

# Homelab for Security Detection & Monitoring

This is a homelab created following Day CyberWox's blueprint and documentation, available on his [website](#). It's been changed slightly to use the more recent, up-to-date software versions and technologies. The lab was created using VMWare Workstation Pro 17; you don't need to buy a licence upfront since VMWare offers a 30-day [free trial](#), which is what I will be using.

## Contents:

[Configuring pfsense as a firewall](#)

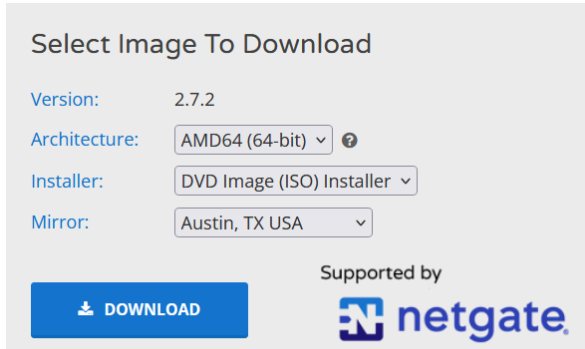
[Configuring Security Onion](#)

[Troubleshooting](#)

# Configuring pfsense as a firewall:

To create the pfsense firewall, we first need to download the ISO file, available on their [website](#).

For 64-bit machines, the following should be selected before downloading (select the nearest location to you from the 'Mirror' dropdown):



Select Image To Download


Version: 2.7.2


Architecture: AMD64 (64-bit) ?

Installer: DVD Image (ISO) Installer

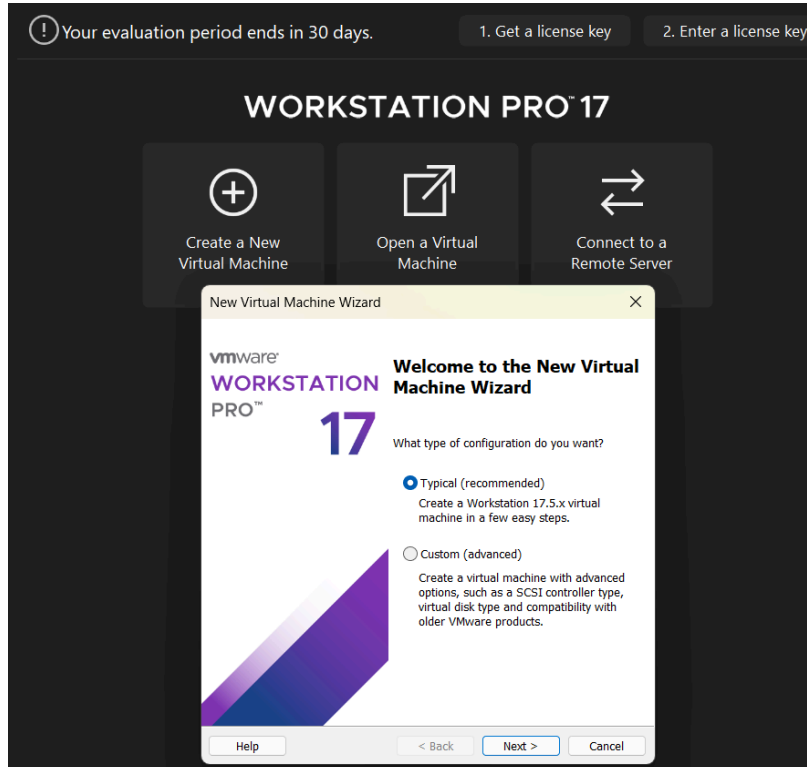
Mirror: Austin, TX USA

Supported by

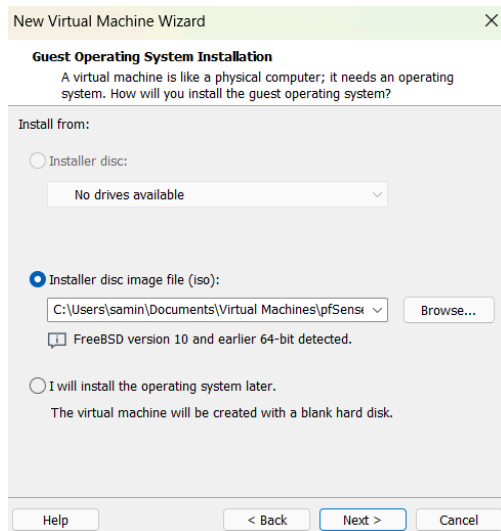
 netgate

 DOWNLOAD

Make sure to extract the downloaded file and then open up VMWare and click “Create a New Virtual Machine” - ensure the “Typical” is selected before clicking “Next”:

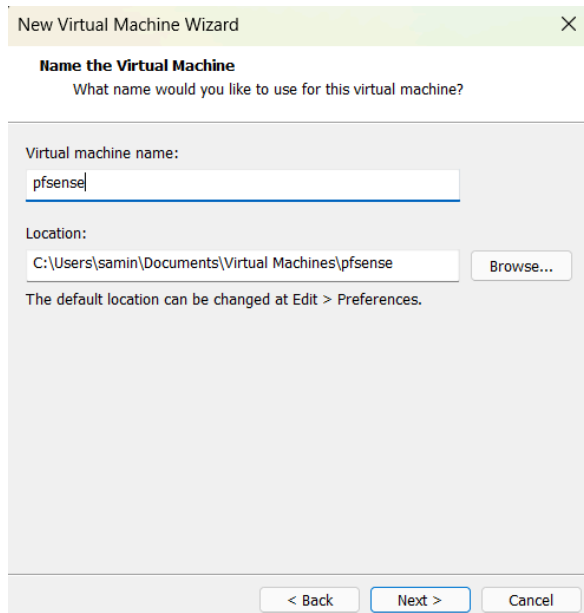


Select the ISO file by clicking “Browse” and browsing to where the file is located before clicking “Next”:



The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Guest Operating System Installation' step. The window title is 'New Virtual Machine Wizard' with a close button. Below the title bar, the section is titled 'Guest Operating System Installation' with a subtitle: 'A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?'. The main area is labeled 'Install from:' and contains three radio button options. The first option is 'Installer disc:' with a dropdown menu showing 'No drives available'. The second option is 'Installer disc image file (iso):', which is selected. It has a dropdown menu showing 'C:\Users\samin\Documents\Virtual Machines\pfSense' and a 'Browse...' button. Below this, a checkbox is checked with the text 'FreeBSD version 10 and earlier 64-bit detected.'. The third option is 'I will install the operating system later.' with a subtitle 'The virtual machine will be created with a blank hard disk.'. At the bottom, there are four buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

Give your virtual machine a name and a location before clicking next:



The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Name the Virtual Machine' step. The window title is 'New Virtual Machine Wizard' with a close button. Below the title bar, the section is titled 'Name the Virtual Machine' with a subtitle: 'What name would you like to use for this virtual machine?'. The main area has two input fields. The first is 'Virtual machine name:' with a text box containing 'pfsense'. The second is 'Location:' with a text box containing 'C:\Users\samin\Documents\Virtual Machines\pfsense' and a 'Browse...' button. Below these fields, a note states: 'The default location can be changed at Edit > Preferences.'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Keep the preselected options and click “Next”:

New Virtual Machine Wizard

×

**Specify Disk Capacity**  
How large do you want this disk to be?

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

Maximum disk size (GB):

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

☐ Store virtual disk as a single file

☒ Split virtual disk into multiple files

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

Help

< Back

Next >

Cancel

On the next screen, click “Customize Hardware” and give it around 2GB RAM.

New Virtual Machine Wizard

×

**Ready to Create Virtual Machine**  
Click Finish to create the virtual machine and start installing FreeBSD version 10 and earlier 64-bit.

The virtual machine will be created with the following settings:

Name:	pfsense
Location:	C:\Users\samin\Documents\Virtual Machines\pfsense
Version:	Workstation 17.5.x
Operating System:	FreeBSD version 10 and earlier 64-bit
Hard Disk:	20 GB, Split
Memory:	256 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Sound Card

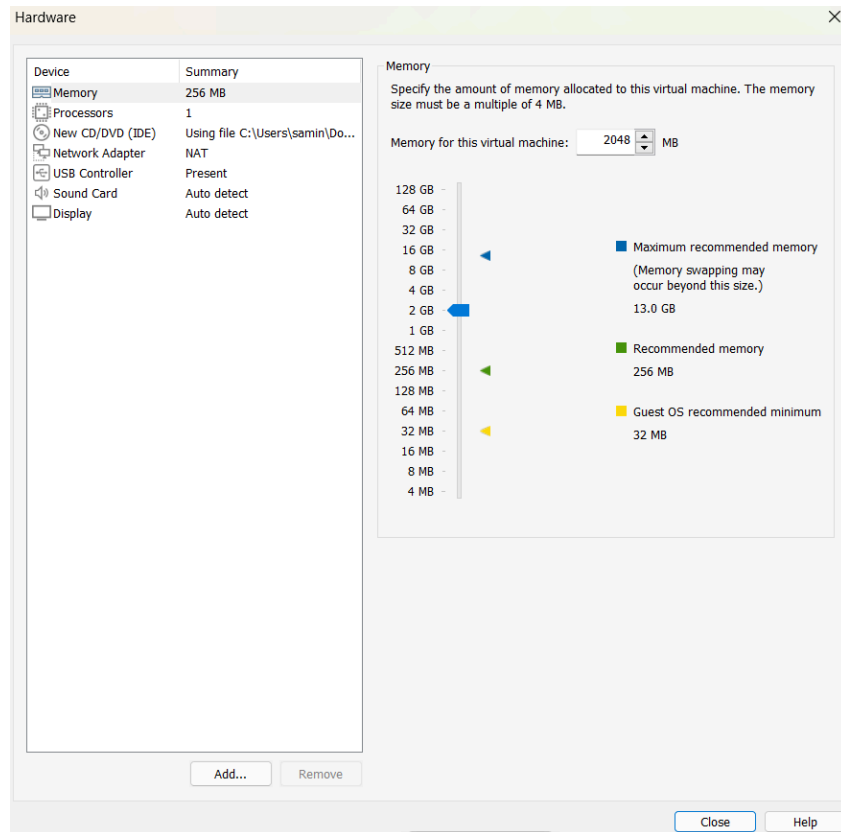
Customize Hardware...

☒ Power on this virtual machine after creation

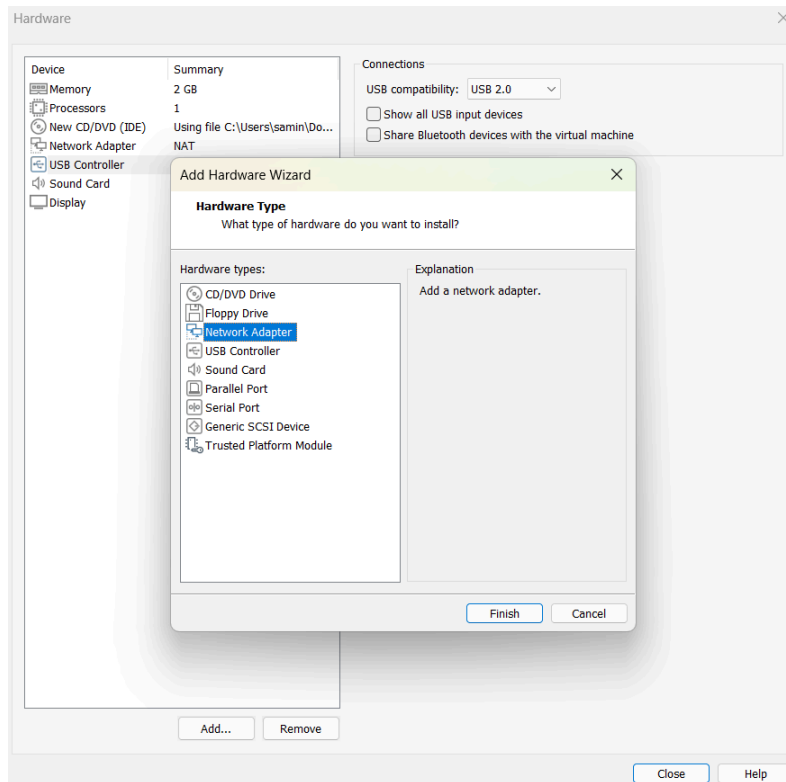
< Back

Finish

Cancel



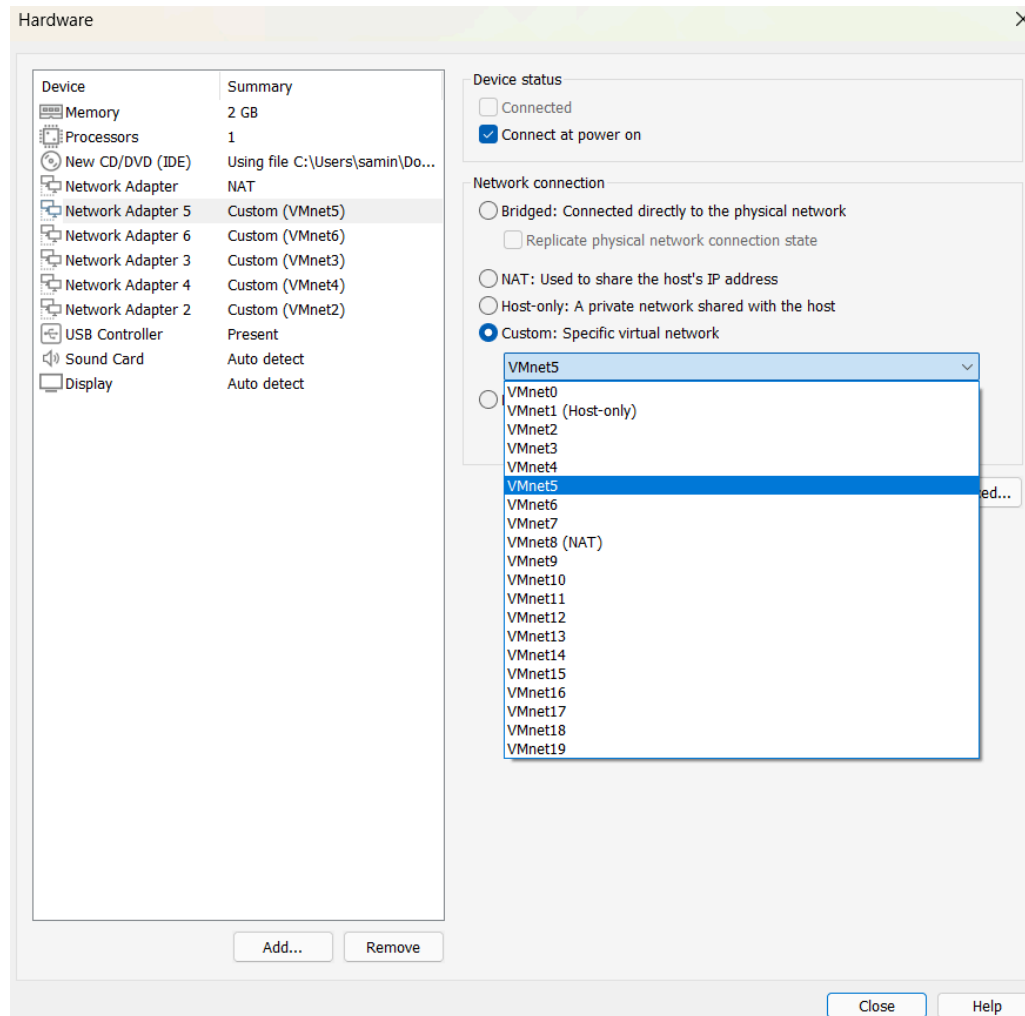
Add a network adapter by clicking “Add”, selecting “Network Adapter” and clicking “Finish”:



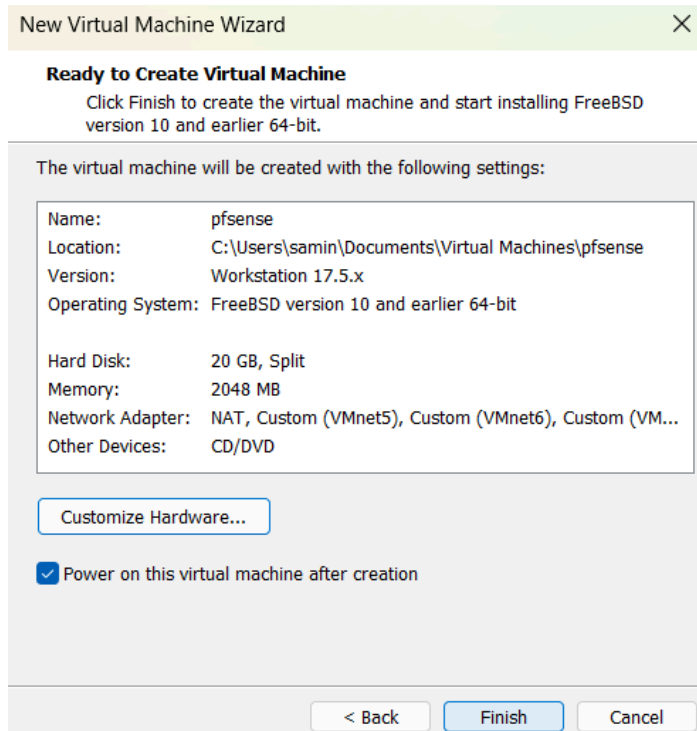
Repeat this 4 more times so that you have 6 network adapters total:

Device	Summary
Memory	2 GB
Processors	1
New CD/DVD (IDE)	Using file C:\Users\samin\Do...
Network Adapter	NAT
Network Adapter 5	NAT
Network Adapter 6	NAT
Network Adapter 3	NAT
Network Adapter 4	NAT
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

For each of the Network adapters, click on them and choose the custom network connection of “VMnetX” where “X” is the network adapter number (eg. for “Network Adapter 5”, choose “VMnet5”, as shown below). Leave the original Network adapter (the one with no number) as NAT:



You can remove the “Sound Card” and “USB Controller” if you wish. Otherwise, you can click “Close” and then “Finish”:



The pfsense machine should launch. Except for the default partition option, where you should select "Auto (UFS) BIOS" from the list, you can press "Enter" through each screen to select the default for the rest of the options. Any warnings about overwriting disk content permanently can be safely disregarded.

Once you reboot the machine and are prompted with "Enter an option", enter "1":

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

VMware Virtual Machine - Netgate Device ID: a5f4f379625442d6778b

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.112.128/24
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: 1
```



Enter “n” at the next prompt when it asks about setting up VLANs:

```
Enter an option: 1

Valid interfaces are:

em0      00:0c:29:34:b1:09  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:34:b1:13  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2      00:0c:29:34:b1:1d  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3      00:0c:29:34:b1:27  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4      00:0c:29:34:b1:31  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5      00:0c:29:34:b1:3b  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

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]? 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 em1 em2 em3 em4 em5 or a):
```

Enter each of the “emX” at the subsequent prompts (ie. em0, em1, ..., em5):

```
Enter an option: 1

Valid interfaces are:

em0      00:0c:29:34:b1:09  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:34:b1:13  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2      00:0c:29:34:b1:1d  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3      00:0c:29:34:b1:27  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4      00:0c:29:34:b1:31  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5      00:0c:29:34:b1:3b  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

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]? 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 em1 em2 em3 em4 em5 or a): em0
```

```

NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 em5 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 em5 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 em5 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 em5 a or nothing if finished): em4

Enter the Optional 4 interface name or 'a' for auto-detection
(em5 a or nothing if finished): em5

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1
OPT1 -> em2
OPT2 -> em3
OPT3 -> em4
OPT4 -> em5

Do you want to proceed [y\N]? █

```

Enter “y” at the prompt asking if you want to proceed.

Next, to set the interface IP addresses, enter “2” at the prompt:

```

Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: a5f4f379625442d6778b

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.112.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->
OPT2 (opt2)    -> em3      ->
OPT3 (opt3)    -> em4      ->
OPT4 (opt4)    -> em5      ->

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: 2█

```

To configure the LAN, enter the associated number (in the screenshot below, it's '2') and enter 'n' when asked about configuring the IPv4 address via DHCP. Enter the IP address that is going

to be used to access the pfSense WebGUI (in this case, we are using 192.168.1.1):

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)
6 - OPT4 (em5)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> █
```

Configure as follows (the start and end addresses are 192.168.1.11 - 192.168.1.200):

```
> 192.168.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.11
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Press "Enter" at the next prompt to continue.

Configure each of the remaining interfaces as follows. OPT1:

Enter an option: 2

Available interfaces:

- 1 - WAN (em0 - dhcp, dhcp6)
- 2 - LAN (em1 - static, dhcp6)
- 3 - OPT1 (em2)
- 4 - OPT2 (em3)
- 5 - OPT3 (em4)
- 6 - OPT4 (em5)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:  
> 192.168.2.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
255.255.0.0 = 16  
255.0.0.0 = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):  
> █

255.255.0.0 = 16  
255.0.0.0 = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):  
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

Enter the new OPT1 IPv6 address. Press <ENTER> for none:  
>

Do you want to enable the DHCP server on OPT1? (y/n) n  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to OPT1...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...█

OPT2:

```
Enter the number of the interface you wish to configure: 4
Configure IPv4 address OPT2 interface via DHCP? (y/n) n
Enter the new OPT2 IPv4 address. Press <ENTER> for none:
> 192.168.3.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT2 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT2 interface via DHCP6? (y/n) n
Enter the new OPT2 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) █
```

```
Configure IPv6 address OPT2 interface via DHCP6? (y/n) n
Enter the new OPT2 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to OPT2...[fib_algo] inet.0 (bsearch4#90
) rebuild_fd_flm: switching algo to radix4_lockless

Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT2 address has been set to 192.168.3.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://192.168.3.1/

Press <ENTER> to continue. █
```

OPT4: (note that we are not touching OPT3 for now)

```

Enter the number of the interface you wish to configure: 6
Configure IPv4 address OPT4 interface via DHCP? (y/n) n
Enter the new OPT4 IPv4 address. Press <ENTER> for none:
> 192.168.4.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT4 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT4 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT4 interface via DHCP6? (y/n) n
Enter the new OPT4 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT4? (y/n) n

```

```

     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT4 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT4 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT4 interface via DHCP6? (y/n) n
Enter the new OPT4 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT4? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to OPT4...
Reloading filter...
Reloading routing configuration...
DHCPD...

```

This is what it should look like at the end:

```

VMware Virtual Machine - Netgate Device ID: a5f4f379625442d6778b

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.112.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.1/24
OPT2 (opt2)    -> em3      -> v4: 192.168.3.1/24
OPT3 (opt3)    -> em4      ->
OPT4 (opt4)    -> em5      -> v4: 192.168.4.1/24

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: █

```

## Configuring Security Onion:

Security onion will be acting as the IDS and Log Management solution.

Download the security onion iso from the Github repo

([https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY\\_ISO.md](https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md))

2.3.280-20231128 ISO image built on 2023/11/28

### Download and Verify

2.3.280-20231128 ISO image:

<https://download.securityonion.net/file/securityonion/securityonion-2.3.280-20231128.iso>

MD5: 0BC68BD73547B7E2FBA6F53BEC174590

SHA1: 1D33C565D37772FE7A3C3FE3ECB05FC1AC1EBFF1

SHA256: ADBD9DC9E1B266B18E0FDBDF084073EF926C565041858060D283CDAEF021EE11

Signature for ISO image:

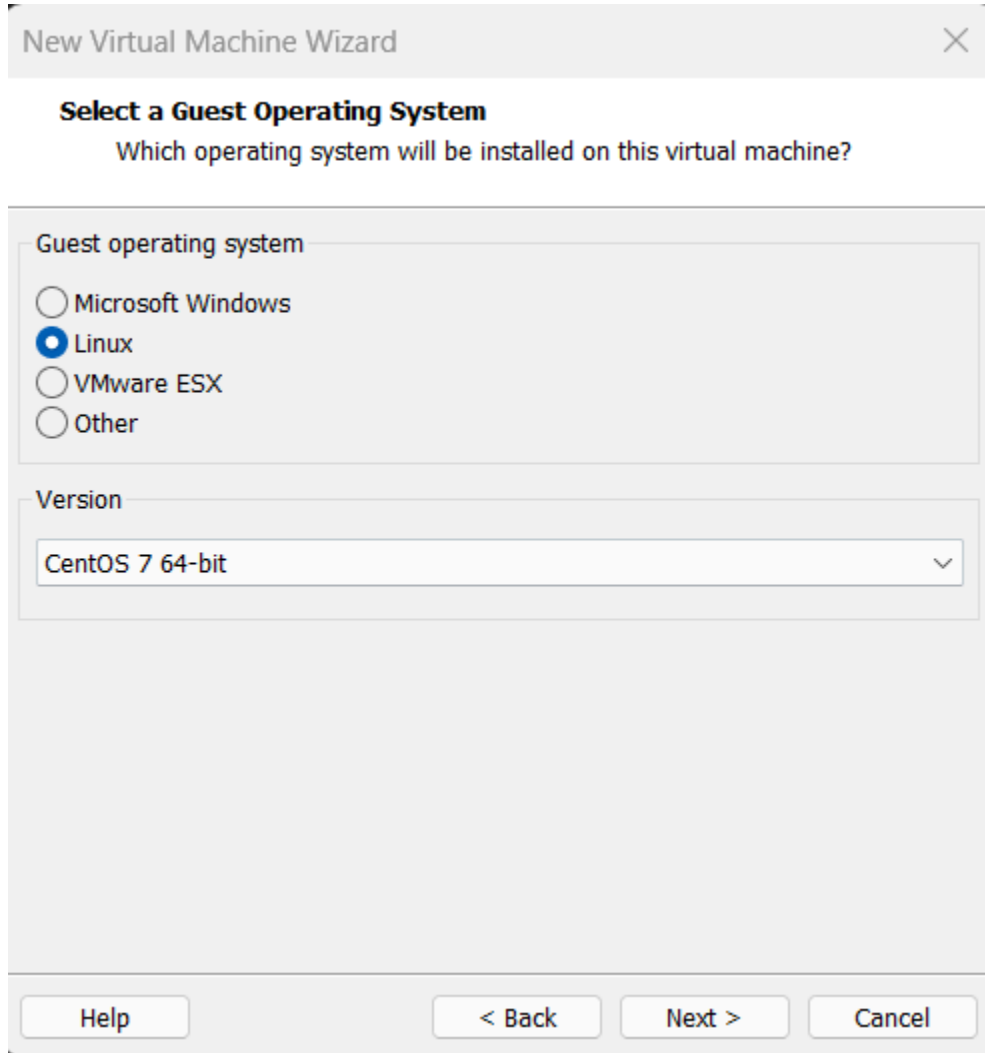
<https://github.com/Security-Onion-Solutions/securityonion/raw/master/sigs/securityonion-2.3.280-20231128.iso.sig>

Signing key:

<https://raw.githubusercontent.com/Security-Onion-Solutions/securityonion/master/KEYS>



Set up a new virtual machine in VMWare as done above (with pfsense) with “Typical” selected on the first screen, and then select the disc image from where you downloaded it. When it asks to select a guest operating system, use the configuration below:



New Virtual Machine Wizard

**Select a Guest Operating System**  
Which operating system will be installed on this virtual machine?

Guest operating system

☐ Microsoft Windows

☒ Linux

☐ VMware ESX

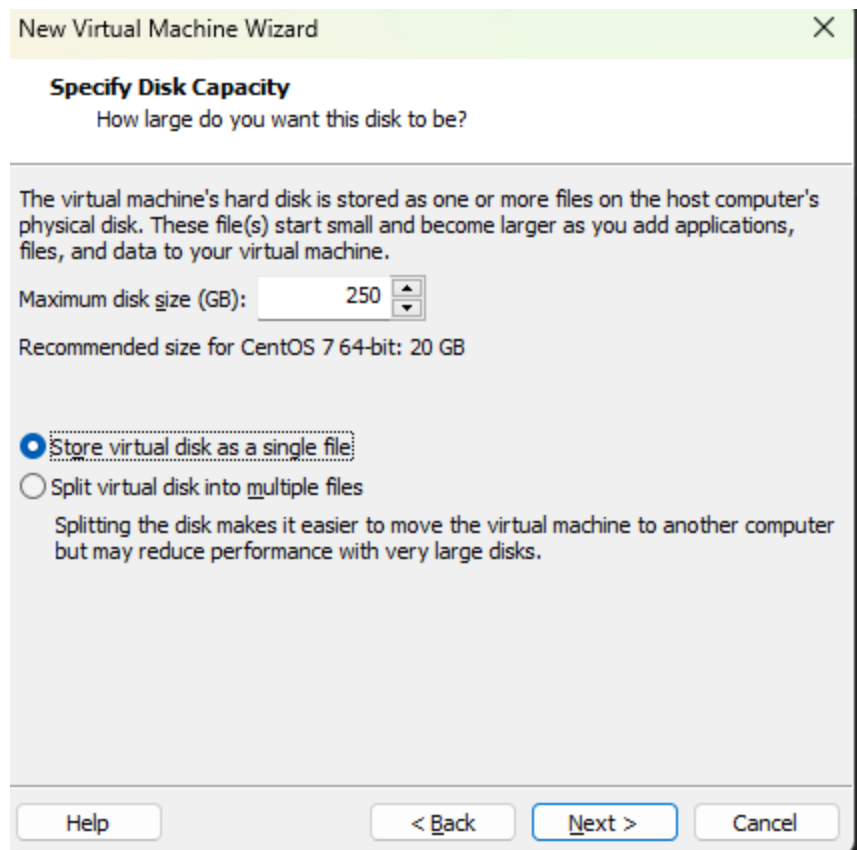
☐ Other

Version

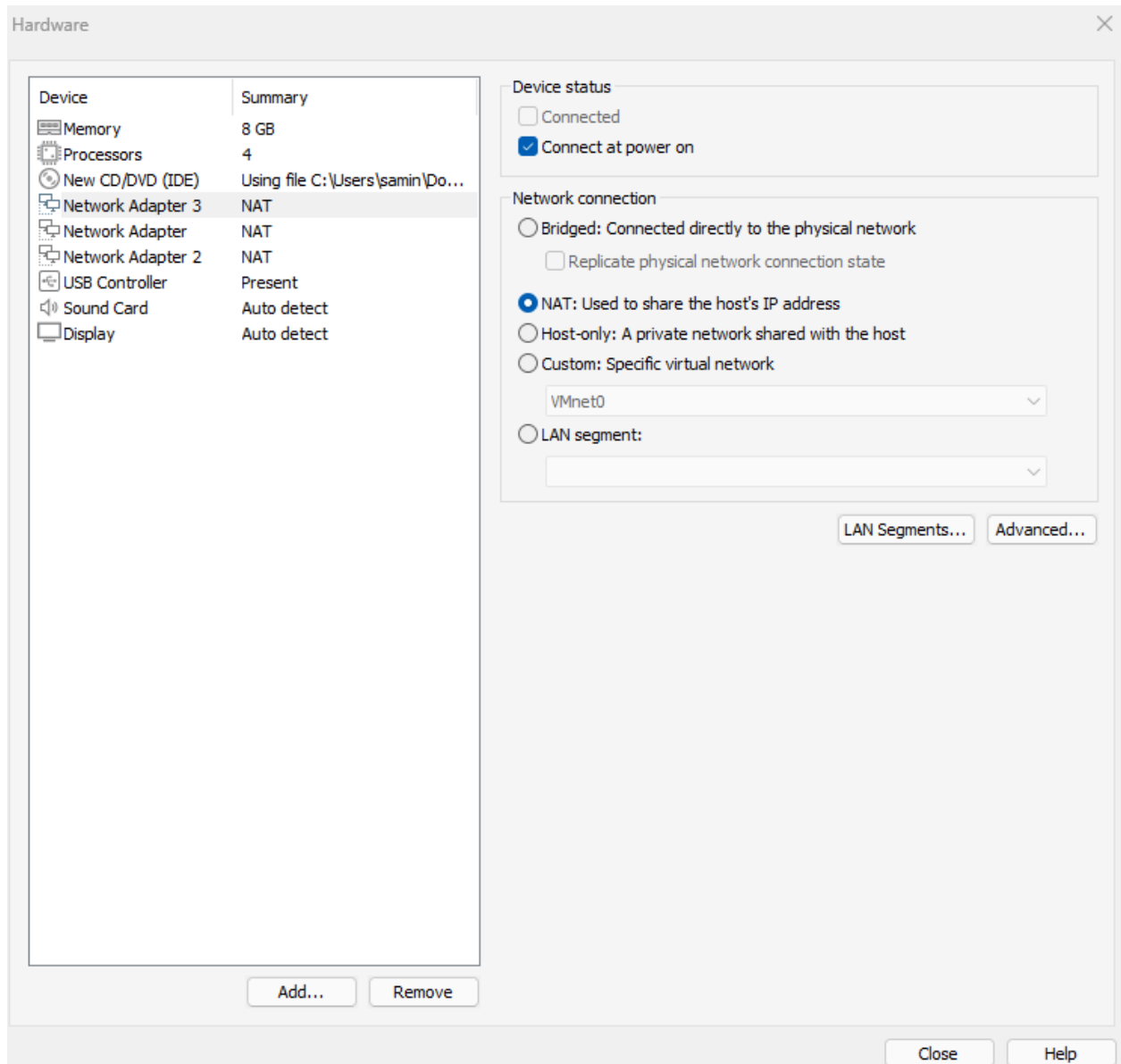
CentOS 7 64-bit

Help < Back Next > Cancel

After clicking “Next”, use the following configuration for the next screen (give the machine at least 200 GB, the more the better):



On the next screen, click “Customize Hardware” and give it more RAM - they recommend 12 GB, but I’ll be giving it 8. Also, give it at least 4 processors and create 2 new network adapters:



Configure Network adapter 2 to VMnet 4, and Network adapter 3 to VMnet 5. You can delete extra pieces like the Sound Card or USB Controller. The final screen looks like this:

Device	Summary
Memory	8 GB
Processors	4
New CD/DVD (IDE)	Using file C:\Users\samin\Do...
Network Adapter 3	Custom (VMnet5)
Network Adapter	NAT
Network Adapter 2	Custom (VMnet4)
Display	Auto detect

You can click “Close” and then “Finish” before powering on the VM.

Once turned on, let the VM load through everything and then enter “yes” when prompted.

Enter a username and password as prompted as well.

```
#####
##          ** W A R N I N G **          ##
##          _____                    ##
##          ##                        ##
##  Installing the Security Onion ISO      ##
##  on this device will DESTROY ALL DATA ##
##          and partitions!              ##
##          ##                        ##
##          ** ALL DATA WILL BE LOST **   ##
#####
Do you wish to continue? (Type the entire word 'yes' to proceed.) yes

A new administrative user will be created. This user will be used for setting up and administering S
ecurity Onion.

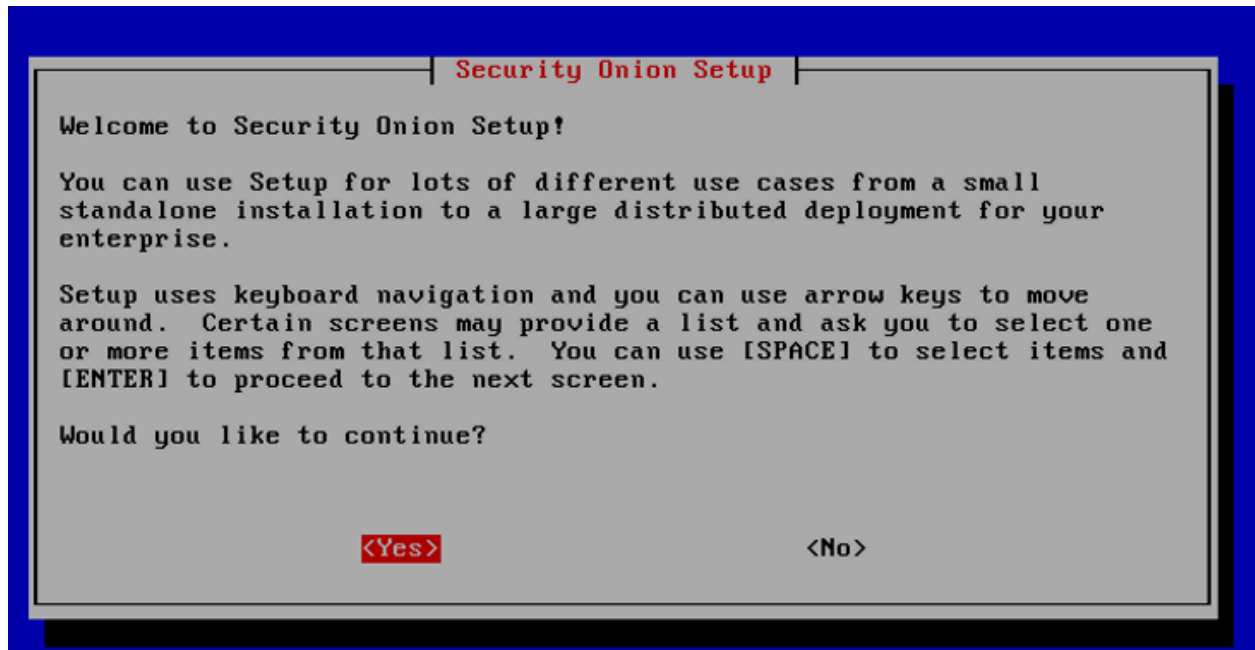
Enter an administrative username: samin

Let's set a password for the samin user:

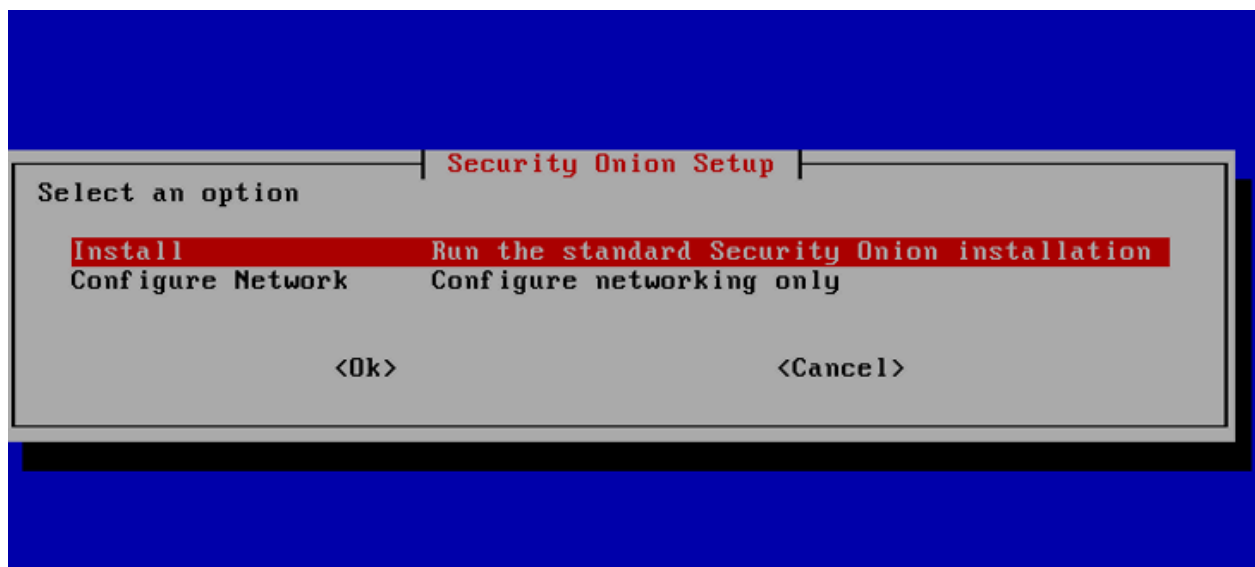
Enter a password:
Re-enter the password: _
```

After entering and waiting, press enter when prompted. Enter your login information once you get to the prompt asking you for it.

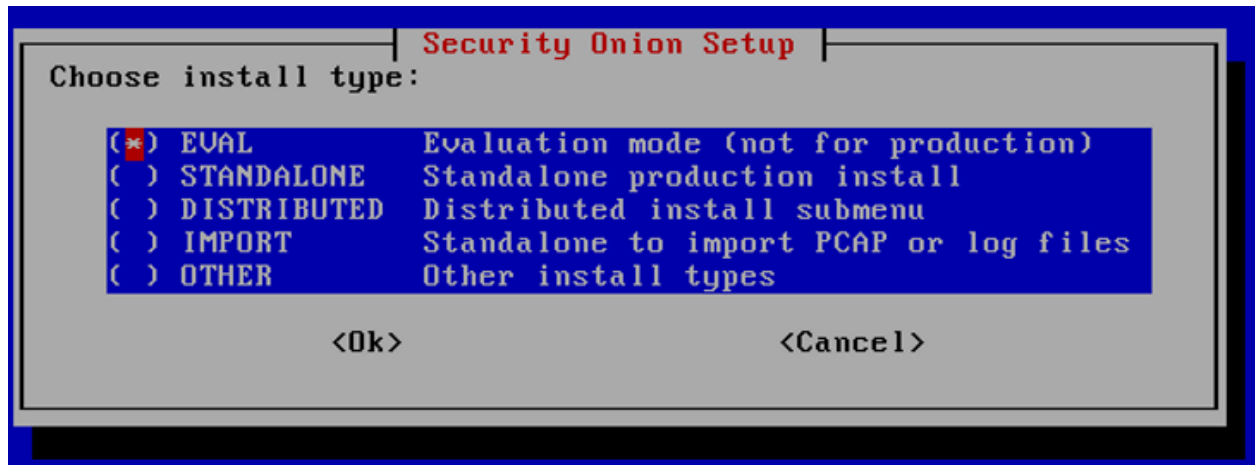
Select “Yes” by pressing enter on the next screen:



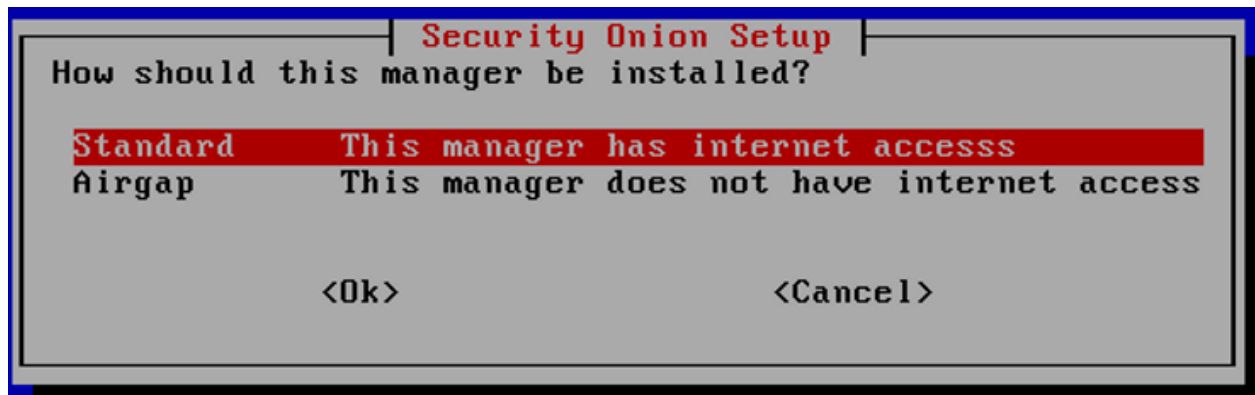
Press enter on the "Install" option on the next screen:



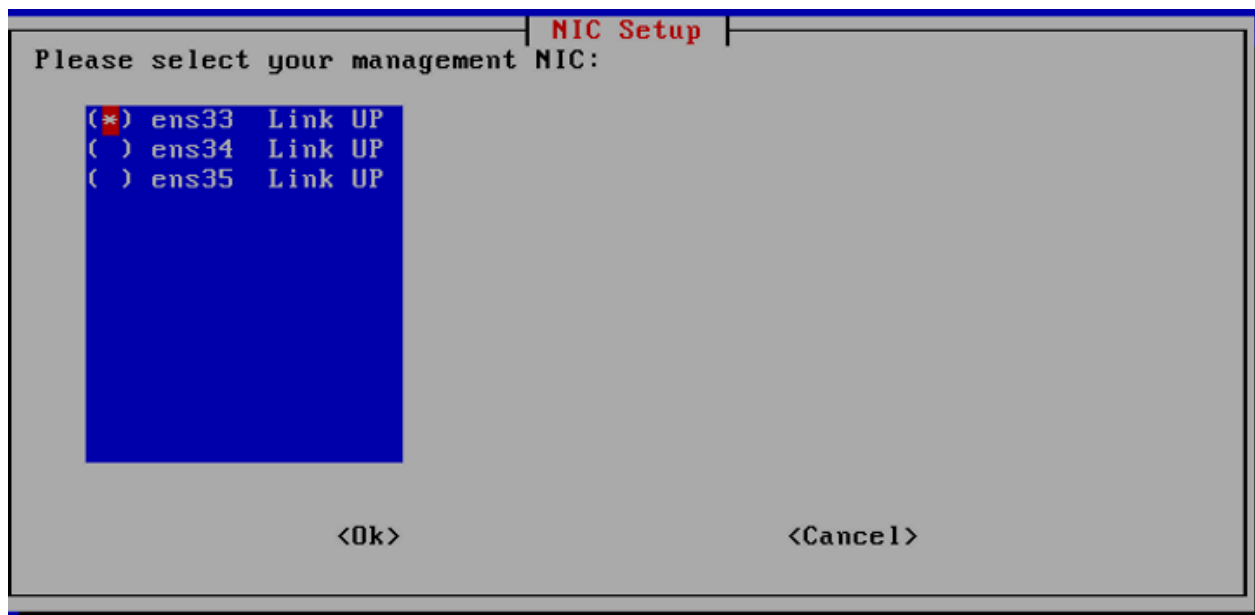
Ensure the "EVAL" option is selected before pressing enter on the screen after:



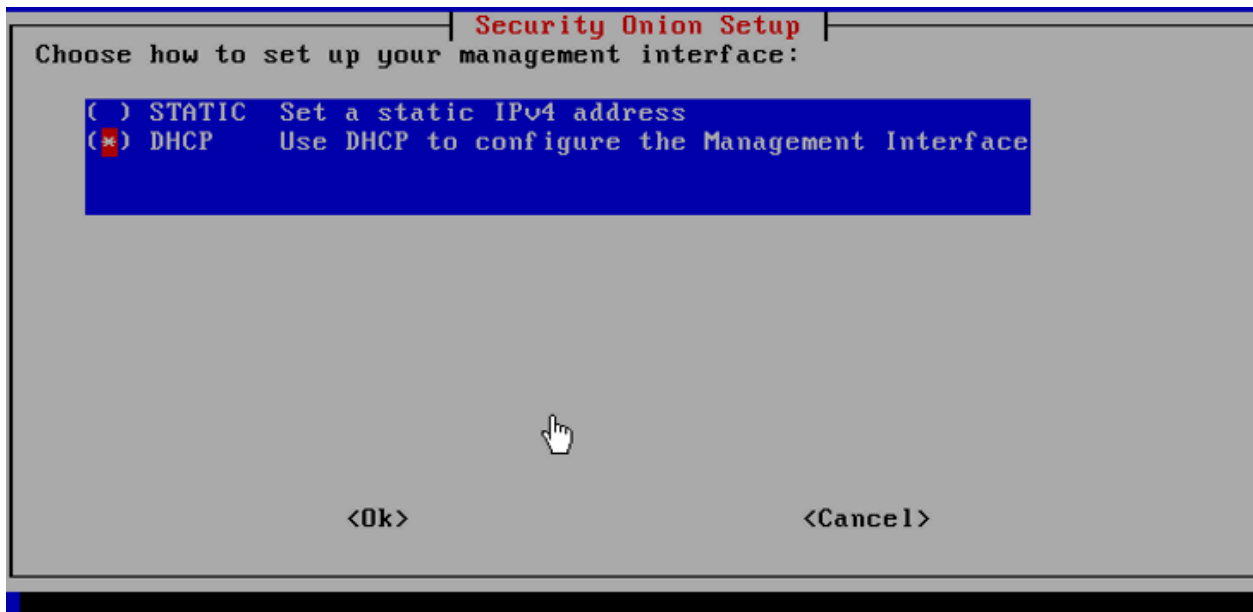
Type out "AGREE" when prompted. Select "Standard" on the next screen:



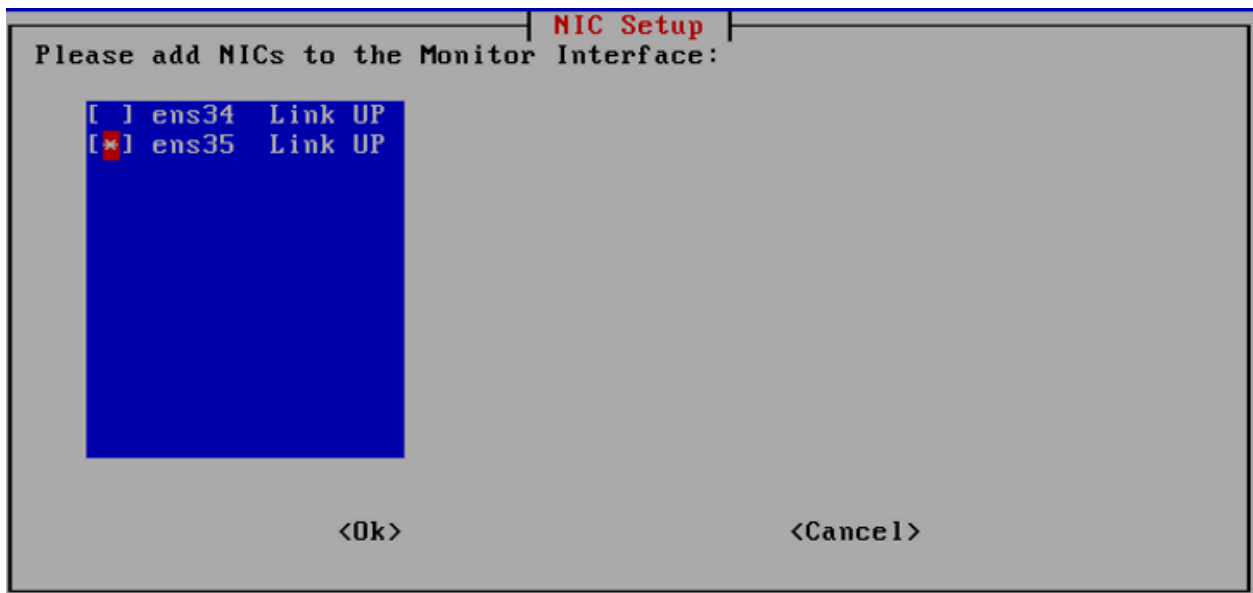
Create a hostname when asked. Select "ens33" on the next screen:



Select "DHCP" on the next screen:



Select "YES", "OK", and then "Direct" for the next 3 prompts. Then select "ens35" at the next prompt:



Select "Automatic" at the next screen. Select the default options for the next couple of screens before reaching the prompt asking for an email. Enter an email and password of your choosing.

Select "IP" at the next screen:

Security Onion Setup

How would you like to access the web interface?

Security Onion uses strict cookie enforcement, so whatever you choose here will be the only way that you can access the web interface.

If you choose something other than IP address, then you'll need to ensure that you can resolve the name via DNS or hosts entry. If you are unsure, please select IP.

☒ IP

Use IP address to access the web interface

☐ HOSTNAME

Use hostname to access the web interface

☐ OTHER

Use a different name like a FQDN or Load Balancer

<Ok>

<Cancel>

Select "Yes" for the NTP server on the next screen and then select all the default options.

When you get to the final screen, save the information displayed; importantly, ensure you know the IP address for web access (next to "Access URL"). Press "Tab" and select "Yes" once you are done. The installation will begin, and it will likely take a long time (it took around 20 minutes for me).



# Troubleshooting:

Trying to unzip the pfsense ISO file from their website with the Windows extractor resulted in the following error:

←  Extract Archive

The Extraction Operation was not Completed

An unexpected error is preventing the archive from being extracted.



Error 0x8000FFFF: Catastrophic failure

I was able to complete the extraction using 7-Zip instead (<https://www.7-zip.org/>).