

Deploying Dual Stack pfSense 2.4.1 in VirtualBox

Lawrence E. Hughes
25 October 2017

Note: the name pfSense is a registered trademark of Electric Sheep Fencing. All uses of it in this document are used to describe the installation and configuration of pfSense, which is covered by the fair use doctrine.

It may seem strange to deploy a firewall in VirtualBox but it makes it much easier to do screen captures of the install process (compared to deploying it on hardware) in order to document the deployment process. Also, VirtualBox has the ability to create complex virtual networks with multiple subnets connected by routers or firewalls. So there is actually a use for a virtual firewall.

Deploying on a machine with keyboard and monitor is not much different from installing on VirtualBox, so you can use these instructions to guide you through that. You will need at least two NICs. It can be a bit more of a challenge to deploy pfSense on a headless “network appliance” box, but even here there may be a way to connect a monitor and keyboard during the install process, then remove it once installed (all remaining configuration is done via network using the nice web admin interface).

If there is no monitor or keyboard possible, you can still write the boot image to a hard drive on another computer, then install the drive and boot.

The install medium can be a CDROM if an optical reader (possible USB connected external drive) is available during the install, but it is possible to create a boot image on a thumbdrive (so long as the target box has a spare USB interface). There is plenty of information online to help with all of these variations. In this documentation, we are going to mount an ISO file on a virtual optical drive and install to a virtual HDD. We can configure two or more virtual NICs as needed.

There are several well designed and affordable “network appliance” boxes available in which to deploy pfSense . A good example can be found at:

https://www.amazon.com/gp/product/B01AJEJG1A/ref=oh_aui_detailpage_o00_s00?ie=UTF8&psc=1

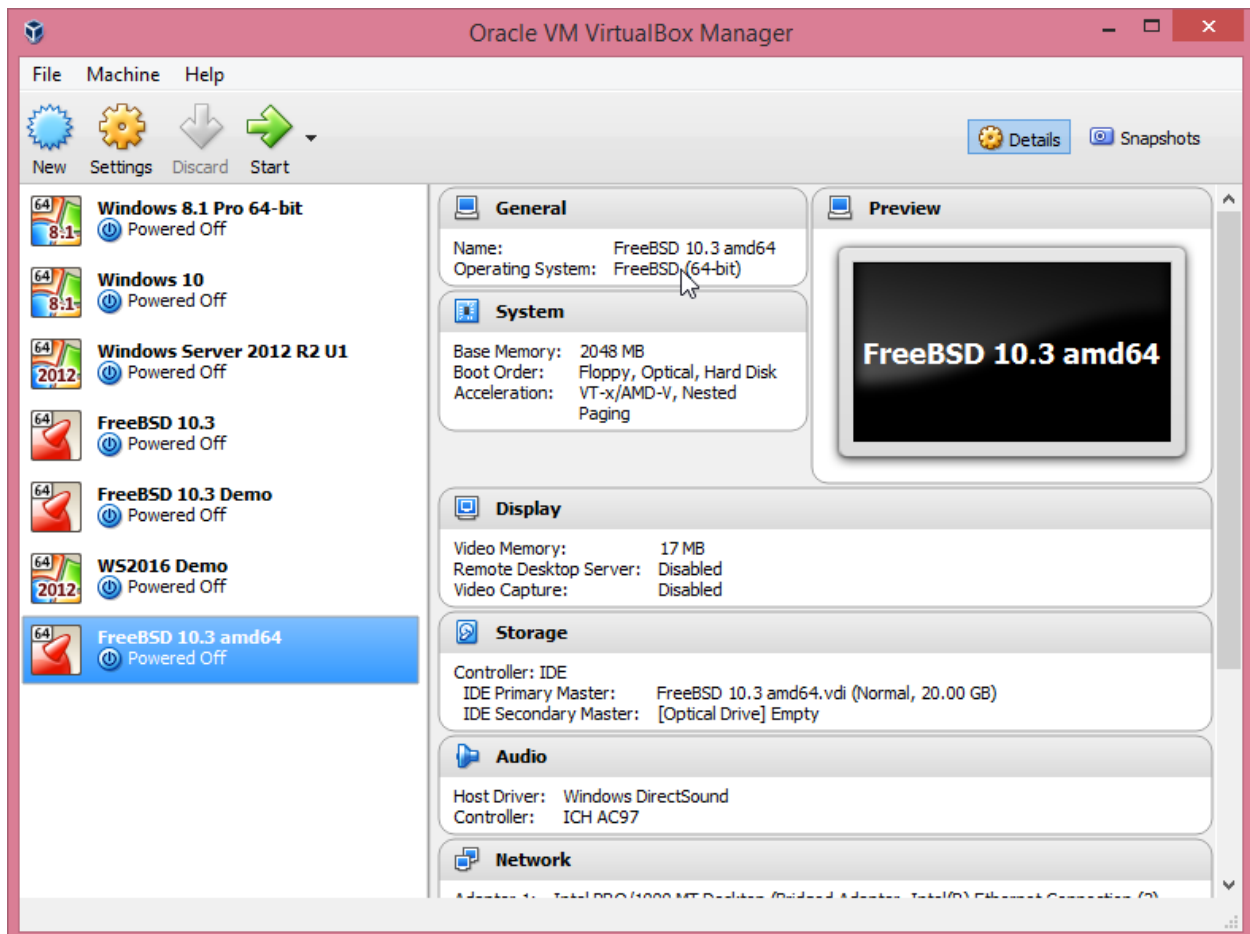
This box has a quad core Celeron J1900 “Bay Trail” CPU running at 2 GHz, 4 GB of DDR3L RAM, 8GB of SSD storage, and four gigabit Intel NICs (Intel NICs are highly recommended for firewalls). The cost is USD 269 (not counting shipping), and Amazon will ship this internationally.

Note: the original licensing of pfSense allowed you to use it for non-commercial or commercial purposes, including installing it on hardware such as this, and selling it as a firewall product. This is no longer allowed. Be careful to observe the new licensing restrictions. You can deploy pfSense for your own use in your own network. Beyond that, consult the Electric Sheep Fencing.



Meanwhile, back to VirtualBox. We will configure two virtual NICs, one for the WAN side, and one for the LAN side. pfSense can support multiple LANs or even multiple WANs, if you want to deploy more complex networks.

Bring up VirtualBox and click on the *New* icon (blue starwheel):



Choose an appropriate name for your VM. The OS type is BSD, 64 bit. 1 GB of RAM is ample.

Create Virtual Machine

Name and operating system

Name: pfSense amd64

Type: BSD

Version: FreeBSD (64-bit)

Memory size

4 MB 1024 MB 32768 MB

Hard disk

Do not add a virtual hard disk

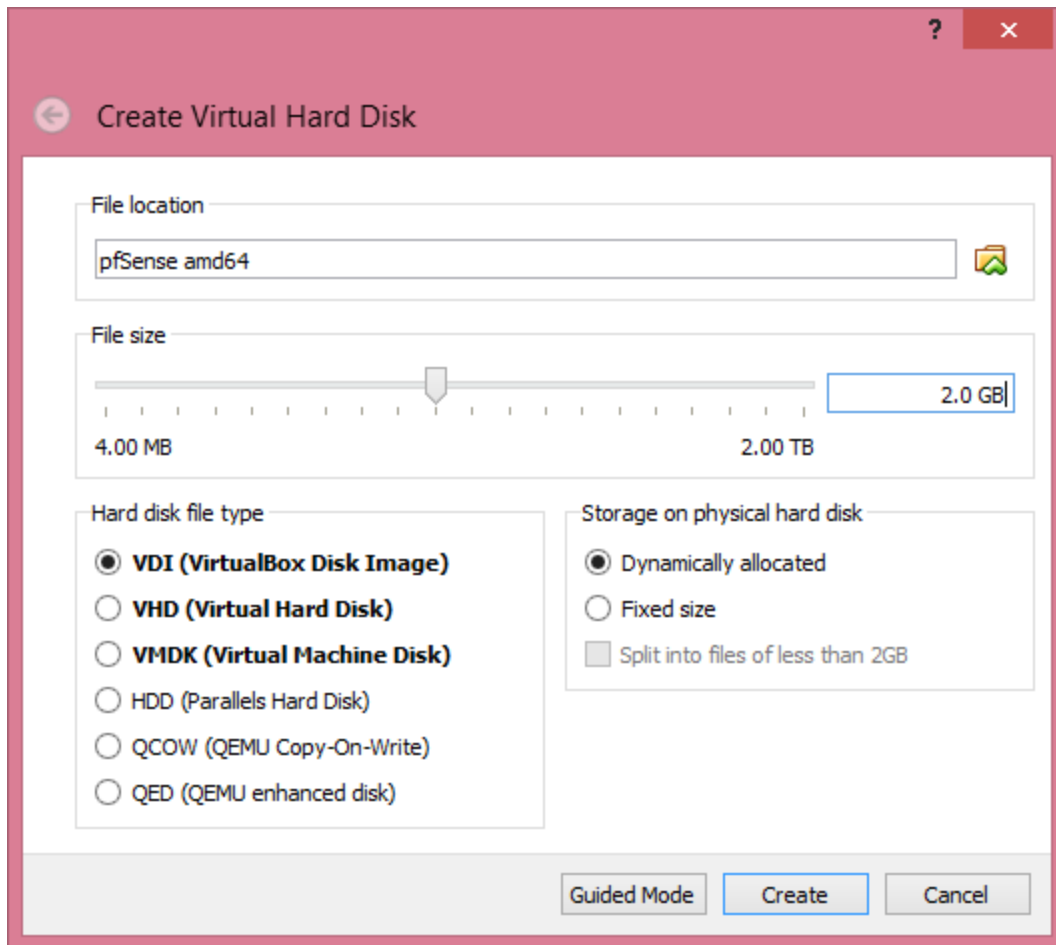
Create a virtual hard disk now

Use an existing virtual hard disk file

Windows Server 2012 R2 U1.vdi (Normal, 60.00 GB)

Guided Mode Create Cancel

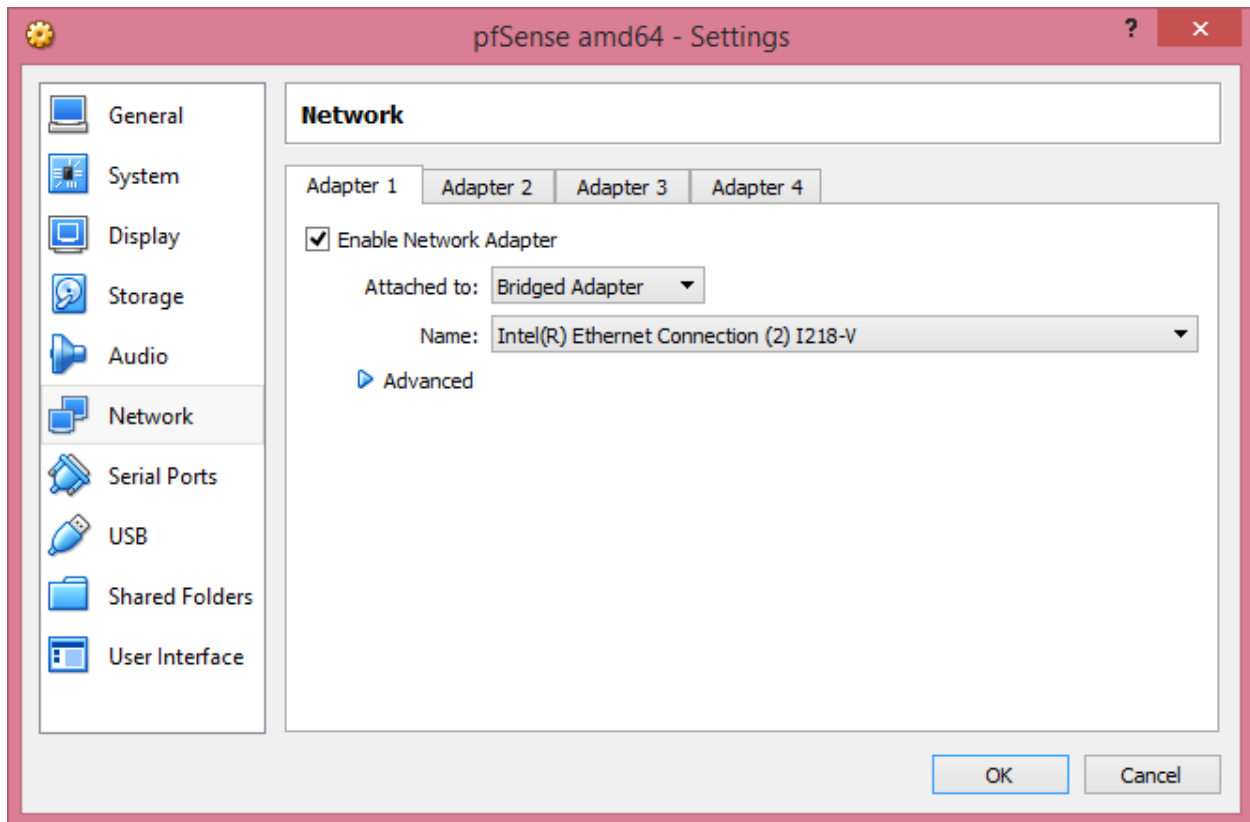
Click *Create*.



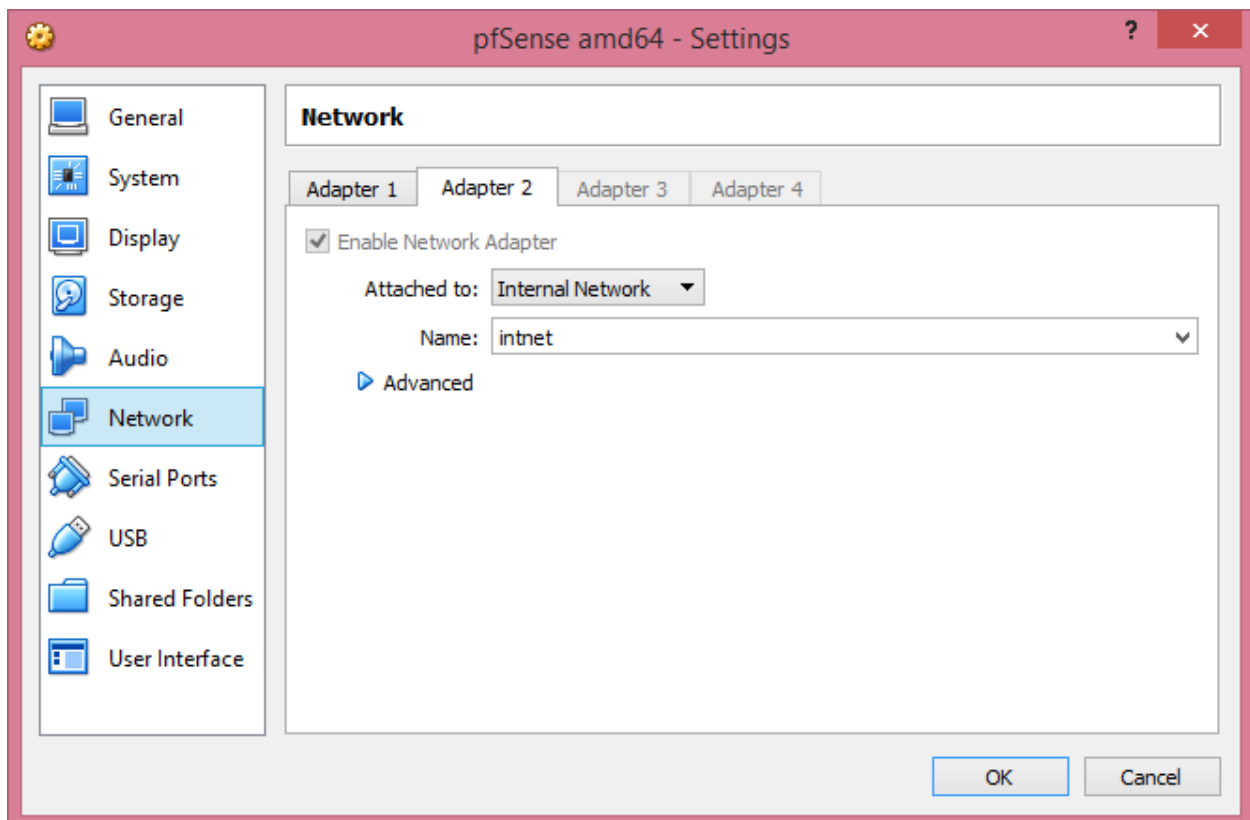
2.0 GB of disk is sufficient for this. If you are deploying a hardware firewall and plan to do significant logging you might want to use a larger HDD.

Click *Create*.

Now select the new VM and click the *Settings* icon (yellow gear wheel). Select *Network*.



Configure the first NIC (em0). Put it in Bridged mode.



Repeat for a second NIC (em1). You will need to enable this adapter. Connect it to the Internal Network, using the default name *intnet*.

You could create even more virtual NICs if you liked. We will work with two for now.

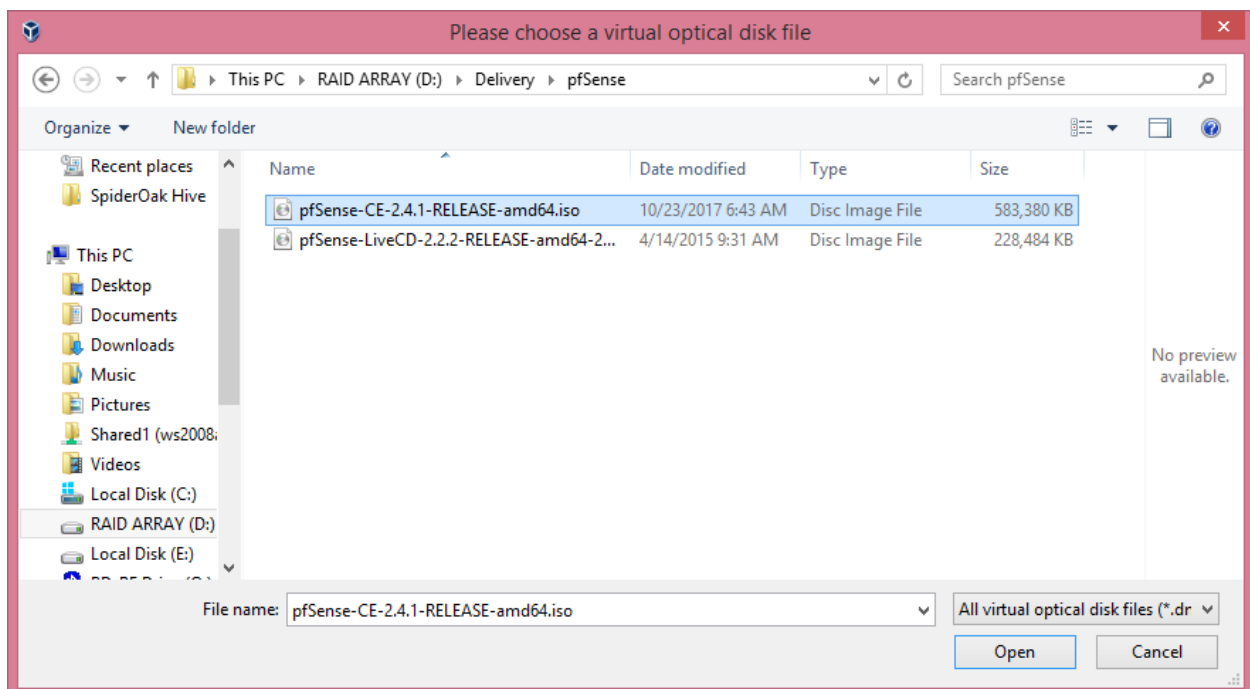
Now select *Storage*.

The virtual HDD is already there and mounted on a virtual IDE interface.

The virtual optical drive is currently empty.

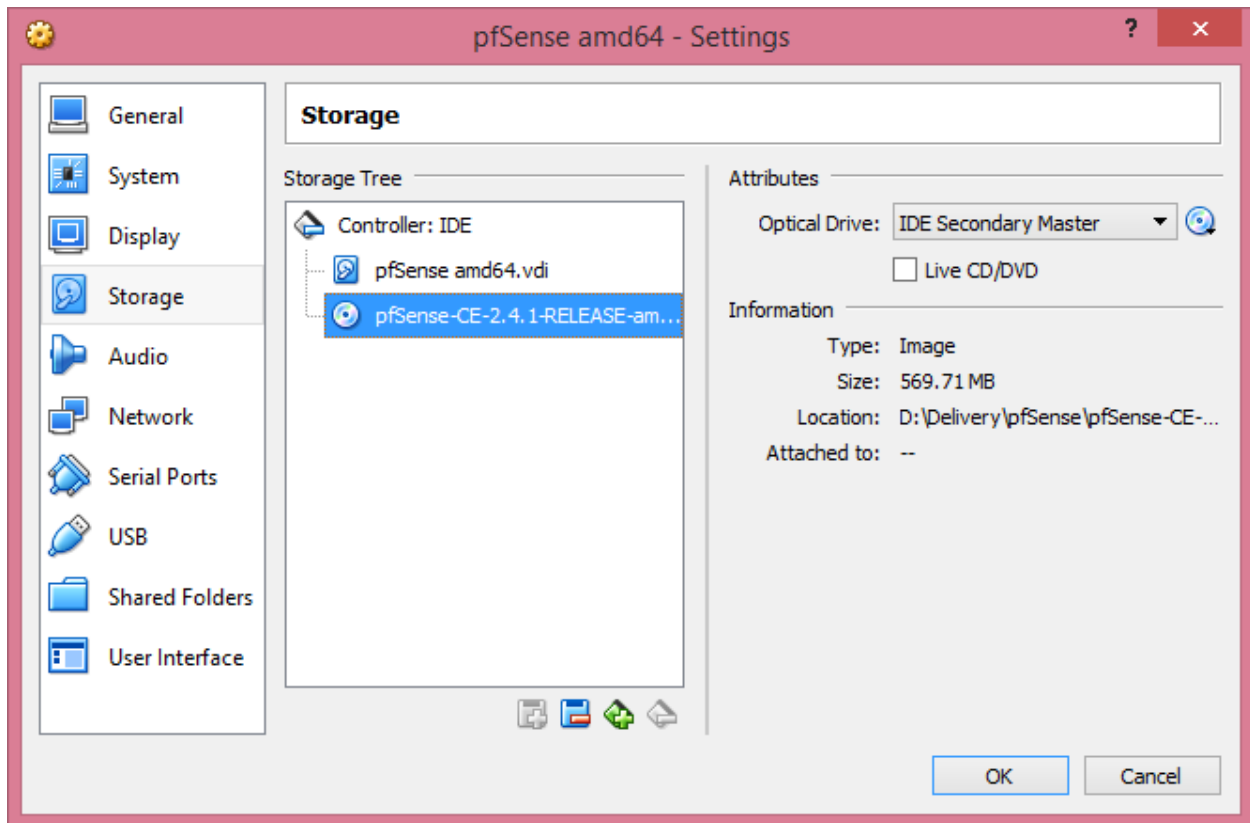
Mount the ISO image you downloaded before:

- Click on the Optical disk icon (by “Empty”)
- On the right panel, it will show the IDE Secondary Master. Click on the optical disk icon by that.
- Select *Choose Virtual Optical Disk File*
- Find the ISO image file and select it.



- Click *Open*

It will now show the ISO image “mounted” on the virtual optical drive:



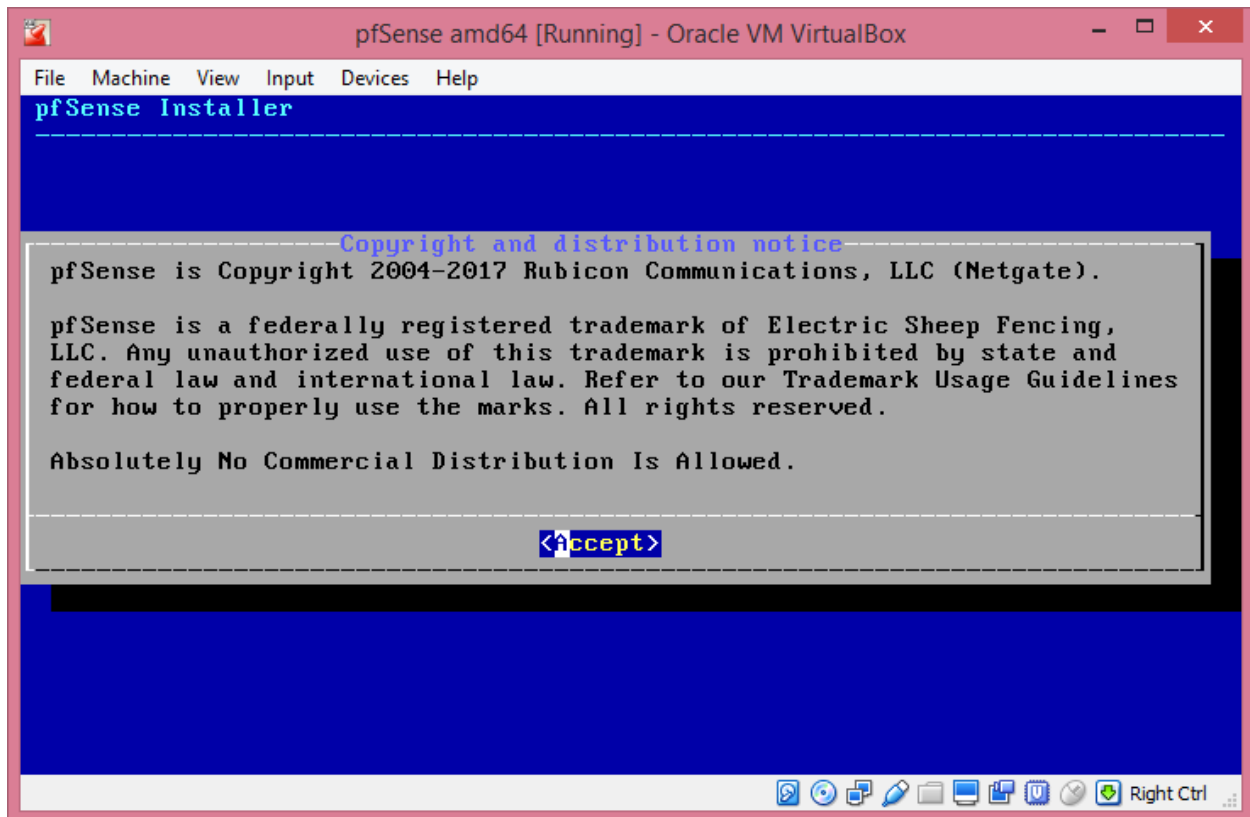
We are now ready to begin the install from the ISO image.

Dismiss the Settings dialog (OK).

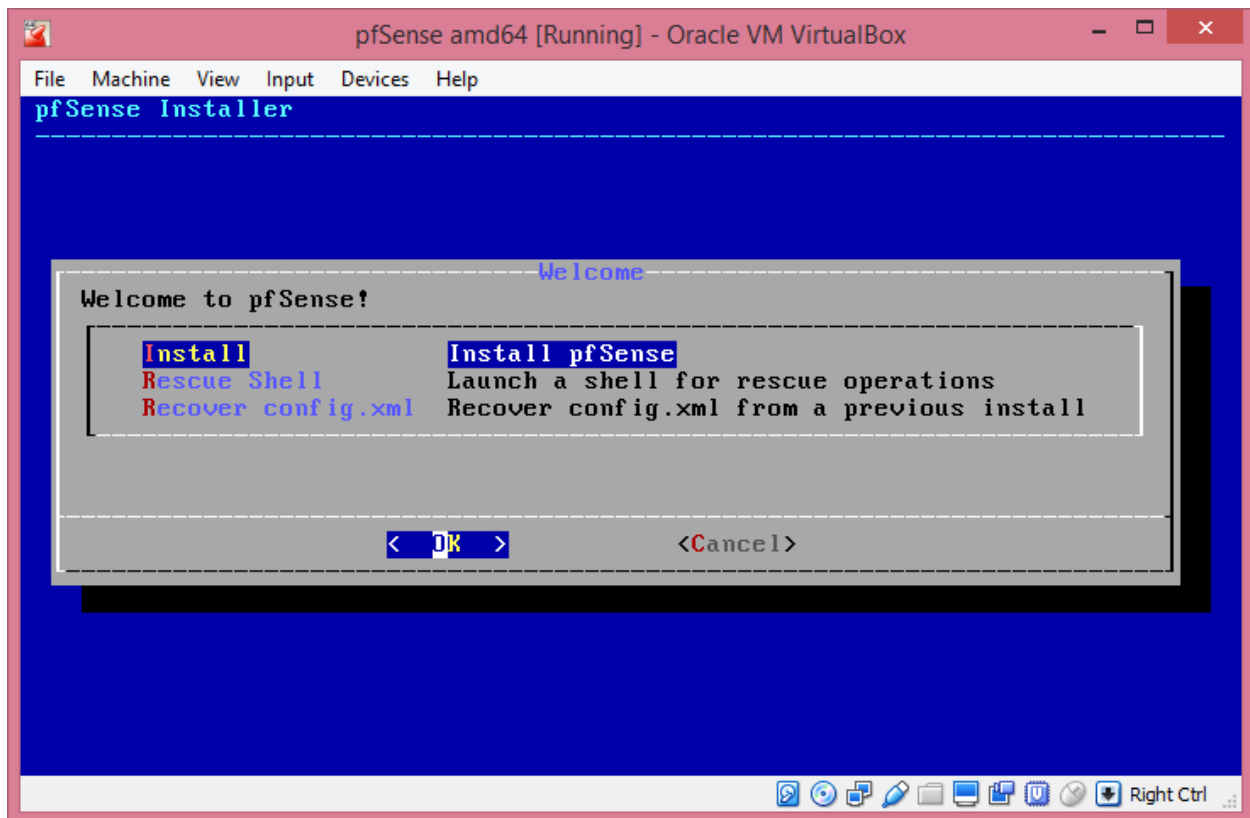
Start the virtual machine by double clicking on the item in the left column of VirtualBox's main window.

A number of lines will fly by on the virtual display while it is loading files and probing the “hardware”.

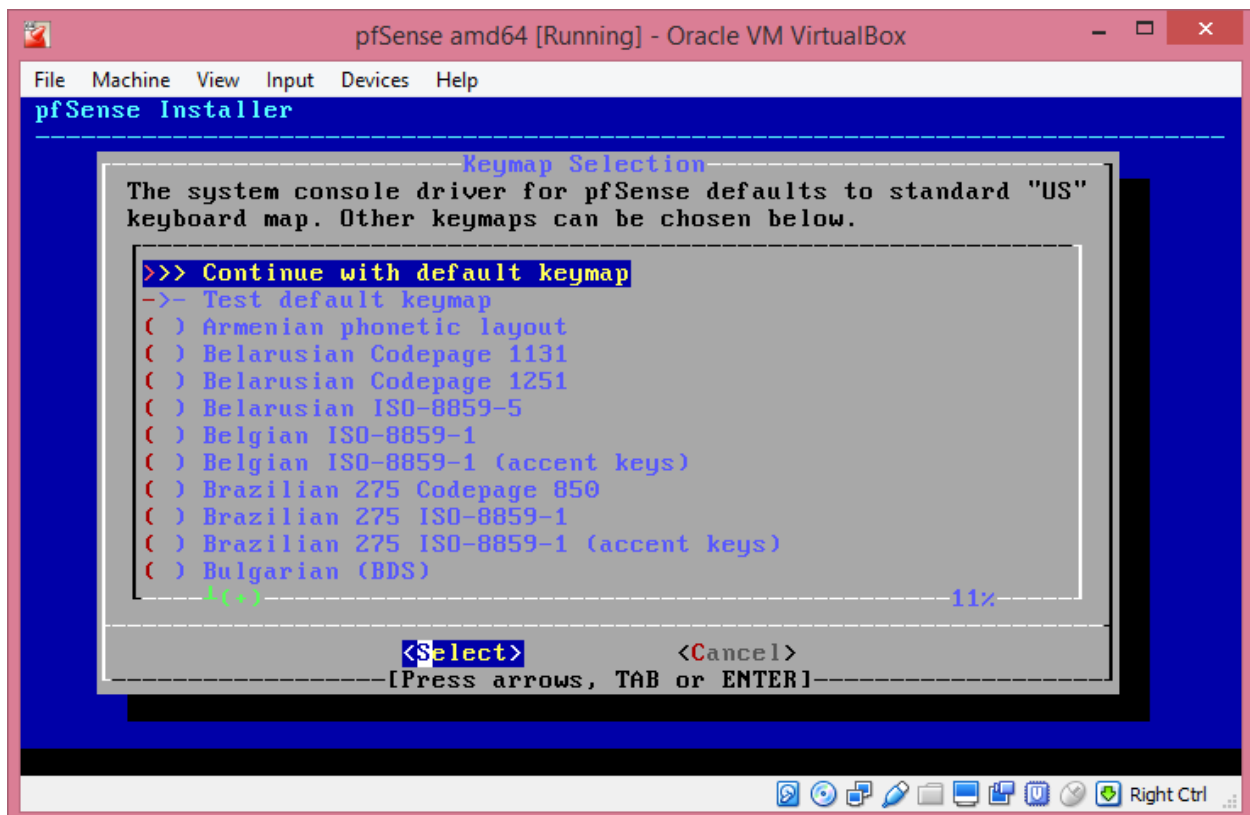
It will finally settle down on the first screen of the *pfSense Installer* wizard.



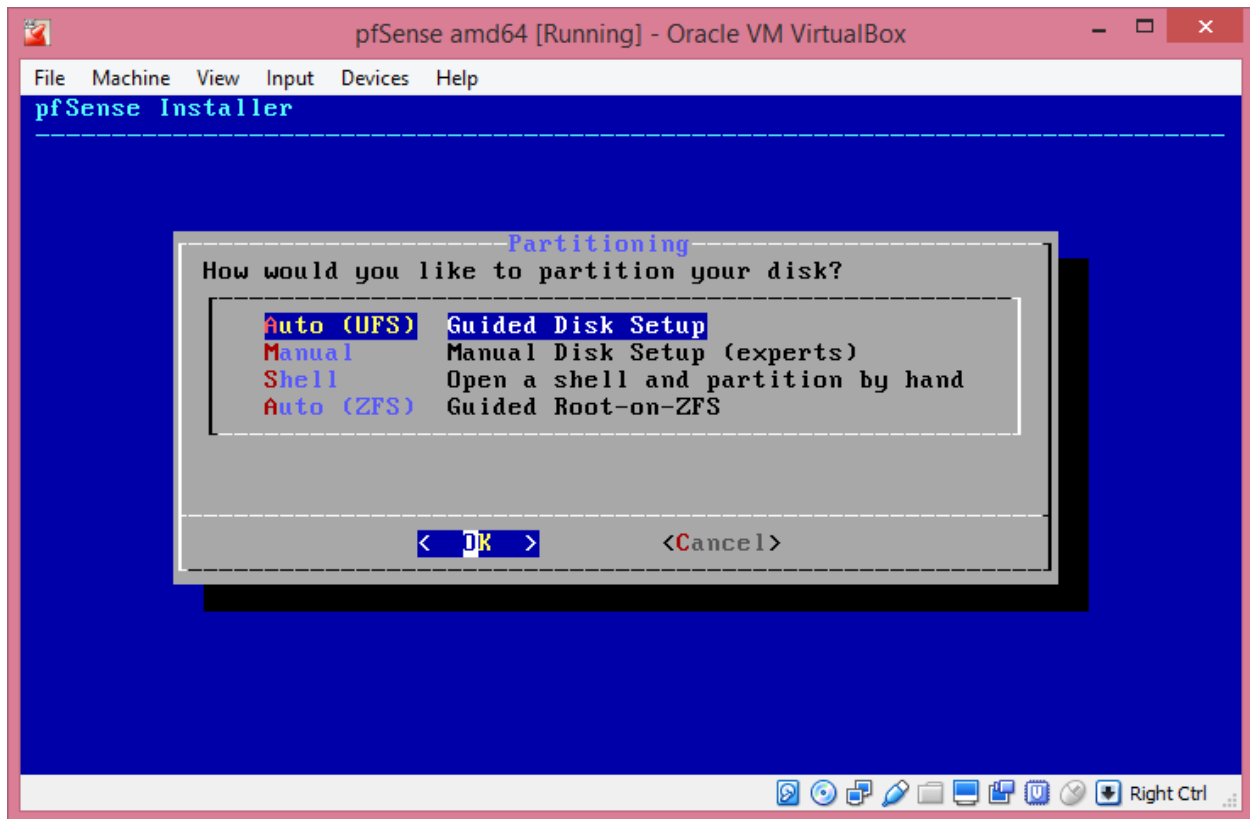
Read the dire warnings about Netgate's trademark and click *Accept* by typing *Enter*.



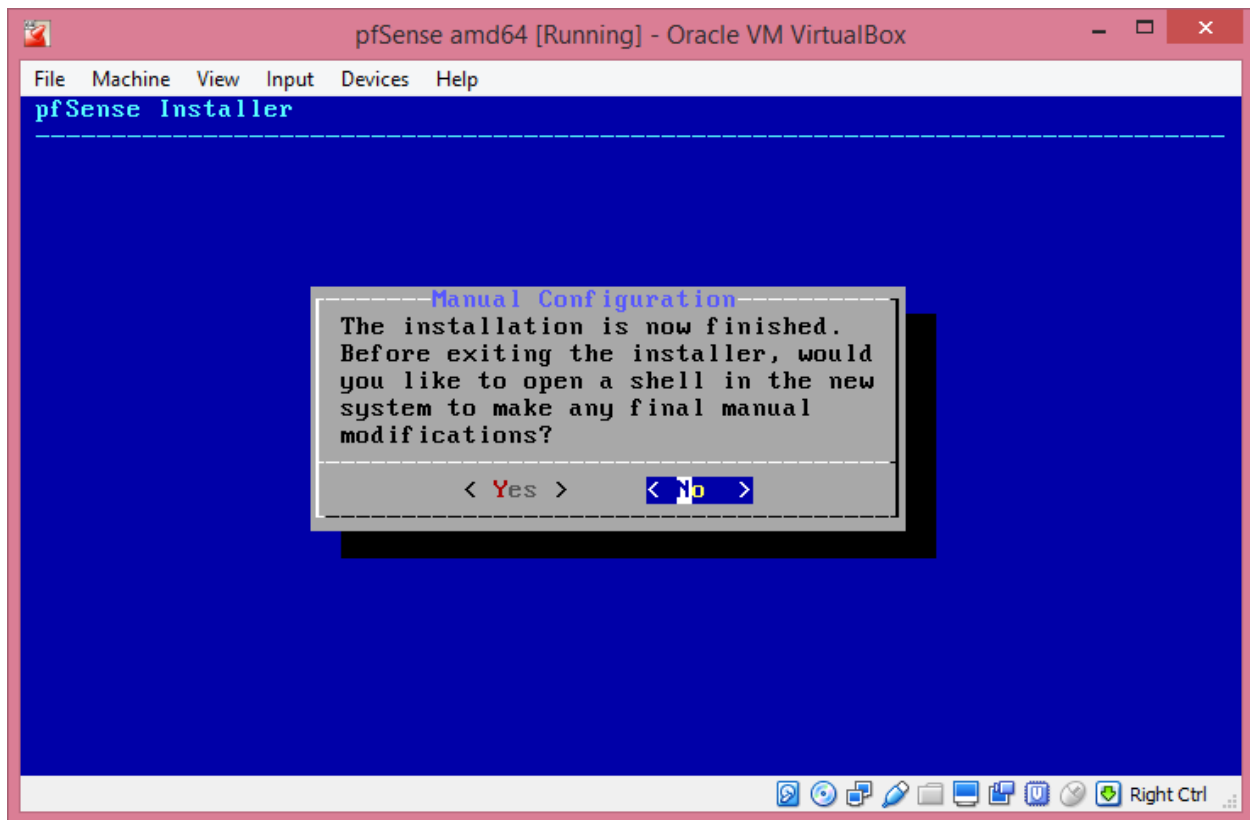
On the Welcome screen, select *Install* by typing *Enter*.



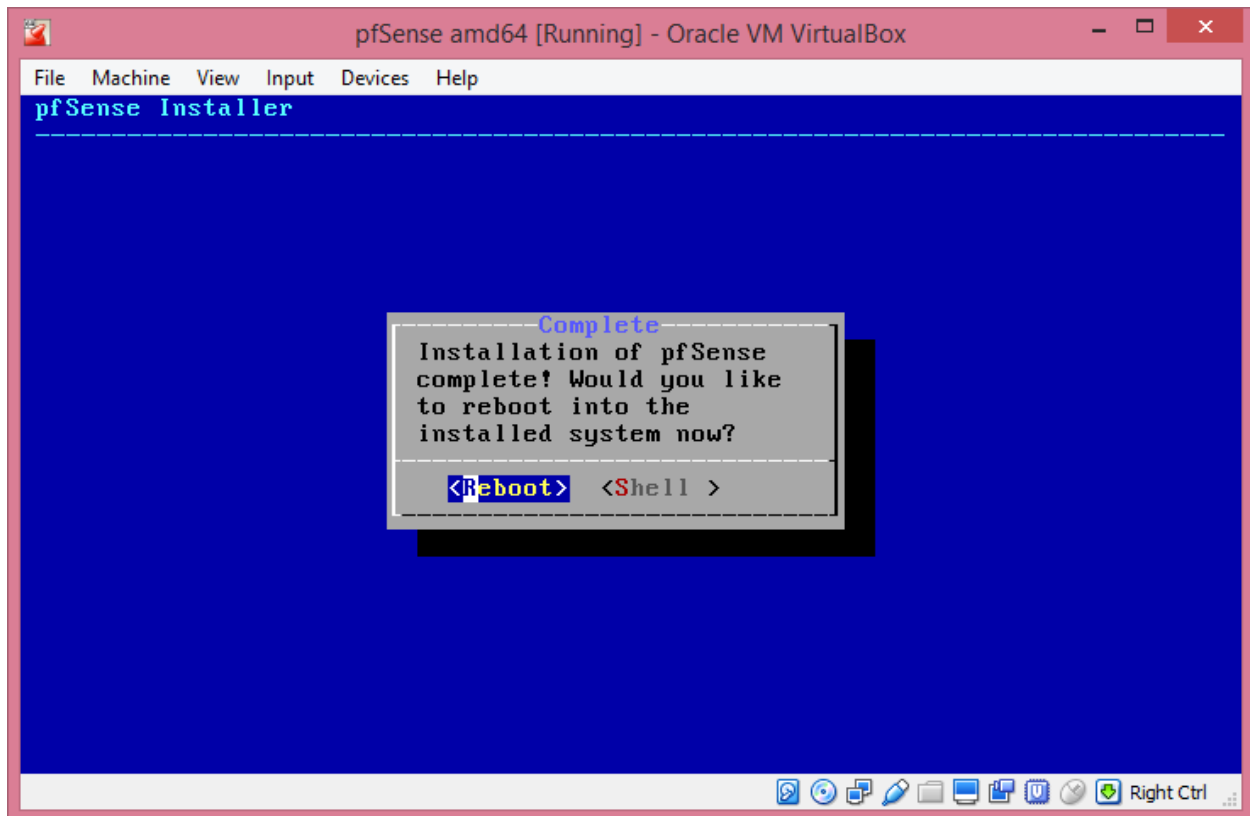
Keymap Selection: Continue with the default keymap by typing *Enter*.



Partitioning – do Guided Disk Setup by typing *Enter*. The disk partitioning will take place quickly, then the files will be copied into the partitions.



There is no need for manual configuration, so select *No* by typing *Enter*.

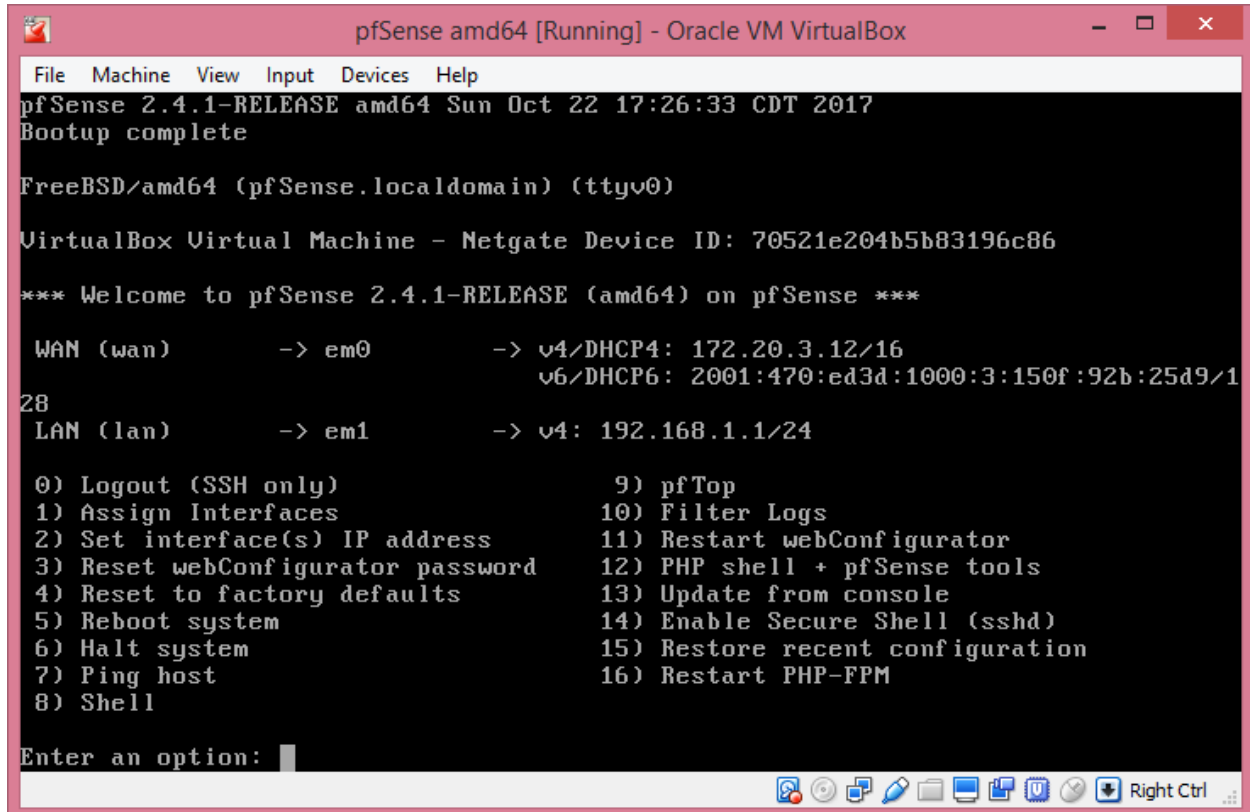


You can now reboot by typing *Enter*. Remove the ISO image from the virtual optical drive:

Devices / Optical Drive / Remove disk from virtual drive

If you are too slow and it boots from the ISO again, just reboot the machine (Machine / Reset) after the ISO image is removed.

It will go through some boot up procedures, probing the “hardware”, etc.



```
File Machine View Input Devices Help
pfSense 2.4.1-RELEASE amd64 Sun Oct 22 17:26:33 CDT 2017
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 70521e204b5b83196c86

*** Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.20.3.12/16
                v6/DHCP6: 2001:470:ed3d:1000:3:150f:92b:25d9/128
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

You now need to configure a few things. In my case, the WAN interface (em0) is bridged to my LAN, which has both native IPv4 and IPv6 on it, including DHCPv4 and DHCPv6. pfSense will configure IPv4 and IPv6 addresses using whatever is available (in this case DHCPv4 and DHCPv6).

There is no need to assign interfaces – it chose em0 as WAN and em1 as LAN.

You can set the IP addresses of the two interfaces if you like, but these are fine.

The web interface is now up and running.

To continue configuration, you will need another VM connected to the Internal Network *intnet*. I am using a Windows 8.1 VM. The network configuration is using DHCPv4 (from the new firewall).

Verify that it has configured its network from the DHCPv4 on your pfSense. Verify that you can ping 192.168.1.1 from your second VM.

Bring up a browser on the second VM and connect to <http://192.168.1.1>. You will first get a “untrusted server” error – let it connect anyway.

A screenshot of a web browser window displaying a security warning. The address bar shows the URL `https://192.168.1.1/`. The page content includes a red shield icon with a white 'X' and the following text:

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- [Click here to close this webpage.](#)
- [Continue to this website \(not recommended\).](#)
- [More information](#)

You should see the entry page:

A screenshot of the pfSense login page. The browser address bar shows `https://192.168.1.1/`. The page features the pfSense logo in the top left and a "Login to pfSense" link in the top right. The main content area has a dark blue background with the text "SIGN IN" centered. Below this, there are two input fields: the first is empty, and the second is labeled "Password". A green "SIGN IN" button is positioned below the password field. At the bottom of the page, a footer contains the text: "pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]"

Login with username *admin* and password *pfSense*.

You should now see the main page of pfSense:

The screenshot displays the pfSense dashboard interface. At the top, there is a navigation menu with options: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Status / Dashboard" and is divided into two columns.

System Information

Name	pfSense.localdomain
System	VirtualBox Virtual Machine Netgate Device ID: 70521e204b5b83196c86
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.4.1-RELEASE (amd64) built on Sun Oct 22 17:26:33 CDT 2017 FreeBSD 11.1-RELEASE-p2 The system is on the latest version. Version information updated at Wed Oct 25 13:15:19 UTC 2017
CPU Type	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz AES-NI CPU Crypto: Yes (inactive)
Uptime	00 Hour 30 Minutes 54 Seconds
Current date/time	Wed Oct 25 13:45:37 UTC 2017
DNS server(s)	• 127.0.0.1 • 172.20.0.11 • 172.20.0.12 • 2001:470:ed3d:1000::12 • 2001:470:ed3d:1000::11
Last config change	Wed Oct 25 21:06:23 UTC 2017
State table size	0% (30/97000) Show states
MBUF Usage	2% (1520/61006)
Load average	0.42, 0.61, 0.56
CPU usage	5%
Memory usage	14% of 979 MiB

Netgate Services And Support

Contract type: **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale, you can [register](#) your community support subscription for access to pfSense Gold.

- [Register Your Support Subscription](#)
- [Upgrade Your Support](#)
- [Netgate Global Support FAQ](#)
- [Netgate Professional Services](#)
- [Log into your portal account](#)
- [Community Support Resources](#)
- [Official pfSense Training by Netgate](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can [purchase support here](#).

Interfaces

WAN	↑ 1000baseT <full-duplex>	172.20.3.12 2001:470:ed3d:1000:3:3019:fa16:7203
LAN	↑ 1000baseT <full-duplex>	192.168.1.1

