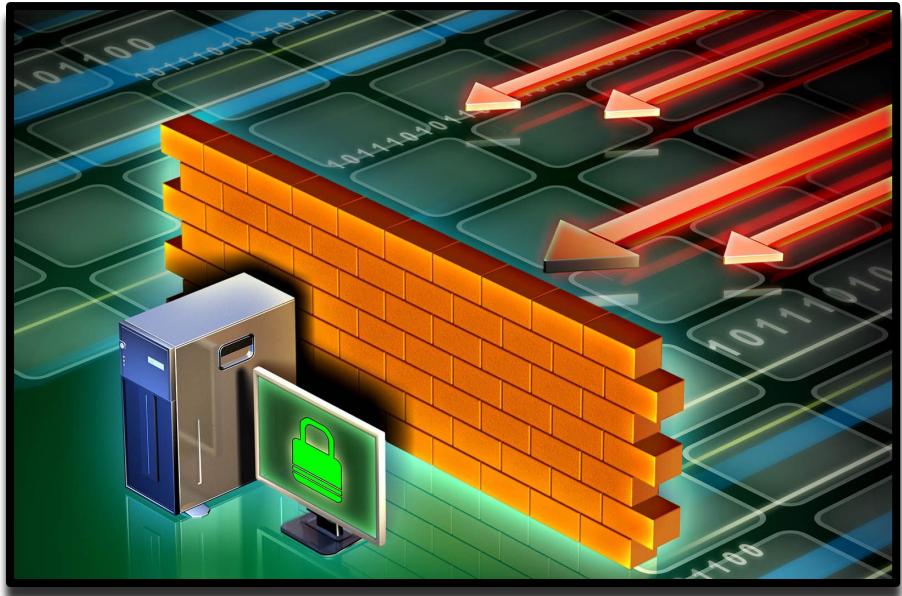


pfSense Firewall

A Step-by-Step Guide

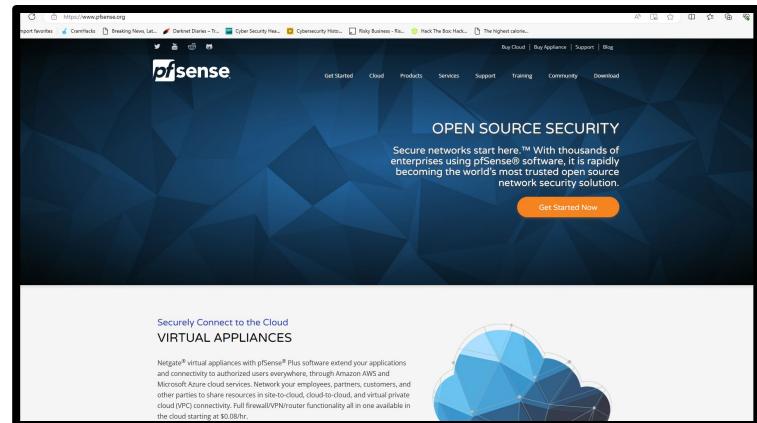
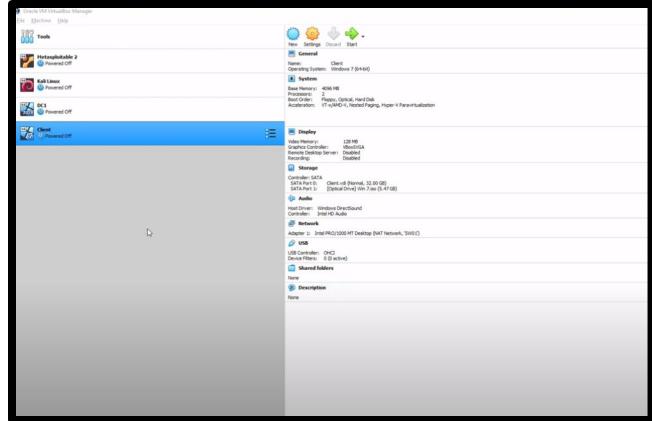
What is a Firewall and why is it necessary?

- 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](https://www.pfsense.org)



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



This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the pfSense® firewall appliances from Netgate.

[RELEASE NOTES](#) [SOURCE CODE](#)

Select Image To Download

Version: 2.7.2
Architecture: AMD64 (64-bit)
Installer: [DVD Image \(ISO\) Installer](#)

[DOWNLOAD](#) Supported by

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
 TMR Appliances

[Subscribe](#) (view our [privacy policy](#))

Downloads

pfSense-CE-2.7.2-RELEASE-amd64.iso.gz [Open file](#)

Cyber Home Lab (1).pdf [Open file](#)

Cyber Home Lab.pdf [Open file](#)

[See more](#)

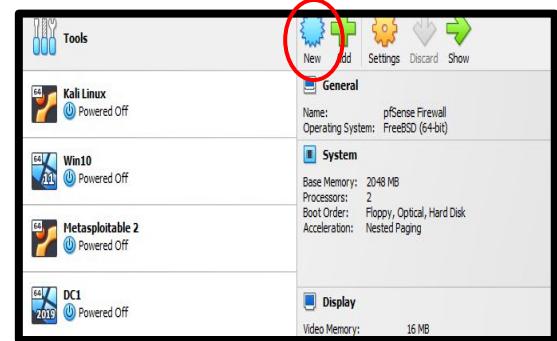
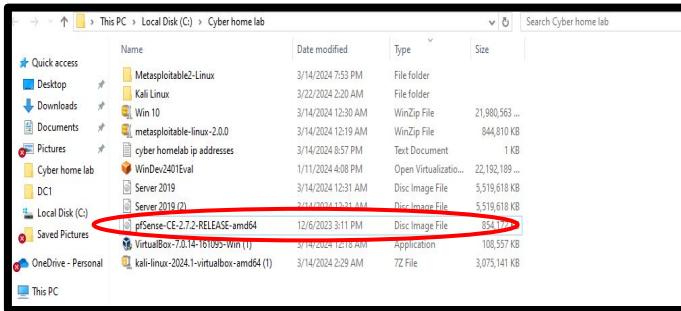
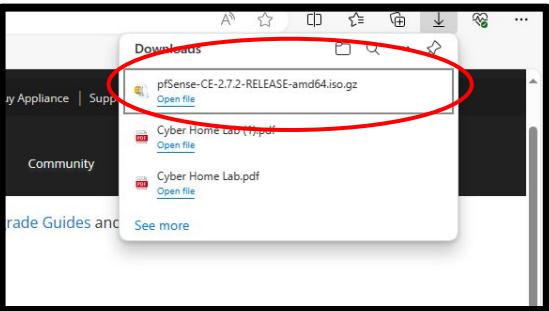
Download the 7 Zip Tool

- Next, in your browser, navigate to the 7 Zip website to download the tool ([Download \(7-zip.org\)](https://www.7-zip.org/download.html)).
- 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.

The screenshot shows the 7-Zip download page at <https://www.7-zip.org/download.html>. The page features three main download sections:

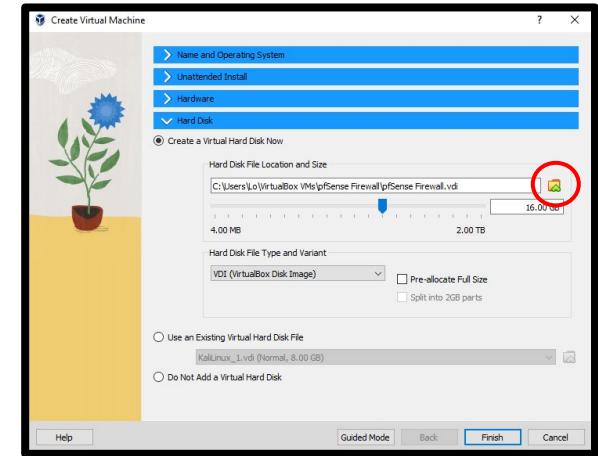
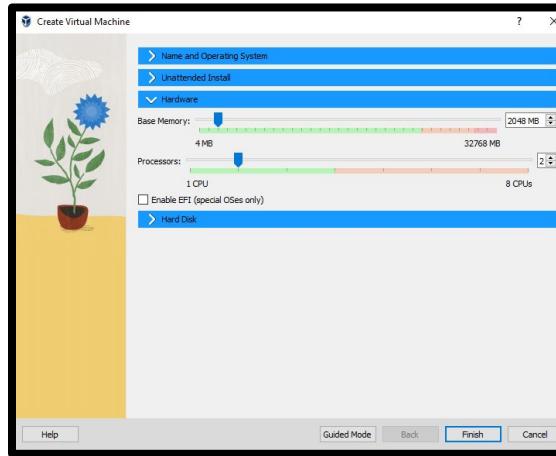
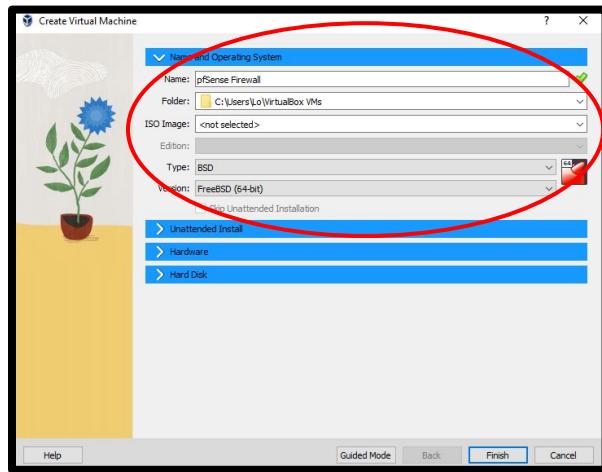
- Download 7-Zip 24.03 beta (2024-03-23) for Windows:** This section lists five download links for Windows: .exe (x64), .exe (x86), .exe (arm64), .msi (x64), and .msi (x86). The .exe (x64) link is highlighted with a green border. Descriptions for the .msi links mention they are alternative MSI installers.
- Download 7-Zip 24.03 beta (2024-03-23) for Linux and MacOS:** This section lists five download links for Linux and Mac OS: .tar.xz (x86-64), .tar.xz (x86), .tar.xz (arm64), .tar.xz (arm), and .tar.xz (macOS). The .tar.xz (x86-64) link is highlighted with a green border. Descriptions for the .tar.xz links mention they are console versions.
- Download 7-Zip 23.01 (2023-06-20):** This section lists seven download links for Windows, Linux, and Mac OS: .exe (x64), .exe (x86), .exe (arm64), .msi (x64), .msi (x86), .7z (x64), and .tar.xz (macOS). The .exe (x64) link is highlighted with a green border. Descriptions for the .msi and .7z links mention they are alternative MSI installers.

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".

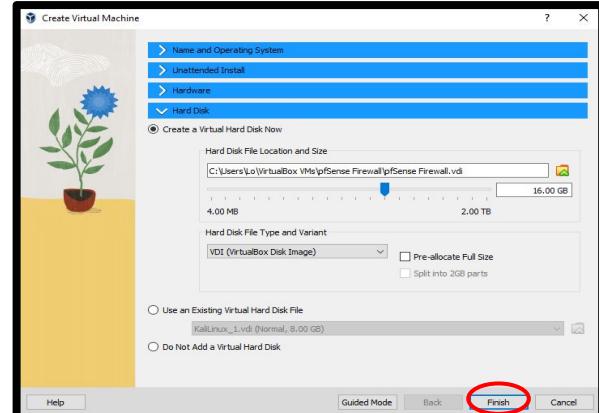
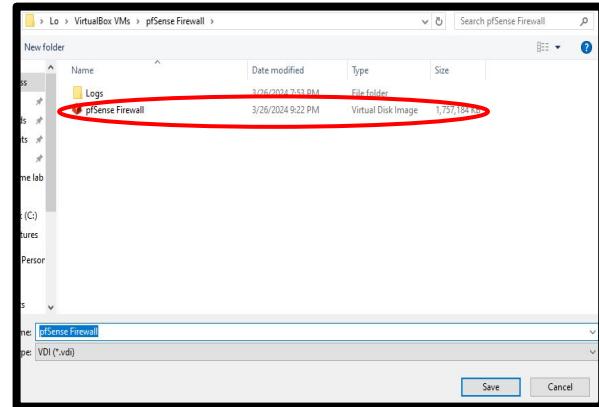
Add pfSense Firewall to Virtualbox



- 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!



Tools

New Add Settings Discard Start

Kali Linux	Powered Off
Win10	Powered Off
Metasploitable 2	Powered Off
DC1	Powered Off
pfSense Firewall	Powered Off

General

Name: pfSense Firewall
Operating System: FreeBSD (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging

Display

Video Memory: 16 MB
Graphics Controller: VMVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Primary Device 0: pfSense Firewall.vdi (Normal, 16.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Ethernet Connection (S) I219-LM)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

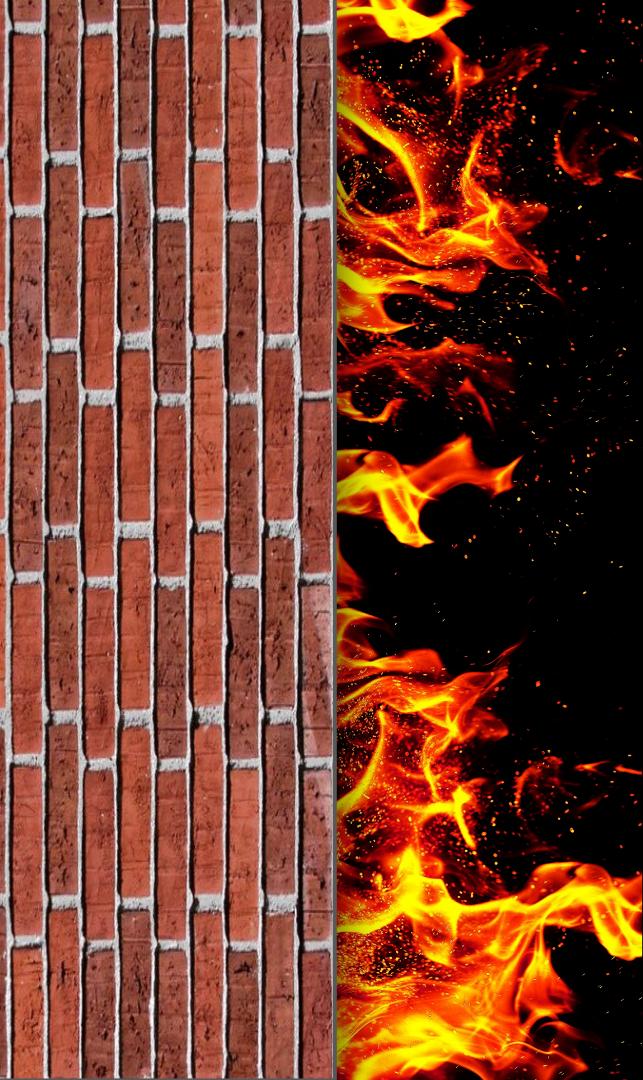
None

Description

None

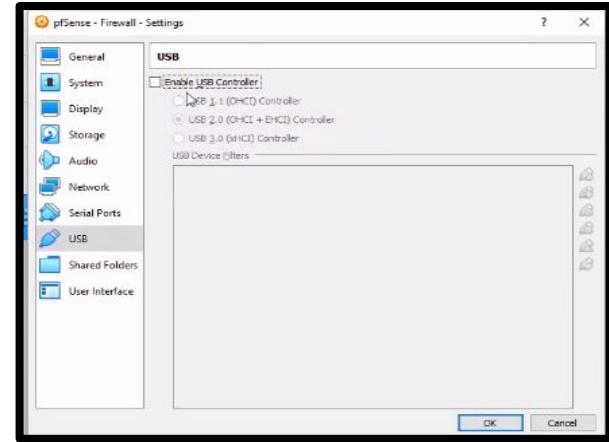
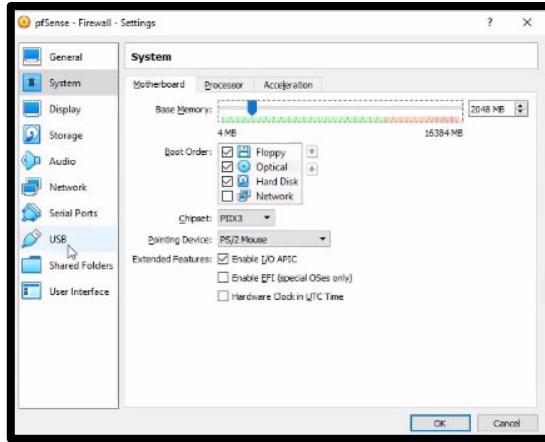
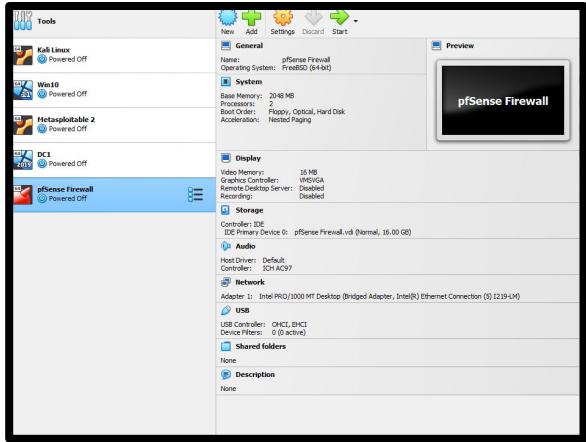
Preview

A screenshot of the Oracle VM VirtualBox Manager interface. On the left, a list of virtual machines includes Kali Linux, Win10, Metasploitable 2, DC1, and pfSense Firewall. The pfSense Firewall entry is highlighted with a red box. To the right, detailed configuration settings for the pfSense Firewall VM are displayed under sections like General, System, Display, Storage, Audio, Network, USB, Shared folders, and Description. A preview window on the far right shows the pfSense Firewall logo.



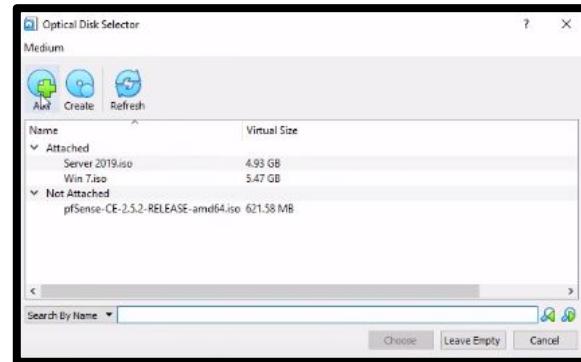
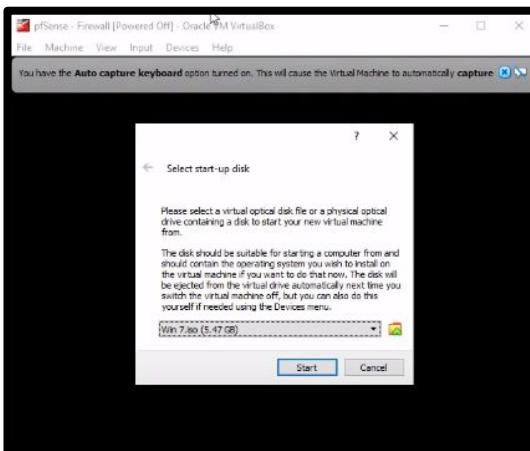
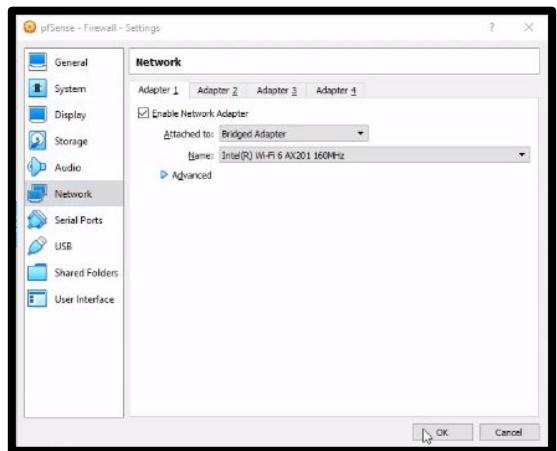
Installation & Configuration

Install & Configure pfSense



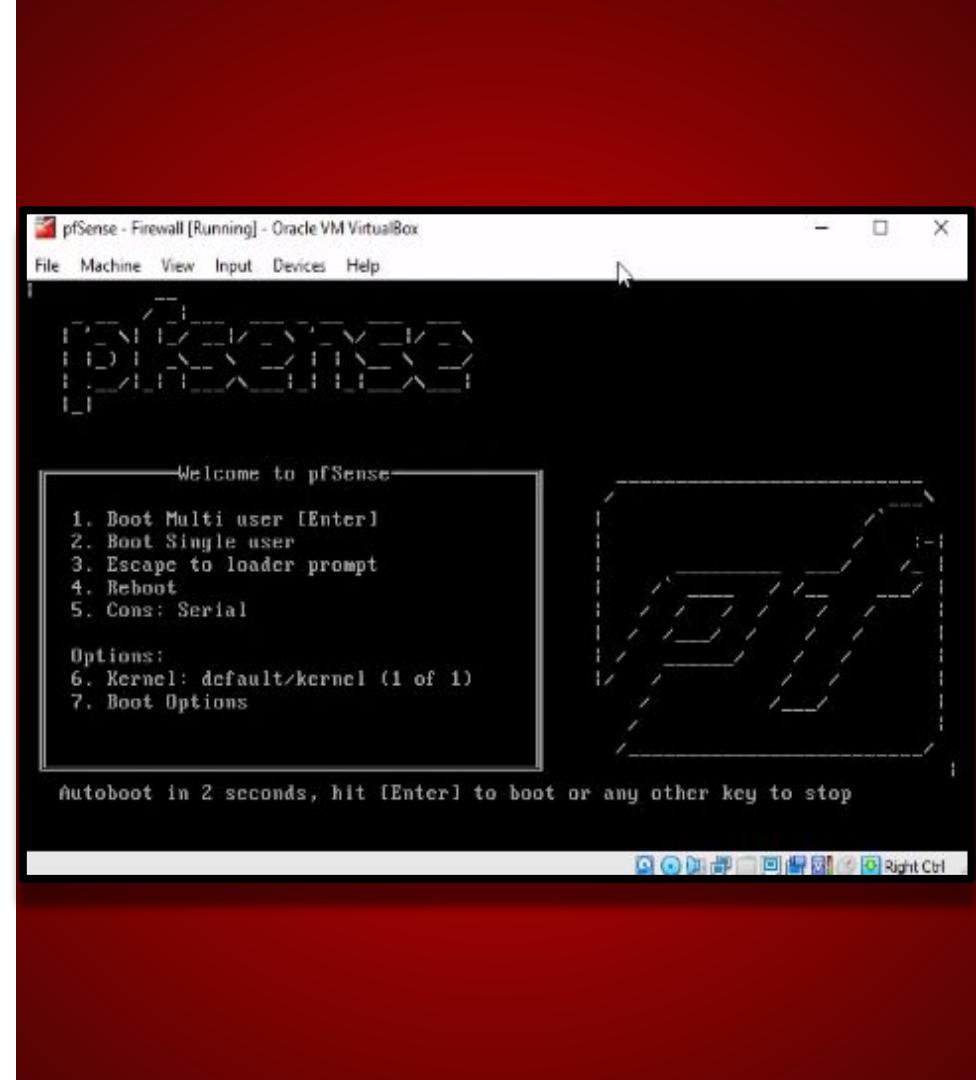
- Right click the “pfSense Firewall” machine and access the “Settings”
- Once in settings, access the “System” option, then the “Motherboard” tab. Set memory to 2048MB. Next, under the “Processor” tab, set CPU to 2
- Next, select “USB” option and ensure that “Enable USB Controller” is deselected

Install & Configure pfSense

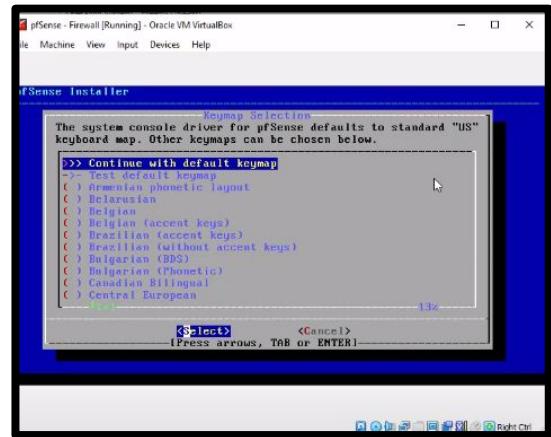
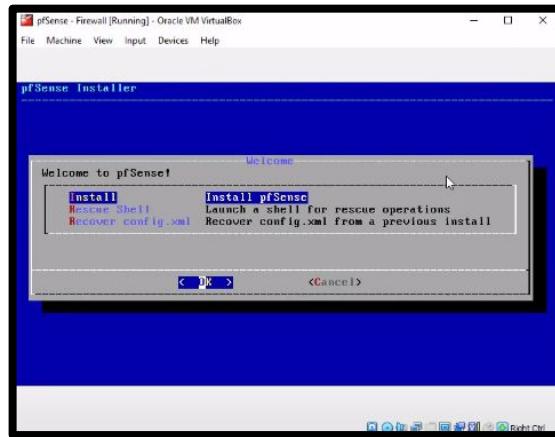
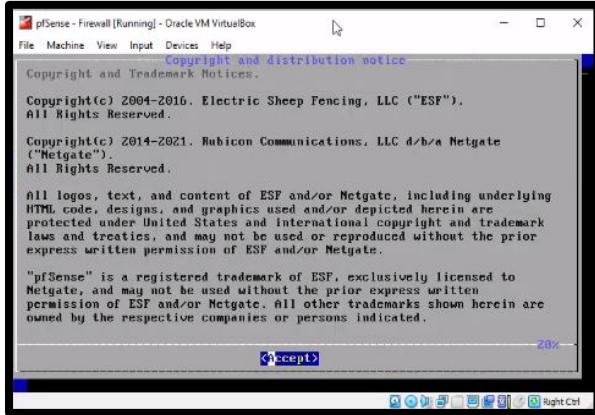


- Select the “Network” option and ensure that “Enable Network Adapter” is selected. Further, the “Attached to” field should be set to “Bridged Adapter”. Select “ok”
- Once out of the setting window, start the pfSense machine. Once this window appears, select the yellow file icon to populate the pfSense iso file
- Select “Add”. You will be 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!

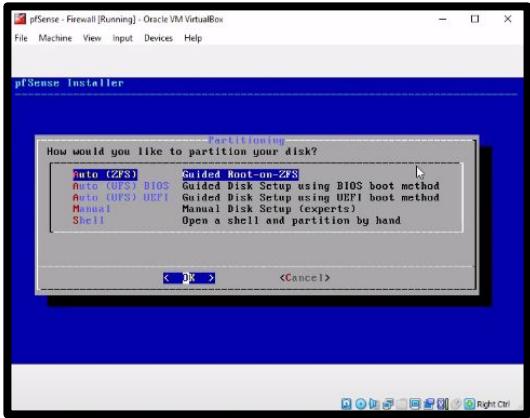


Install & Configure pfSense



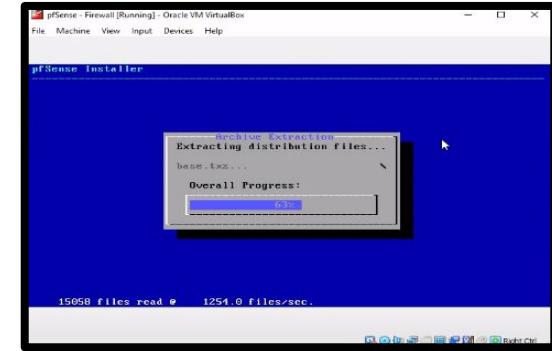
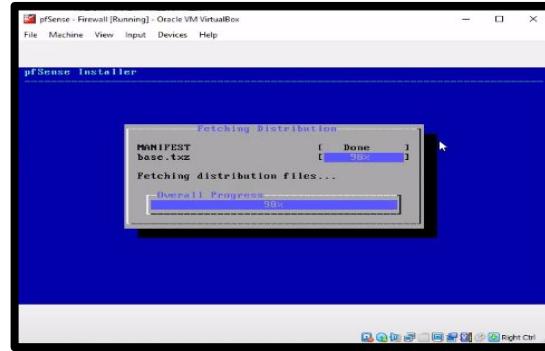
- Once at the copyright and distribution notice window select the enter key to accept notice. While configuring pfSense you will need to use your keyboard to navigate the machine.
- Highlight "Install pfSense" then with "Ok" highlighted, hit enter
- Next highlight "Continue with default keymap" then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

Install & Configure pfSense



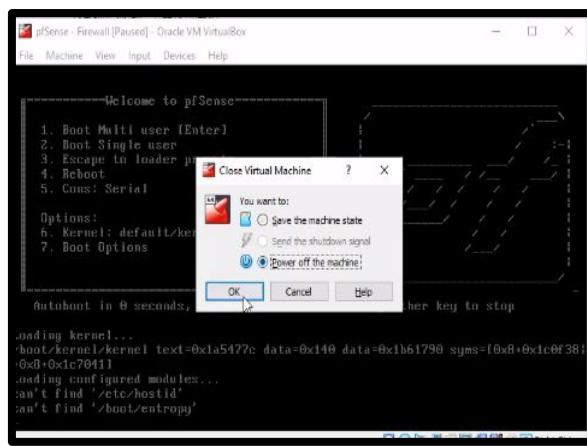
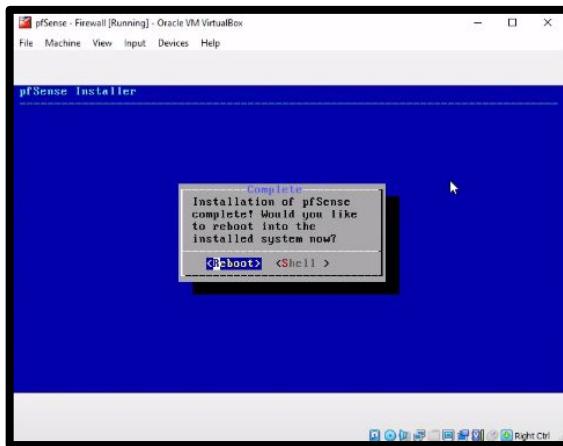
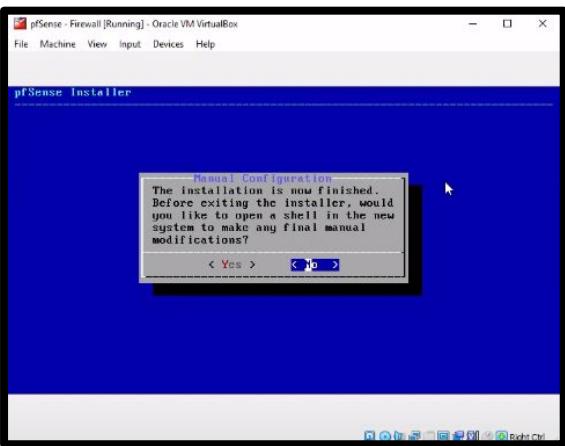
- Next, at the “How would you like to partition your disk?” prompt select “Auto (UFS) BIOS”. Hit enter on keyboard.
- At this prompt, you will select “vtb0 32GB Disk” then hit enter key.
- Select “Entire Disk” when prompted. pfSense software does not support sharing a disk with another operating system.

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

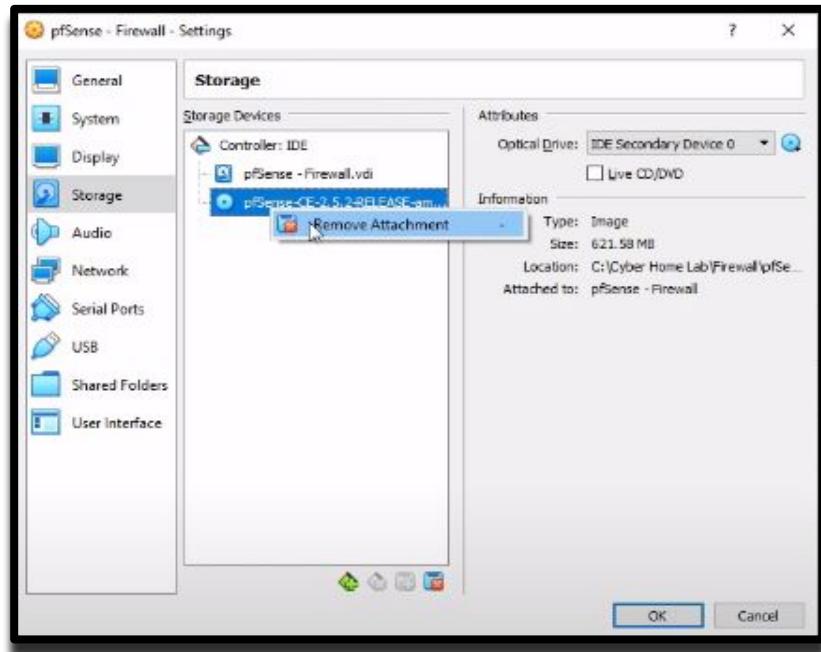
Install & Configure pfSense



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

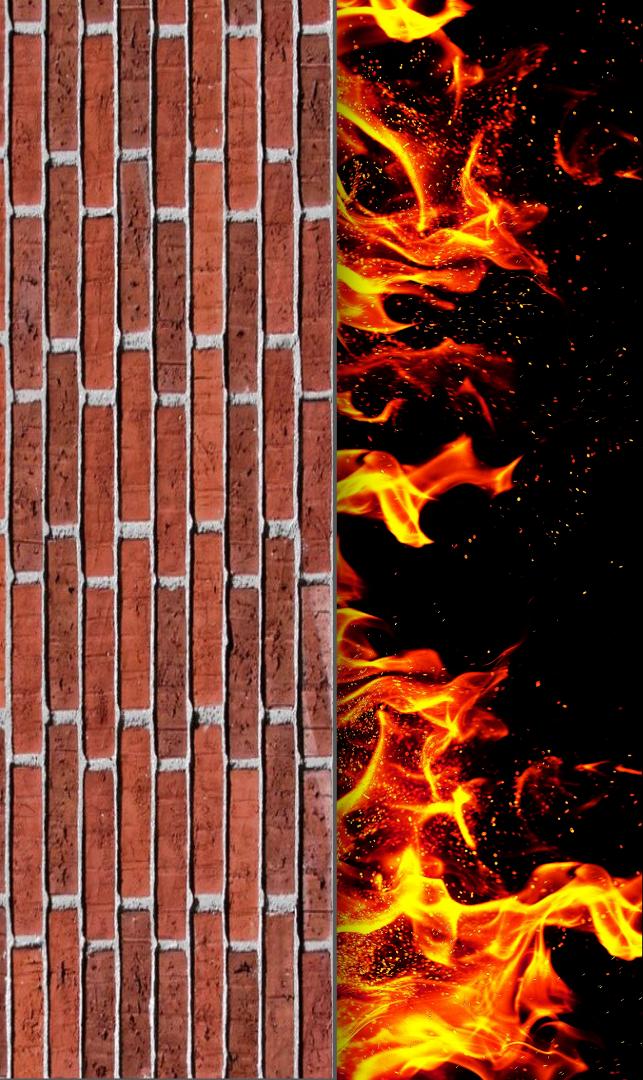
Install & Configure pfSense

- 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”



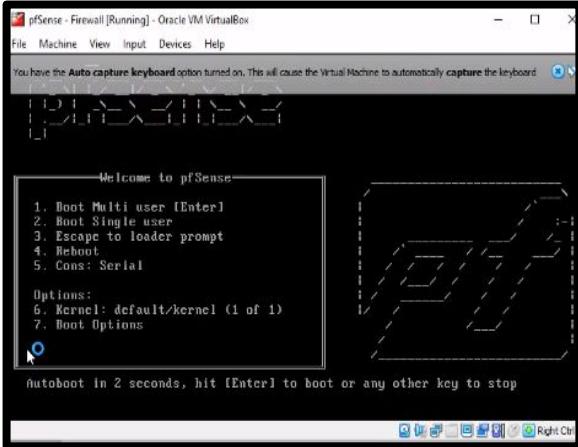
Success! Great Job!





Finalize the Installation

Finalize the Installation



```
File Machine View Input Devices Help
Structured Extended Features=0x842421<FSGSBASE,AUX2,INUPCID,NFPUISG,BDSEED,CLFL,USSHOT>
Structured Extended Features3=0x30000400<MD_CLEAR,L1DFL,ARCH_CAP>
IN32_ARCH_CAPS=0x29<RDCL_NO,SKIP_L1DFL,ARCH_CAP>
TSC: P-state invariant
Done.
.....done.
Initializing.....done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em1
Network interface mismatch -- Running interface assignment option.
Valid interfaces are:
em0    00:00:27:5e:47:70 (down) Intel(R) PRO/1000 Network Connection
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y/n]? em0: link state changed to UP
n
```

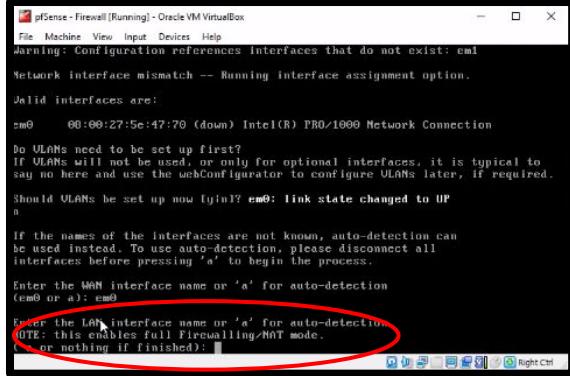
The terminal output shows the boot process. It initializes, starts the device manager, loads and updates configuration, and then checks for network interface mismatch. It lists valid interfaces (em0) and asks if VLANs should be set up. The user types "n" to skip VLAN setup.

```
File Machine View Input Devices Help
Initializing.....done.
Starting device manager (devd)...done.
Loading configuration.....done.
Updating configuration.....done.
Warning: Configuration references interfaces that do not exist: em1
Network interface mismatch -- Running interface assignment option.
Valid interfaces are:
em0    00:00:27:5e:47:70 (down) Intel(R) PRO/1000 Network Connection
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y/n]? em0: link state changed to UP
n
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'n' to begin the process.
Enter the WAN interface 'em0' or 'a' for auto-detection
(y/n or a):
```

The terminal output continues with a warning about network interface mismatch. It then asks if VLANs should be set up. The user types "n". It then asks for the WAN interface name or "a" for auto-detection. The input field is circled in red.

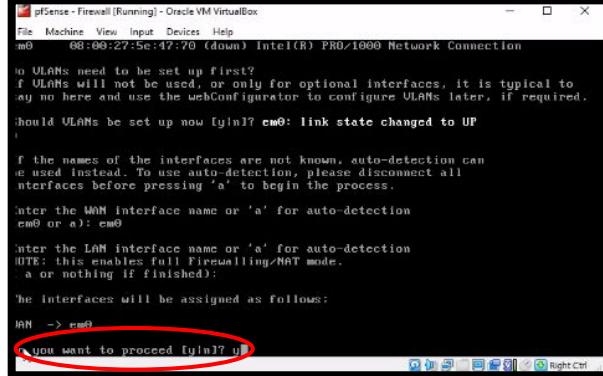
- Relaunch the pfSense Firewall machine and allow the machine to complete its autoboot process
- Once the machine has booted, you will see a prompt that asks if we would like to configure VLANs. Type “n”, then hit enter on keyboard.
- Next, when prompted to enter the WAN interface, type “em0”.

Finalize the Installation



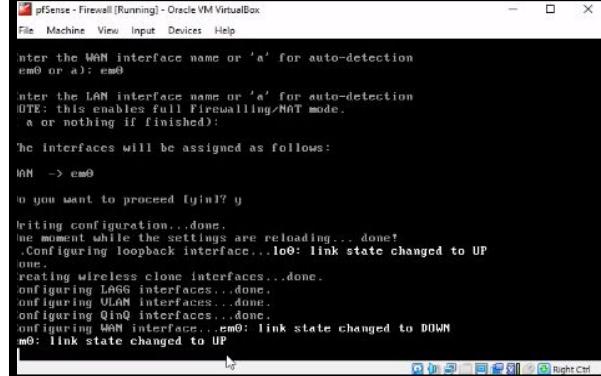
```
pfSense - Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Warning: Configuration references interfaces that do not exist: em1
Network interface mismatch -- Running interface assignment option.
Valid interfaces are:
em0  00:00:27:5e:47:70 (down) Intel(R) PRO/1000 Network Connection
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now? [y/n]? em0: link state changed to UP
n
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 or a): em0
Enter the LAN interface name or 'a' for auto-detection.
NOTE: this enables full Firewalling/NAT mode.
[nothing is finished]:
```



```
pfSense - Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
em0  00:00:27:5e:47:70 (down) Intel(R) PRO/1000 Network Connection
no VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now? [y/n]? em0: link state changed to UP
n
The names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 or a): em0
Enter the LAN interface name or 'a' for auto-detection.
NOTE: this enables full Firewalling/NAT mode.
[nothing is finished]:
```

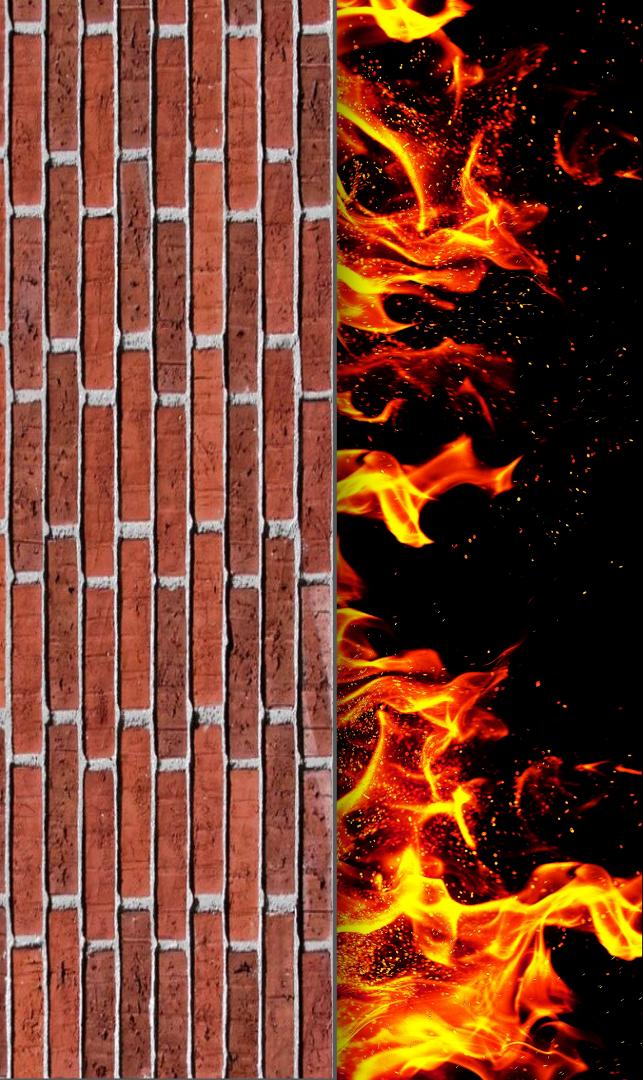


```
pfSense - Firewall [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Inter the WAN interface name or 'a' for auto-detection
em0 or a): em0
Inter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
[a or nothing if finished]:
The interfaces will be assigned as follows:
WAN -> em0
Do you want to proceed [y/n]? y
Hitting configuration...done.
In the moment while the settings are reloading... done!
Configuring loopback interface...lo0: link state changed to UP
Configuring wireless interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring WAN interface...em0: link state changed to DOWN
em0: link state changed to UP
```

- 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!

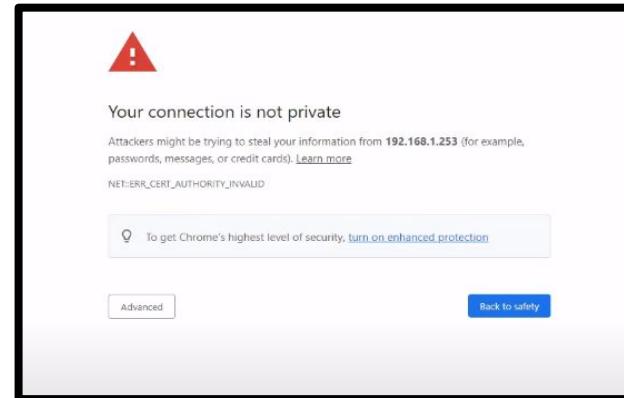
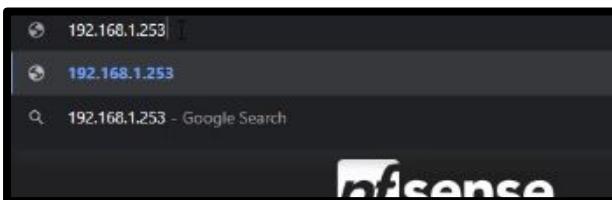




Configure pfSense Firewall in website

Configure pfSense Firewall website

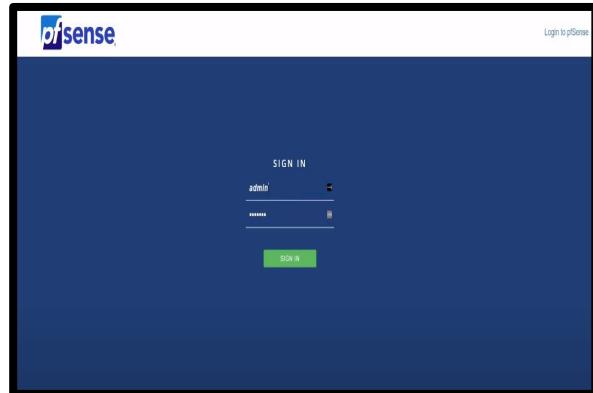
A screenshot of a terminal window titled "pfSense - Firewall [Running] - Oracle VM VirtualBox". The window shows the pfSense boot process starting CHOM... done. It then displays the pfSense 2.5.2-RELEASE amd64 build information. The configuration menu is shown, with option 1) Assign Interfaces highlighted by a red oval. The menu includes options for interfaces, webConfigurator, and various system functions like ping and shell. At the bottom, it says "Enter an option: " followed by a cursor.



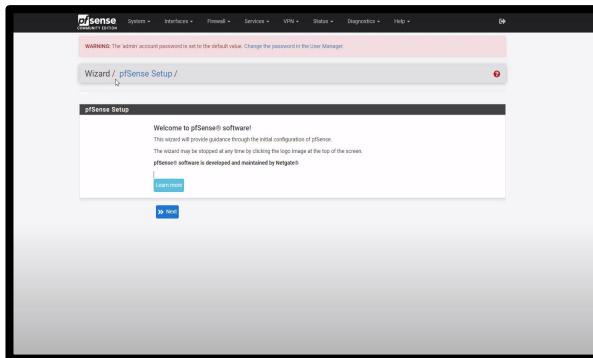
- In pfSense make note of its IP address and subnet mask.
Also, in your physical host's cmd tool, note the IP and default gateway addresses.
- Input the pfSense IP address in the url search bar
- You will reach this warning page due to untrusted certificates. To bypass this, select "Advanced".

Configure pfSense Firewall website

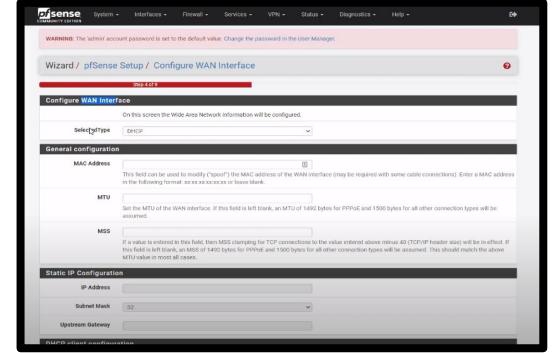
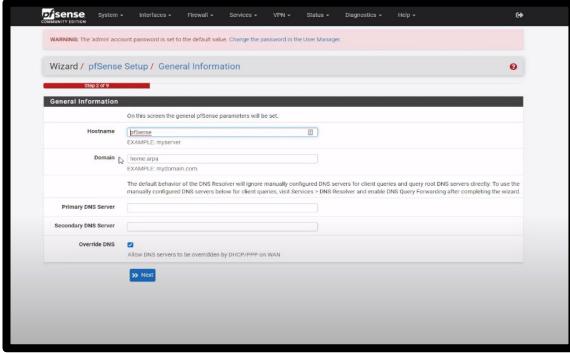
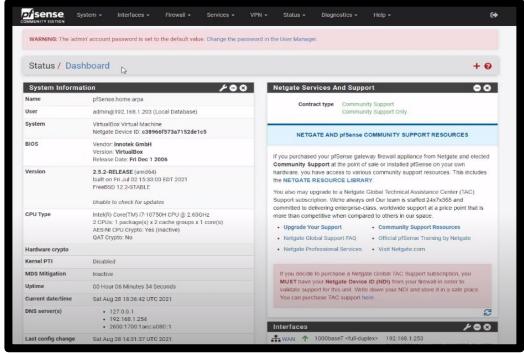
- Sign into pfSense with username “admin” and password “pfsense”



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



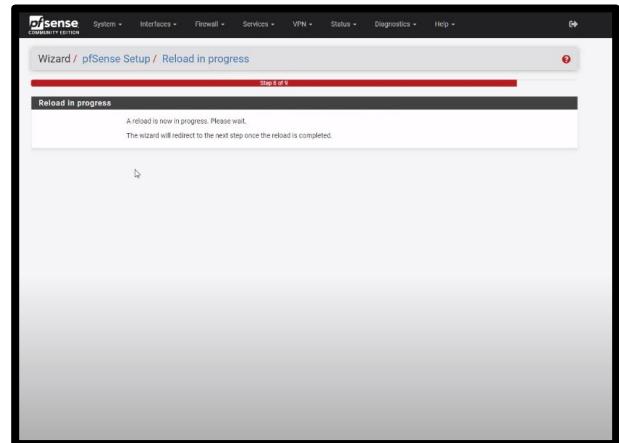
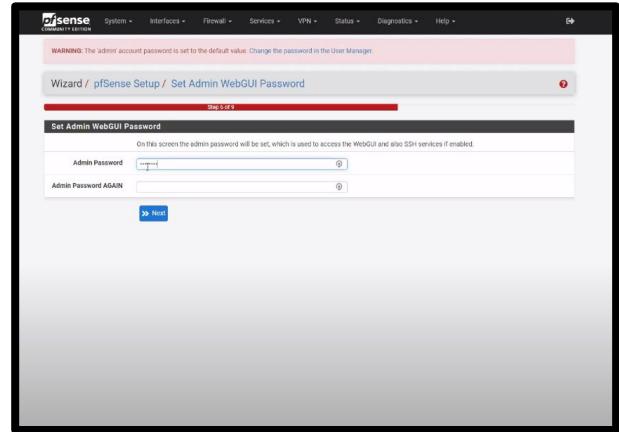
Configure pfSense Firewall website



- 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

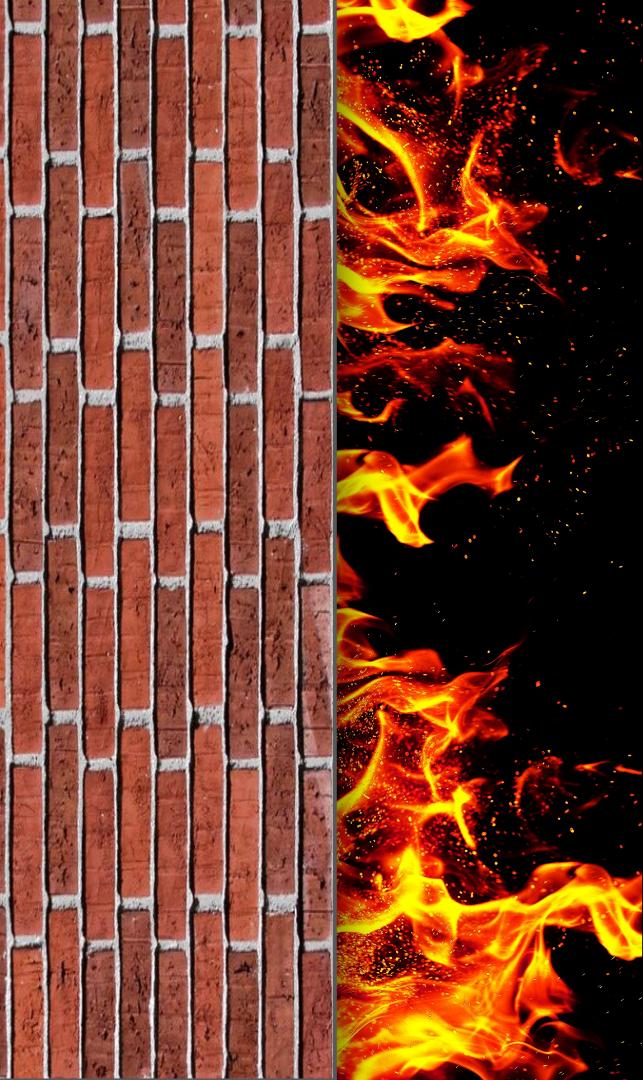


Success! Great Job!



A screenshot of the pfSense Setup Wizard completed screen. The page title is "Wizard / pfSense Setup / Wizard completed." and it indicates "Step 9 of 9". A banner at the top says "Wizard completed." Below it, a message says "Congratulations! pfSense is now configured." with a link to "Check for updates". A note encourages users to check for software updates. Another section, "User survey", asks for help in improving the software with a link to "Anonymous User Survey". A "Useful resources" section lists links to Netgate's website, store, forum, and newsletter. A "Finish" button is at the bottom.

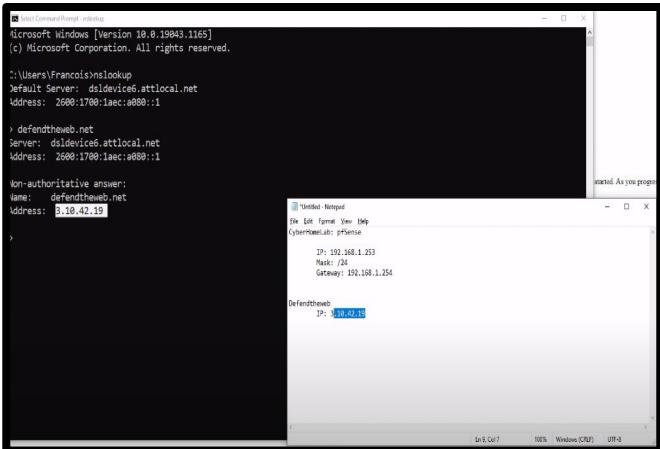
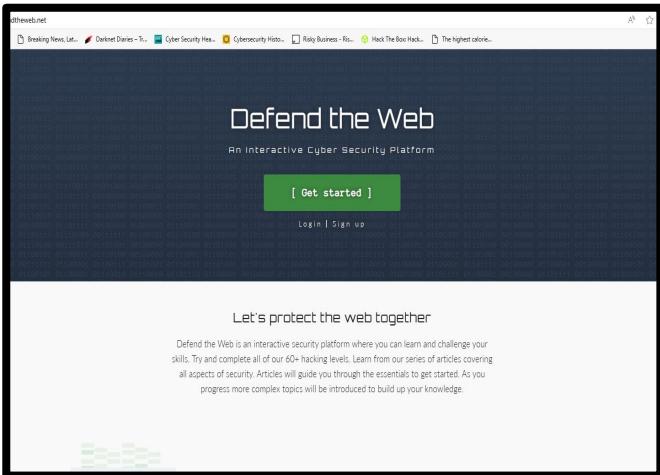
*Select “Finish”, then accept the copyright and trademark notices.



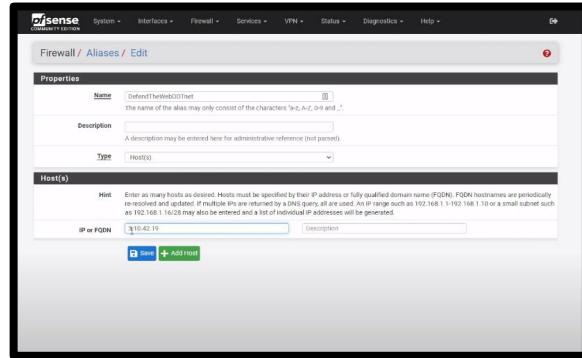
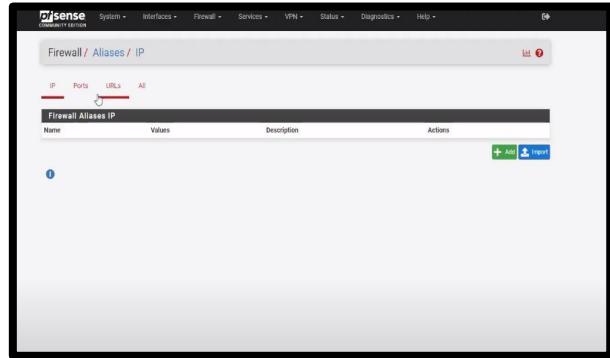
Create a Firewall Rule

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



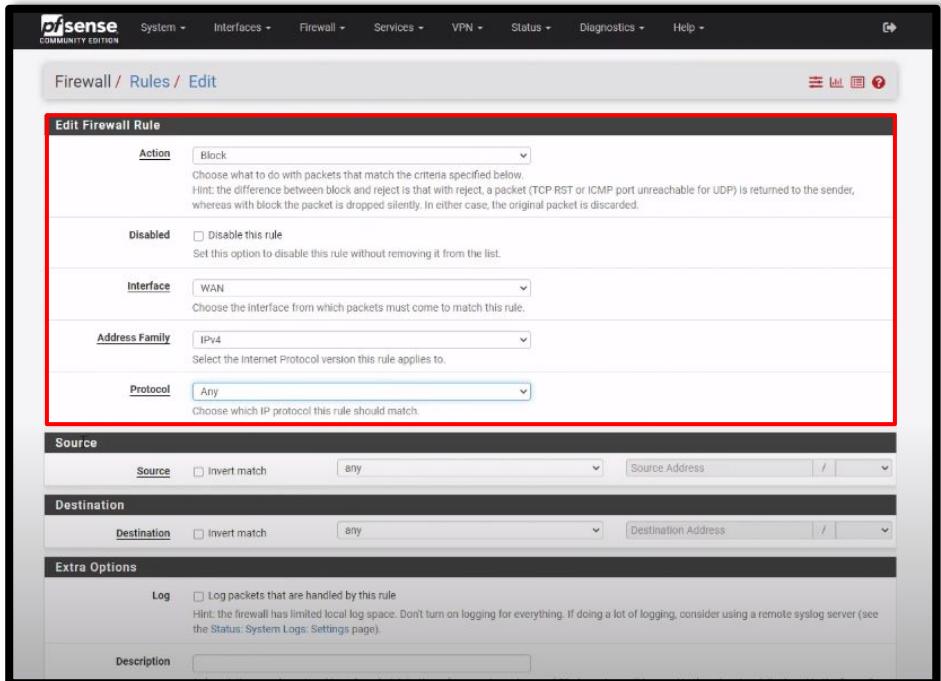
Create a Firewall Rule



- 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”.

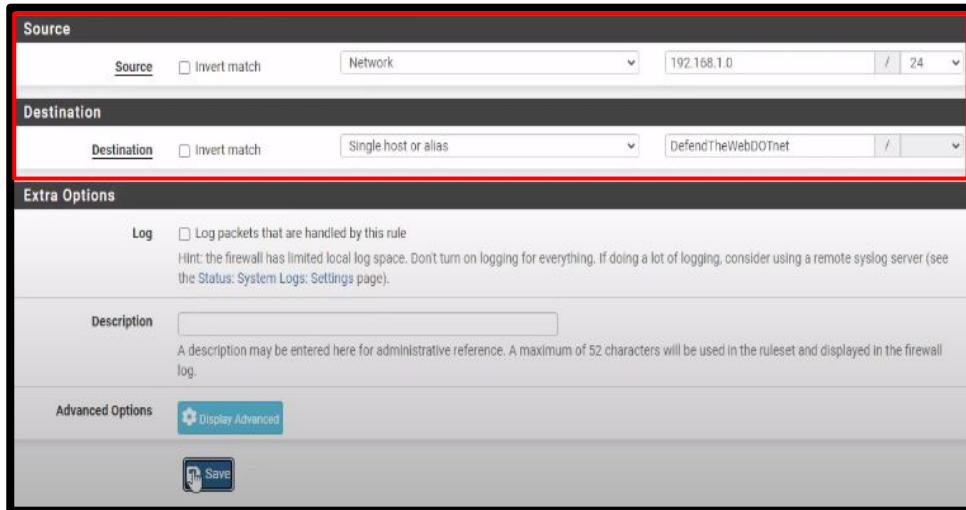
Create a Firewall Rule

- 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!



pfSense
COMMUNITY EDITION

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

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

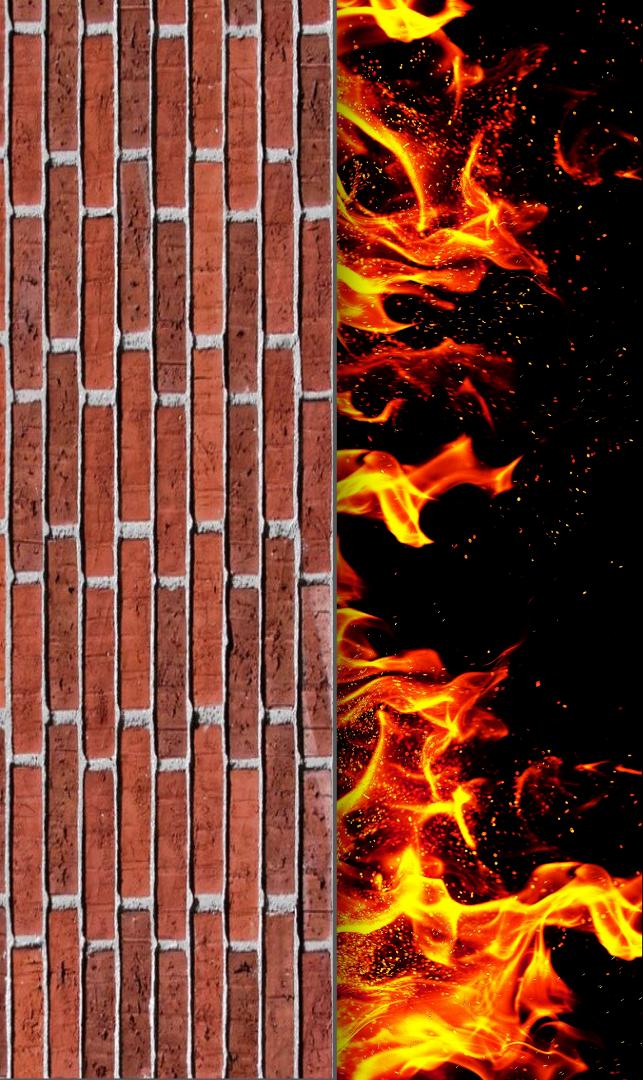
Floating WAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 / 502 KIB	*	*	*	WAN Address	443 80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	192.168.1.0/24	*	DefendTheWebDOTNet	*	*	none		

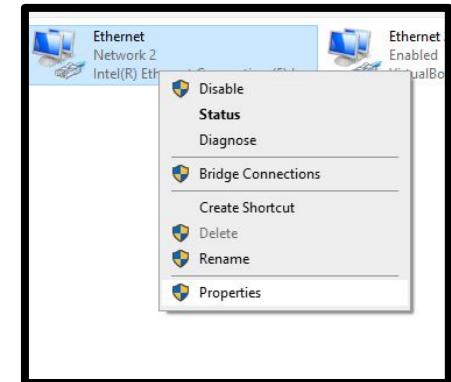
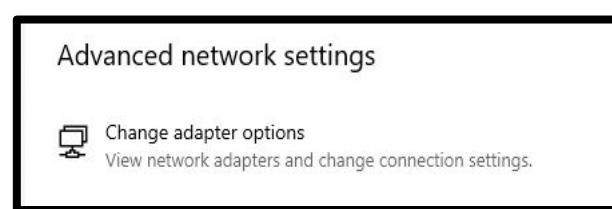
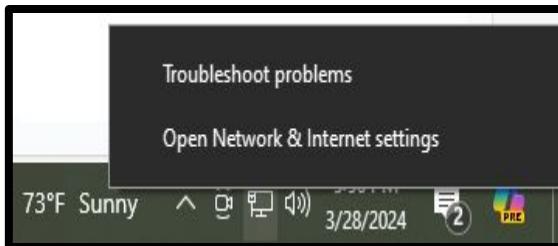
Add Down arrow Delete Save + Separator

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



Add Firewall to Physical Host's Network

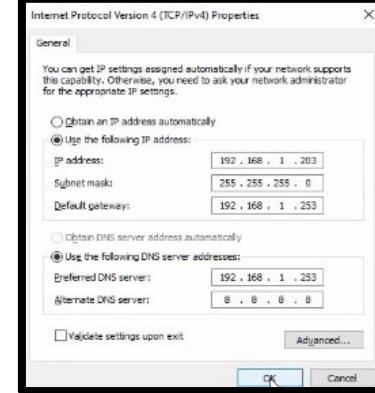
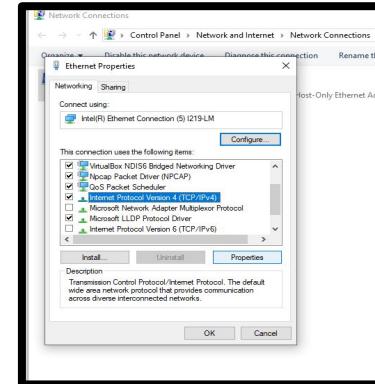
Add Firewall to Physical Host's Network



- 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

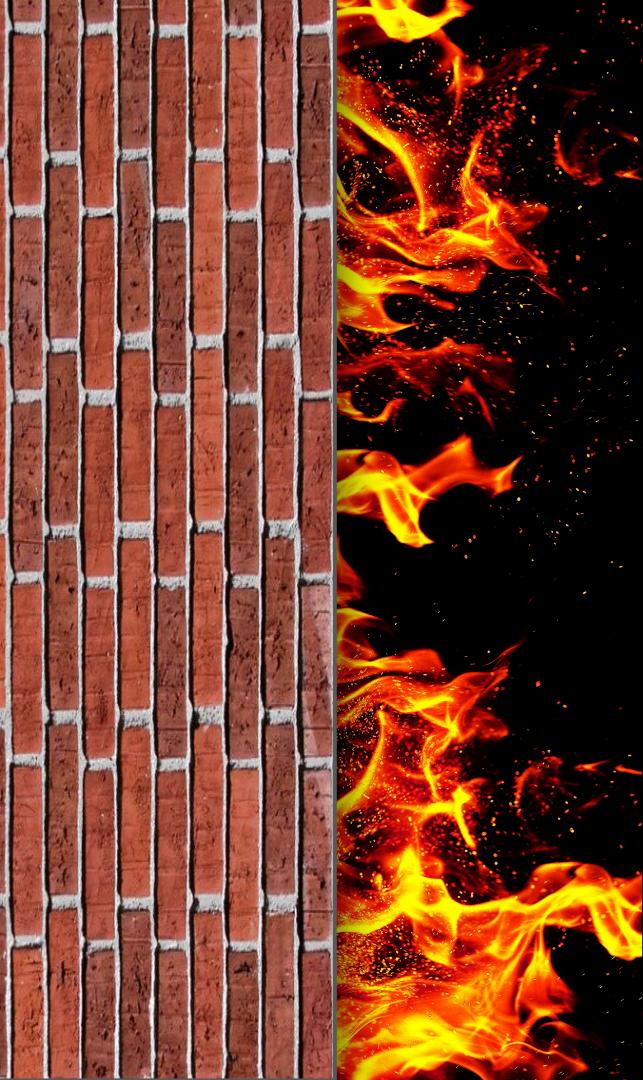
Add Firewall to Physical Host's Network

- 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!

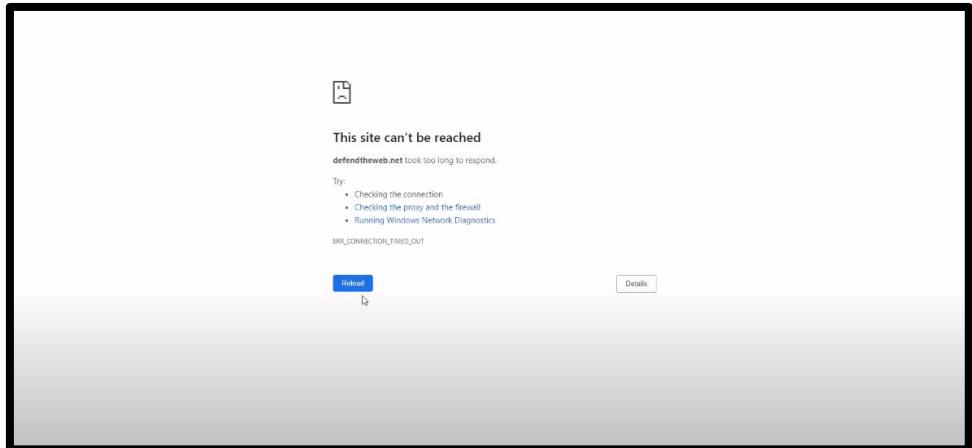




Test the Firewall

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!**

