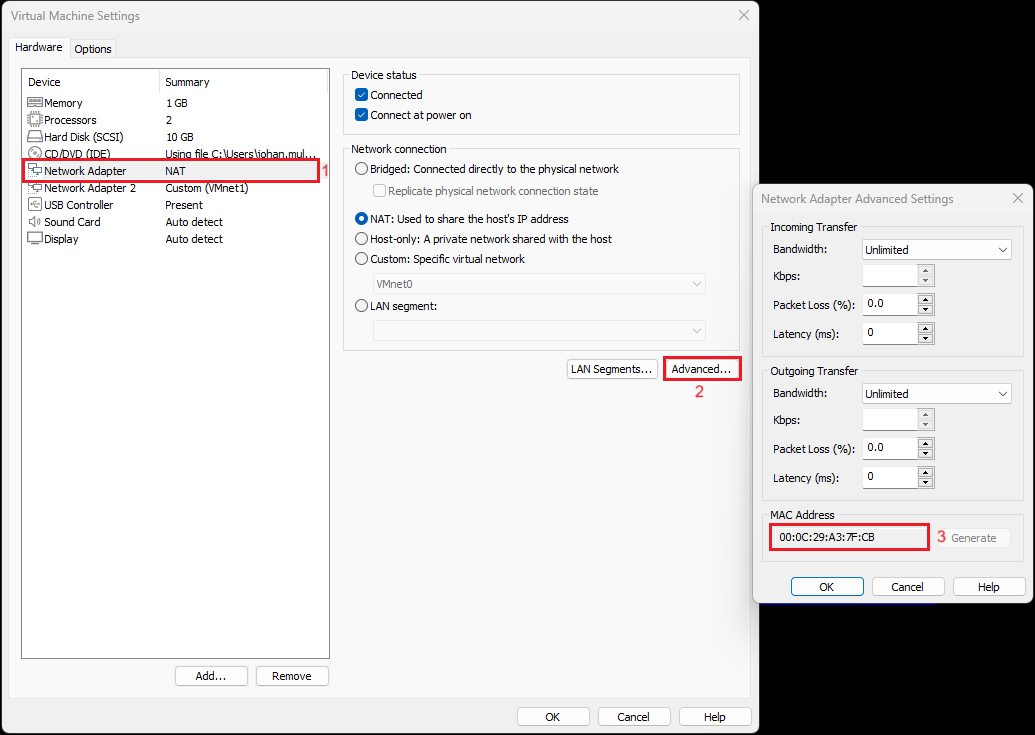
1. Based on it’s MAC Address, select the Network Adapter to use as the WAN interface. This should be the first Adapter that was set to NAT during the New VM Wizard. It should be the first option, but use the below steps to double check the MAC Address.



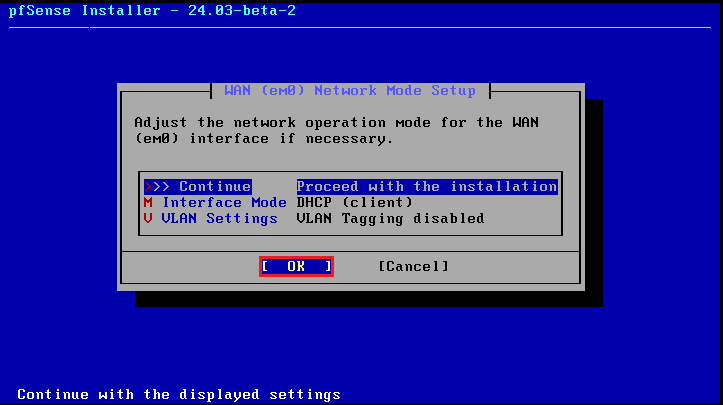
* + To confirm which adapter to select, open the VM settings by Right-Clicking on the VM name, and clicking Settings.



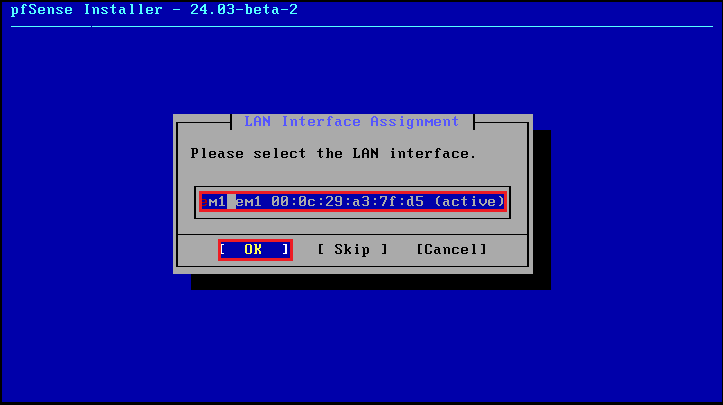
* + Select the NAT adapter (1), and click Advanced (2). Confirm the MAC address from the advanced settings menu (3). Exit out of the settings menu by clicking Cancel, and then Cancel.



* + Leave Interface mode as DHCP. VMWare Workstation will automatically provide an IP address to interface, and using NAT, that interface will then be able to connect directly to the network of the Host Machine, giving the VM access to the Internet. Select OK.

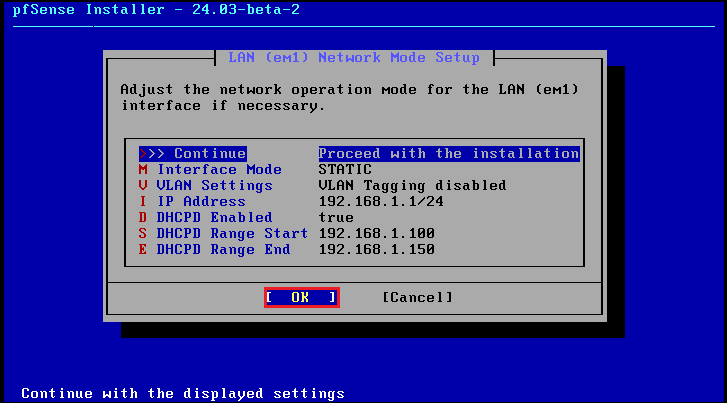


1. Select the Interface to use as the LAN interface. There is only have one unassigned adapter, there is only one option here. Select OK.

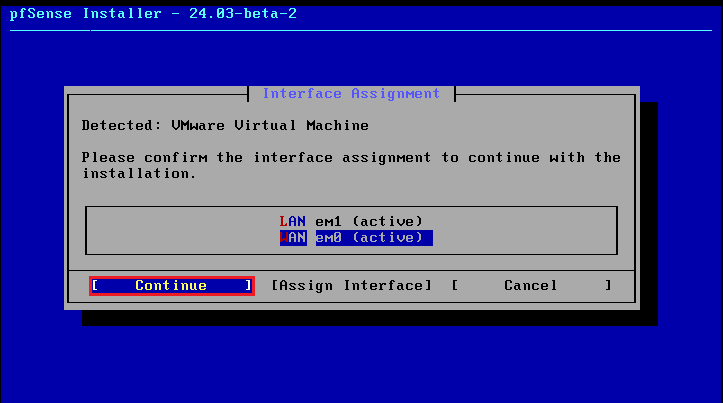


* + This should be your HOST ONLY/VMNet1 adapter. You can confirm the MAC Address using the same steps used before.

1. Leave the LAN settings as default. These settings will determine the IP address of the LAN network, and LAN interface, and also enable pfSense to distribut IP addresses to our LAN clients via DHCP. From the below screenshots, DHCP addresses will be distributed starting from 192.168.1.100/24 to 192.168.1.15/24. Click OK



1. Confirm the Interface assignment, and click OK. Your pfSense will attempt to access the internet to validate your WAN settings.



1. As we do not have an active pfSense Plus subscription, we will install the Community Edition (CE) of pfSense. Select Install CE.

**NOTE: IF you see following error:**

1. **please select OK.**

**A computer screen with a blue background

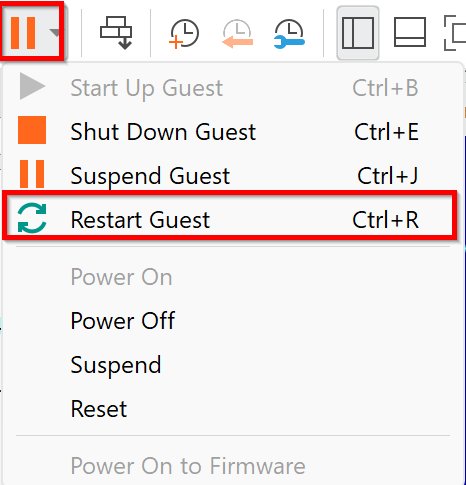
Description automatically generated**

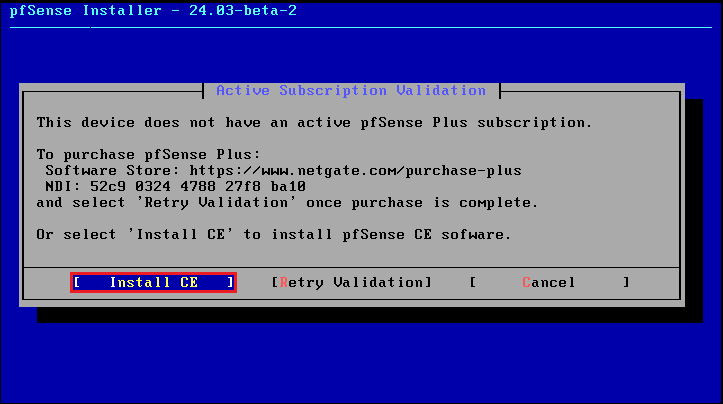
1. **Select Restart.**

**A computer screen shot of a blue screen

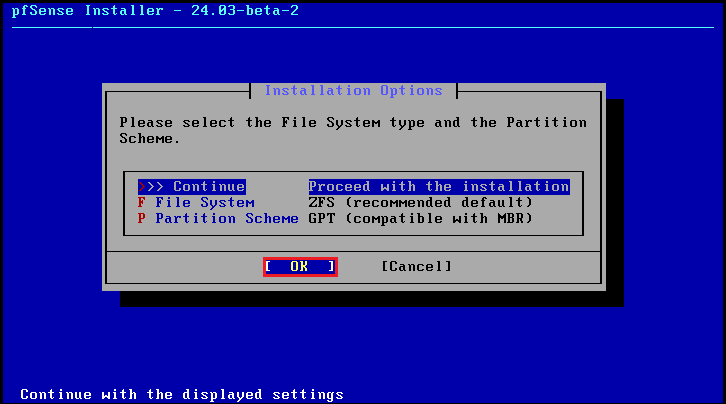
Description automatically generated**

1. **If this does not solve issue Restart pfSense.**

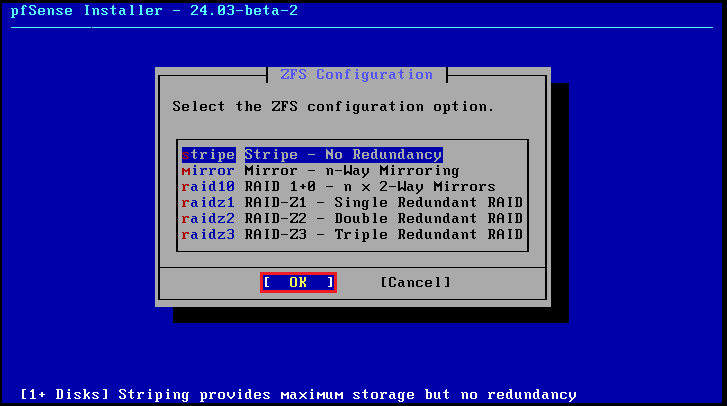
****



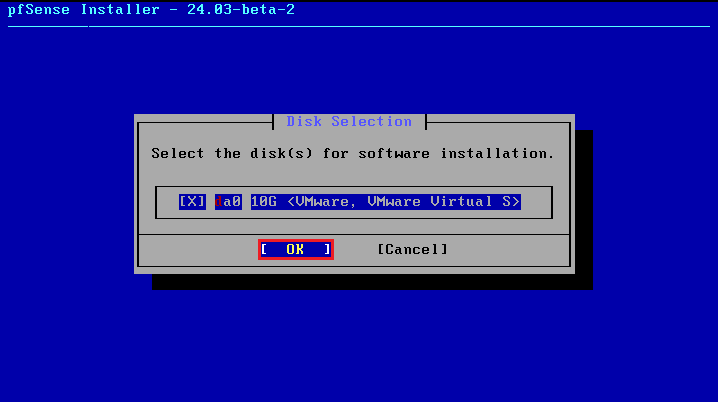
1. For setting up the File System, leave as default. Select OK.



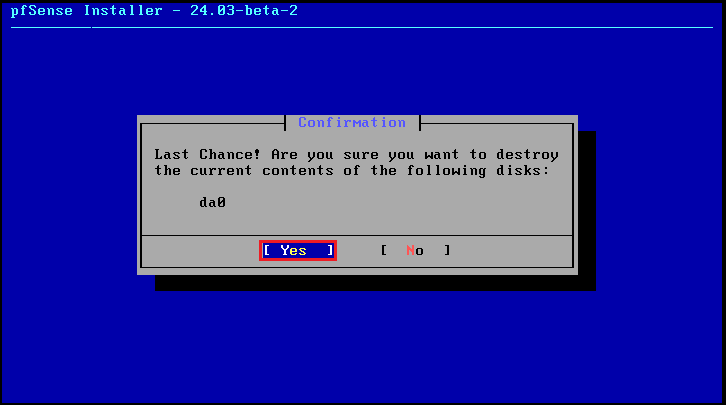
1. Leave the ZFS configuration as default. Select OK.



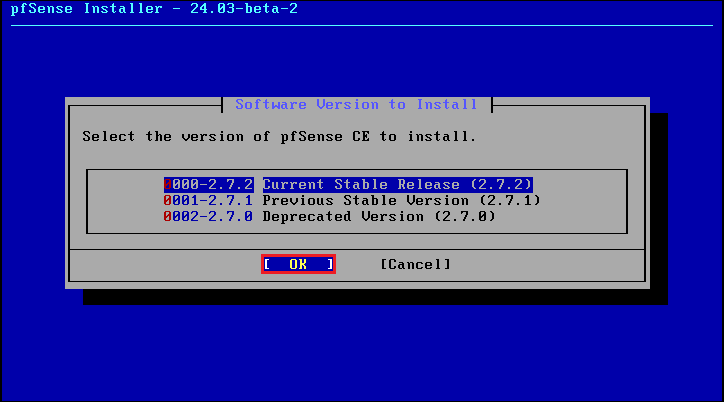
1. The VM only has one storage disk, which will already have been chosen. Select OK



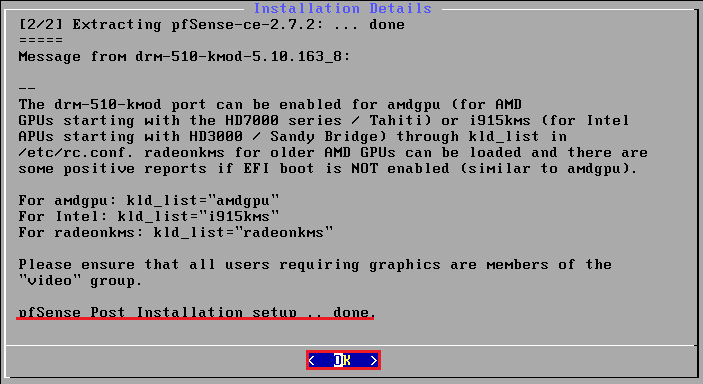
1. Confirm that you are writing changes to the disk. This will erase all current data. Select Yes.



1. Select the version of pfSense to install. Use the Current Stable Release (2.7.2 at time of writing). Select OK.

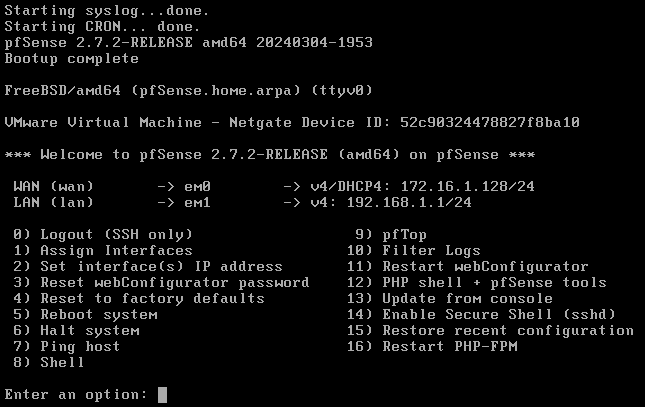


1. The installation process will take a few minutes. Upon completion (if successful), you will see pfSense Post Installation Setup done. Select OK.



### Step 3: pfSense menu

Once pfSense has been installed and booted, you will see the following screen.

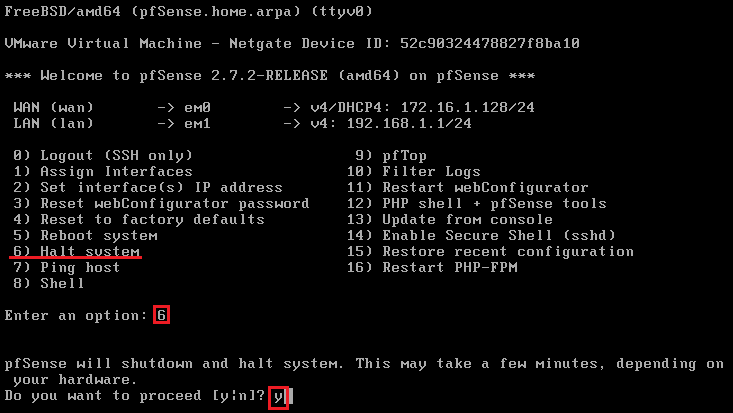


### Step 4: Unmount ISO

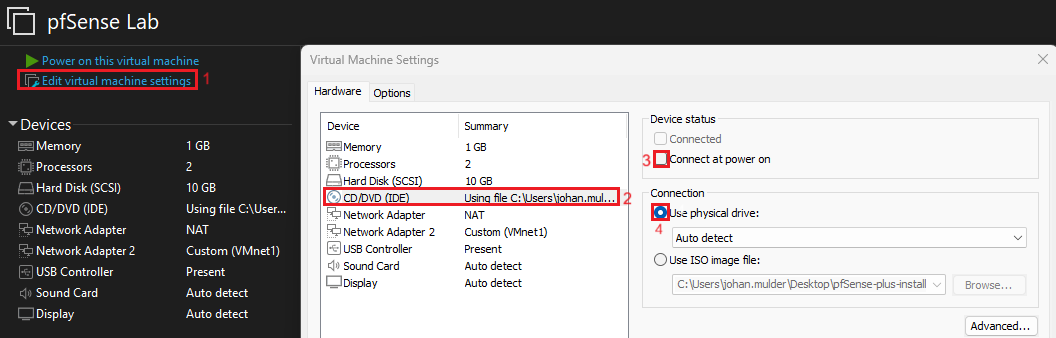
Before we connect and configure pfSense further, we need to shut down the VM and unmount the ISO from the disc drive.

To select option from the console screen, use the numerical keys that correspond to the numbered options, and hit Enter.

1. Select option “6” to halt the system (shut down) and hit Enter. Confirm shutdown by typing “y” and Enter.



1. Click on the Edit virtual machine settings option (1). Select the CD/DVD drive (2) and uncheck the Connect at power on option (3). Change the Connection from Use ISO image file to Use physical drive (4).



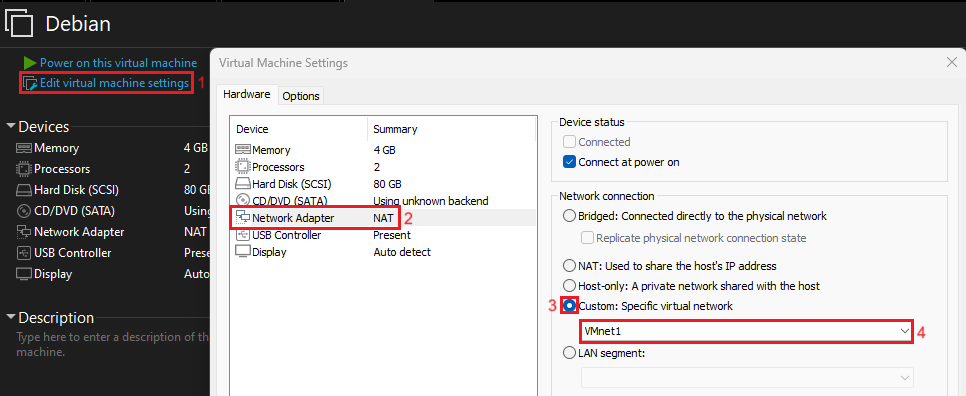
You can now exit out of the settings menu and power on the VM again.

# Task 4 – Connecting to Web Interface of pfSense

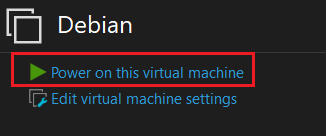
You’ll be using a Debian VM to access the pfSense’s WebGUI for further configurations. But before you can access the WebGUI, you’ll need to make sure the Debian VM is on the same network as the pfSense LAN adapter. To do this, you need to Network adapter to VMNet1.

### Step 1. Connect your Debian VM to LAN Internal Network

1. Open your Debian VM’s settings by clicking on Edit virtual machine settings (1). Select the network adapter (2). Change the Network Connection to Custom (3) and select VMNet1 from the dropdown menu (4). Exit out of the settings menu by clicking Ok.



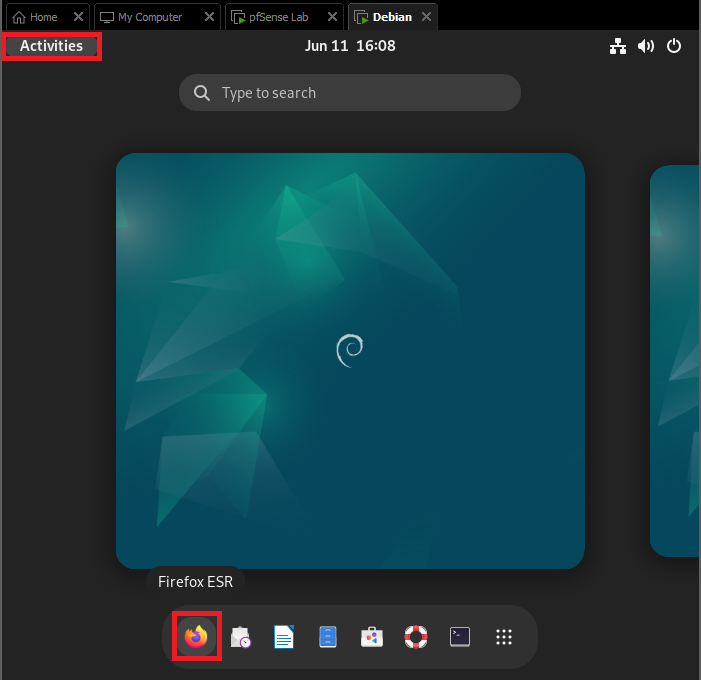
1. Power on the VM



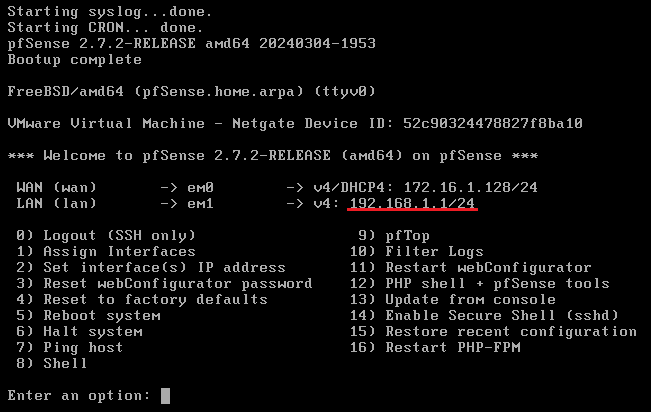
### Step 2: Connect to pfSense WebGUI

The WebGUI for pfSense is access via entering the IP address of the LAN interface in your web browser.

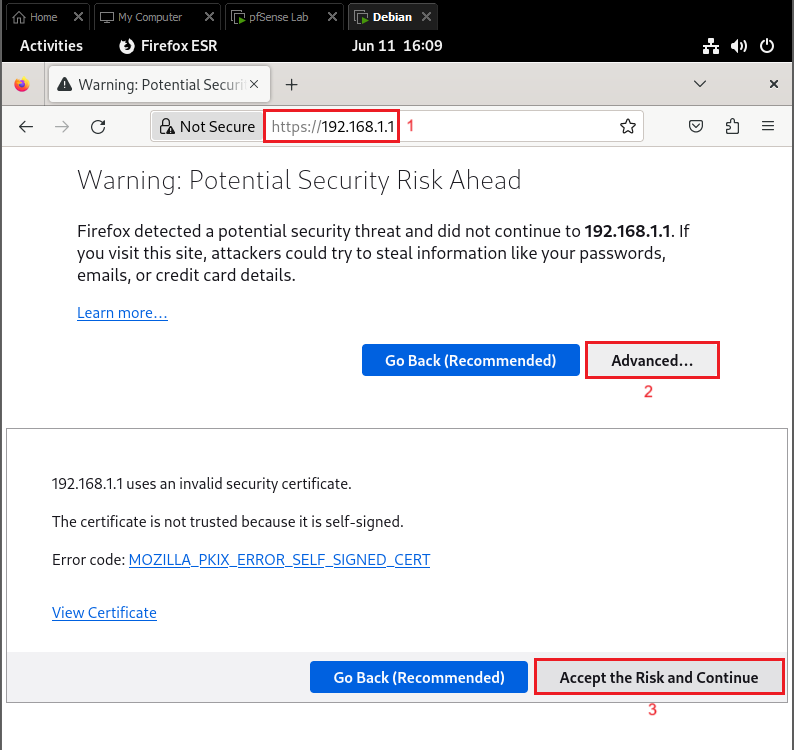
1. On your Debian machine, Click Activities (1) and open Firefox.



1. You can get the IP address of your pfSense LAN interface directly from the pfSense console menu, as highlighted below.



1. Type the IP address of the pfSense LAN interface into the address bar (1). This will cause a warning page to load. Click Advanced (2), and select Accept the risk and Continue (3) to open the pfSense WebGUI.



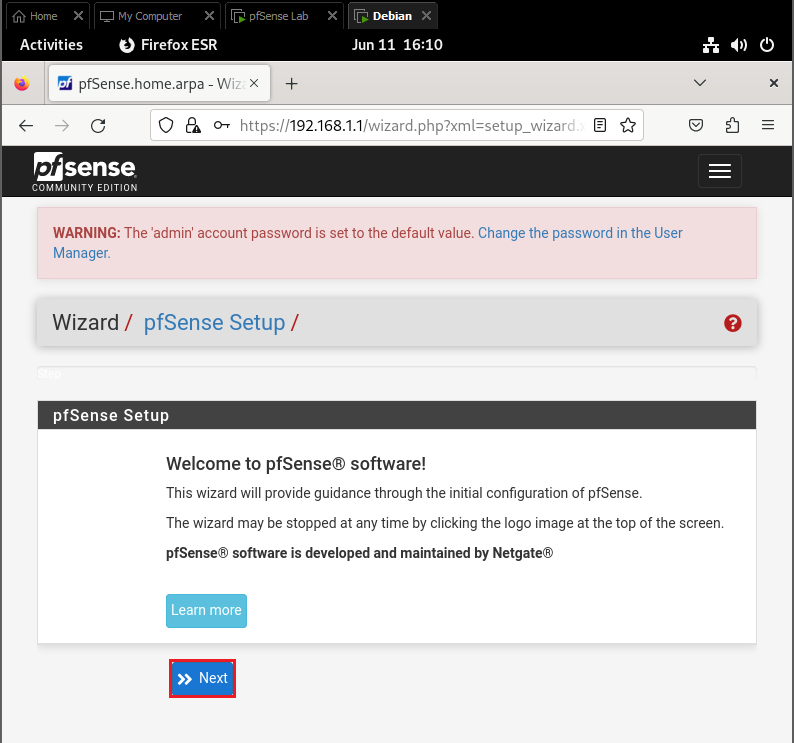
1. The default login information for pfSense WebGUI is as follows:  
   Username: admin

Password: pfsense

### Step 3 – pfSense Configuration Wizard

The first time you log into the WebGUI after installing pfSense, you will be greeted by the pfSense Setup Wizard. The Setup Wizard will guide you through the required first-time configuration.

1. This is the welcome screen for the Setup Wizard. Click Next when ready to begin the configuration.



1. Set the General information for your pfSense instance as follows:

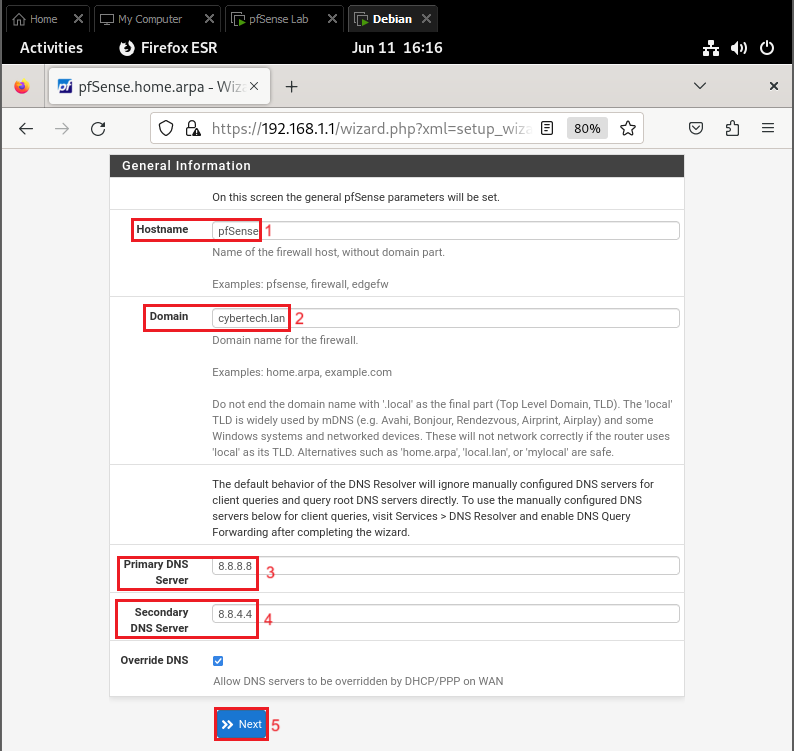
**Hostname** (1): pfsense

**Domain** (2): cybertech.lan

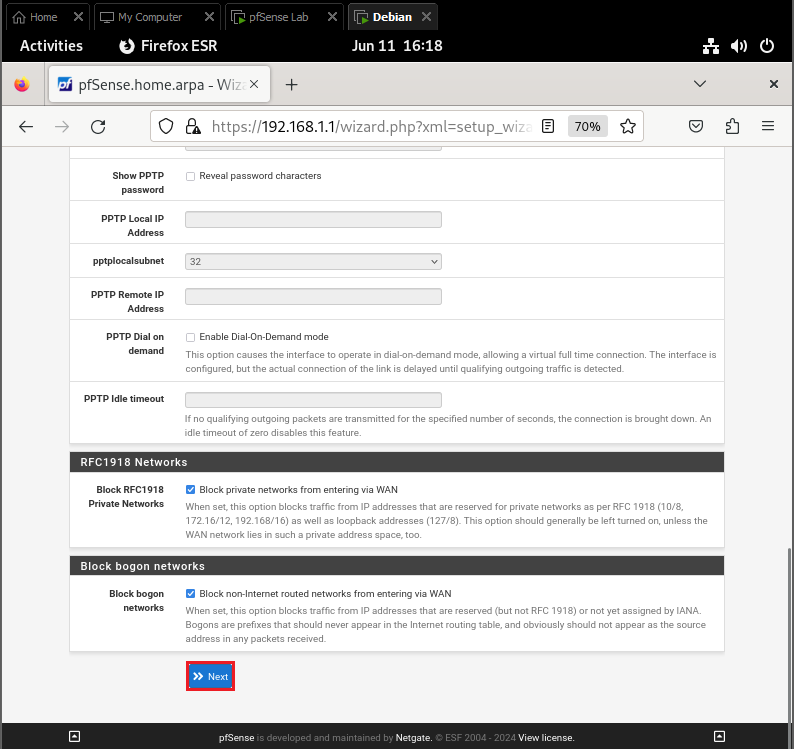
**Primary DNS** (3): 8.8.8.8

**Secondary DNS** (4) 8.8.4.4

Click Next (5) to proceed.



1. The next page is the WAN Configuration. These settings can be left on their default. Click Next.

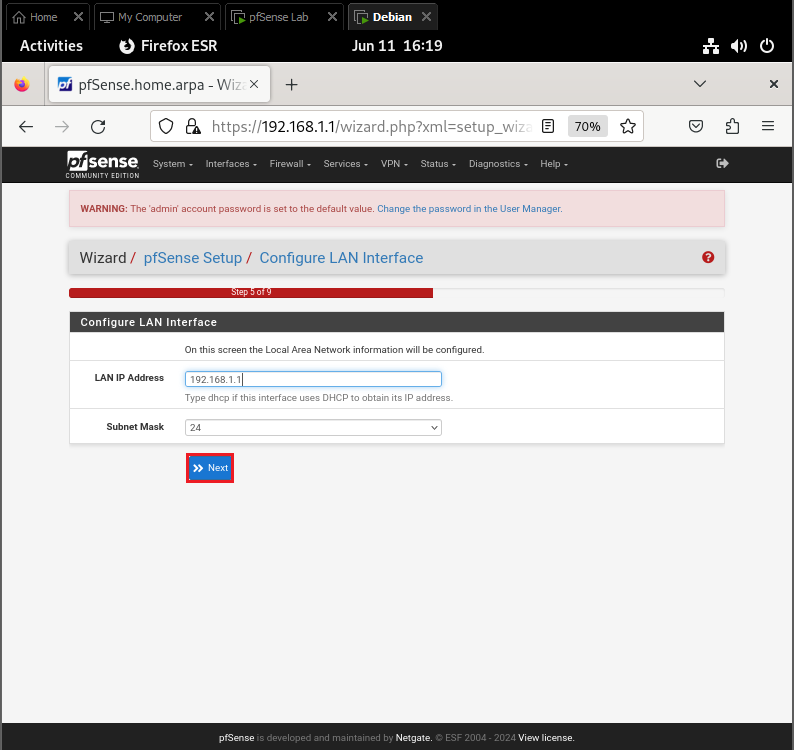


1. Configure the LAN Interface with the following information if it was not automatically set up:

**LAN IP Address**: 192.168.1.1

**Subnet Mask**: 24

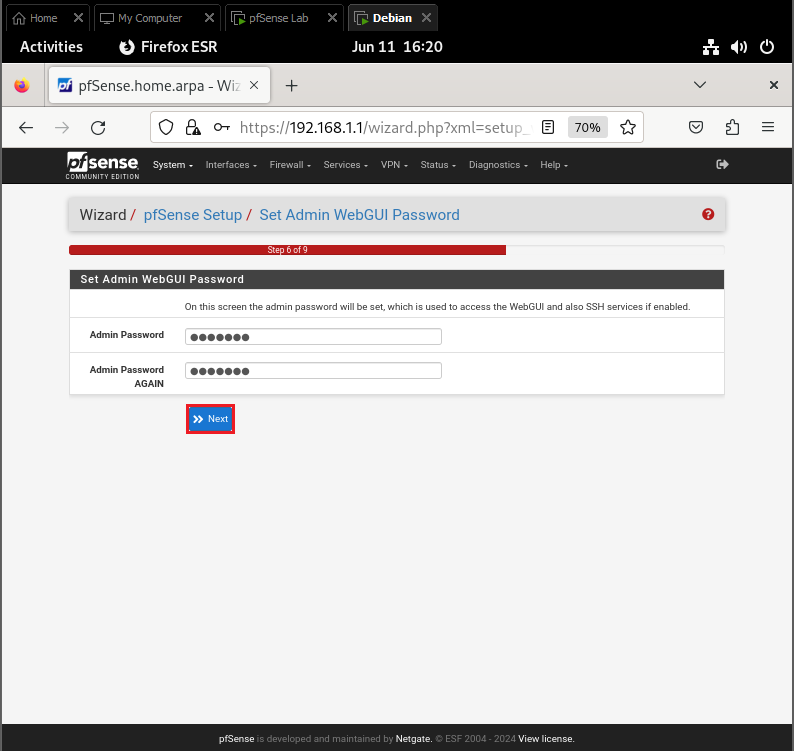
Click Next.



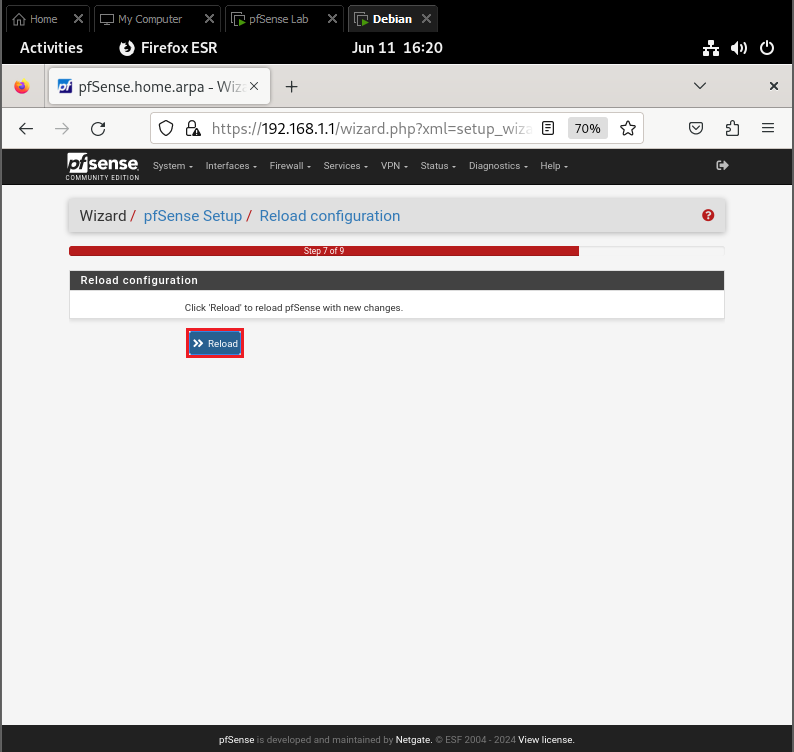
1. Set a new password for the WebGUI. Change the password to:

student

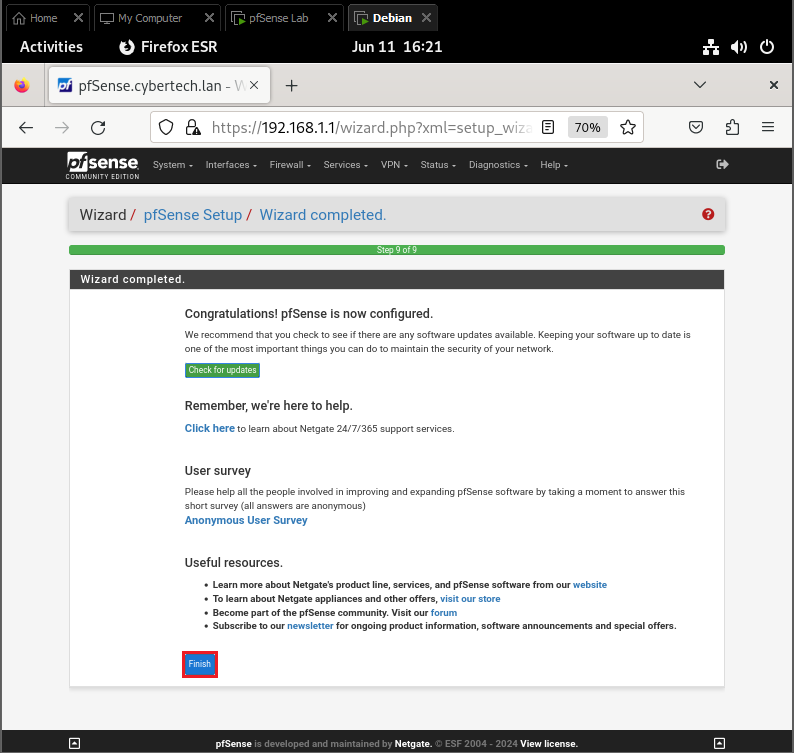
Click Next.



1. To apply these settings, the WebGUI needs to be reloaded. Click Reload.



1. The setup should now be complete. The last page of the Wizard can be used to look for updates (not required at the time of writing), and also has a link to netgate support. Click Finish.



1. After closing the Setup Wizard, a Terms & Conditions window will pop up. Read the Terms & Conditions and click Accept to continue.

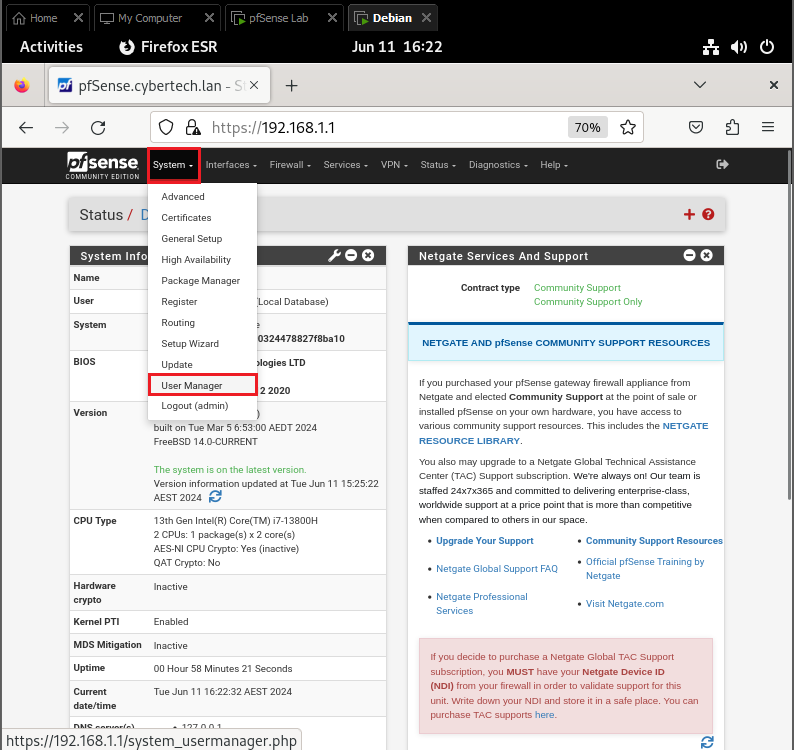


# Task 5 – Create a new user

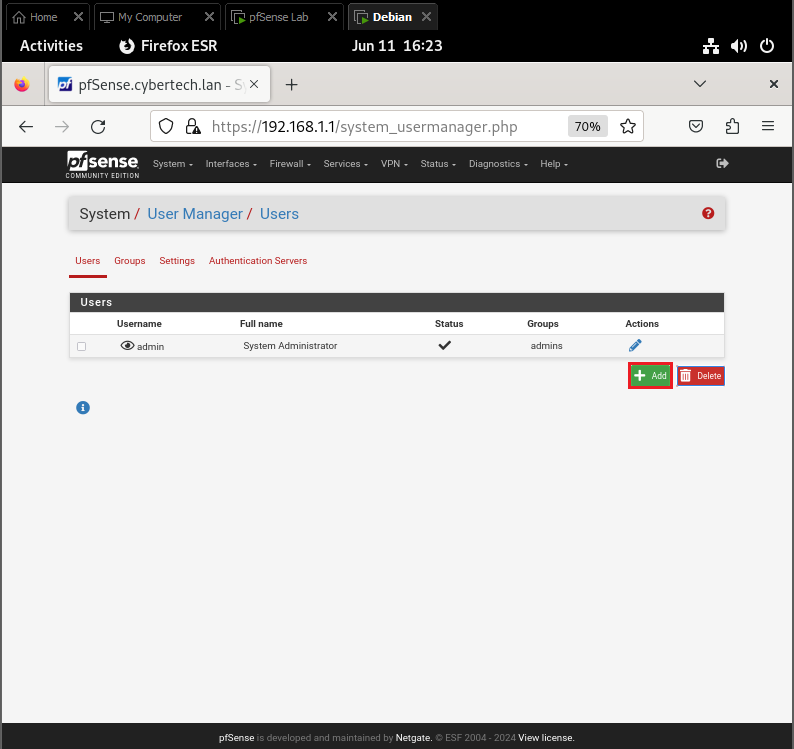
It is recommended to create a new Administrator account and disable the built-in Admin account.

### Step 1: Create a new Administrator account

1. Open User Management by opening the System tab and clicking User Management.



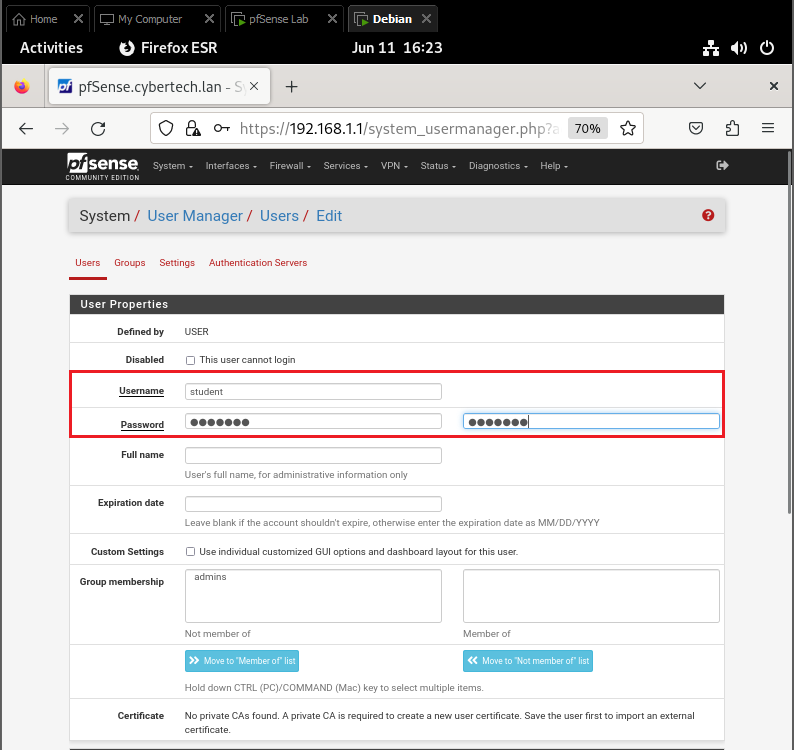
1. To adda new user, click Add.



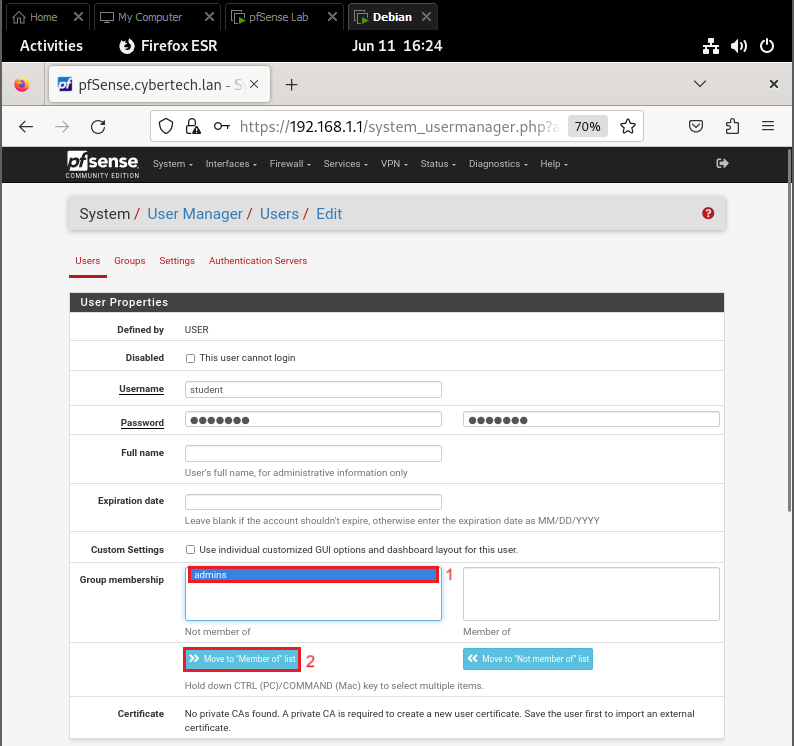
1. Set Username and Password as follows:

**Username**: student

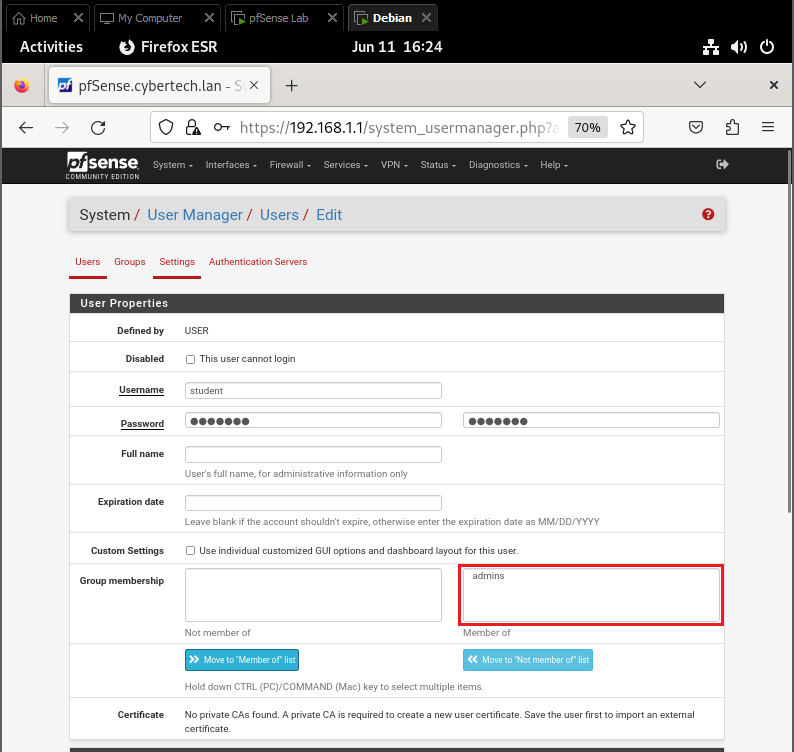
**Password**: student



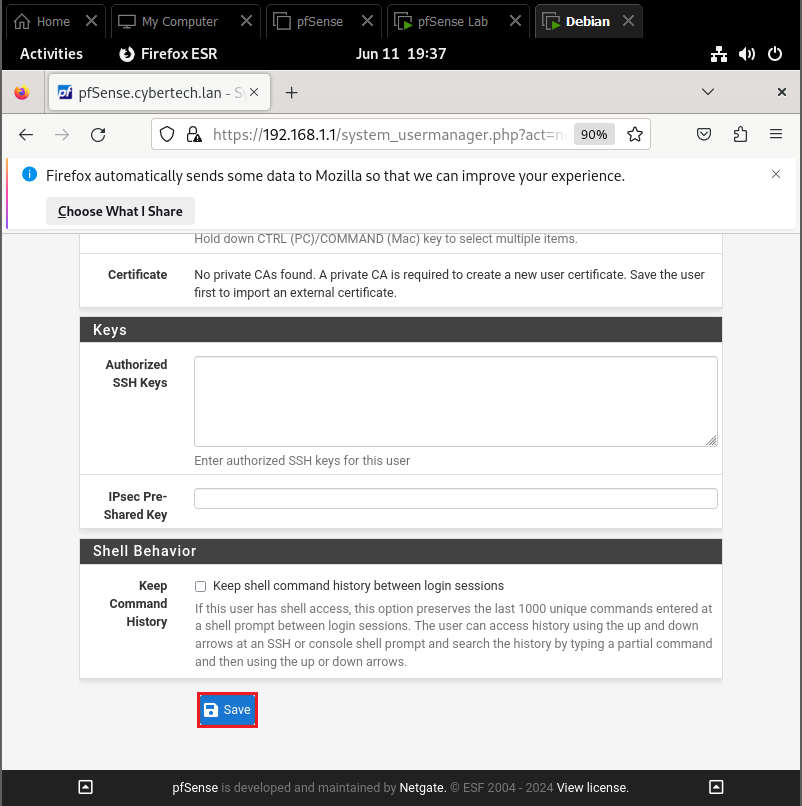
1. Add the new user to the admins group. Under Group membership, select the admins group (1), and click Move to members of list (2).



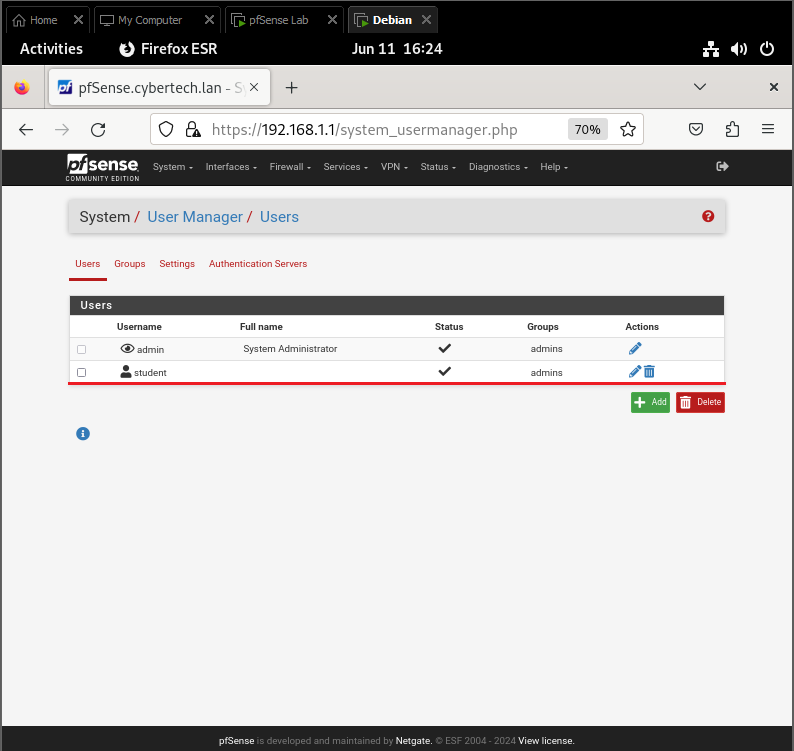
* Admins will have been added to the “Member of” column as seen below:



1. Save the new user by clicking Save on the bottom of the page.



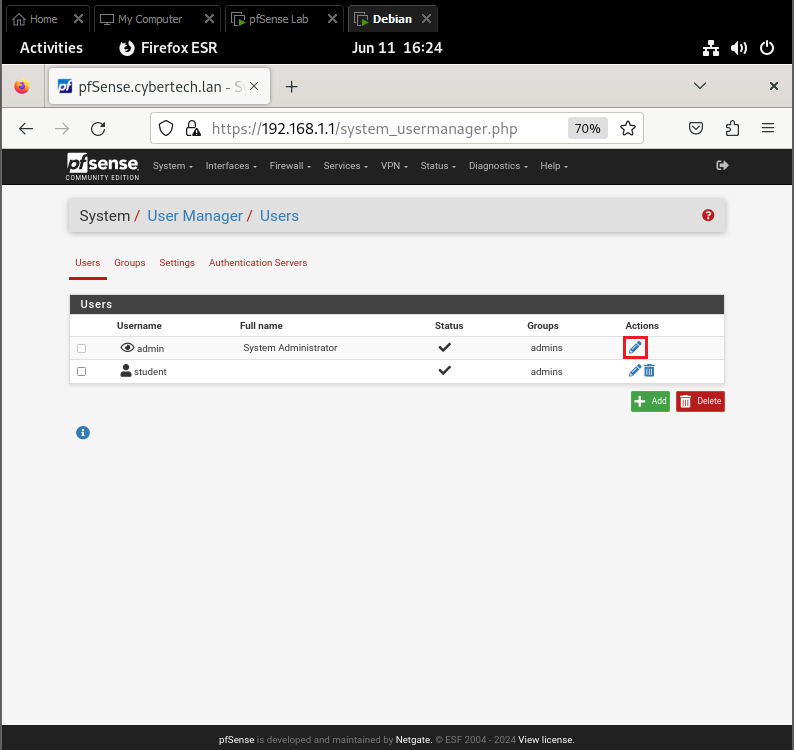
1. You should be returned to the Users page, and should see the newly created account, as below:



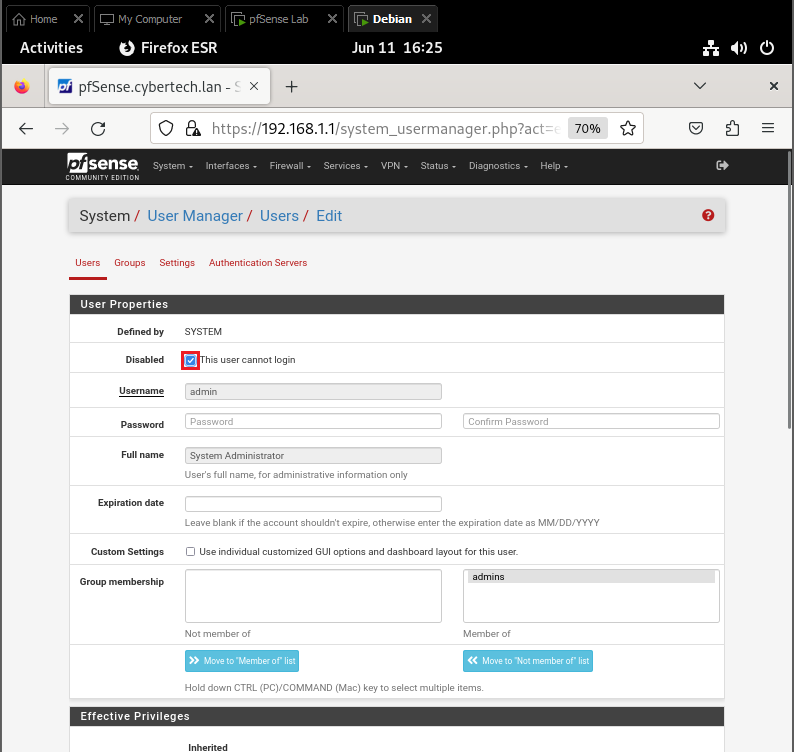
### Step 2: Disable Admin login

Now that there is a new admin account, disable the default admin account.

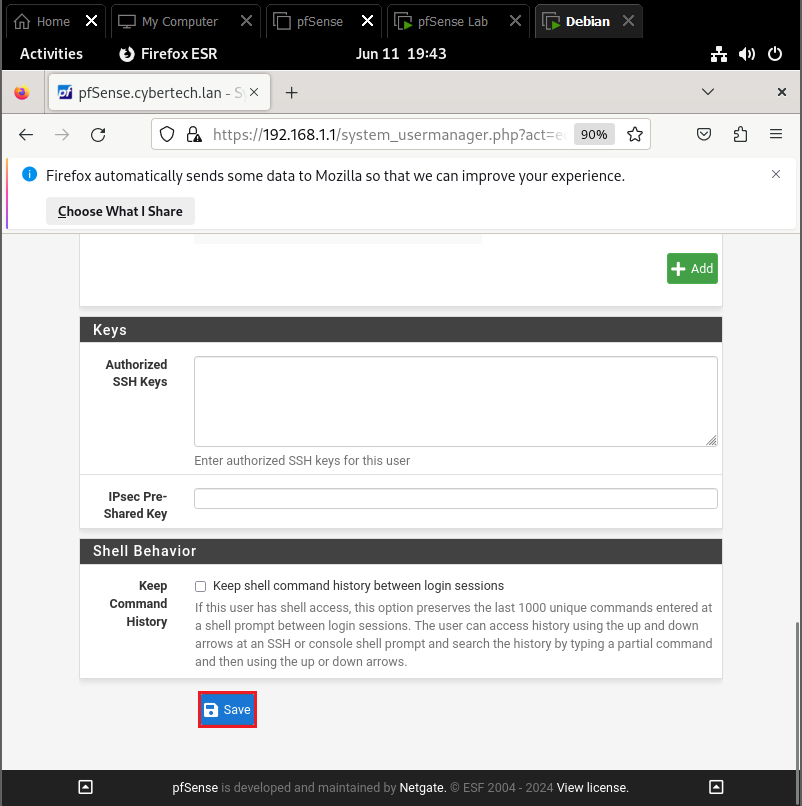
1. Edit the admin account by clicking the pencil.



1. Select the checkbox to disable login



1. Save changes.



1. You should be returned to the Users page again. That status of the default account will have changed, as seen below:

