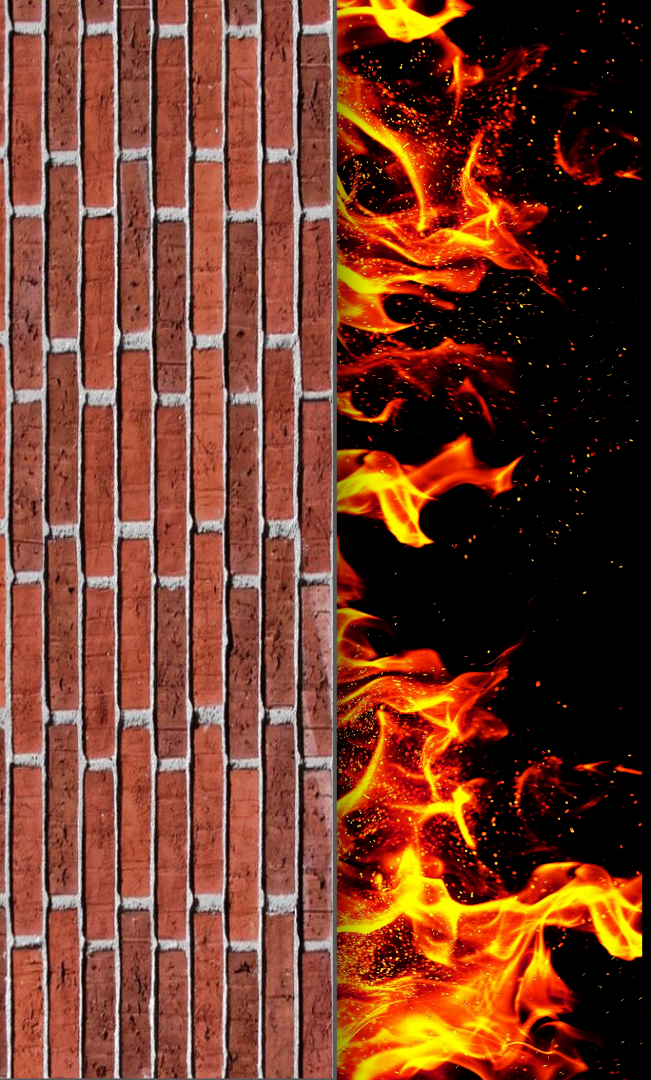


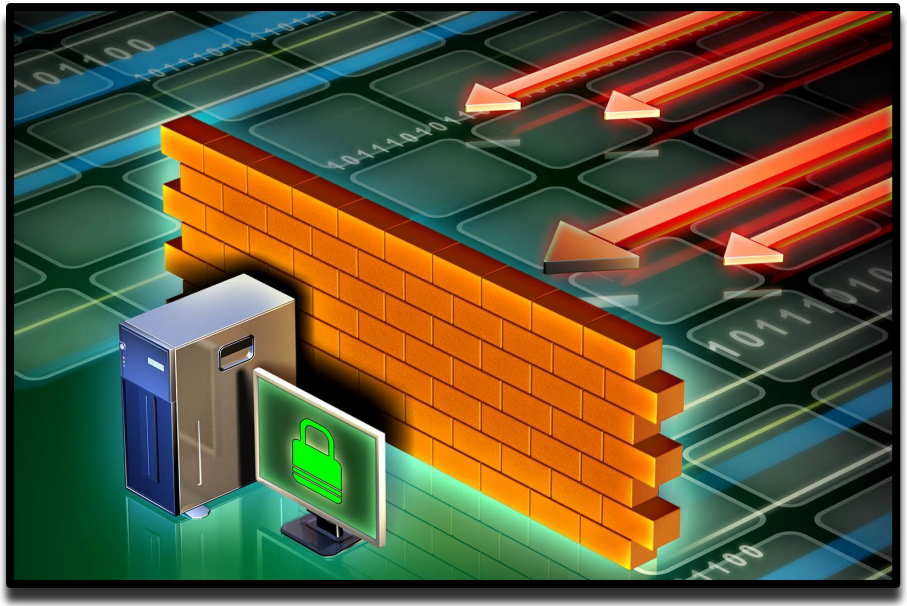
pfSense Firewall

A Step-by-Step Guide

What is a Firewall and why is it necessary?

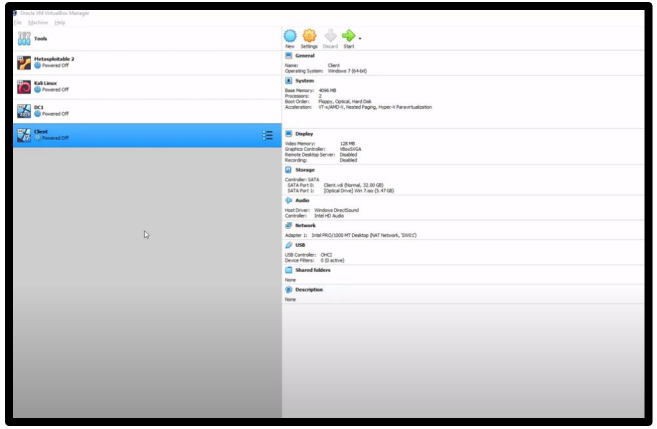
- A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.

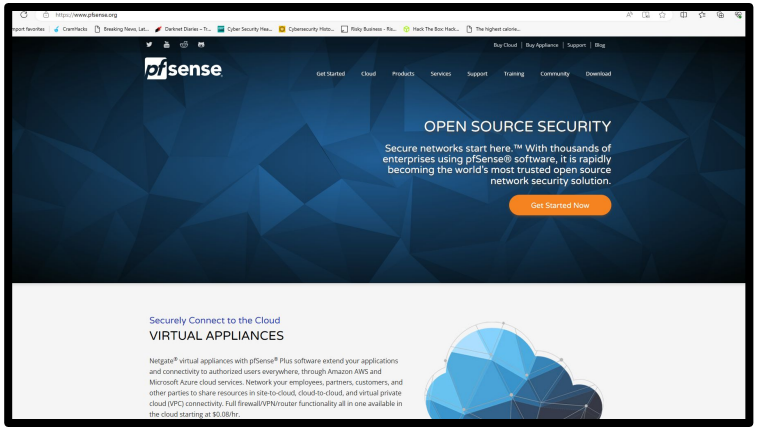
- Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.



Let’s Get Started

- Access the Virtualbox home lab created during previous project (See Virtual home Lab in Github)
- Once accessed, navigate to browser and input the following url in the search bar: pfSense® - World's Most Trusted Open Source Firewall

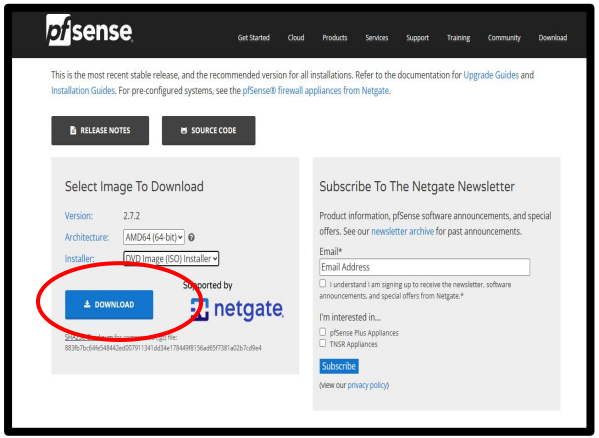


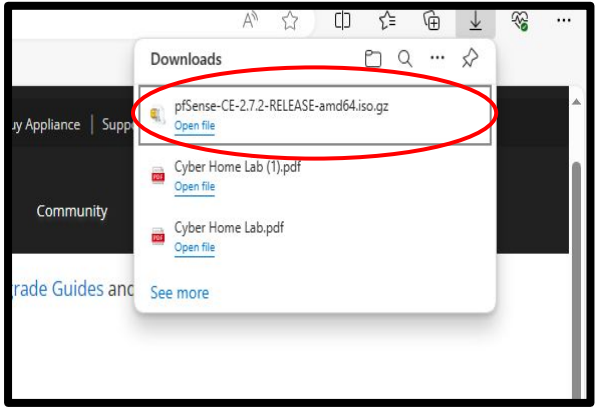


pfSense Website

- Select “Download” in top right corner of website
- Once at the download webpage, input the values shown
- Select “Download”

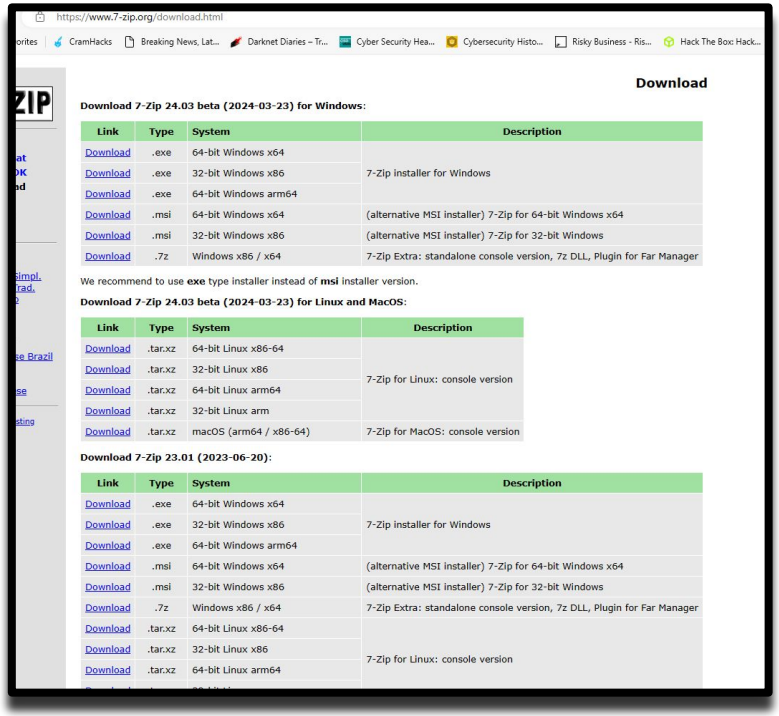
- Ensure that the download has completed before moving to new slide



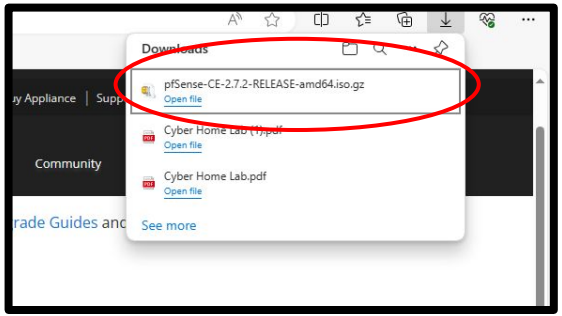


Download the 7 Zip Tool

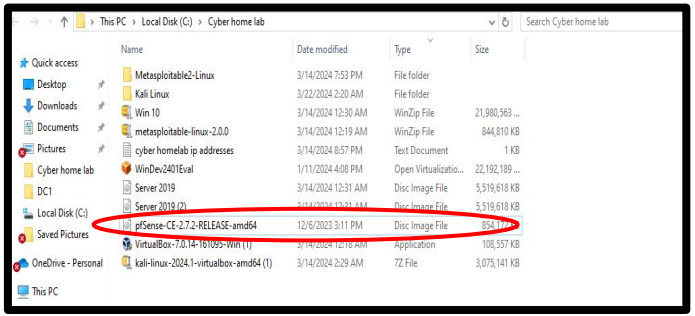
- Next, in your browser, navigate to the 7 Zip website to download the tool (Download (7-zip.org)).
- This tool will allow you to unzip and extract the appropriate pfSense files from the download, giving you accessibility to the tool.
- Be sure to download appropriate version of 7 Zip according to your OS. Also, select the 64-bit option that coincides.



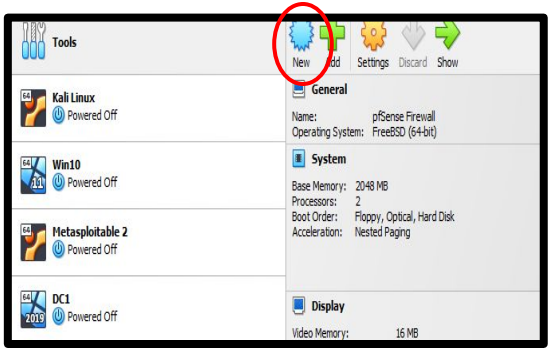
Add pfSense Firewall to Virtualbox



- Navigate back to pfSense download. In file explorer, you will need to unzip this file via 7 Zip. Right click the pfSense file and locate 7 Zip. Then, select “Extract’.

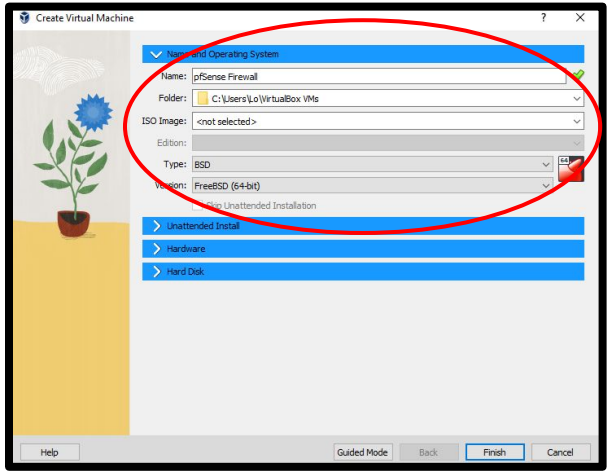


- Once the file is extracted, move it to the “Cyber Home Lab” folder you created in the cyber home lab guide. The file should identify as a “Disk Image File”.

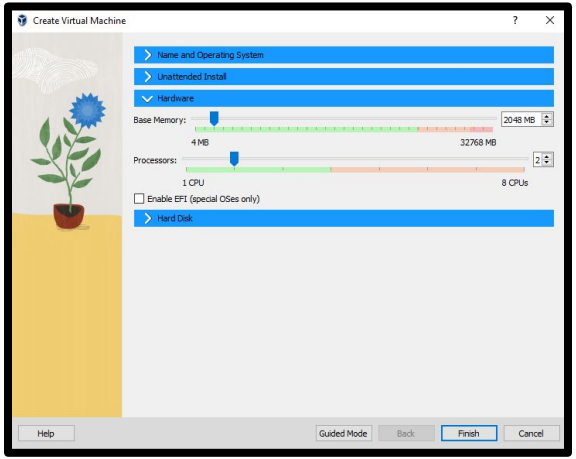


- After the previous step is completed, navigate to Virtualbox and select “New”.

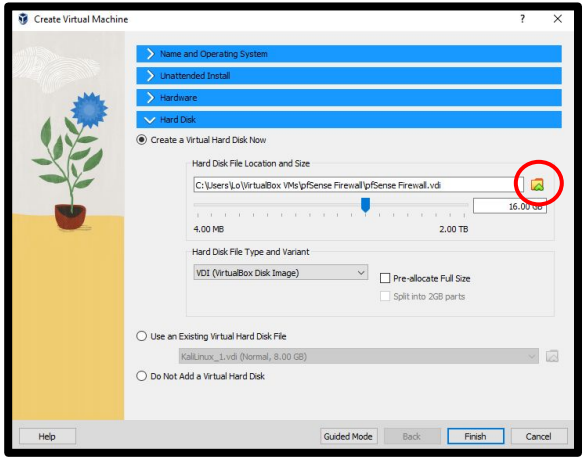
Add pfSense Firewall to Virtualbox



- Once at the “Create Virtual Machine” window, input the following values under the “Name and Operating System” dropdown



- Next, under the “Hardware” dropdown, set the base memory to 2048 MB

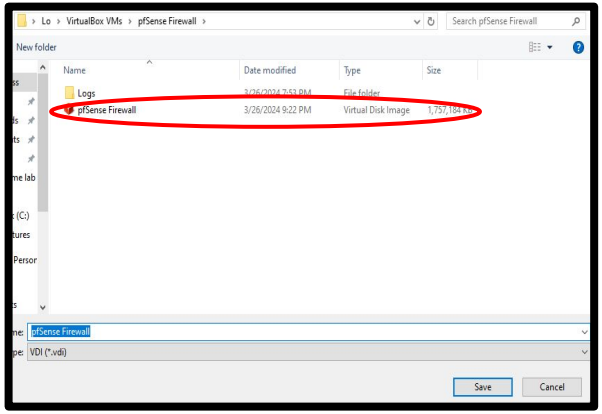


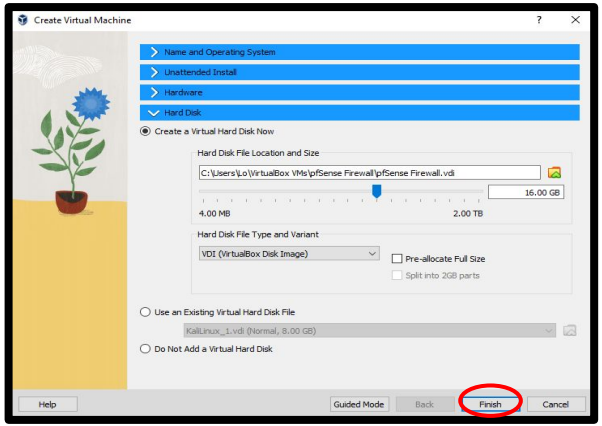
- Under the “Hard Disk” dropdown, locate the pfSense iso file by selecting the yellow file icon

Add pfSense Firewall to Virtualbox

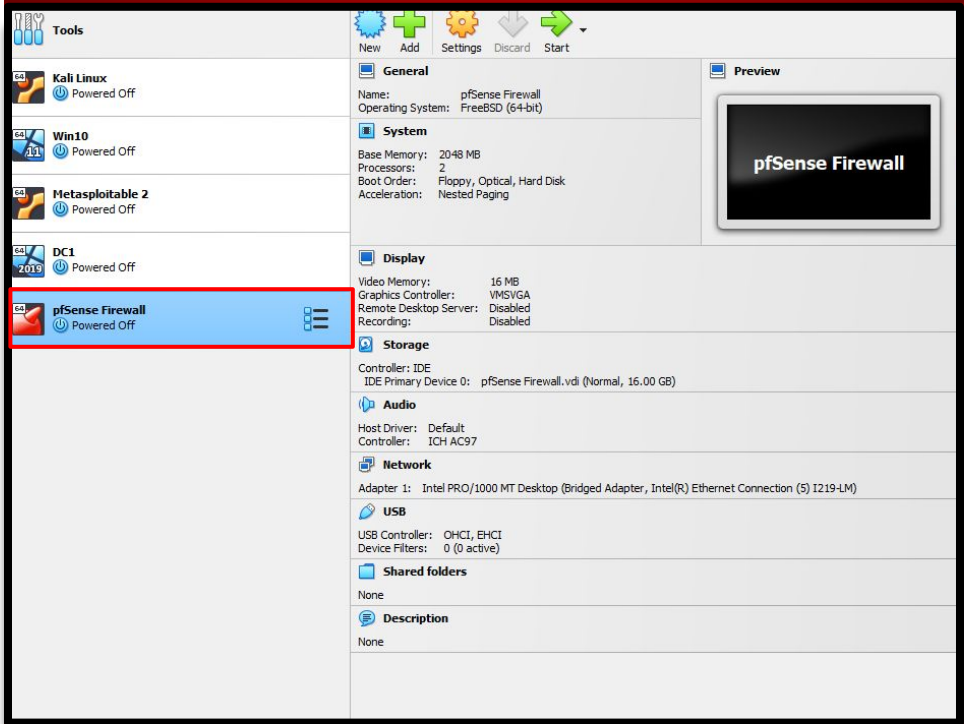
- After selecting the file icon, you will be relocated to the File Explorer. Locate the pfSense file and select it.

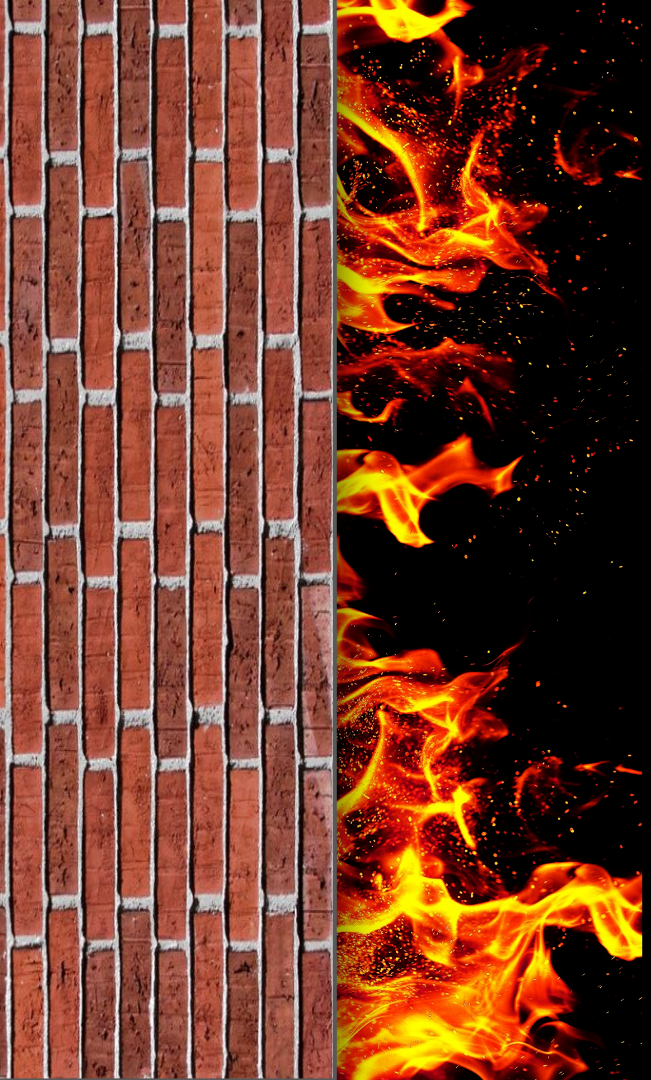
- Once the file has populated in the “Hard Disk” dropdown, select “Finish” in the bottom right corner of window





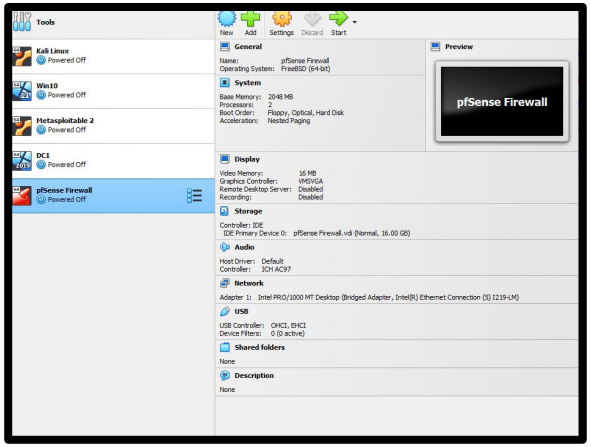
Success! Great Job!



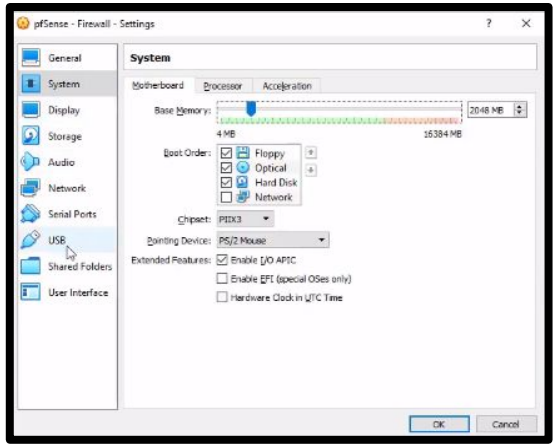


Installation & Configuration

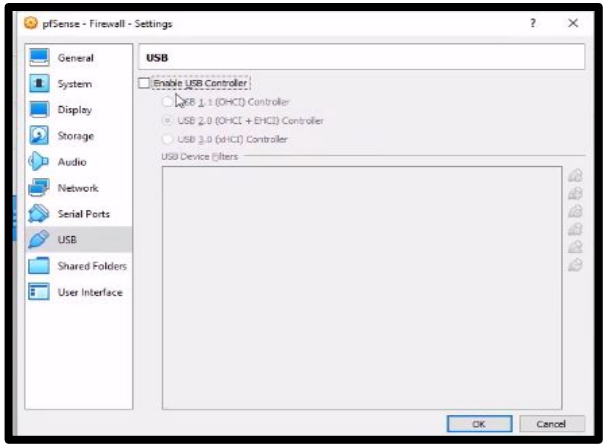
Install & Configure pfSense



- Right click the “pfSense Firewall” machine and access the “Settings”

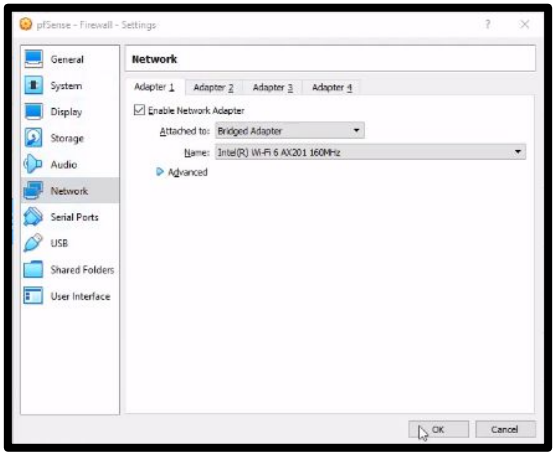


- Once in settings, access the “System” option, then the “Motherboard” tab. Set memory to 2048MB. Next, under the “Processor” tab, set CPU to 2

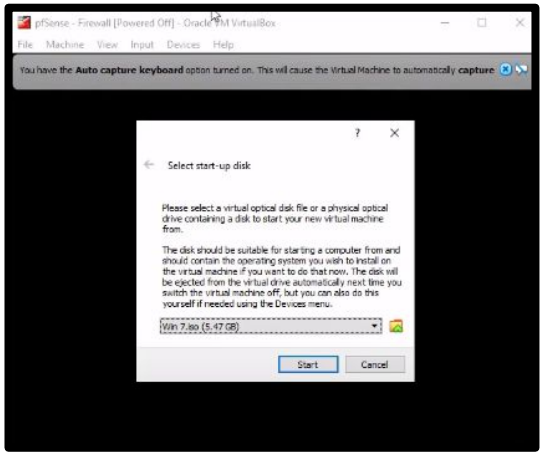


- Next, select “USB” option and ensure that “Enable USB Controller” is deselected

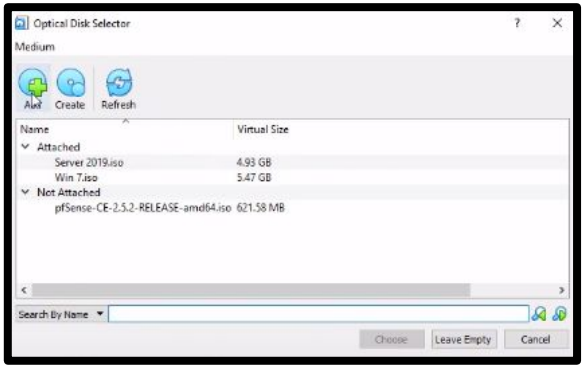
Install & Configure pfSense



- Select the “Network” option and ensure that “Enable Network Adapter” is selected. Further, the “Attached to” field should be set to “Bridged Adapter”. Select “ok”

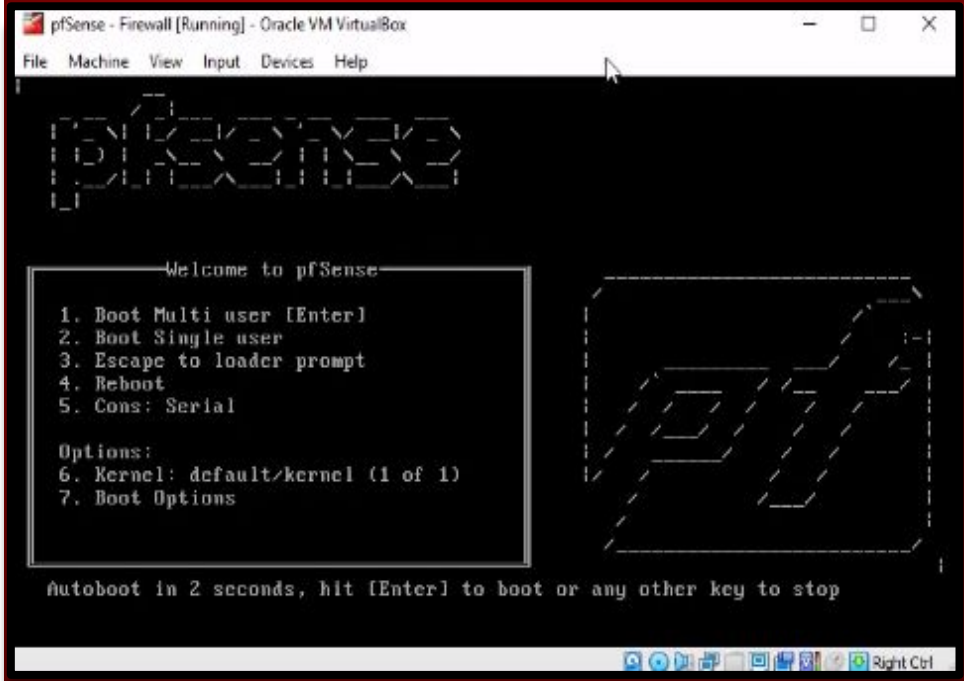


- Once out of the setting window, start the pfSense machine. Once this window appears, select the yellow file icon to populate the pfSense iso file

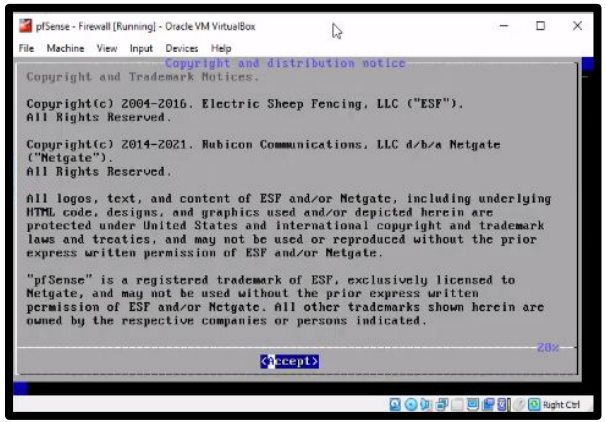


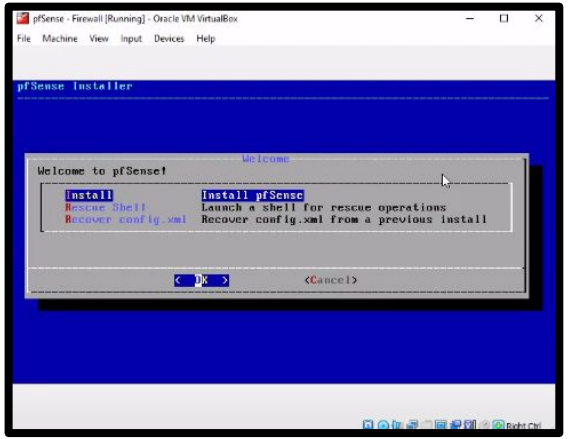
- Select “Add”. You will b directed to the file explorer where you will need to locate the pfSense iso file. Select “Choose” once file is located. Then, at startup disk menu, select “Start”.

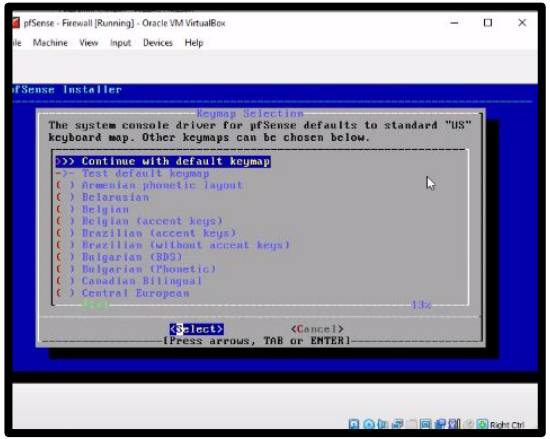
Success! Great Job!



Install & Configure pfSense

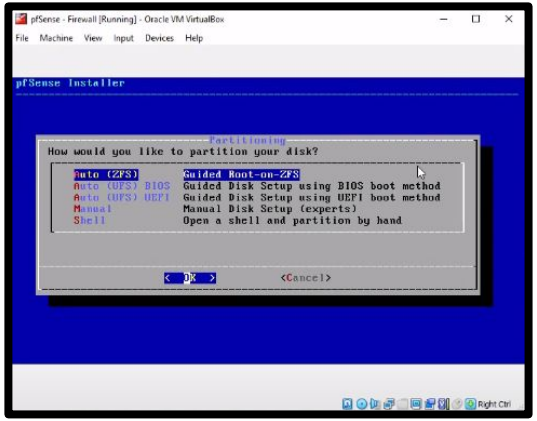




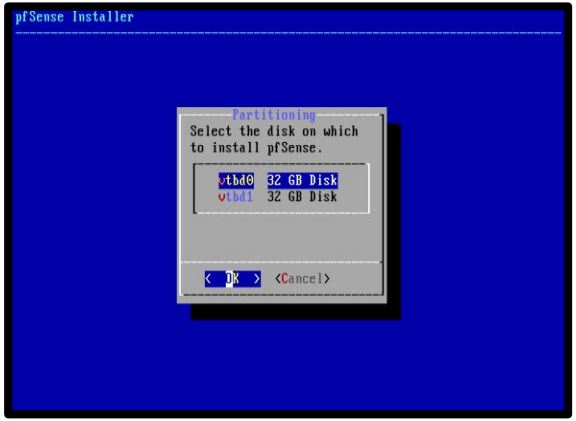


- Once at the copyright and distribution notice window select the enter key to accept notice. While configuring pfsense you will need to use your keyboard to navigate the machine.
- Highlight install pfSense then with “Ok’ highlighted, hit enter
- Next highlight “Continue with default keymap” then with “Select” highlighted hit “Enter”.

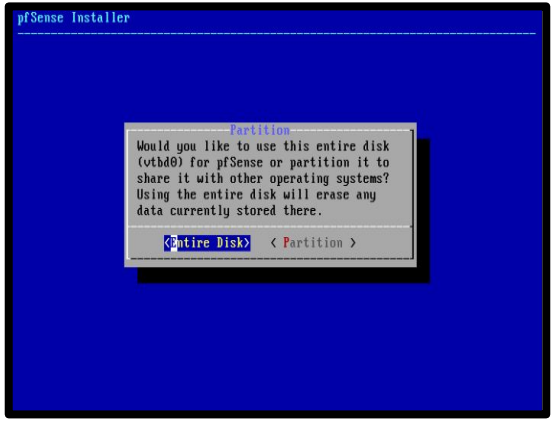
Install & Configure pfSense



- Next, at the “How would you like to partition your disk?” prompt select “Auto (UFS) BIOS”. Hit enter on keyboard.



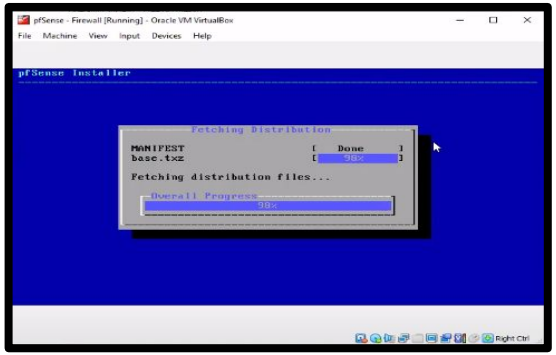
- At this prompt, you will select “vtb0 32GB Disk” then hit enter key.



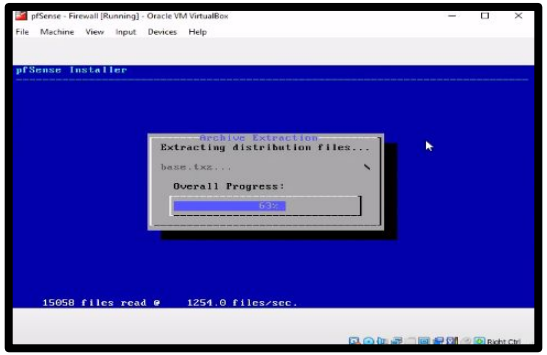
- Select “Entire Disk” when prompted. pfSense software does not support sharing a disk with another operating system.

Install & Configure pfSense

- Select “GPT” for the partition scheme

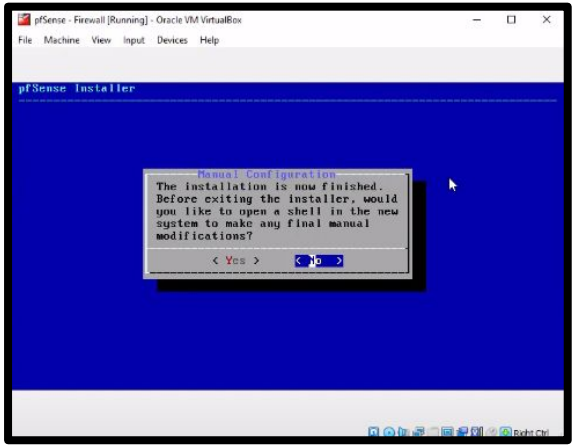


- Allow patching distribution process to run

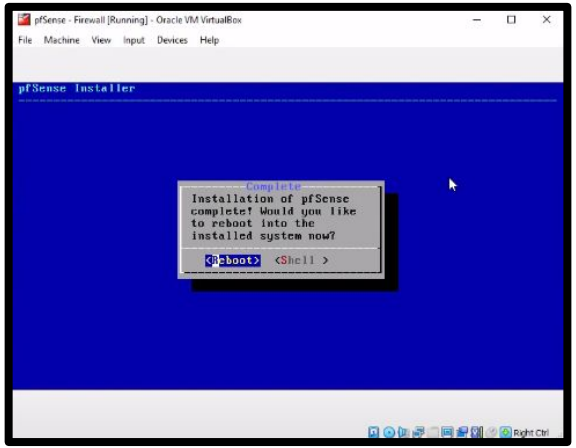


- Allow files to extract and copy into virtual hard disk

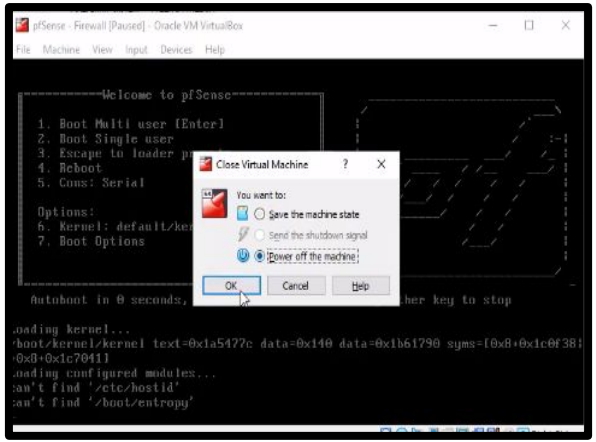
Install & Configure pfSense



- Since we are done configuring the pfSense firewall, you will highlight “Yes” then hit your enter key



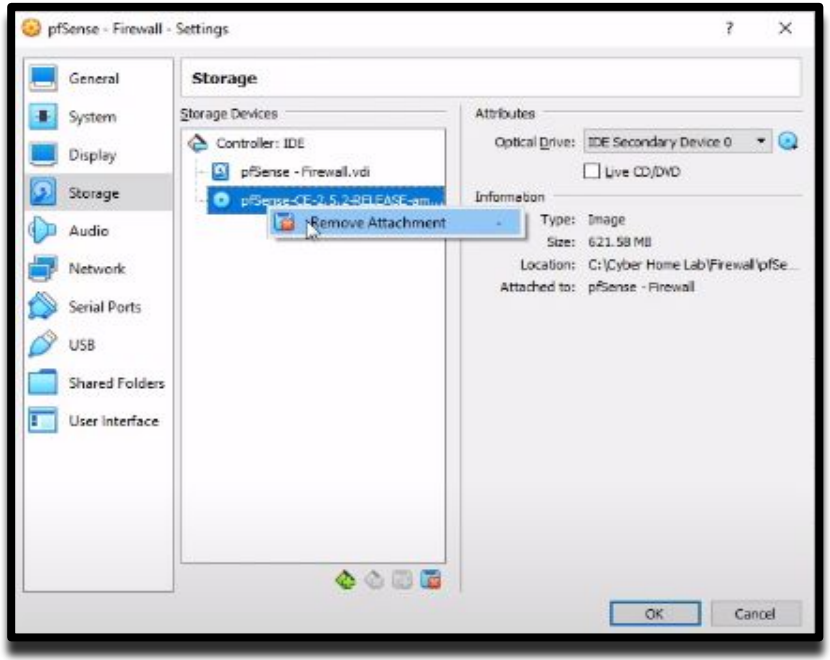
- Highlight “Reboot” then hit enter key



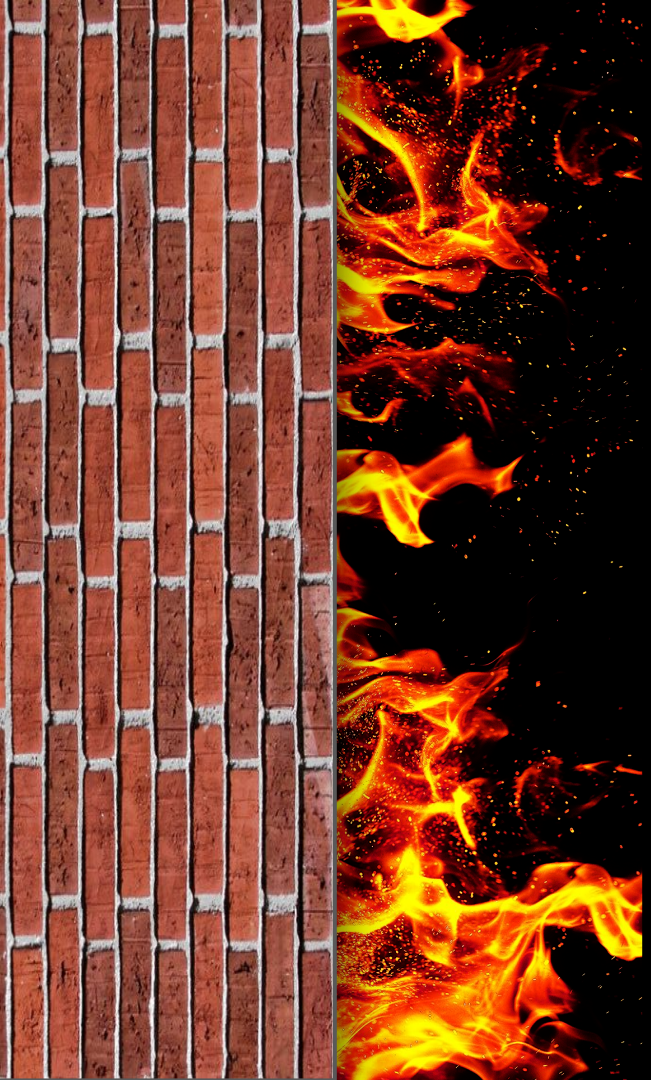
- Once the machine reboots and reaches the pfSense welcome screen, click the X in the top right corner of window to power off the machine before it autoboots.

Install & Configure pfSense

- Once you have powered off the pfSense Firewall machine, right click the machine name to access the settings
- Under the “Storage” option, select the listed pfSense iso file and “Remove Attachment”.
- Doing so will allow users to avoid the installation process recurring when powering on the machine
- Once completed select “Ok”

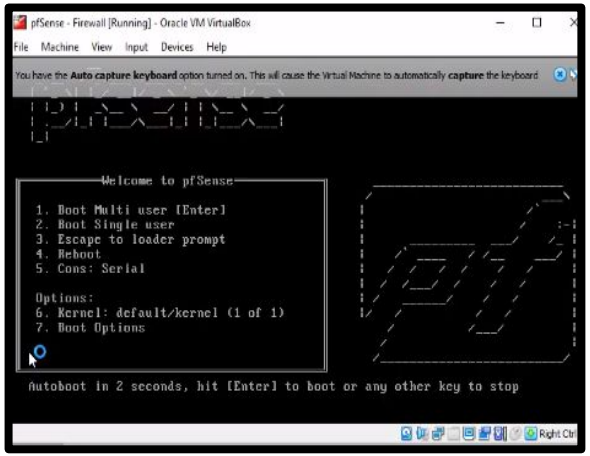


Success! Great Job!

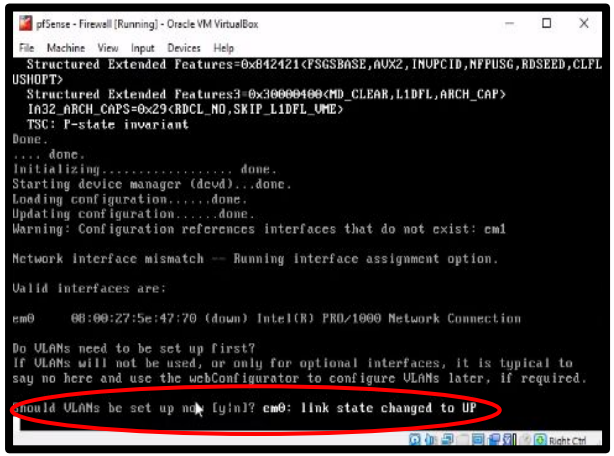


Finalize the Installation

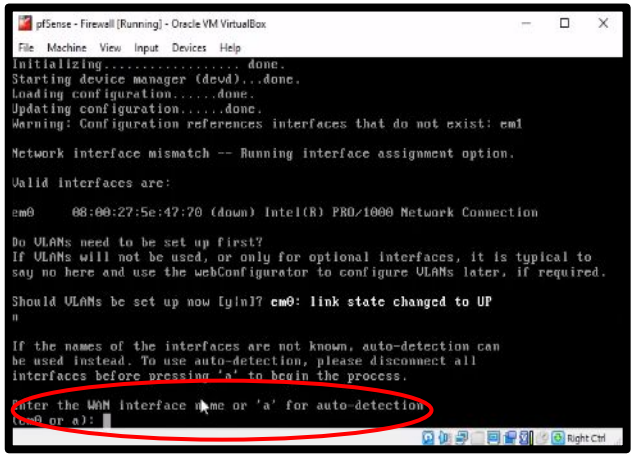
Finalize the Installation



- Relaunch the pfSense Firewall machine and allow the machine to complete its autoboot process

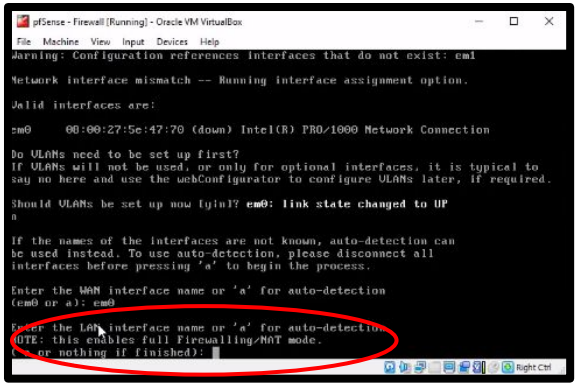


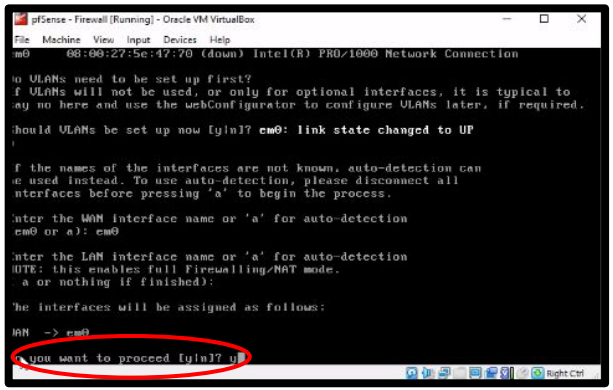
- Once the machine has booted, you will see a prompt that asks if we would like to configure VLANs. Type “n”, then hit enter on keyboard.

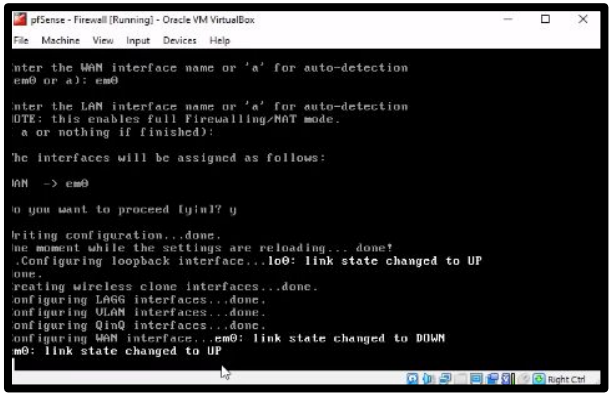


- Next, when prompted to enter the WAN interface, type “em0”.

Finalize the Installation

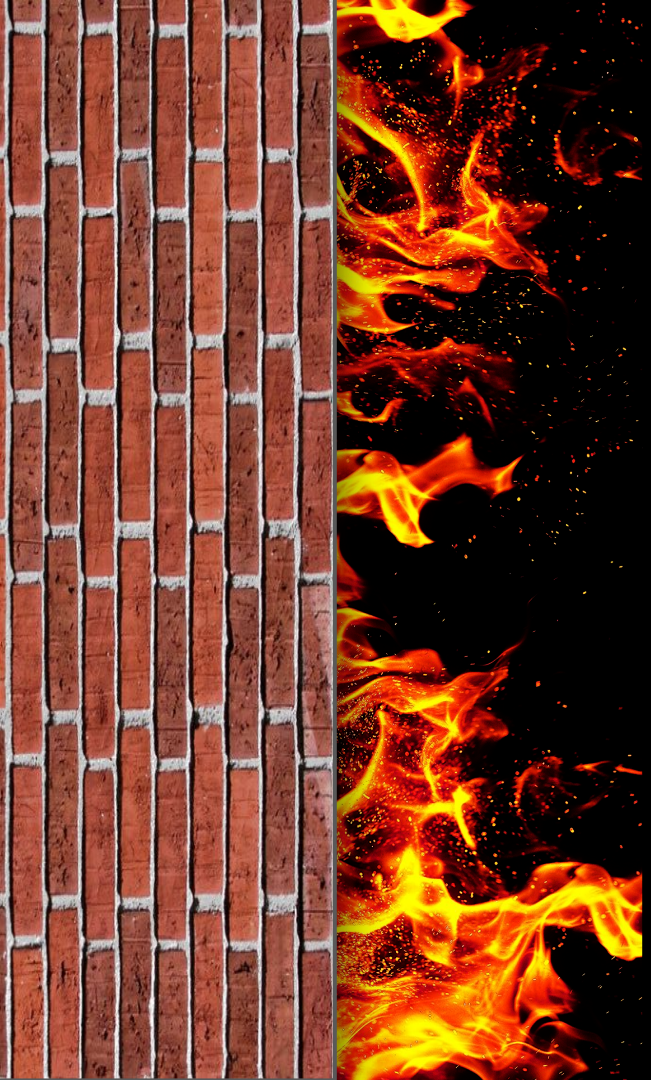






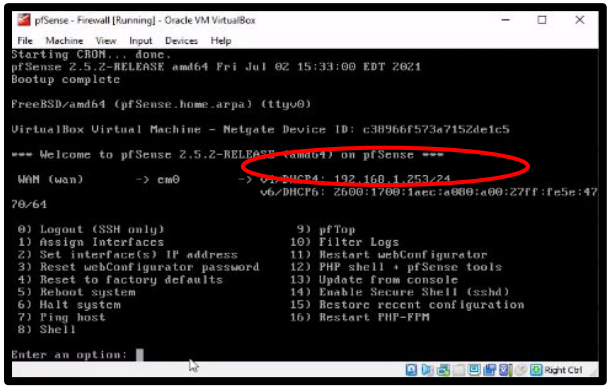
- Once at the LAN interface configuration prompt, bypass it by hitting enter key on keyboard. We will only be configuring the WAN for sake of project.
- Next, the prompt should read “Do you want to proceed [y/n]?” Type “y” then hit enter key.
- Allow the pfSense machine to complete its installation process

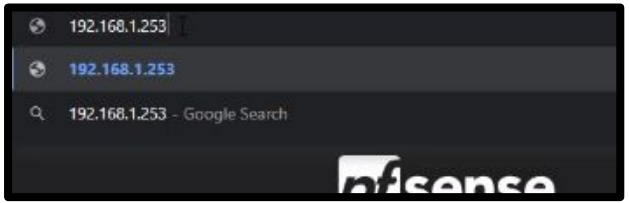
Success! Great Job!

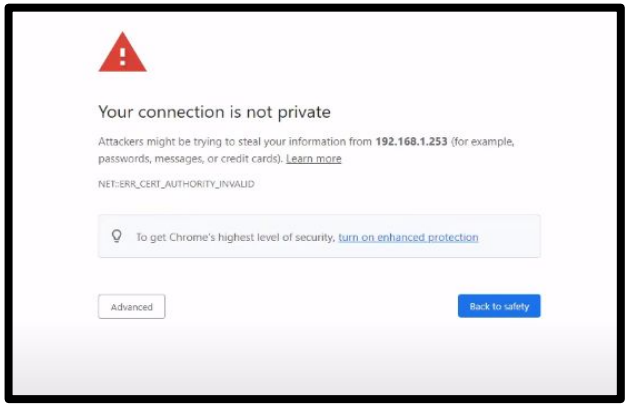


Configure pfSense Firewall in website

Configure pfSense Firewall website







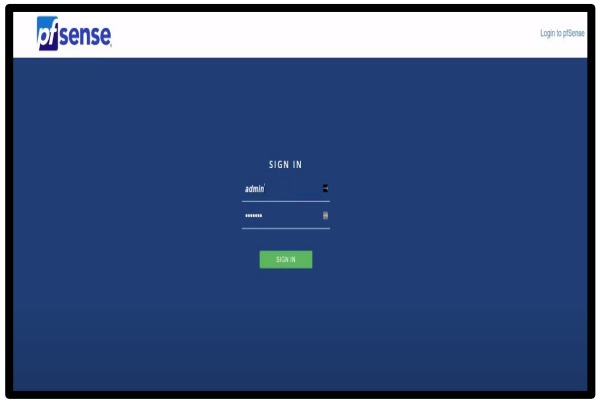
- In pfSense make note of its IP address and subnet mask.
  Also, in your physical host's cmd tool, note the IP and default gateway addresses.

- Input the pfSense IP address in the url search bar

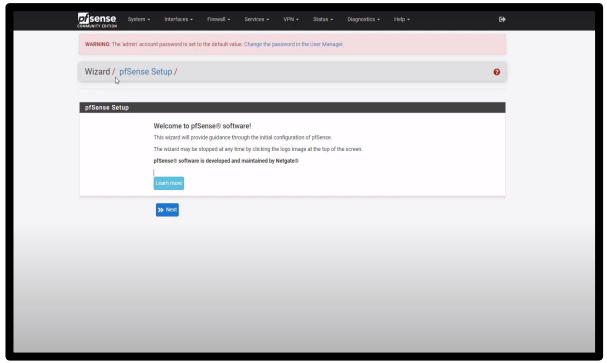
- You will reach this warning page due to untrusted certificates. To bypass this, select "Advanced".

Configure pfSense Firewall website

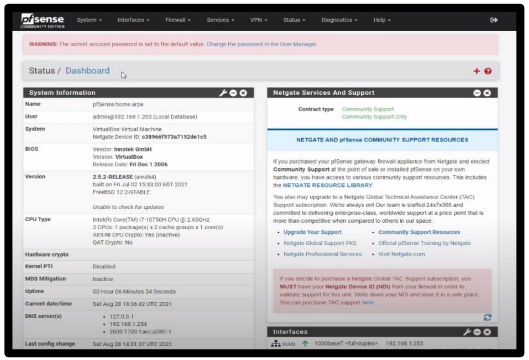
- Sign into pfSense with username “admin” and password “pfsense”



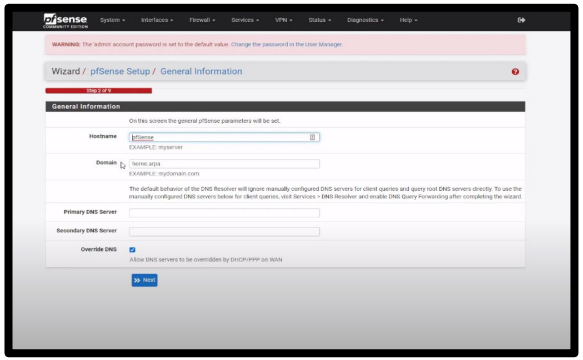
- Select “Next” once signed in. If you are prompted to sign in again, repeat this step.



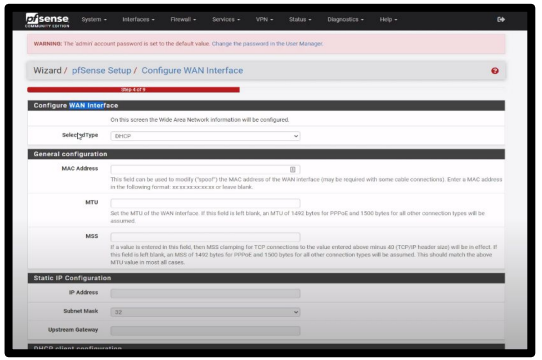
Configure pfSense Firewall website



- Navigate to “System” at top of the webpage, then access “Setup Wizard”



- Click “Next” until you reach this webpage. In the “Primary DNS Server” field input 8.8.8.8

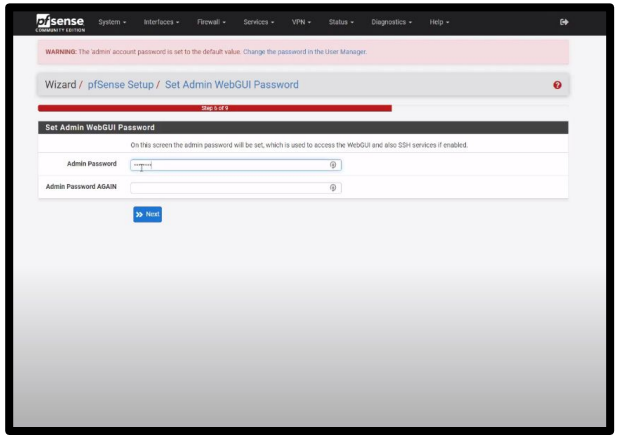


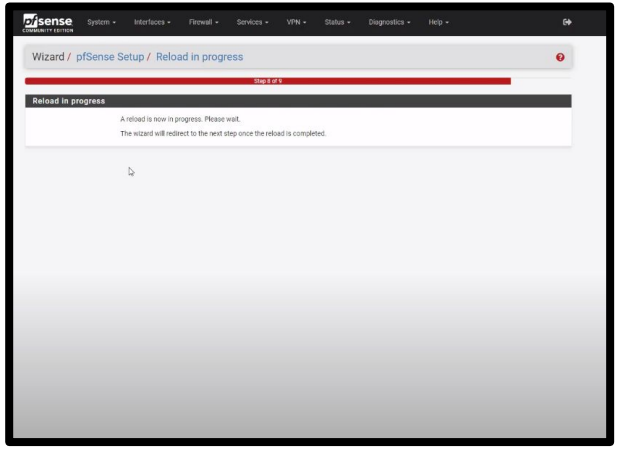
- Click “Next” until you reach the webpage with “Configure WAN Interface” option. Select “Static”. Scroll down to “Static IP Address” and type the pfSense Firewall IP address. Also input the subnet mask and your host’s upstream, aka default gateway

Configure pfSense Firewall website

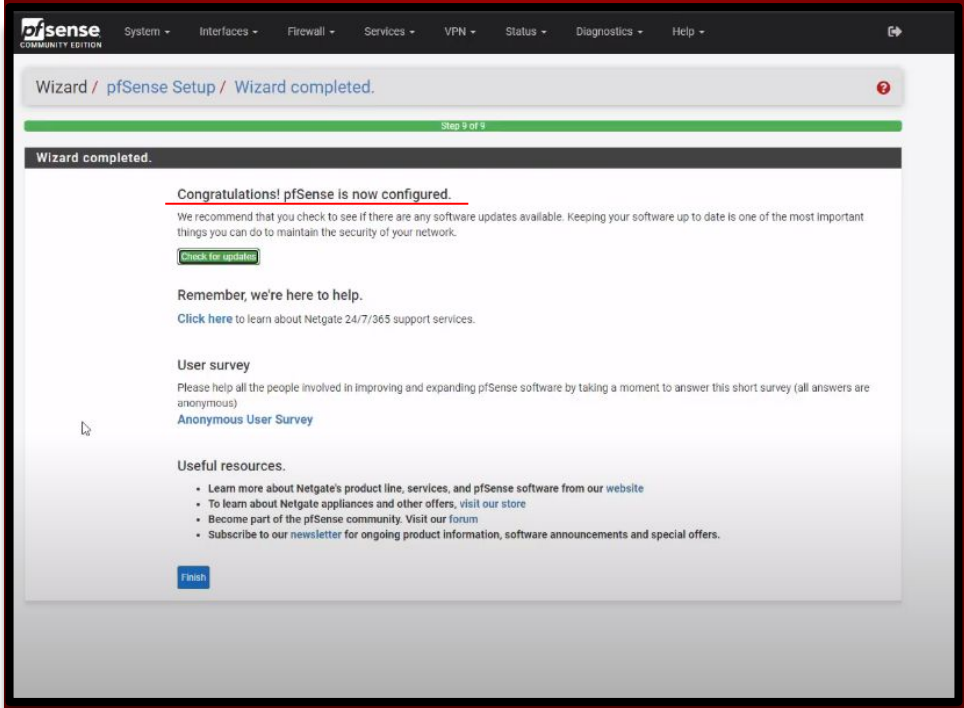
- On the next webpage you should be prompted to set a new password for your pfSense account

- Once your new password is set allow pfSense to reload

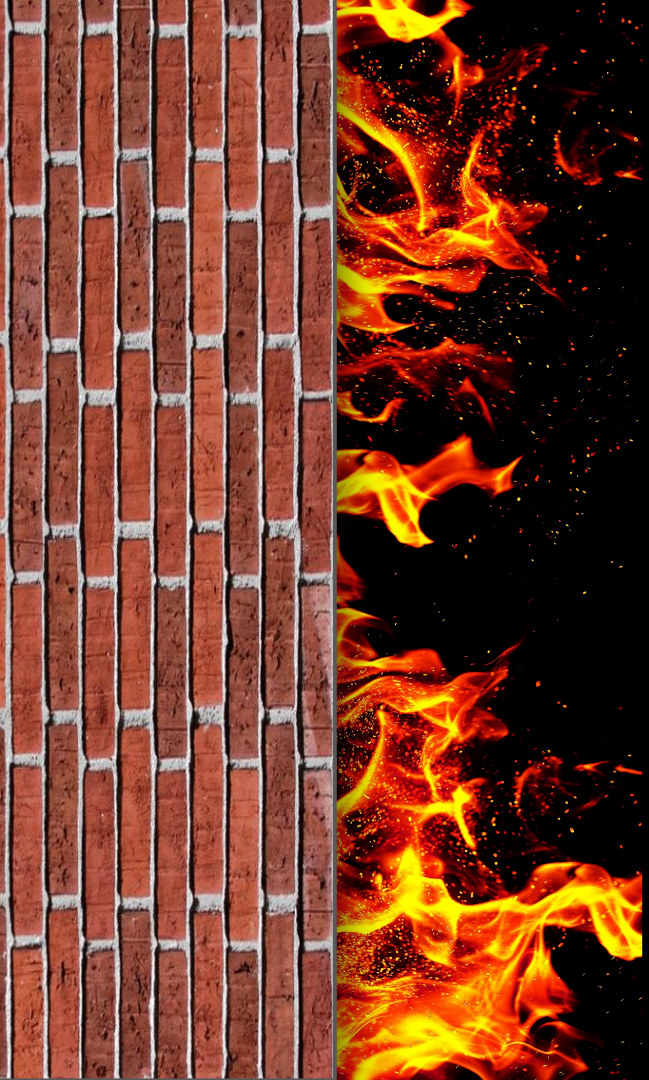




Success! Great Job!



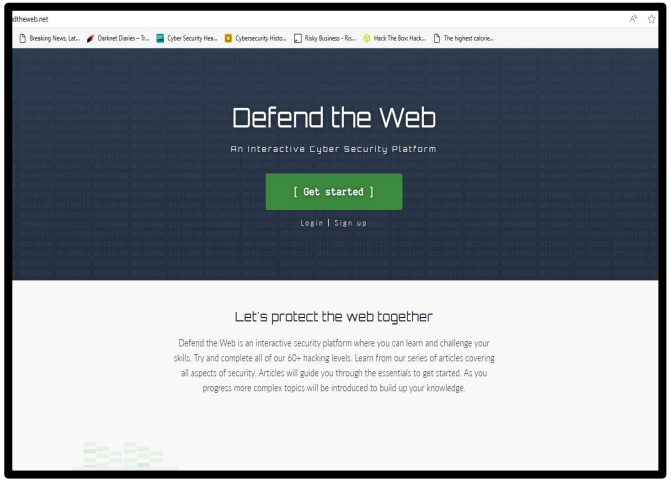
*Select “Finish”, then accept the copyright and trademark notices.

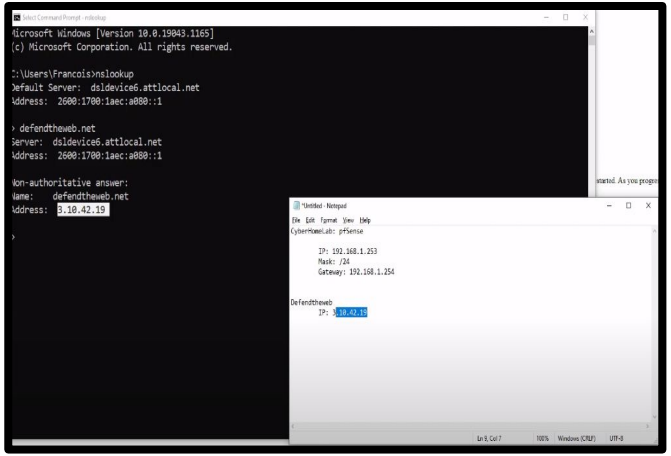


Create a Firewall Rule

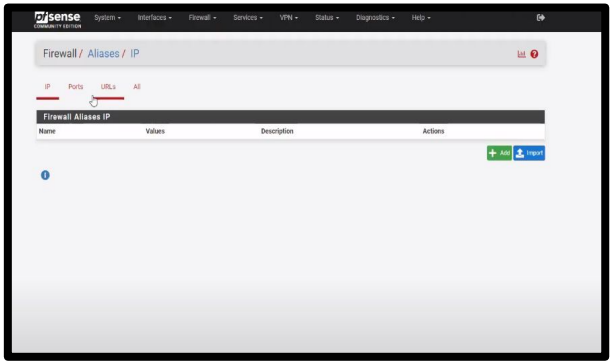
Create a Firewall Rule

- Navigate to your browser and access the An Interactive Cyber Security Platform | Defend the Web link to access the Defend the Web website.
- After accessing the site, navigate to the cmd line tool and type “ns lookup” then the domain name “defendtheweb.net”
- Note the IP address associated with the site

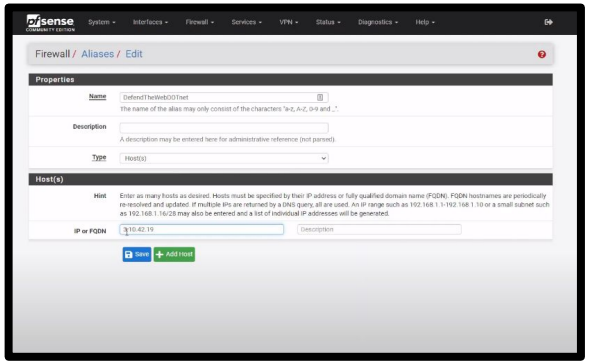




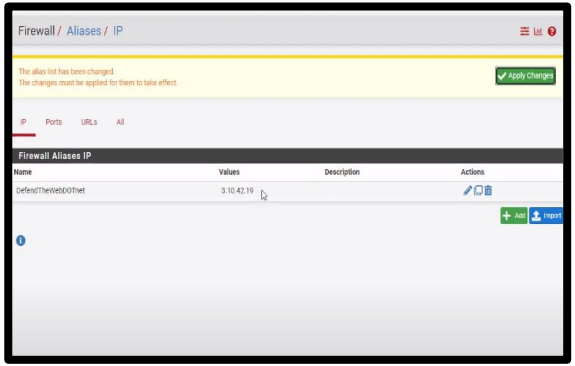
Create a Firewall Rule



- Navigate back to the pfSense website and select “Firewall” then “Aliases”. On the next page select “Add”.



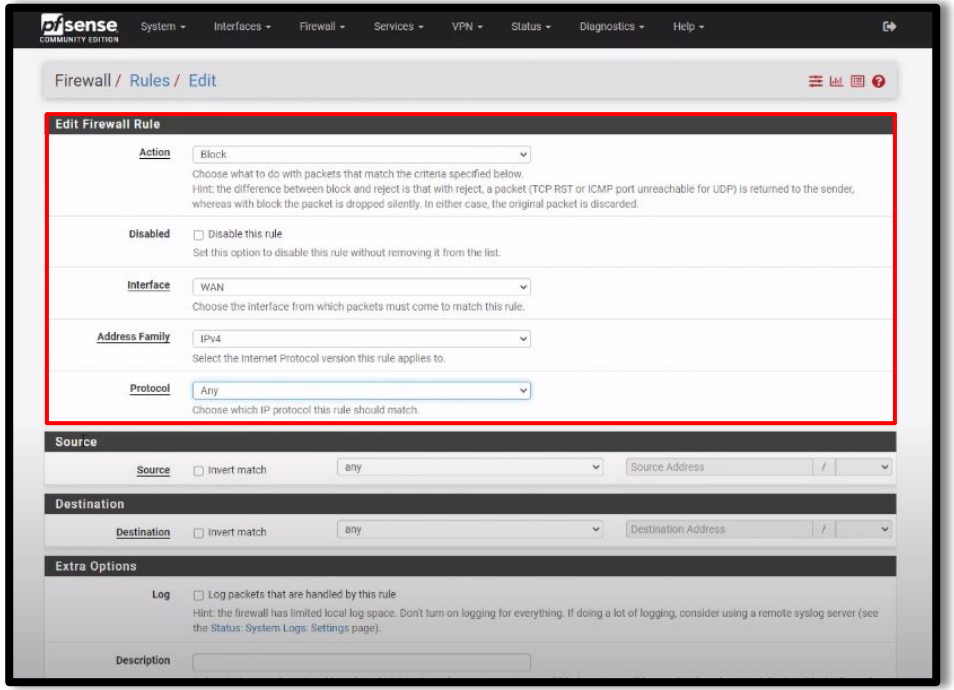
- In the “Name” field, input DefendTheWebDOTnet”. Next, input the Defend the Web IP address in the “IP or FQDN” field. Select “Save” once completed.



- On this page, select “Apply changes”. After completing this step, access “Firewall” at top of page and navigate to “Rules”.

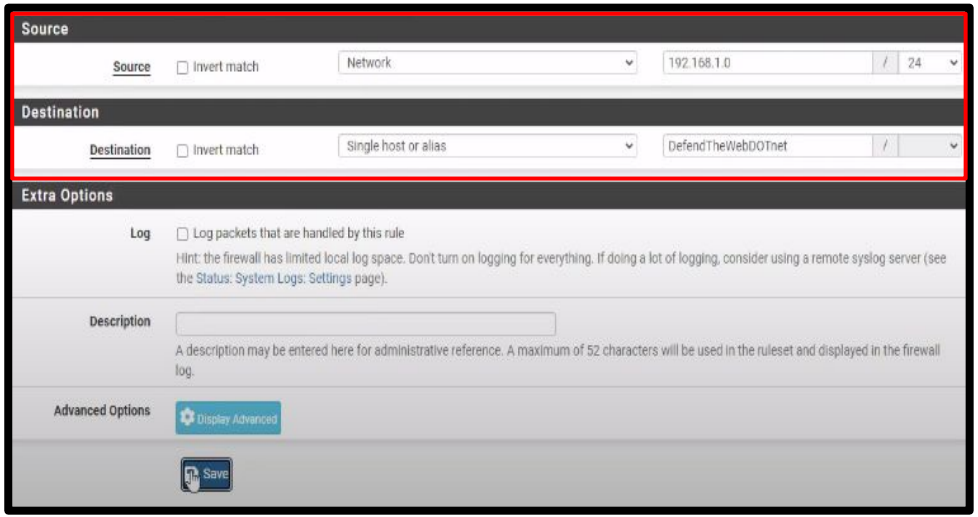
Create a Firewall Rule

- Select “Add” then edit the firewall rules by inputting the following values in each field.
- Note: These rules will be configured against the DefendtheWeb.net site

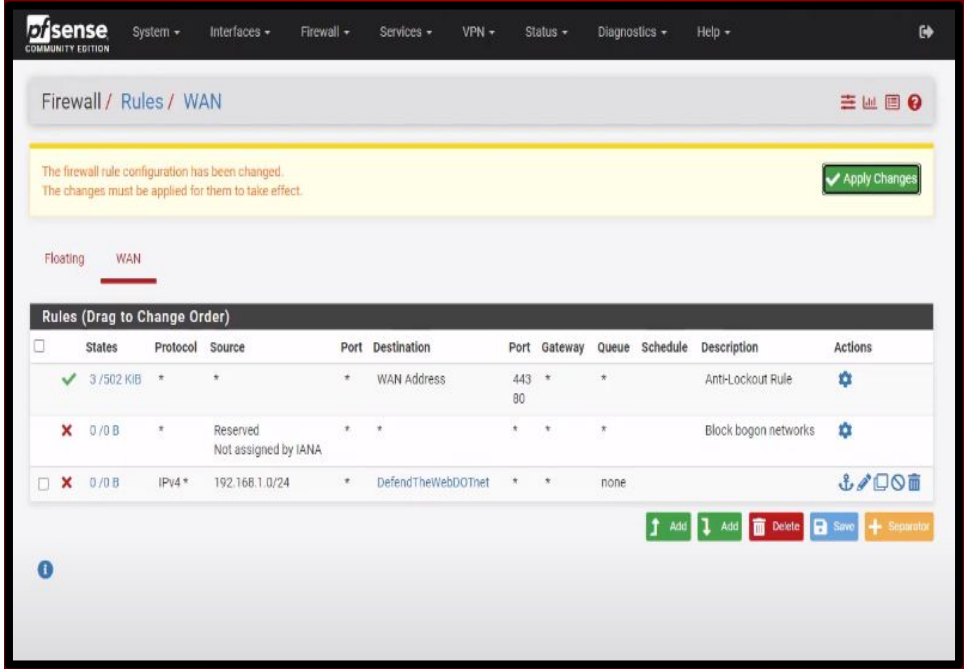


Create a Firewall Rule

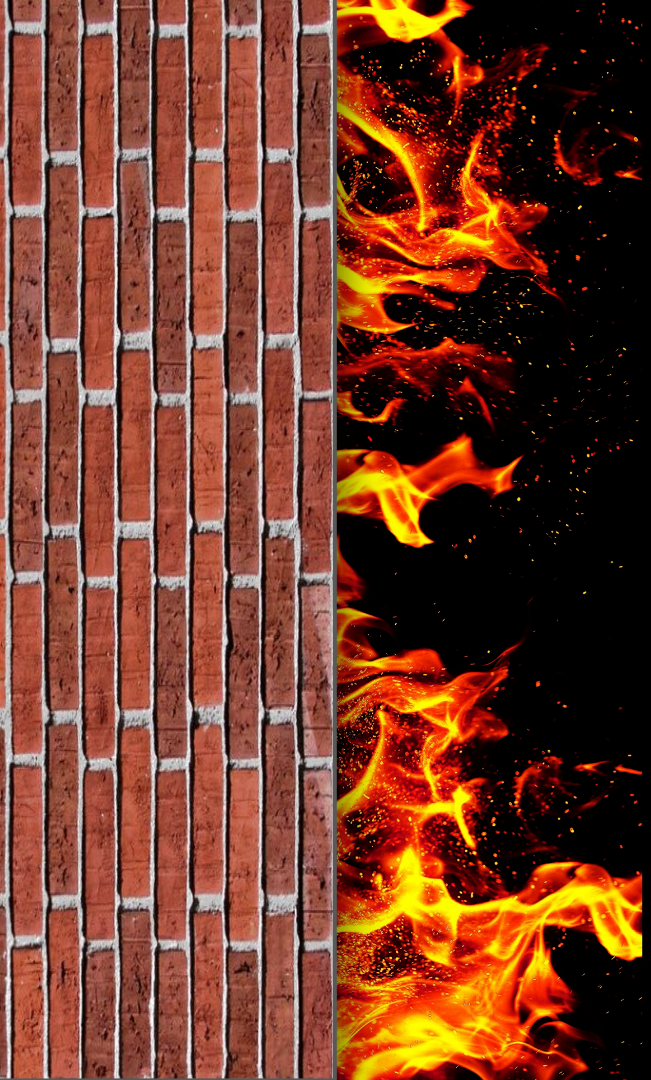
- On the same webpage, in the “Source” field select “Network” then input your physical host’s Ip address along with the subnet mask
- In the “Destination” field select “Single host or alias” then, input “DefendtheWebDOTnet”
- Once these steps are completed, “Save” the modifications.



Success! Great Job!

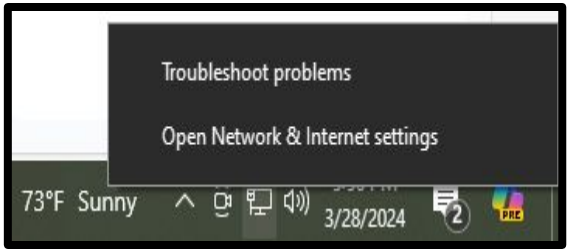


*The new rule should populate here. Once populated, select “Apply changes”.

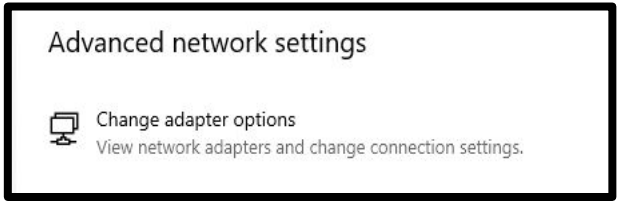


Add Firewall to Physical Host's Network

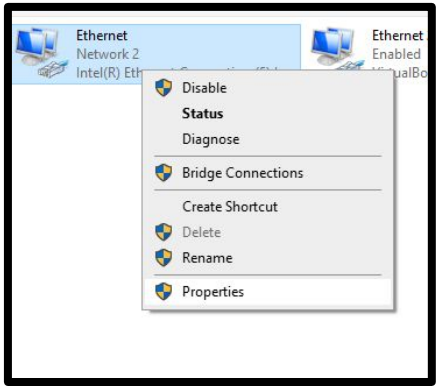
Add Firewall to Physical Host's Network



- Right click the network icon in bottom right corner of screen



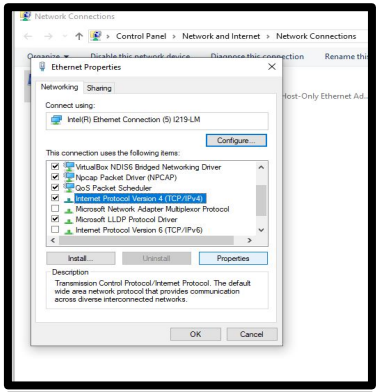
- Under "Advanced network settings", select "Change adapter options"

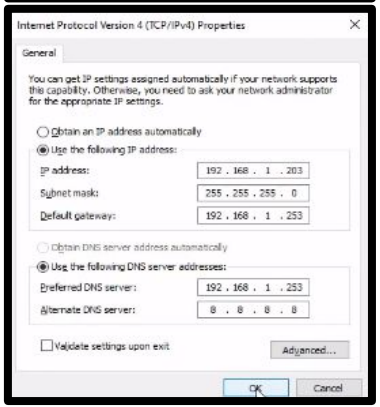


- Right click appropriate network, then select properties

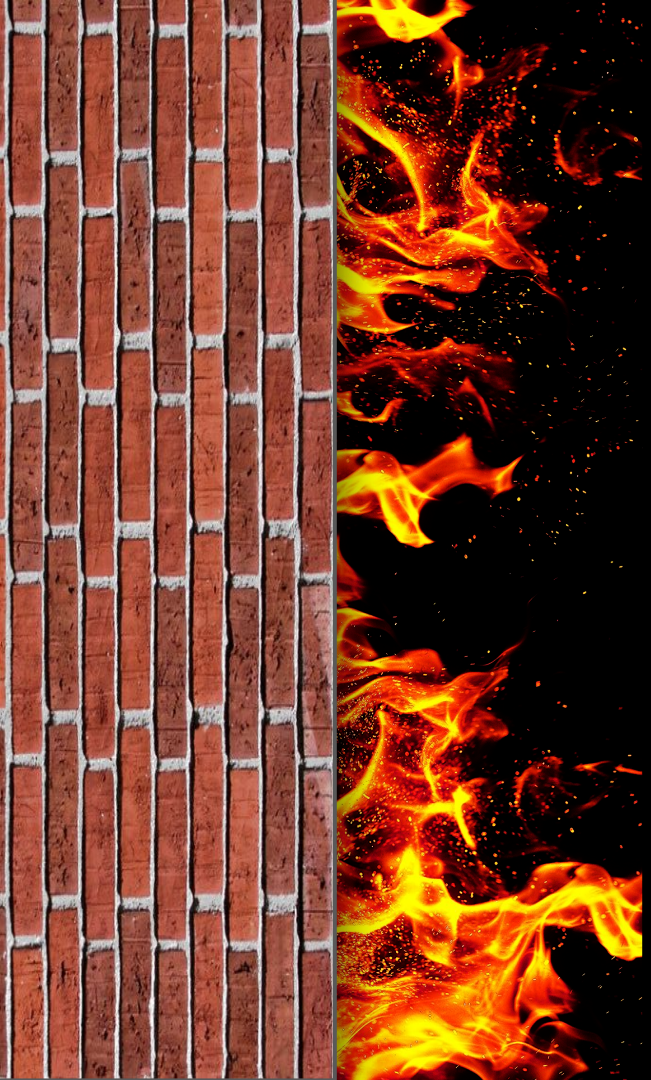
Add Firewall to Physical Host's Network

- Highlight IPv4, then select properties
- Input physical host's IP and subnet mask. In the default gateway and preferred DNS server fields, input the pfSense firewall IP address and 8.8.8.8 for the alternate DNS server.





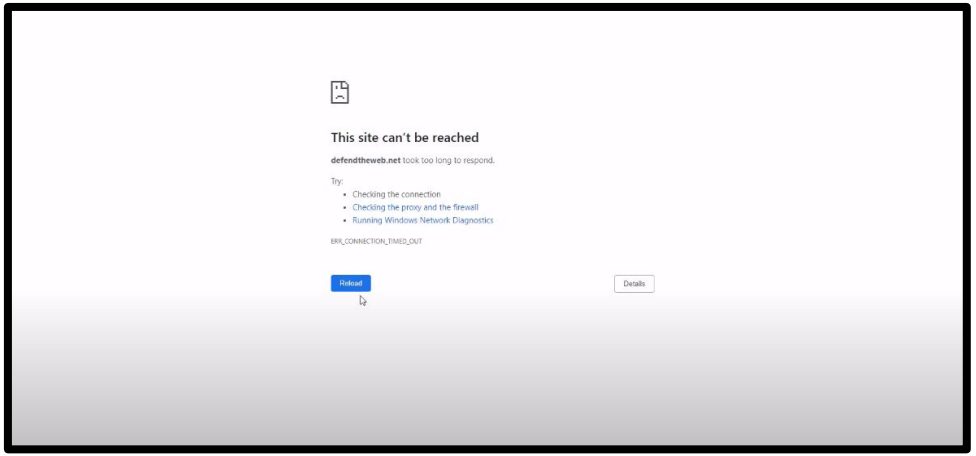
Success! Great Job!



Test the Firewall

Test the Firewall

- Search defendtheweb.net in url bar.
- Due to the implementation of the firewall, the website will not load
- You will eventually see this page, denying access to the targeted IP



Congratulations, you configured a pfSense Firewall!