Homelab for Security Detection & Monitoring

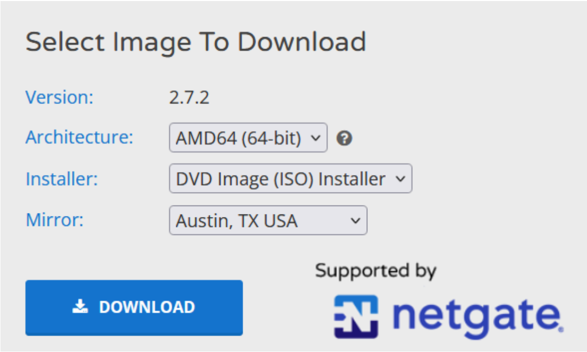
This is a homelab created following Day CyberWox's blueprint and documentation, available on his website. It's been changed slightly to use the more recent, up-to-date software versions and technologies. The lab was created using VMWare Workstation Pro 17; you don't need to buy a licence upfront since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

Contents:

Configuring pfSense as a Firewall

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

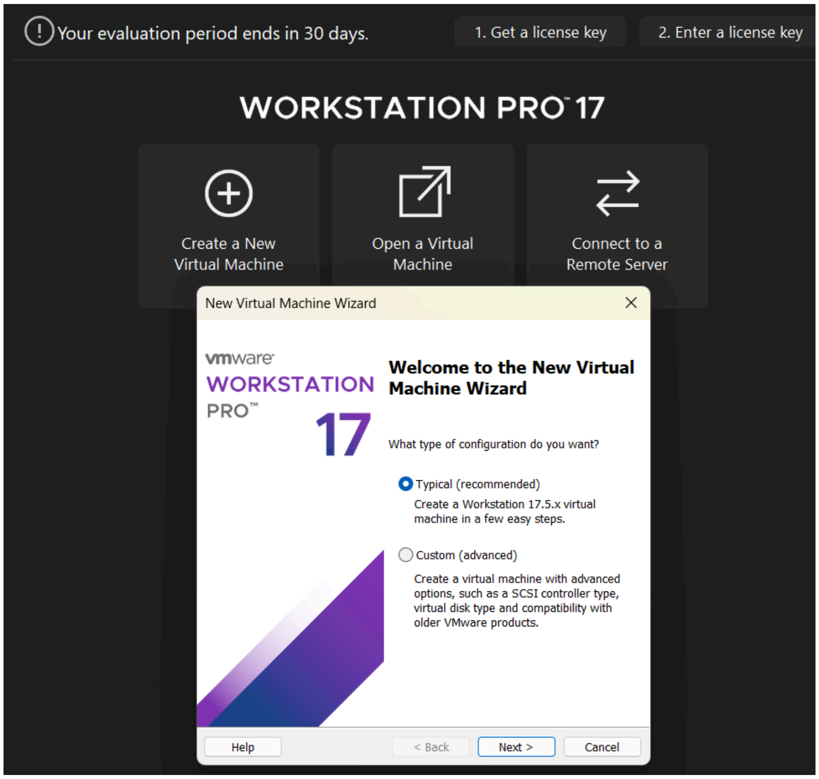
Version: 2.7.2

Architecture: AMD64 (64-bit)

Installer: DVD Image (ISO) Installer

Mirror: Austin, TX USA

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”:



Your evaluation period ends in 30 days.

New Virtual Machine Wizard

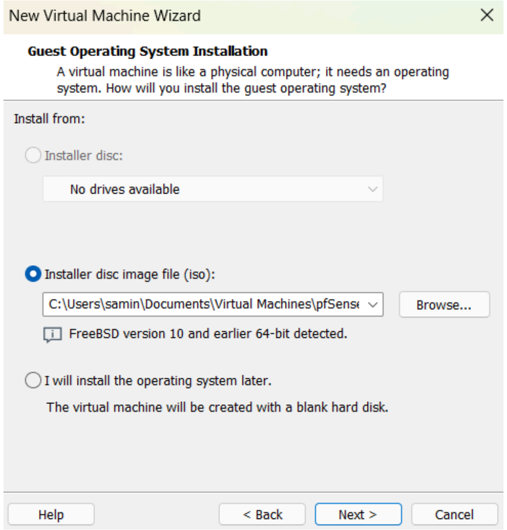
Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

● Typical (recommended)
Create a Workstation 17.5.x virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

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



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

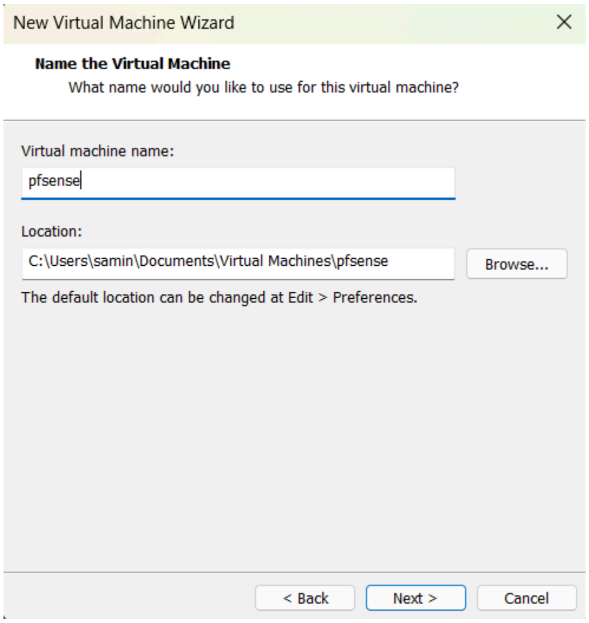
C:\Users\samin\Documents\Virtual Machines\pfSense

FreeBSD version 10 and earlier 64-bit detected.

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

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



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

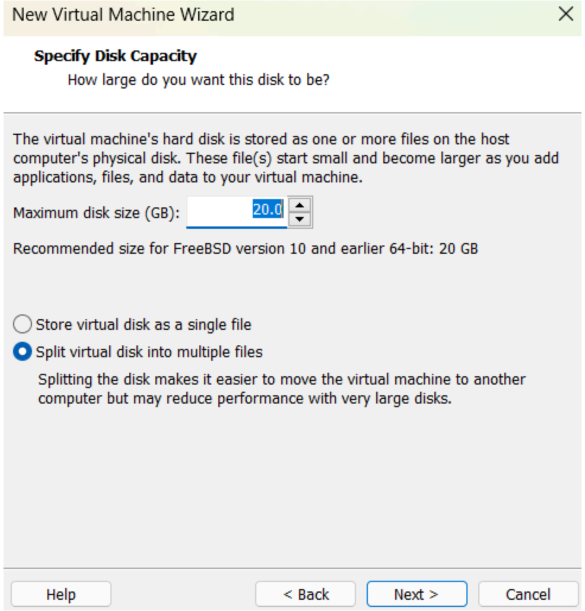
pfsense

Location:

C:\Users\samin\Documents\Virtual Machines\pfsense

The default location can be changed at Edit > Preferences.

Keep the preselected options and click “Next”:



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): 20.0

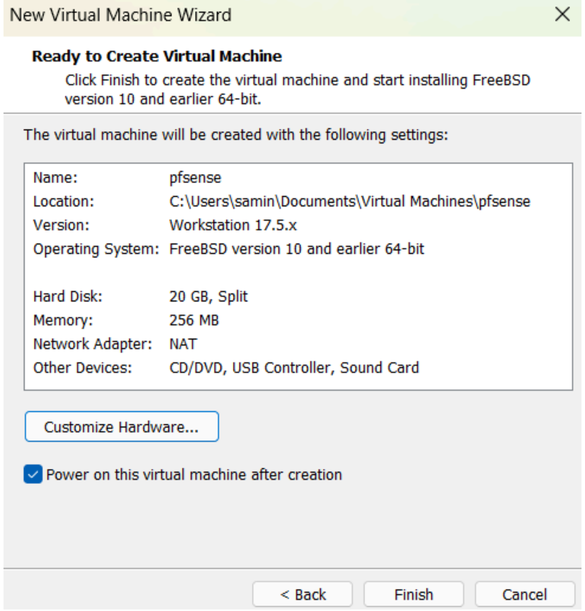
Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

○ 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.

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



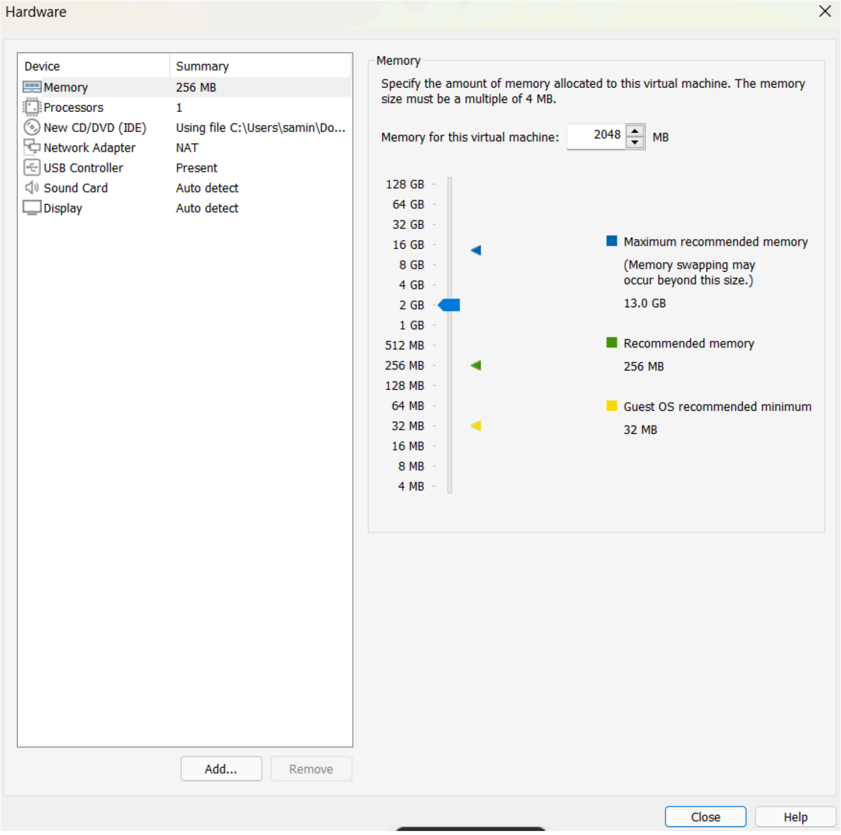
Ready to Create Virtual Machine

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

☑ Power on this virtual machine after creation



Device	Summary
Memory	256 MB
Processors	1
New CD/DVD (IDE)	Using file C:\Users\samin\Do...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 2048 MB

🟦 Maximum recommended memory

(Memory swapping may occur beyond this size.)

13.0 GB

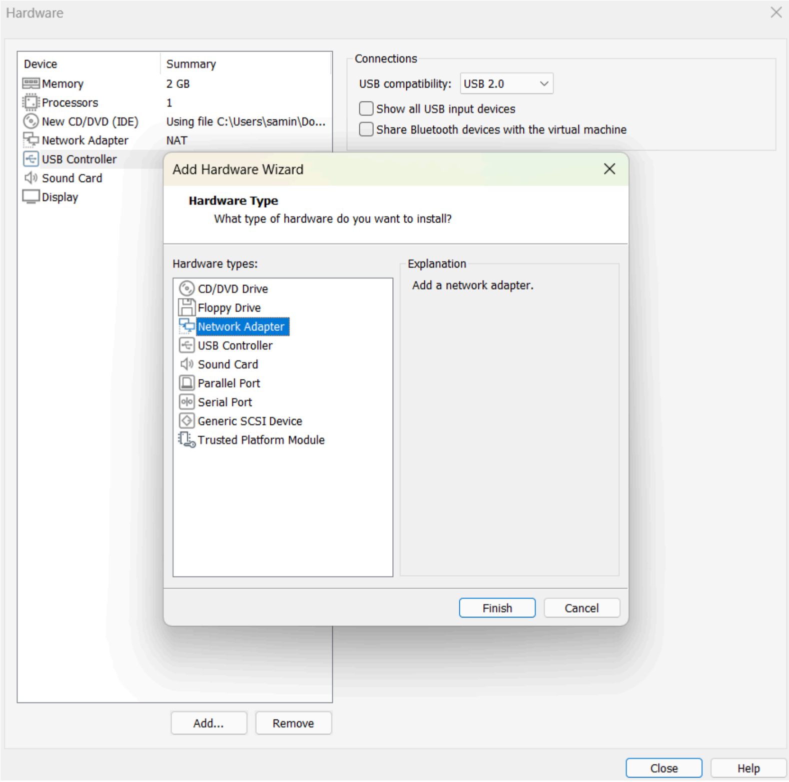
🟩 Recommended memory

256 MB

🟨 Guest OS recommended minimum

32 MB

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



Hardware

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

Connections

USB compatibility: USB 2.0

□ Show all USB input devices

□ Share Bluetooth devices with the virtual machine

Add Hardware Wizard

Hardware Type

What type of hardware do you want to install?

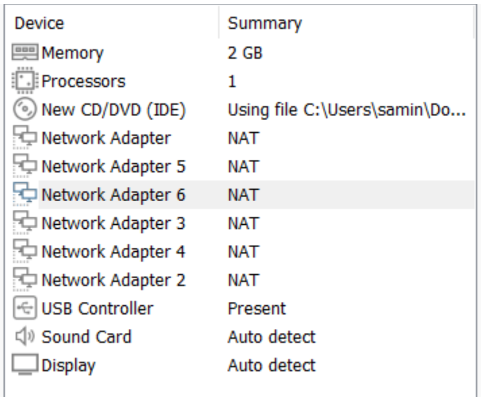
Hardware types:

- CD/DVD Drive
- Floppy Drive
- Network Adapter
- USB Controller
- Sound Card
- Parallel Port
- Serial Port
- Generic SCSI Device
- Trusted Platform Module

Explanation

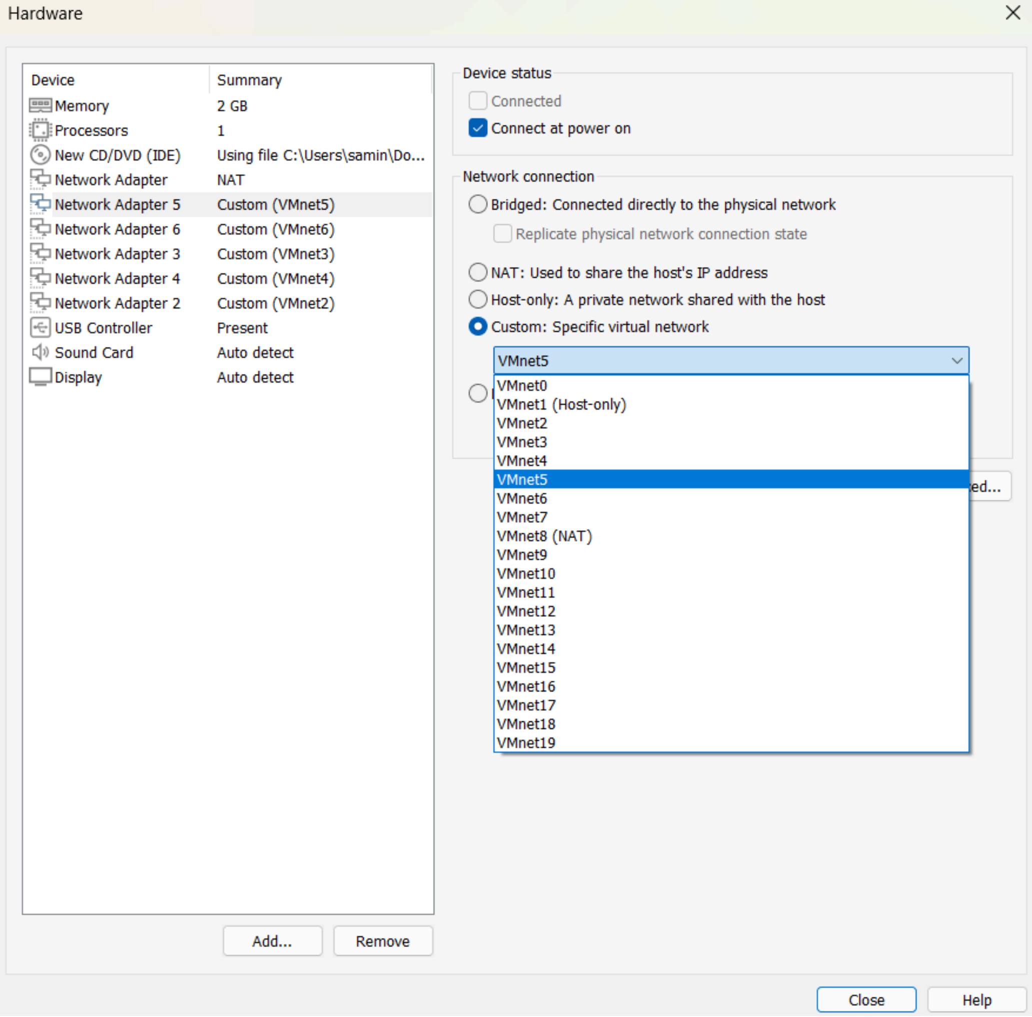
Add a network adapter.

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:



Hardware

Device	Summary
Memory	2 GB
Processors	1
New CD/DVD (IDE)	Using file C:\Users\samin\Do...
Network Adapter	NAT
Network Adapter 5	Custom (VMnet5)
Network Adapter 6	Custom (VMnet6)
Network Adapter 3	Custom (VMnet3)
Network Adapter 4	Custom (VMnet4)
Network Adapter 2	Custom (VMnet2)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

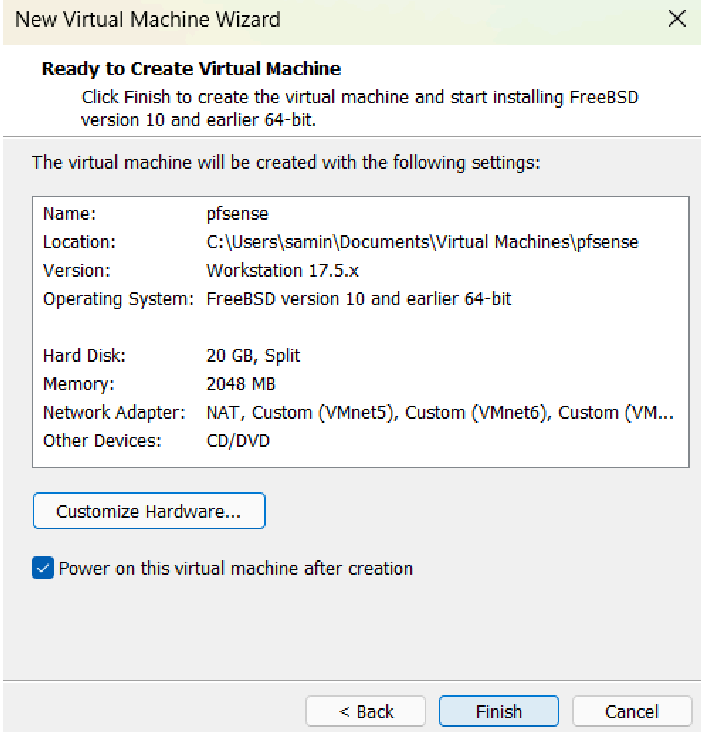
○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet5

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



Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing FreeBSD version 10 and earlier 64-bit.

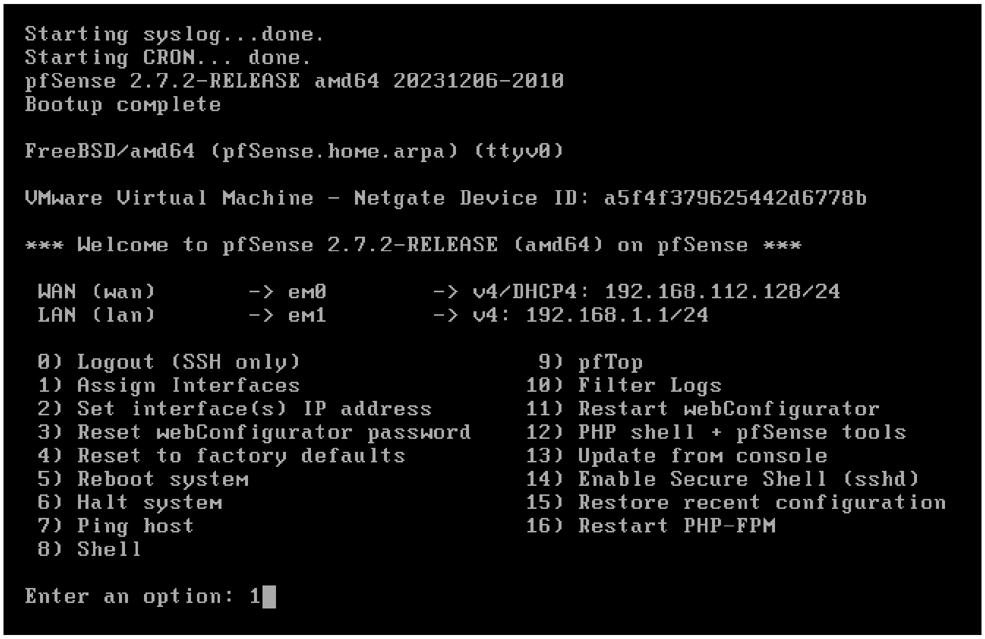
The virtual machine will be created with the following settings:

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:	2048 MB
Network Adapter:	NAT, Custom (VMnet5), Custom (VMnet6), Custom (VM...
Other Devices:	CD/DVD

☑ Power on this virtual machine after creation

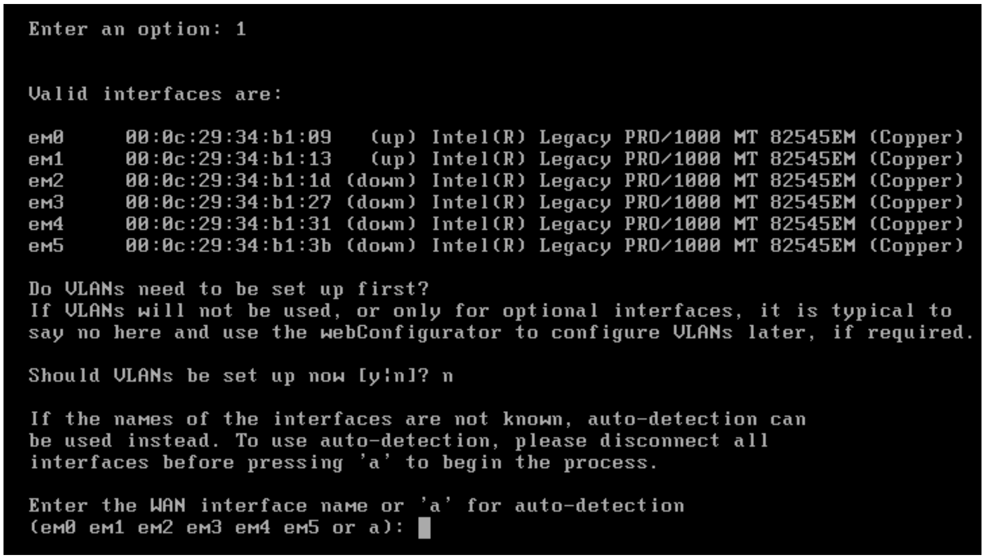
The pfSense machine should launch. Except for the default partition option, where you should select "Auto (UFS) BIOS” from the list, you can press “Enter” through each screen to select the default for the rest of the options. Any warnings about overwriting disk content permanently can be safely disregarded.

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



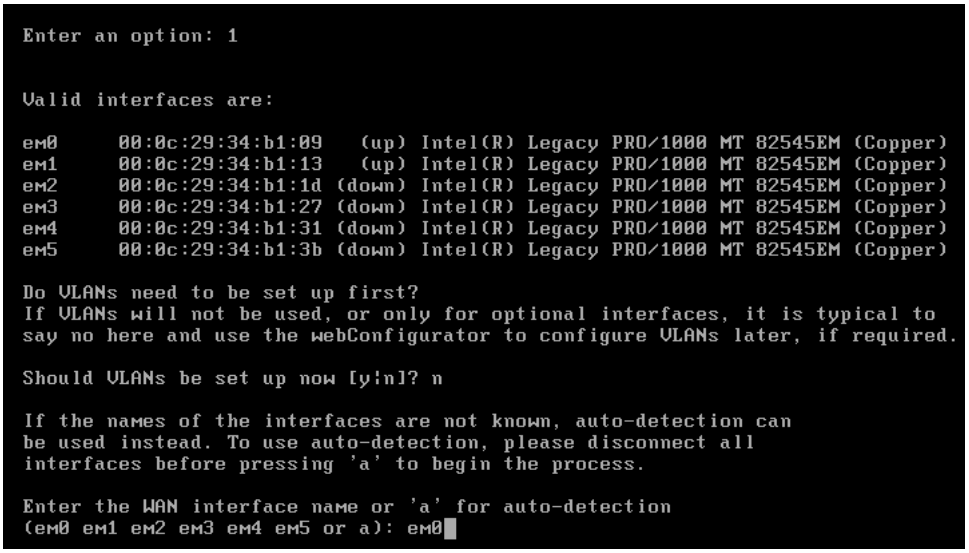
```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (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:

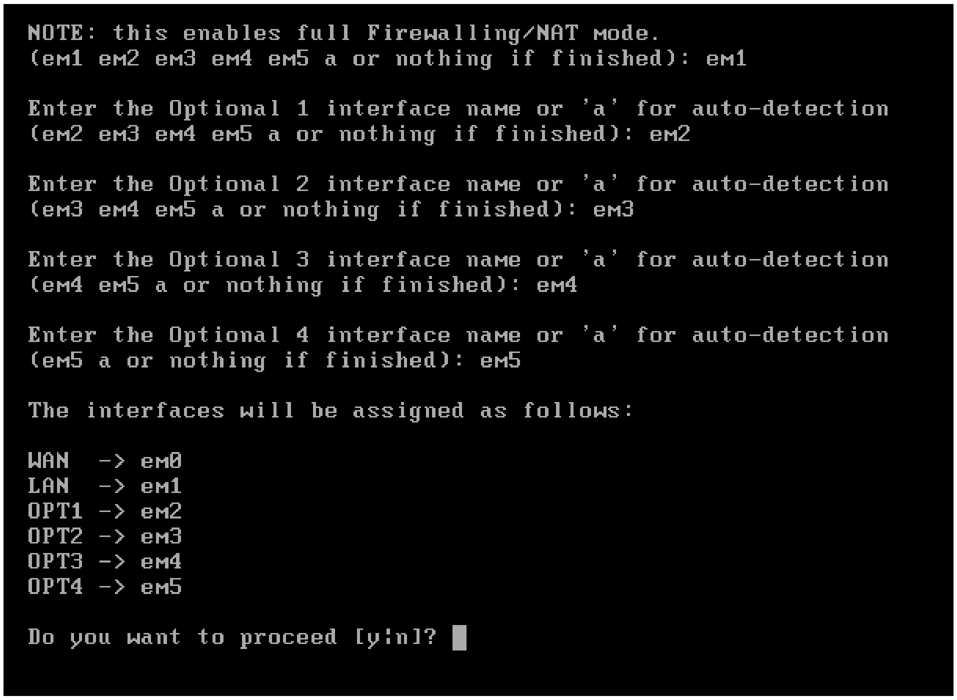


```
Enter an option: 1


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):



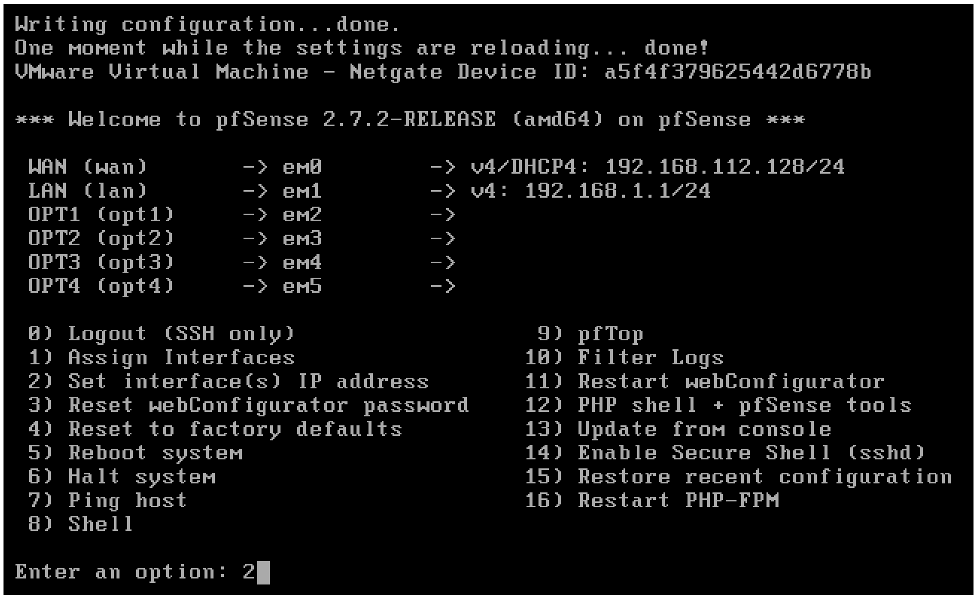
```
Enter an option: 1


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]?
```

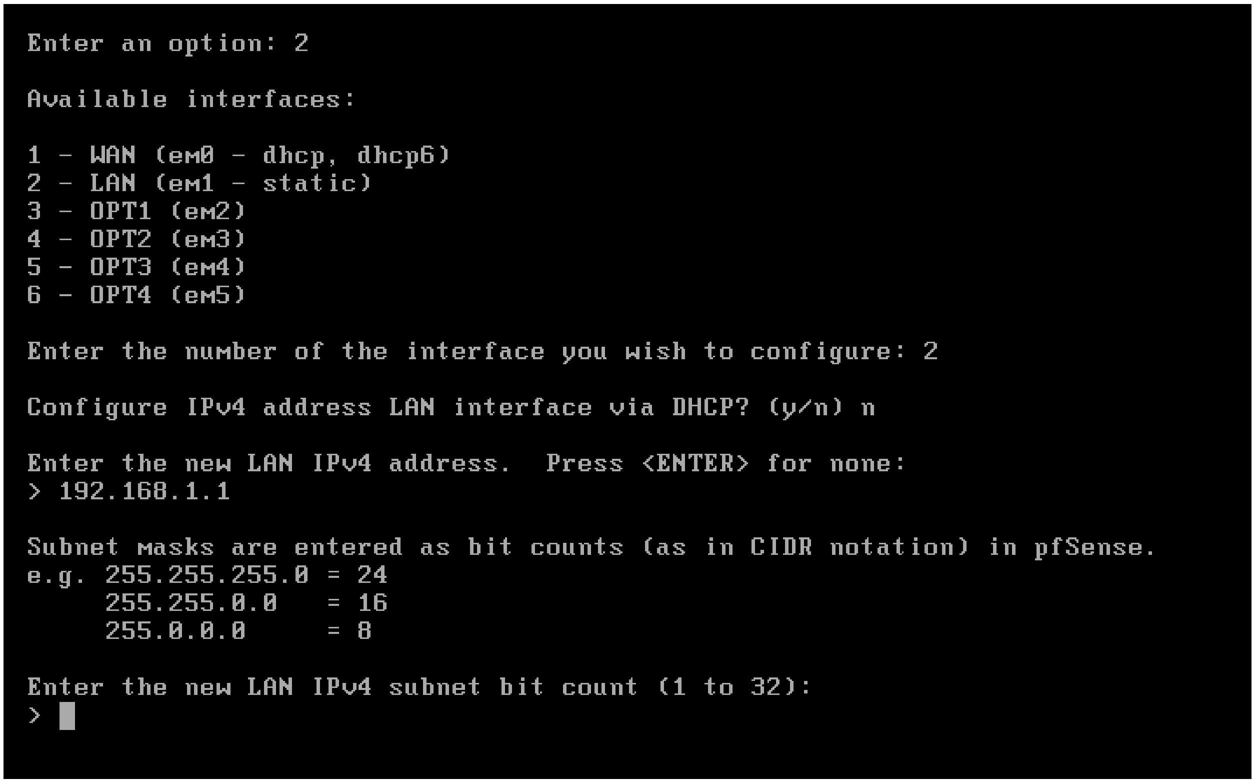
Enter “y” at the prompt asking if you want to proceed.

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



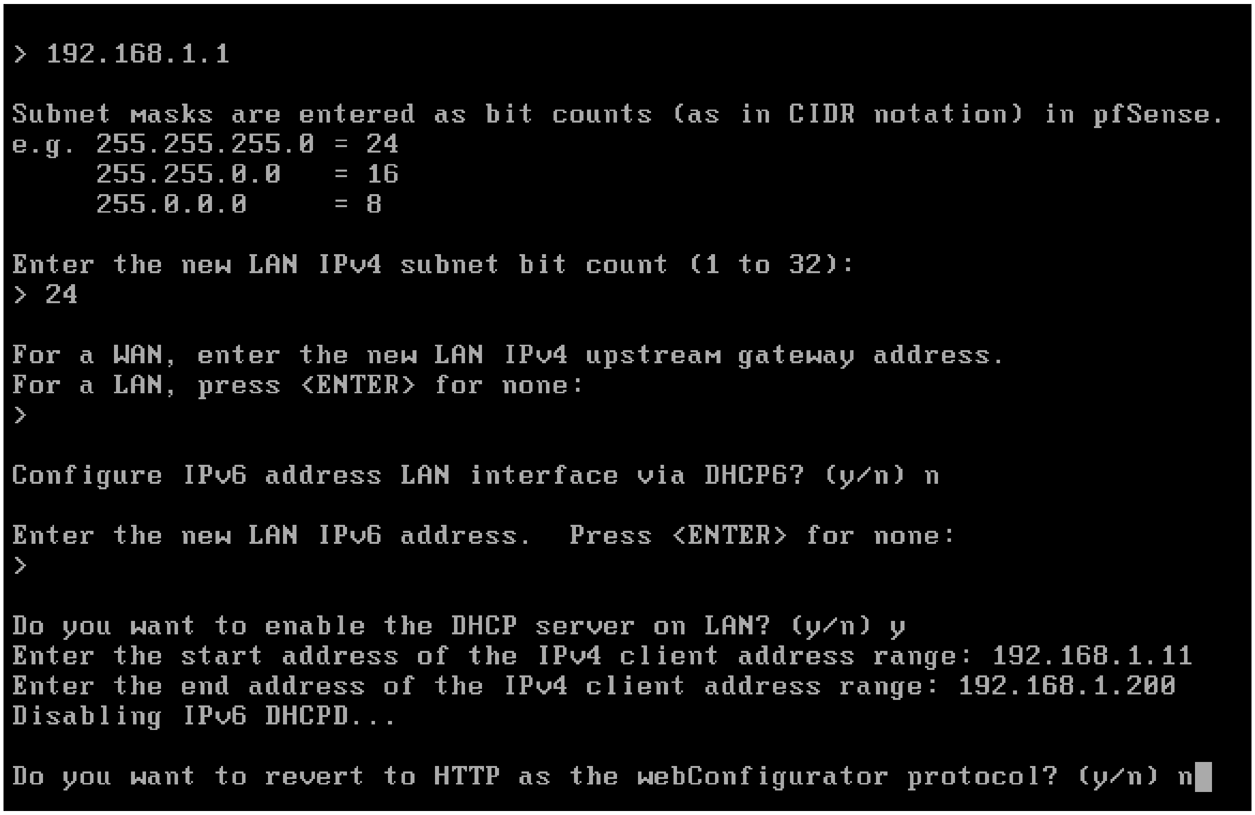
```
Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: a5f4f379625442d6778b

*** 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):
>
```

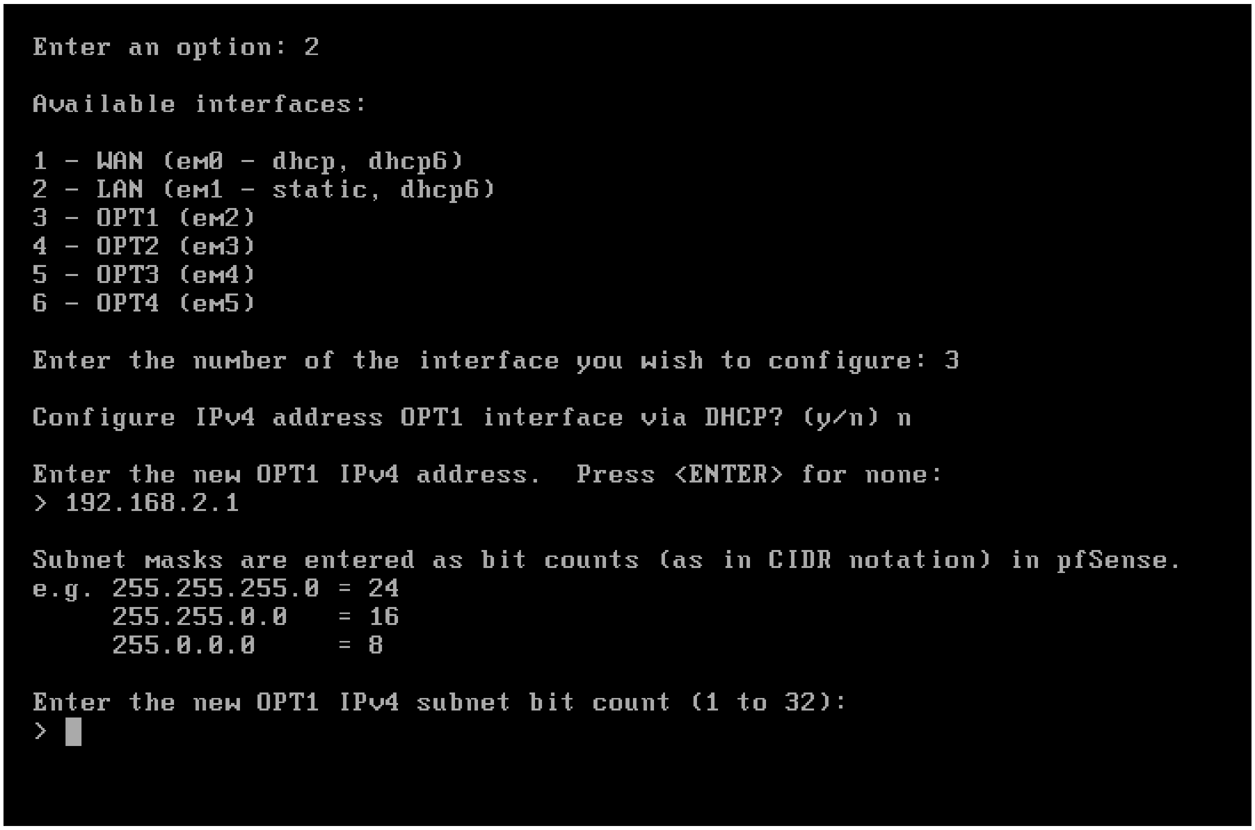
Configure as follows (the start and end addresses are 192.168.1.11 - 192.168.1.200):



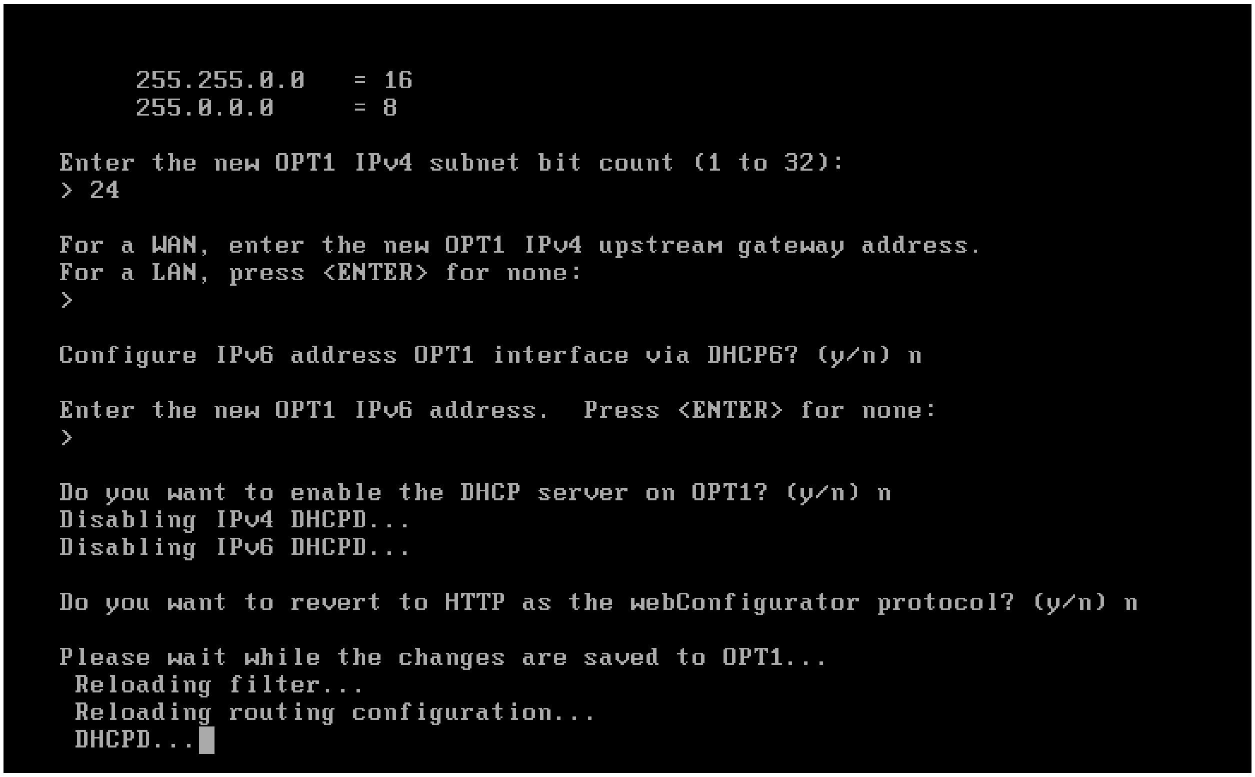
```
> 192.168.1.1

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:

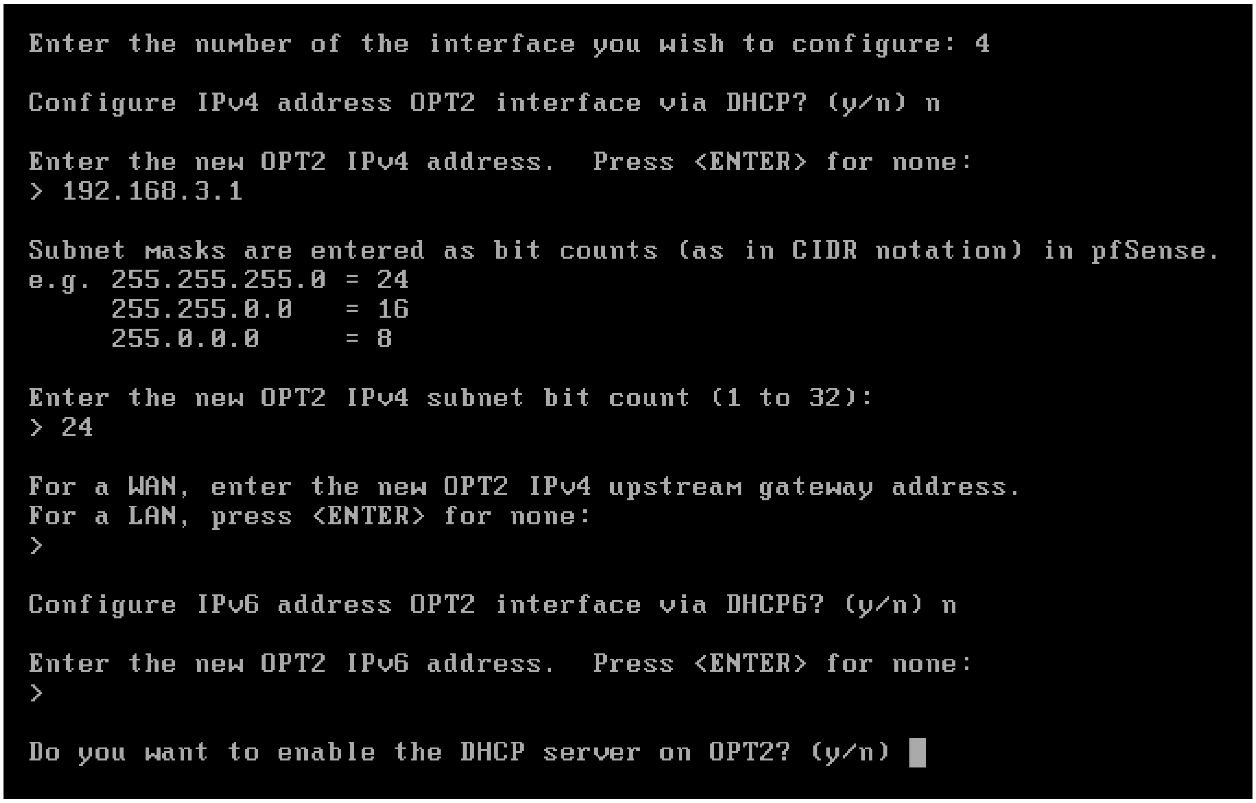


```
Enter an option: 2

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):
> 
```

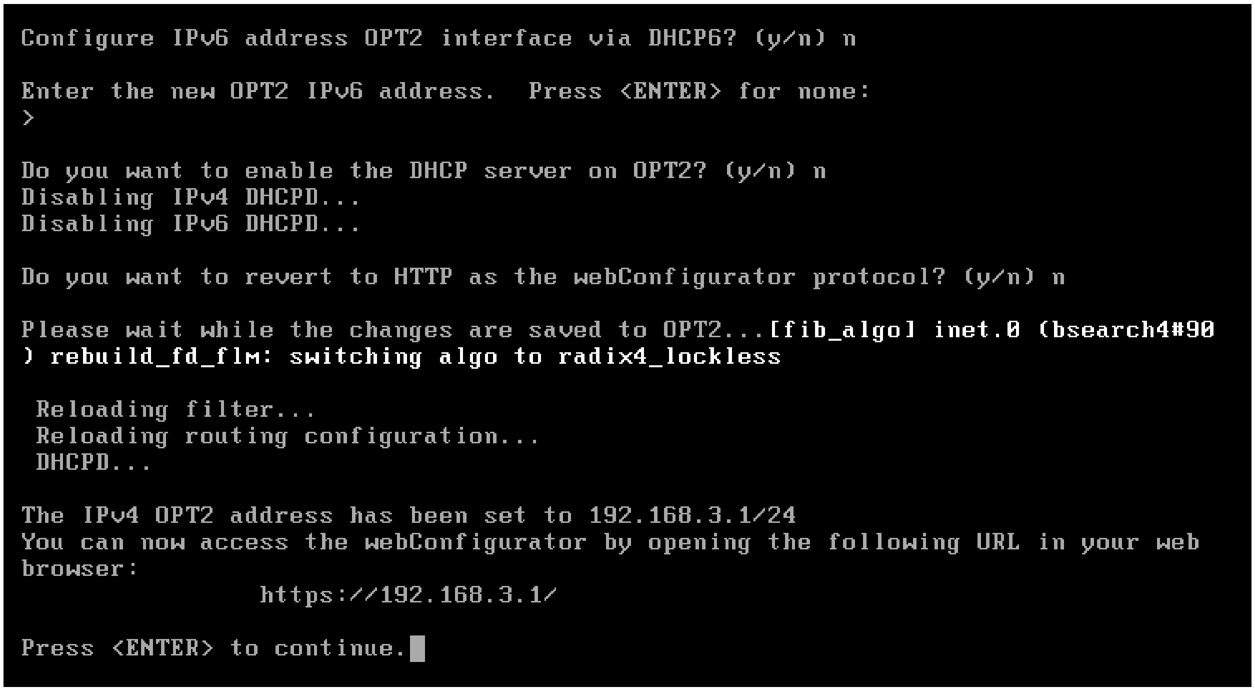


```
      255.255.0.0   = 16
      255.0.0.0     = 8

  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:

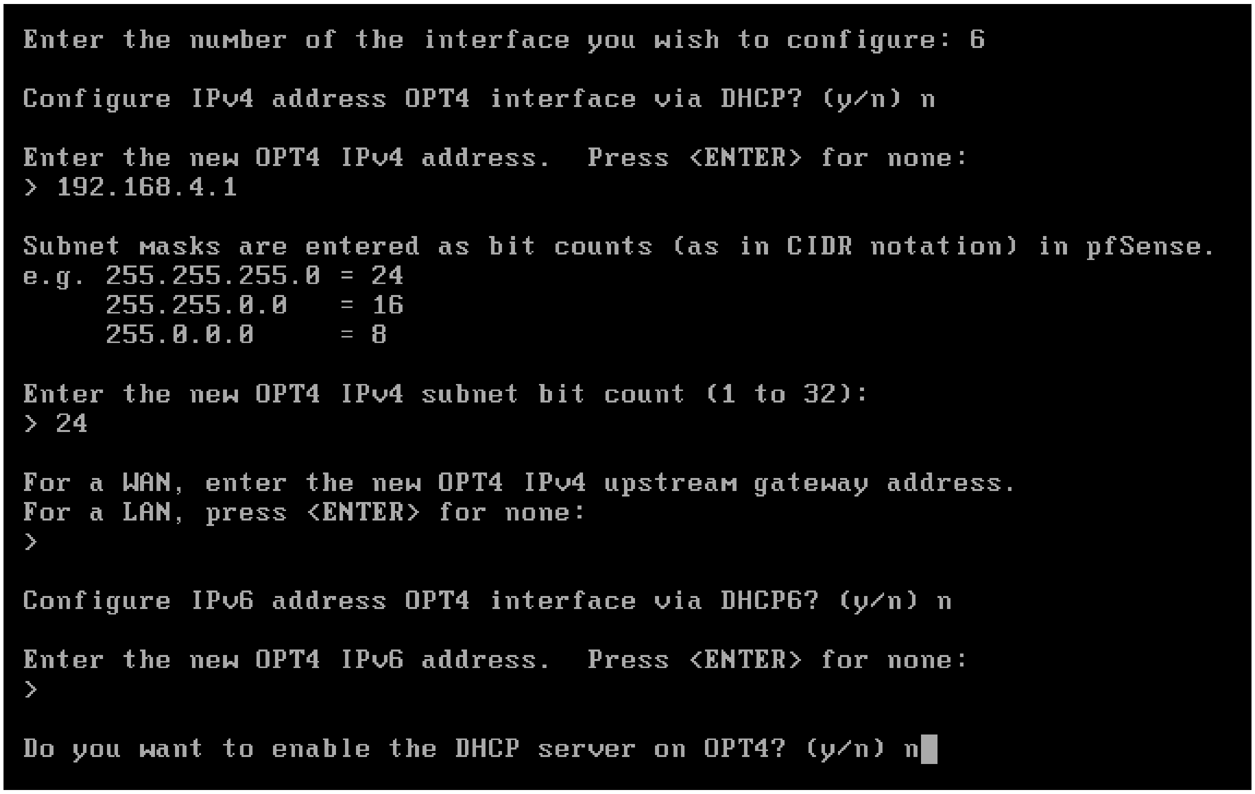


```
Enter the number of the interface you wish to configure: 4

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)
```

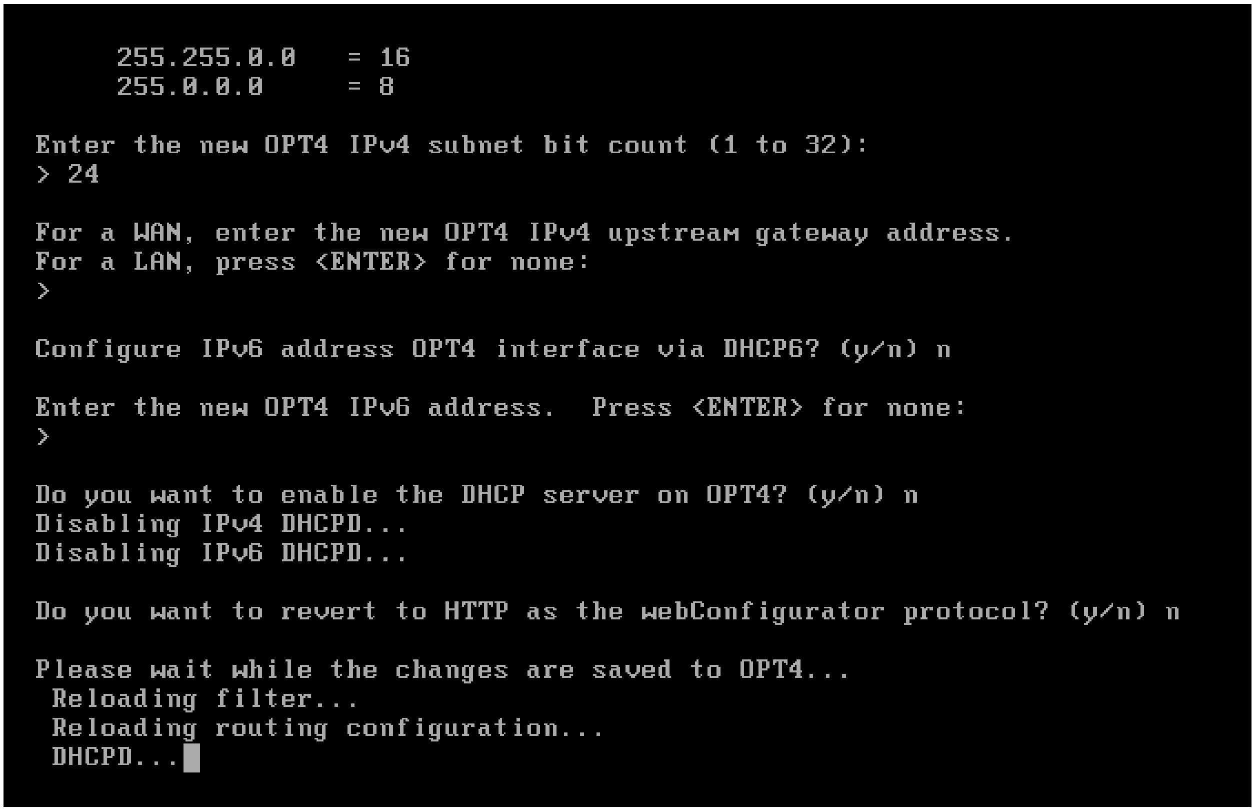


```
Configure IPv6 address OPT2 interface via DHCP6? (y/n) n

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)

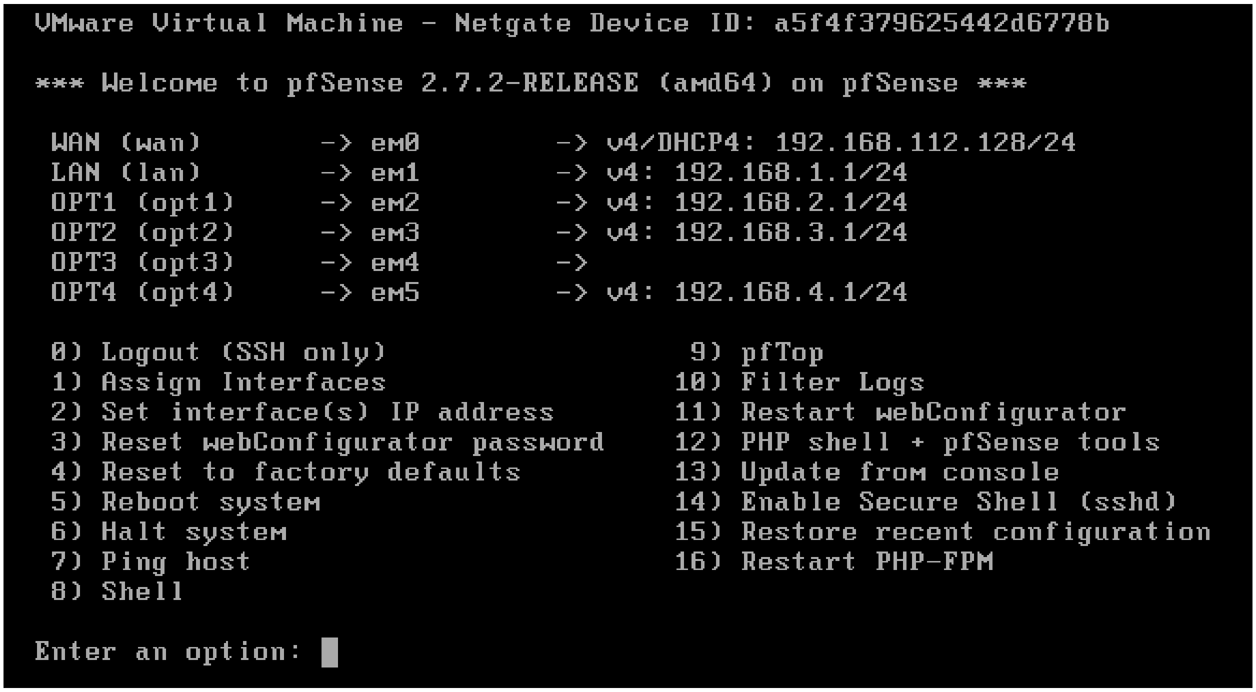


```
Enter the number of the interface you wish to configure: 6

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:

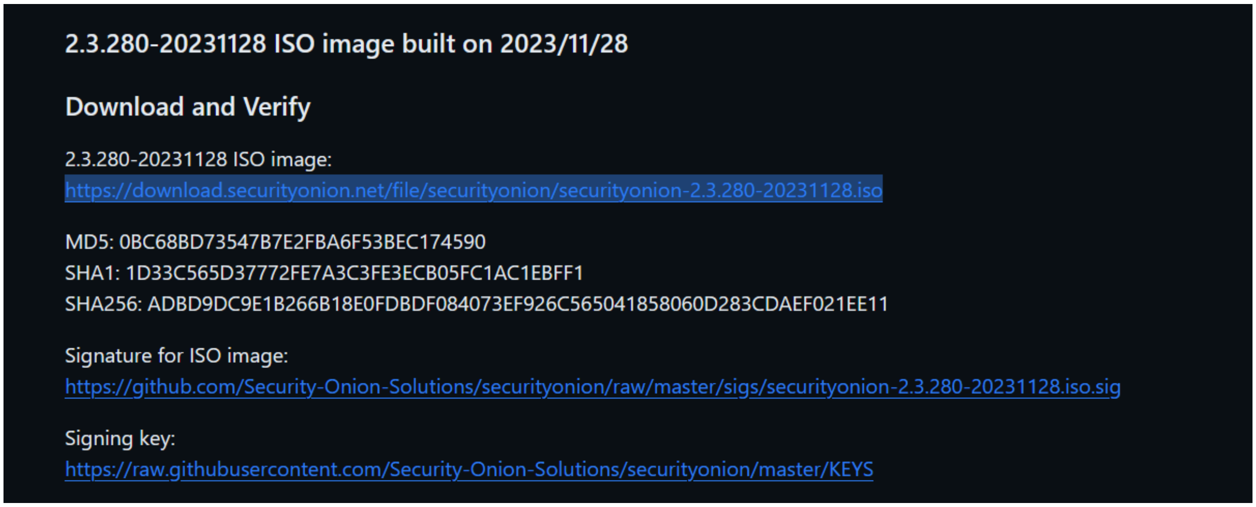


```
VMware Virtual Machine - Netgate Device ID: a5f4f379625442d6778b

*** 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)



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

Download and Verify

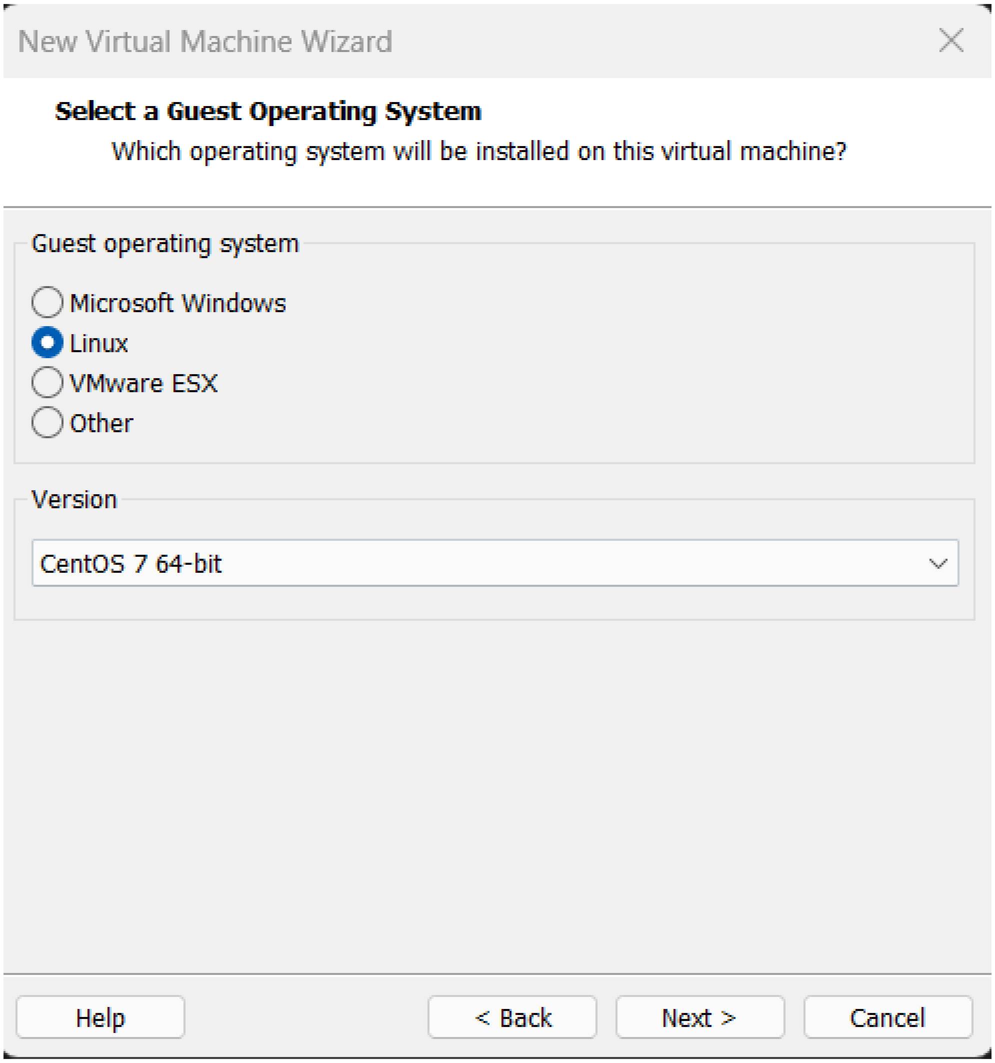
2.3.280-20231128 ISO image:
https://download.securityonion.net/file/securityonion/securityonion-2.3.280-20231128.iso

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?

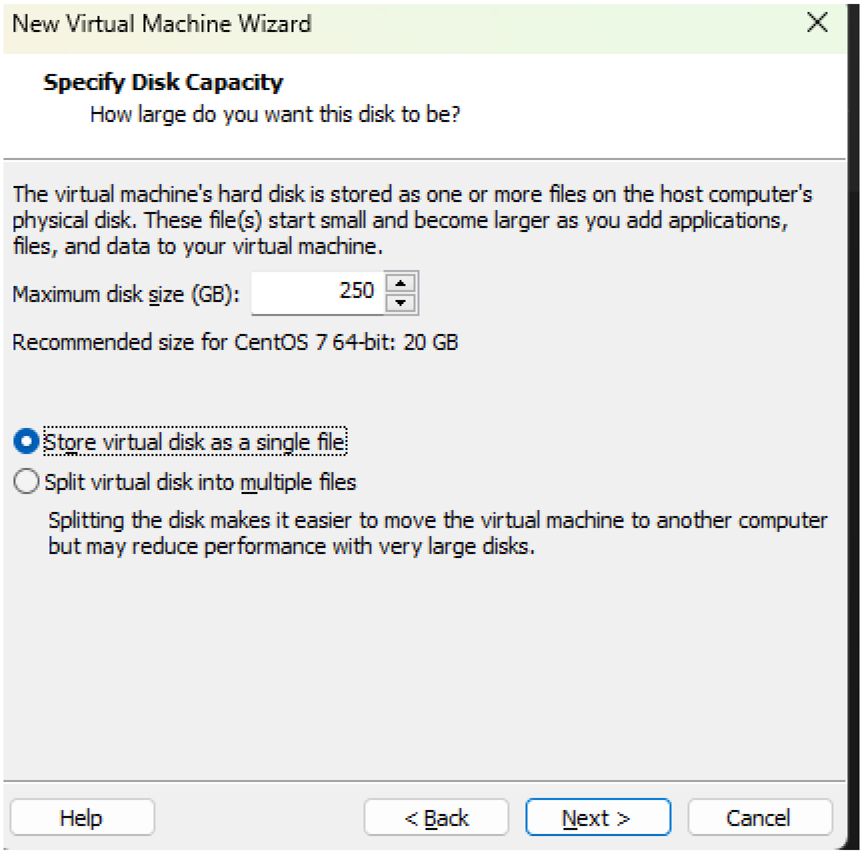
Guest operating system

○ Microsoft Windows
● Linux
○ VMware ESX
○ Other

Version

CentOS 7 64-bit

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



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): 250

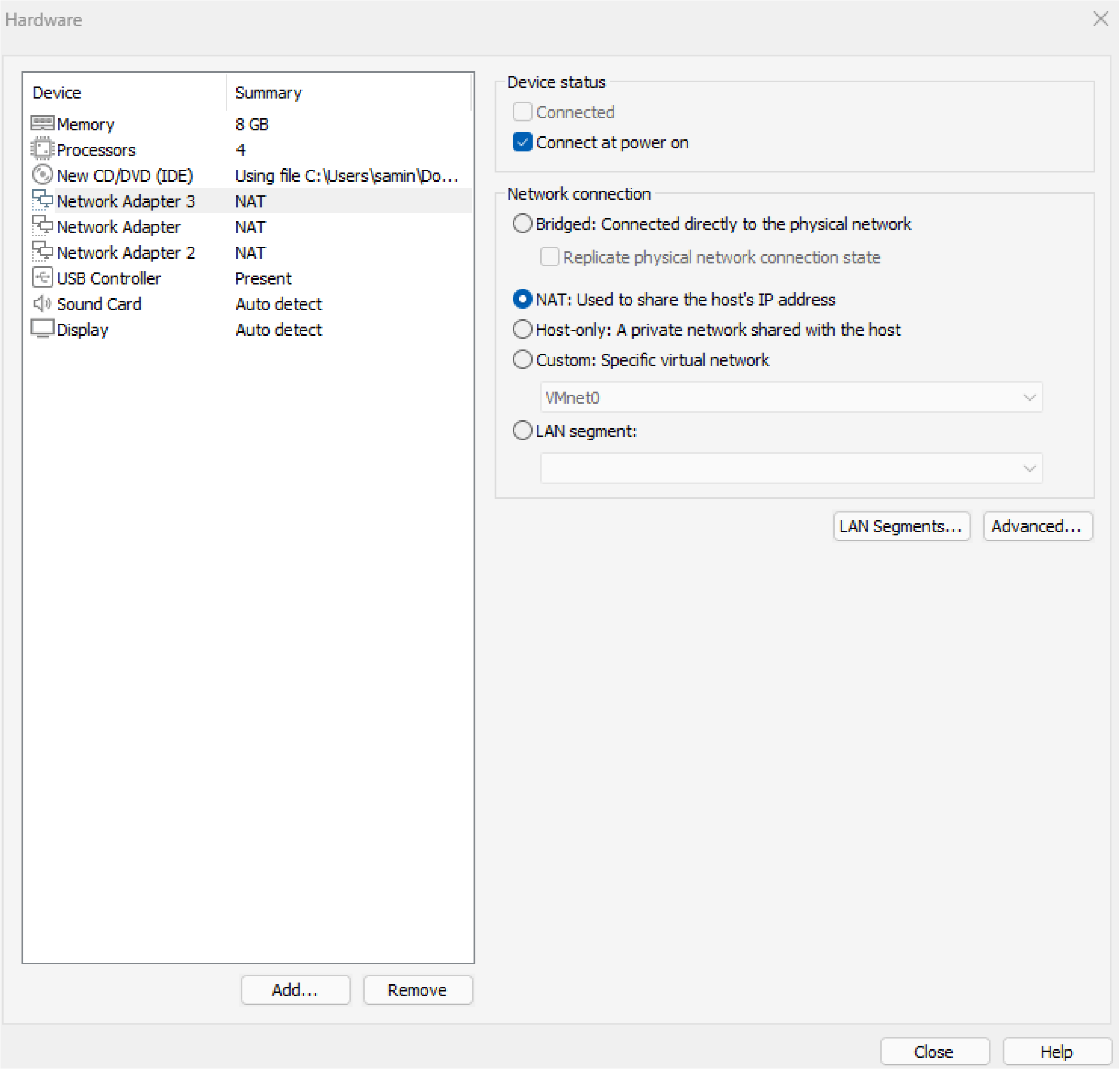
Recommended size for CentOS 7 64-bit: 20 GB

● 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.

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:



Device	Summary
Memory	8 GB
Processors	4
New CD/DVD (IDE)	Using file C:\Users\samin\Do...
Network Adapter 3	NAT
Network Adapter	NAT
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

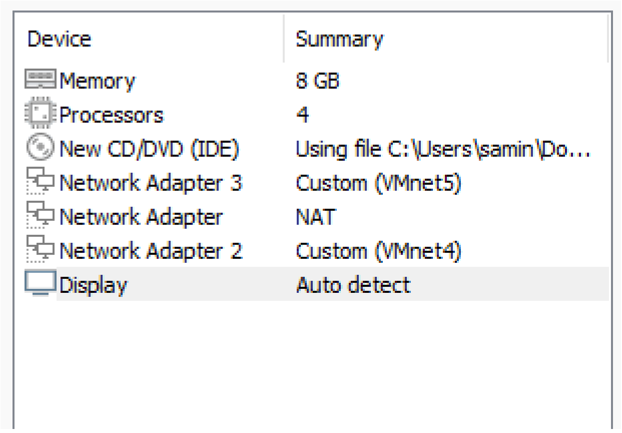
Device status

□ Connected
☑ Connect at power on

Network connection

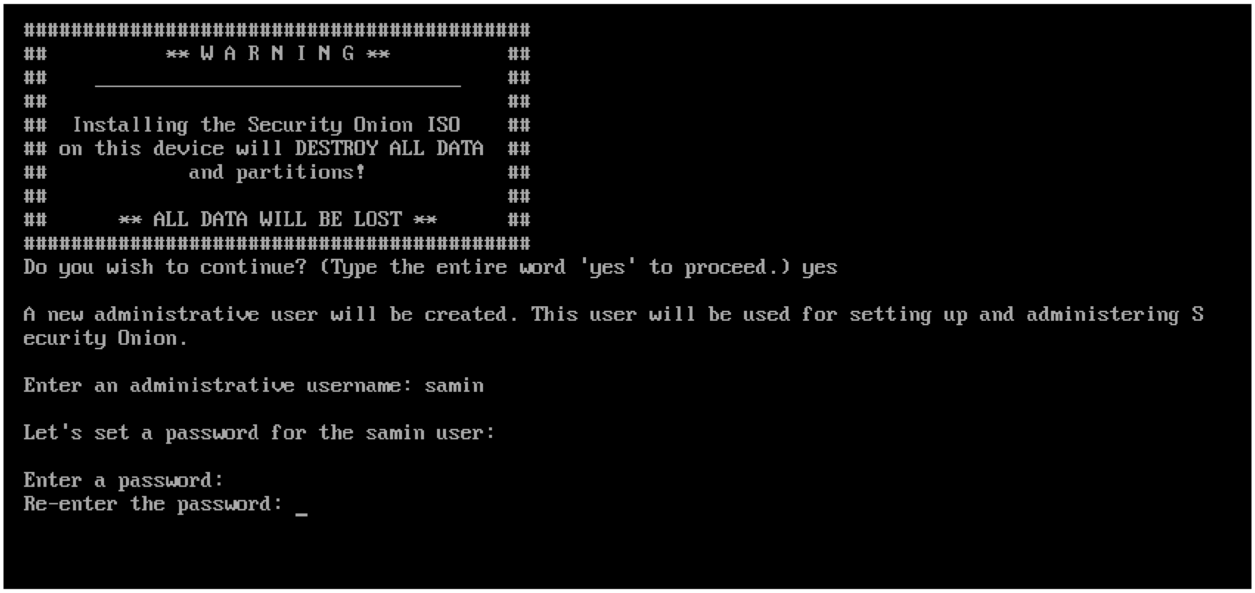
○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
● NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0
○ LAN segment:

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

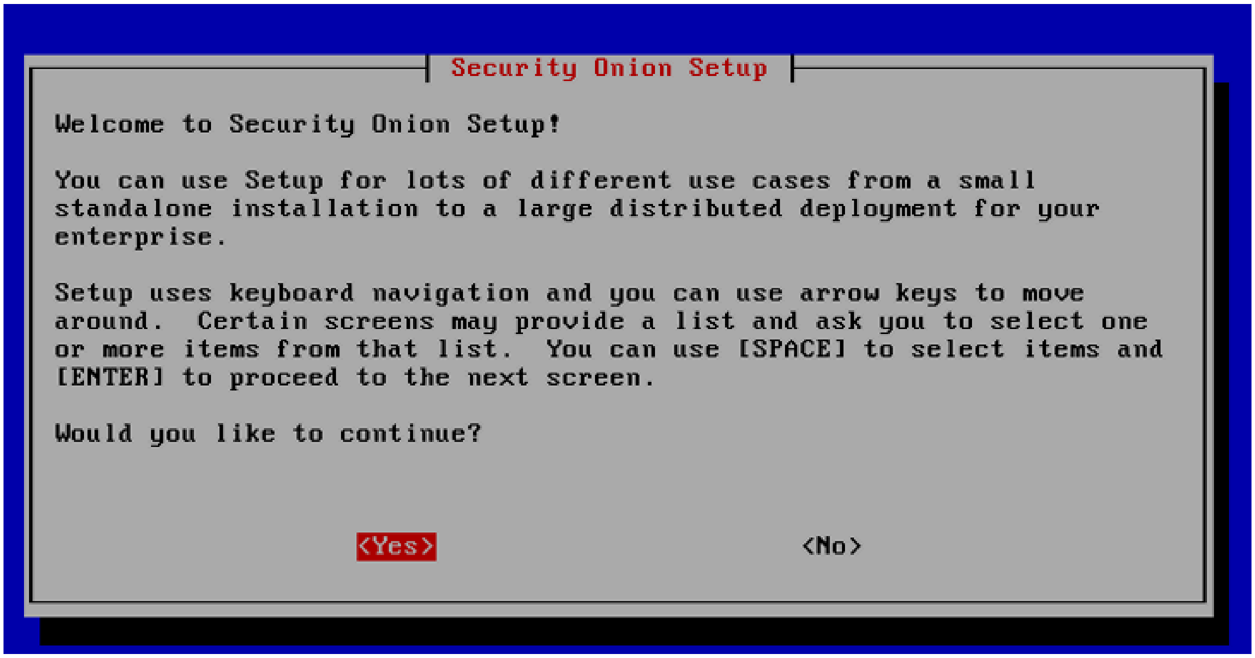
You can click “Close” and then “Finish” before powering on the VM.
Once turned on, let the VM load through everything and then enter “yes” when prompted.
Enter a username and password as prompted as well.



```
###########################################
##          ** 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: _
```

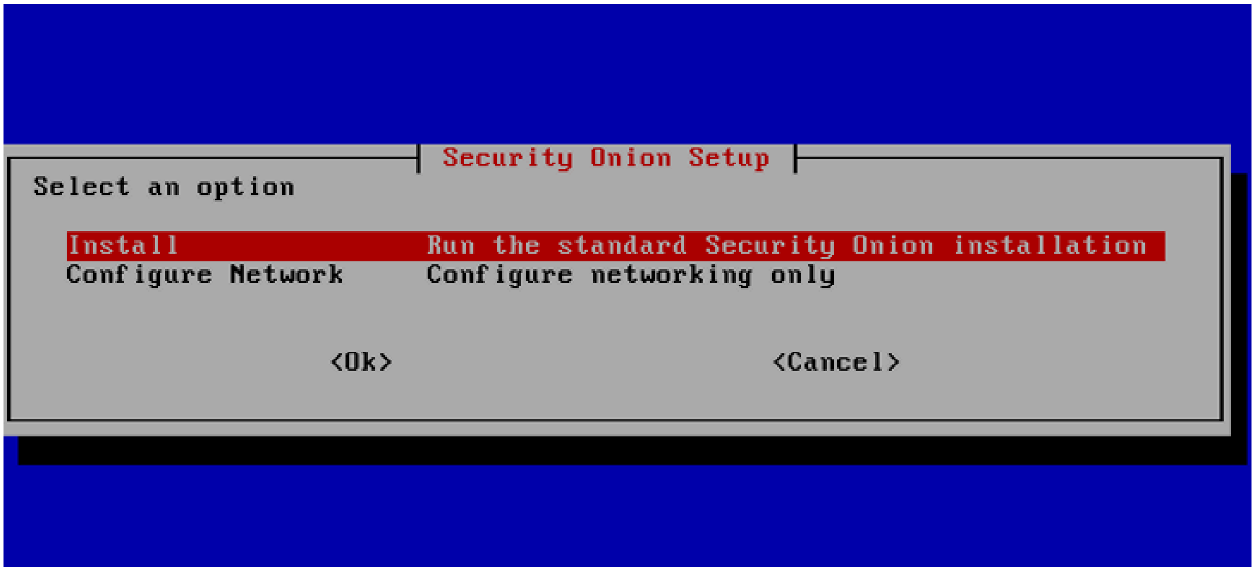
After entering and waiting, press enter when prompted. Enter your login information once you get to the prompt asking you for it.

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



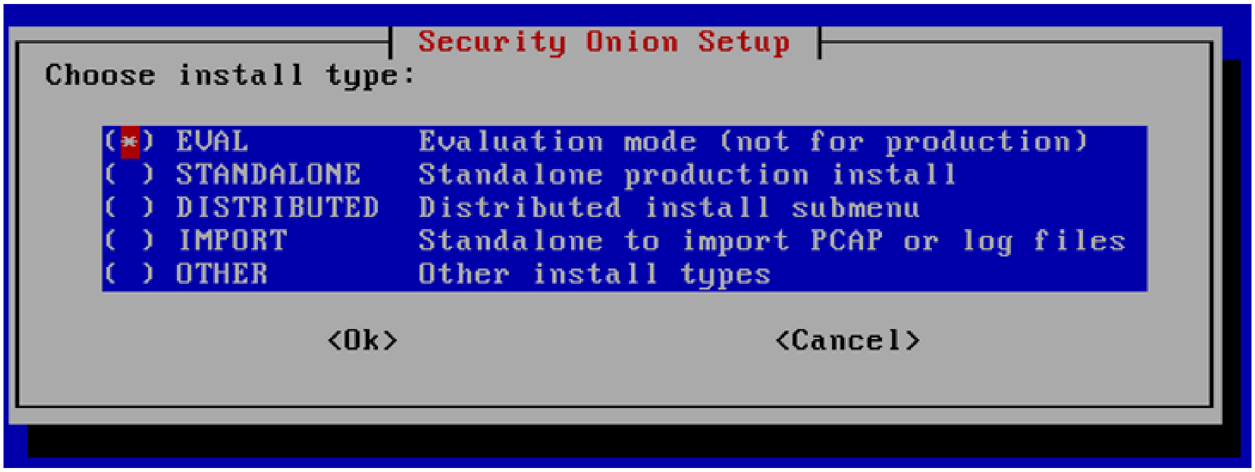
```
Security Onion Setup

Welcome to Security Onion Setup!

You can use Setup for lots of different use cases from a small
standalone installation to a large distributed deployment for your
enterprise.

Setup uses keyboard navigation and you can use arrow keys to move
around.  Certain screens may provide a list and ask you to select one
or more items from that list.  You can use [SPACE] to select items and
[ENTER] to proceed to the next screen.

Would you like to continue?
```

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



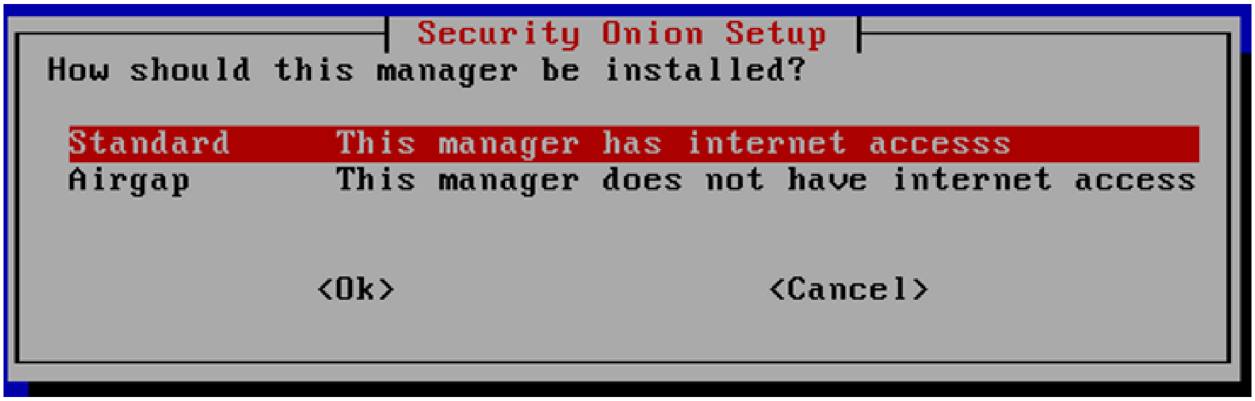
```
Security Onion Setup

Select an option

  Install              Run the standard Security Onion installation
  Configure Network    Configure networking only
```

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



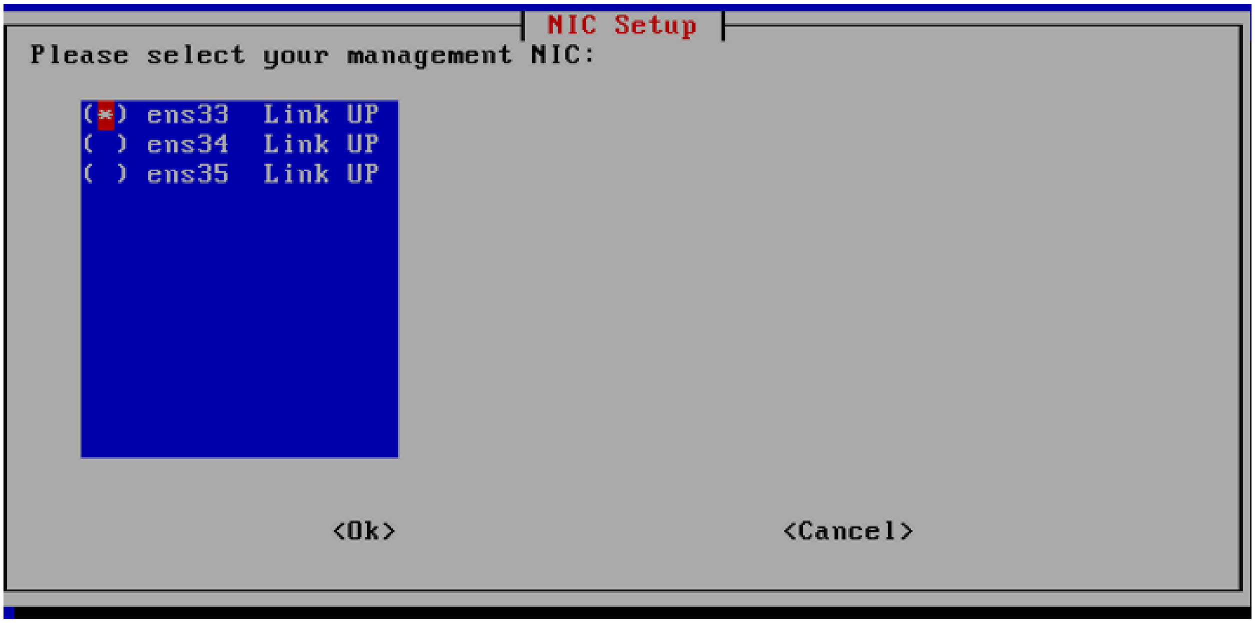
```
Security Onion Setup
Choose install type:

(*) EVAL          Evaluation mode (not for production)
( ) STANDALONE    Standalone production install
( ) DISTRIBUTED   Distributed install submenu
( ) IMPORT        Standalone to import PCAP or log files
( ) OTHER         Other install types

            <Ok>                    <Cancel>
```

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



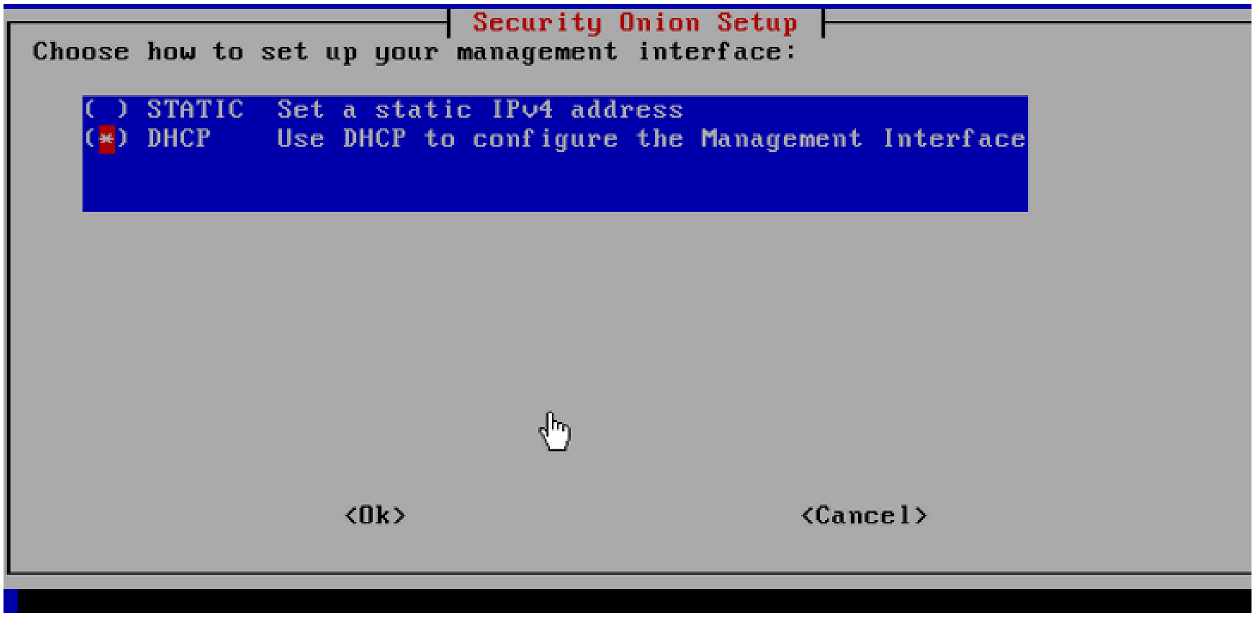
```
Security Onion Setup
How should this manager be installed?

 Standard       This manager has internet accesss
 Airgap         This manager does not have internet access

          <Ok>                    <Cancel>
```

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



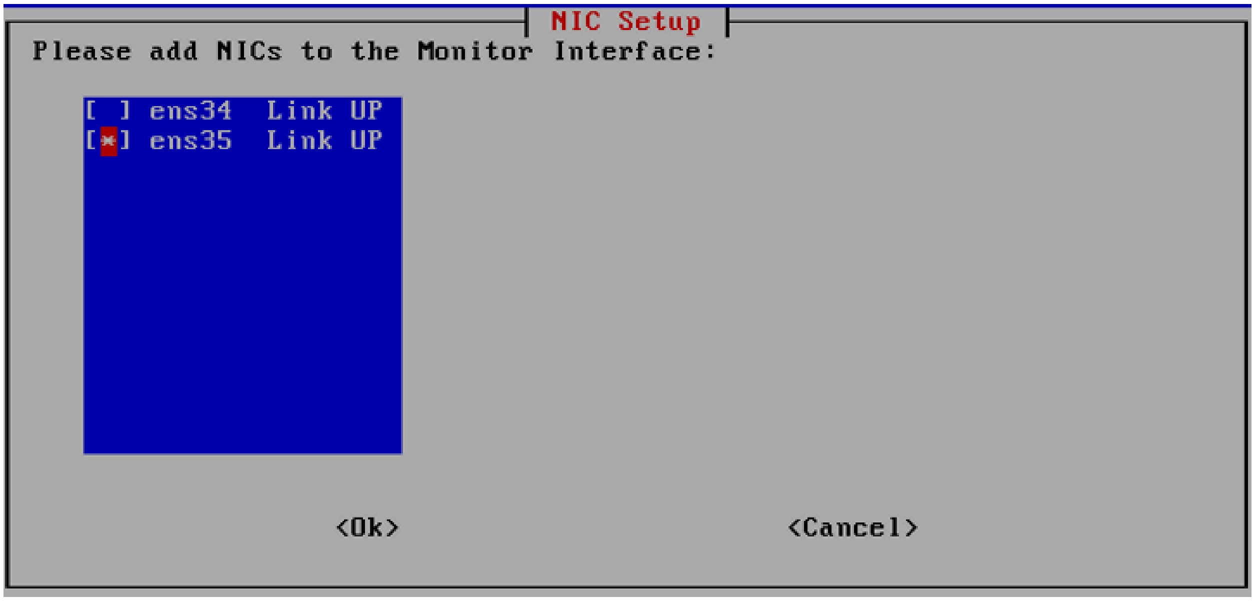
```
NIC Setup
Please select your management NIC:

   (*) ens33   Link UP
   ( ) ens34   Link UP
   ( ) ens35   Link UP

              <Ok>                     <Cancel>
```

Select “DHCP” on the next screen:



```
Security Onion Setup
Choose how to set up your management interface:

( ) STATIC   Set a static IPv4 address
(*) DHCP     Use DHCP to configure the Management Interface

        <Ok>                         <Cancel>
```

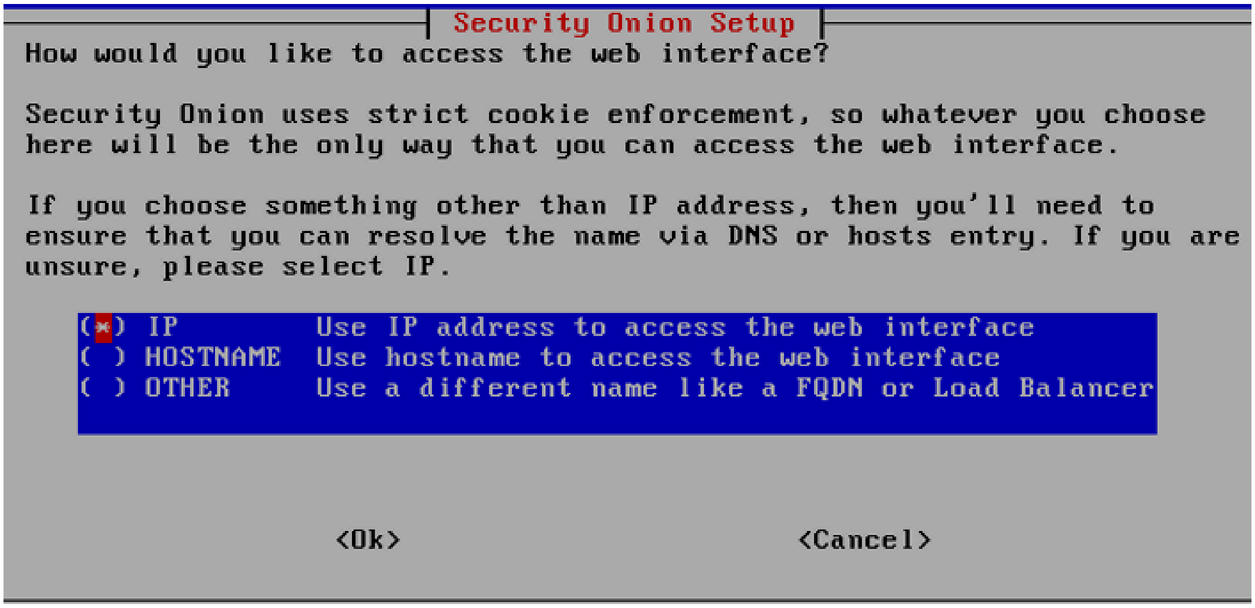
Select “YES”, “OK”, and then “Direct” for the next 3 prompts. Then select “ens35” at the next prompt:



```
NIC Setup
Please add NICs to the Monitor Interface:

[ ] ens34   Link UP
[*] ens35   Link UP

        <Ok>                         <Cancel>
```

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>
```

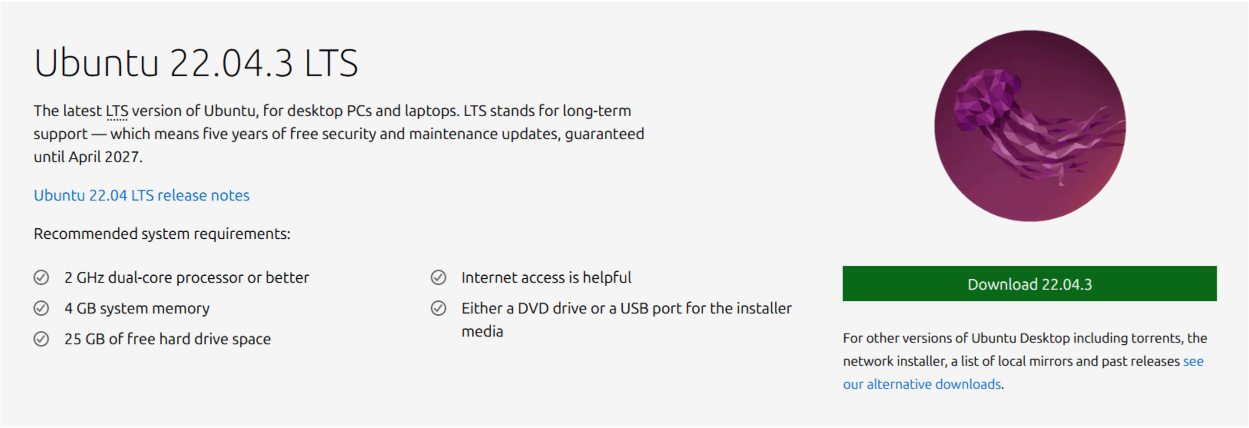
Select "Yes" for the NTP server on the next screen and then select all the default options.

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).

Configure the Security Onion Analyst Machine

Here we will be configuring an Ubuntu machine that will be used to access the Security Onion web interface, simulating how a SOC Analyst would access a SIEM.

First, we download the Ubuntu Desktop image from their website:



Ubuntu 22.04.3 LTS

The latest LTS version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years of free security and maintenance updates, guaranteed until April 2027.

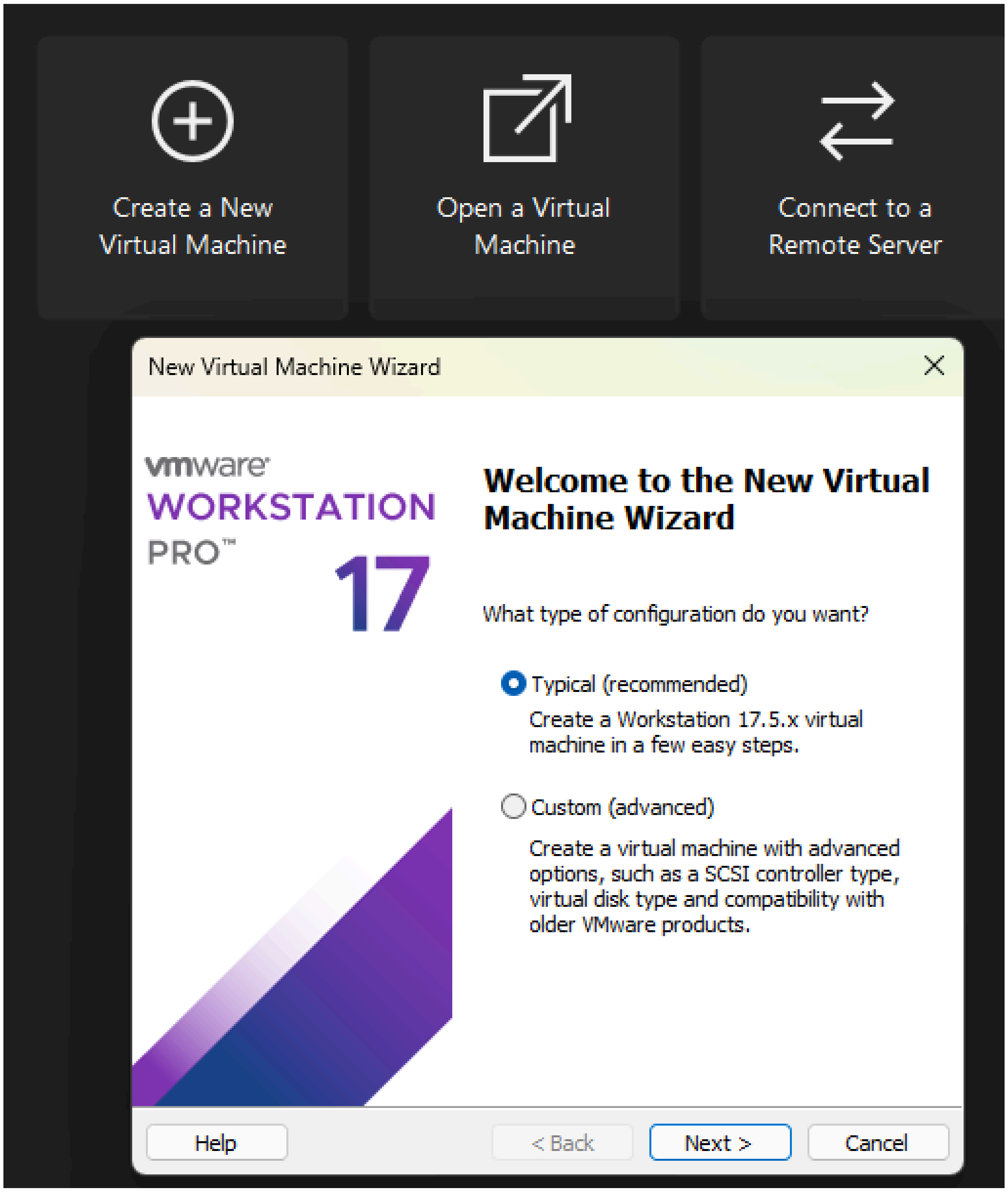
Ubuntu 22.04 LTS release notes

Recommended system requirements:

- 2 GHz dual-core processor or better
- 4 GB system memory
- 25 GB of free hard drive space
- Internet access is helpful
- Either a DVD drive or a USB port for the installer media

For other versions of Ubuntu Desktop including torrents, the network installer, a list of local mirrors and past releases see our alternative downloads.

On VMware, create a new virtual machine with typical selected before clicking “Next”:



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

What type of configuration do you want?

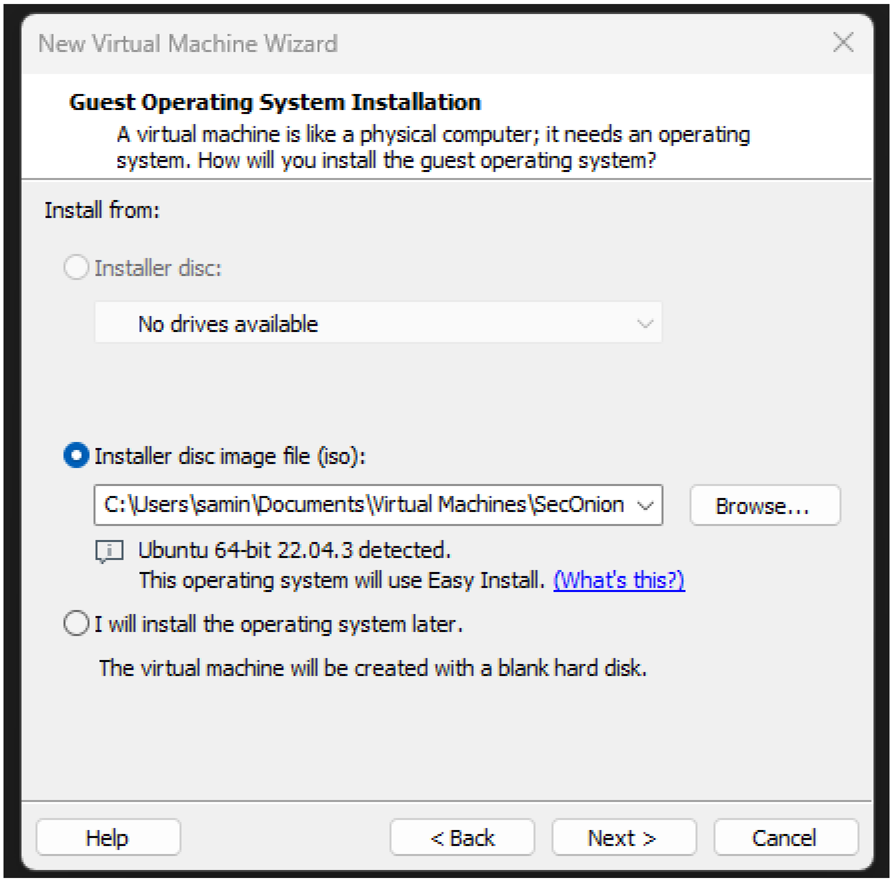
● Typical (recommended)

Create a Workstation 17.5.x virtual machine in a few easy steps.

○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Select the disk image from where you downloaded it before clicking “Next”:



Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

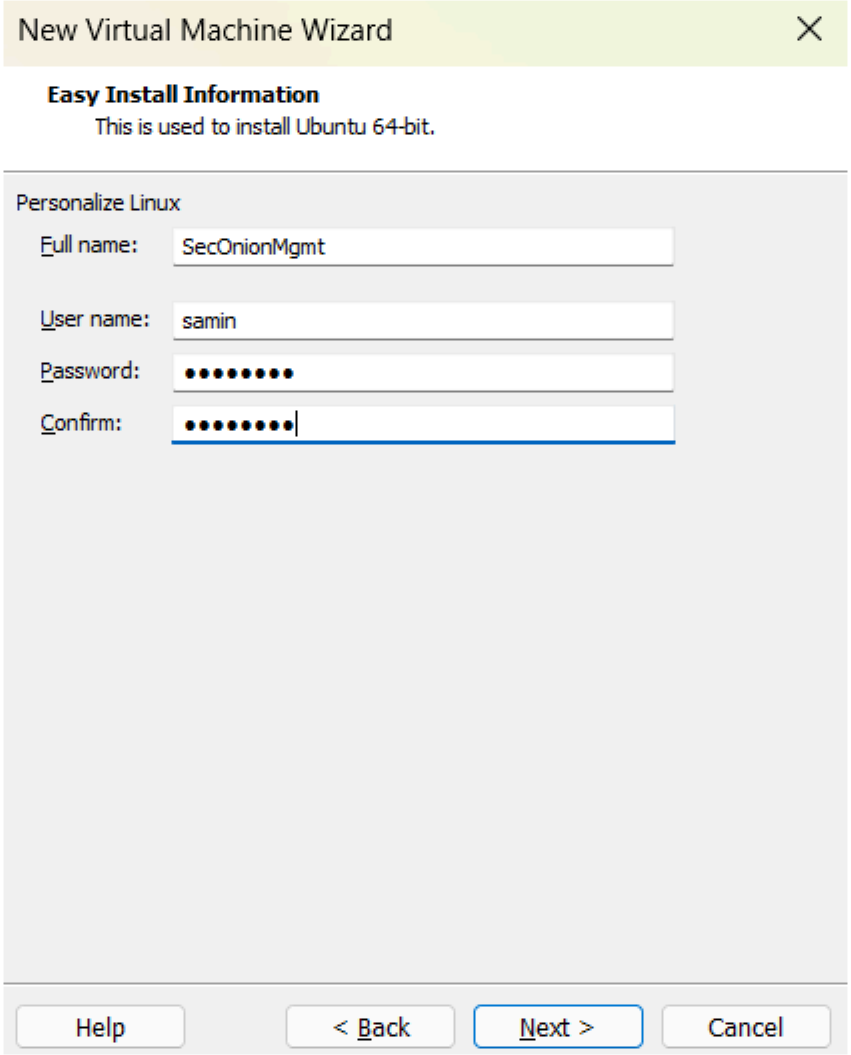
C:\Users\samin\Documents\Virtual Machines\SecOnion

Ubuntu 64-bit 22.04.3 detected.
This operating system will use Easy Install. (What's this?)

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Fill in the fields as you choose, then click “Next”:



New Virtual Machine Wizard

Easy Install Information

This is used to install Ubuntu 64-bit.

Personalize Linux

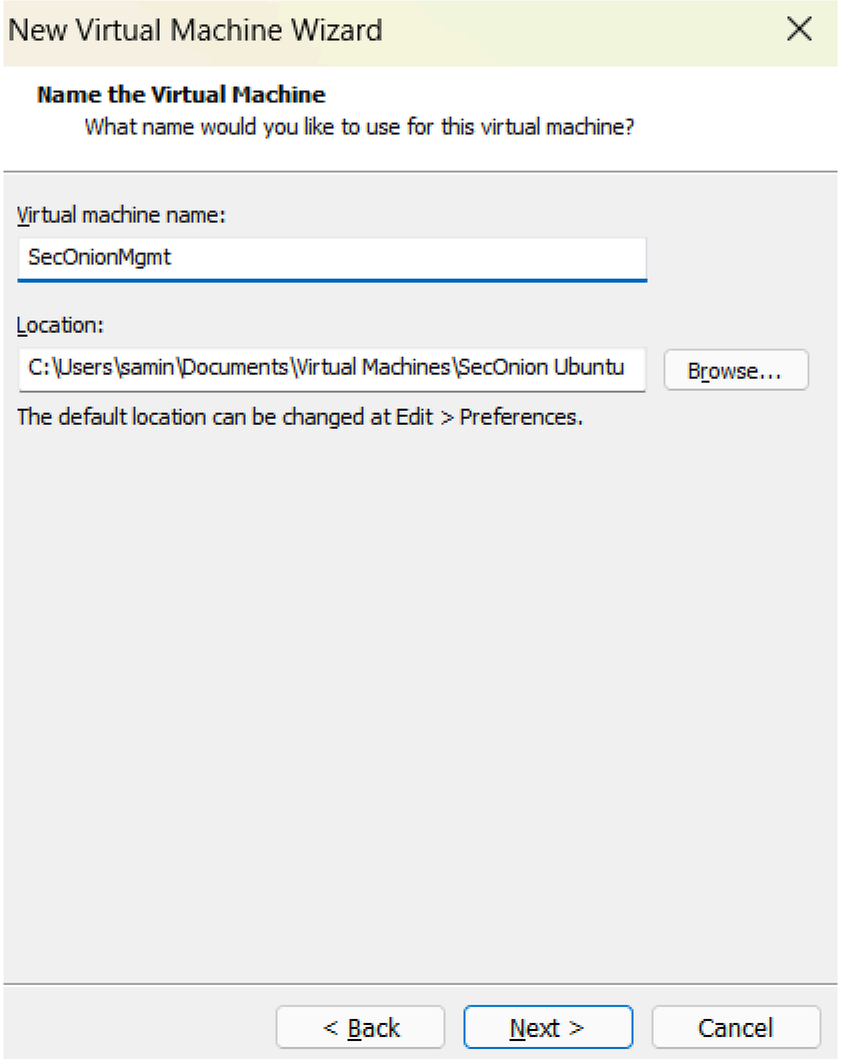
Full name: SecOnionMgmt

User name: samin

Password: ●●●●●●●●

Confirm: ●●●●●●●●

Give the machine a name and choose the location to store it before clicking “Next”:



Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

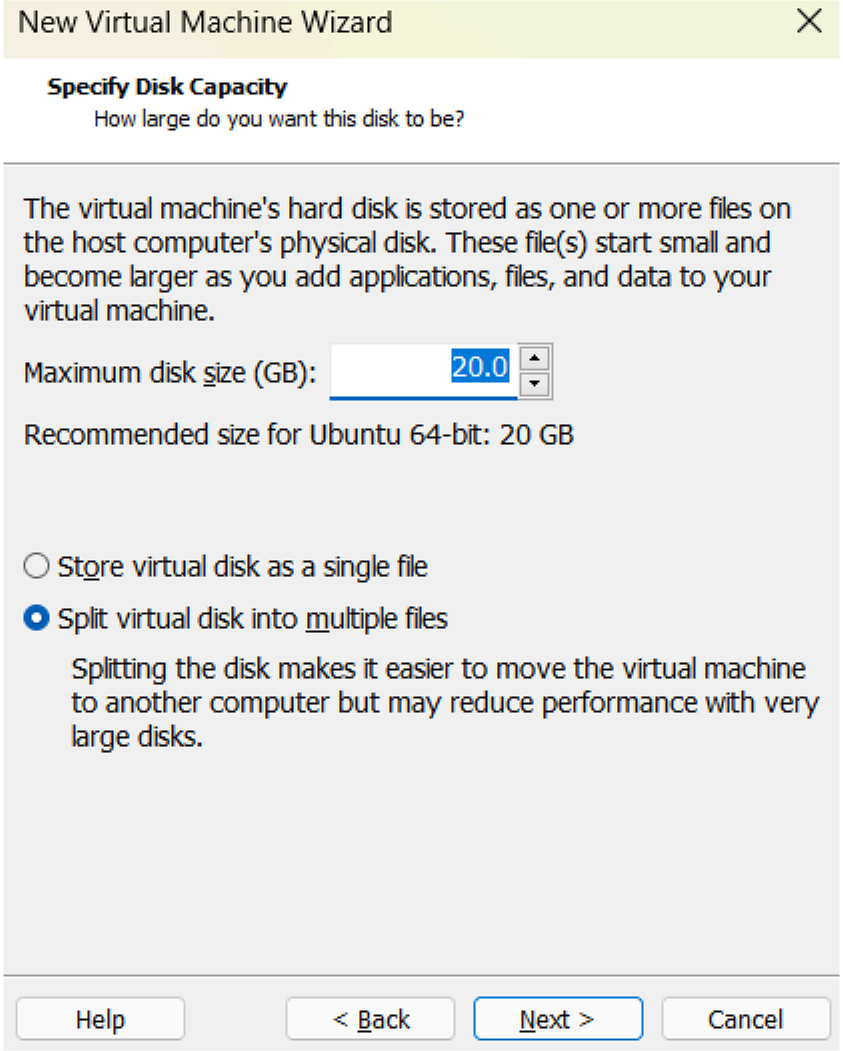
SecOnionMgmt

Location:

C:\Users\samin\Documents\Virtual Machines\SecOnion Ubuntu

The default location can be changed at Edit > Preferences.

The next two screens you can leave at the defaults:



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.

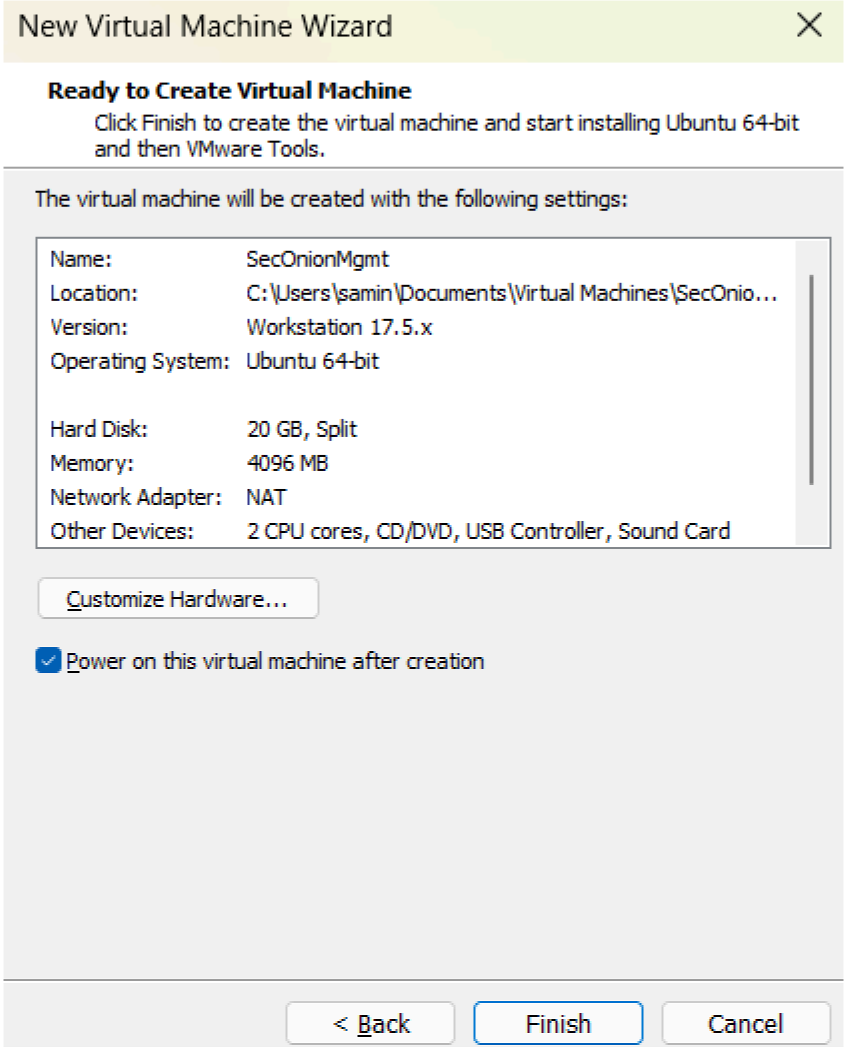
Maximum disk size (GB): 20.0

Recommended size for Ubuntu 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.



Ready to Create Virtual Machine

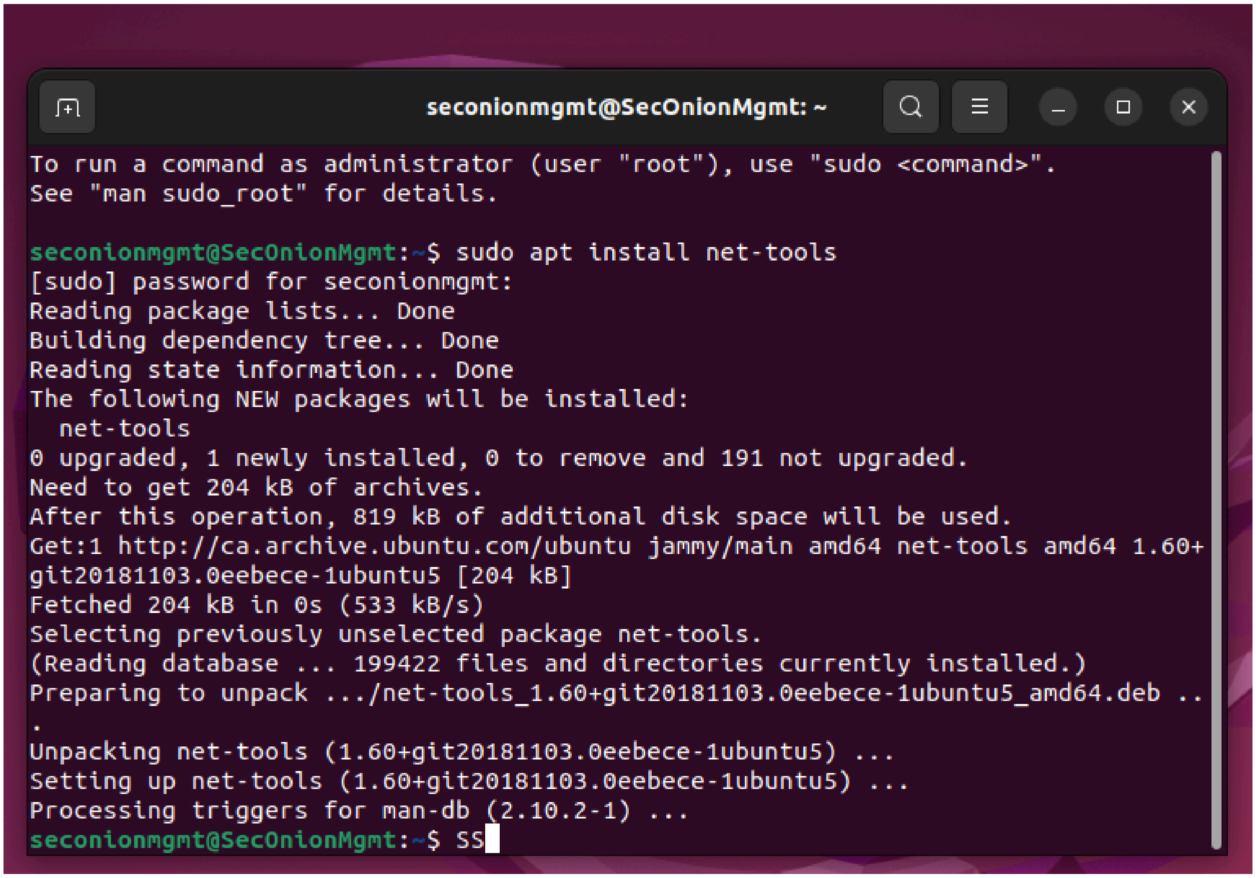
Click Finish to create the virtual machine and start installing Ubuntu 64-bit and then VMware Tools.

The virtual machine will be created with the following settings:

Name:	SecOnionMgmt
Location:	C:\Users\samin\Documents\Virtual Machines\SecOnio...
Version:	Workstation 17.5.x
Operating System:	Ubuntu 64-bit
Hard Disk:	20 GB, Split
Memory:	4096 MB
Network Adapter:	NAT
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Sound Card

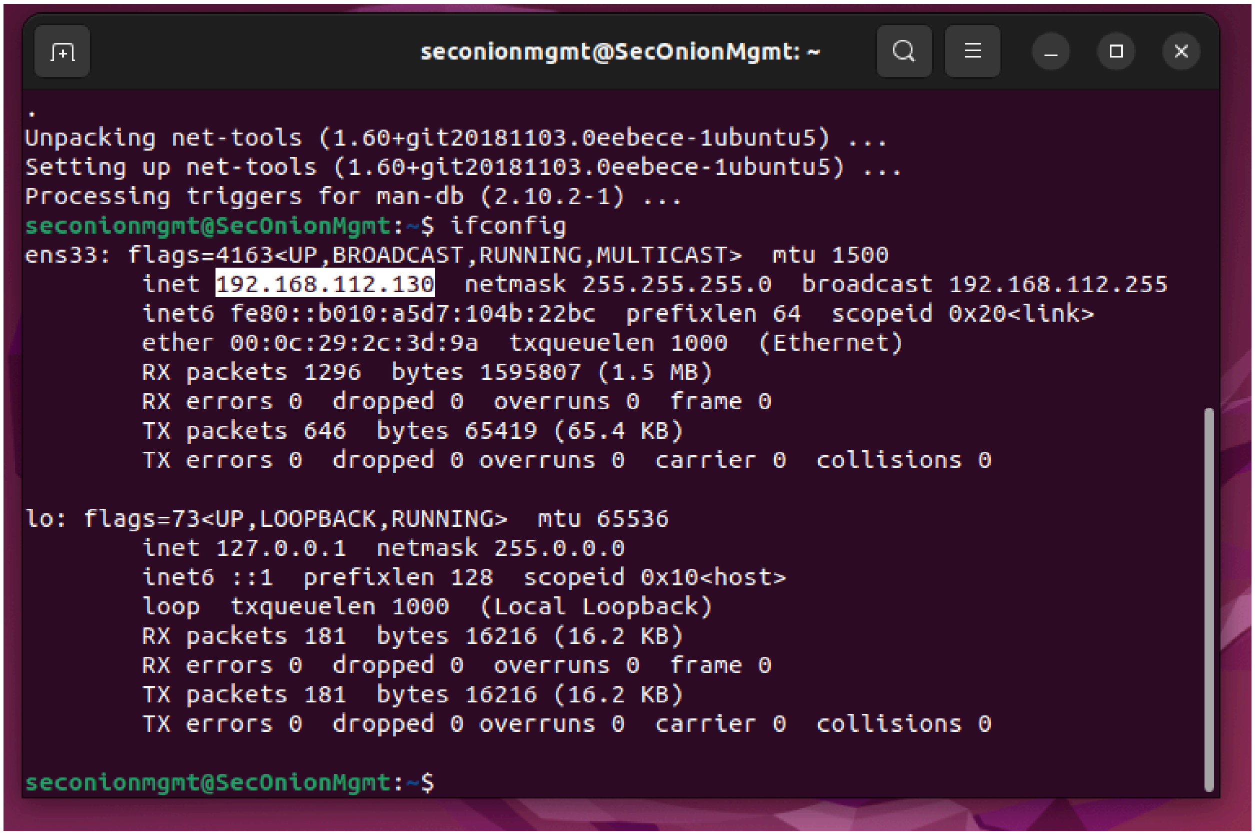
☑ Power on this virtual machine after creation

Load up the virtual machine and configure it as you wish; for this lab, all the default options were used (ignore any warnings about overwriting the defaults). Once you are able to log into the machine, open up a terminal and enter “sudo apt install net-tools”:



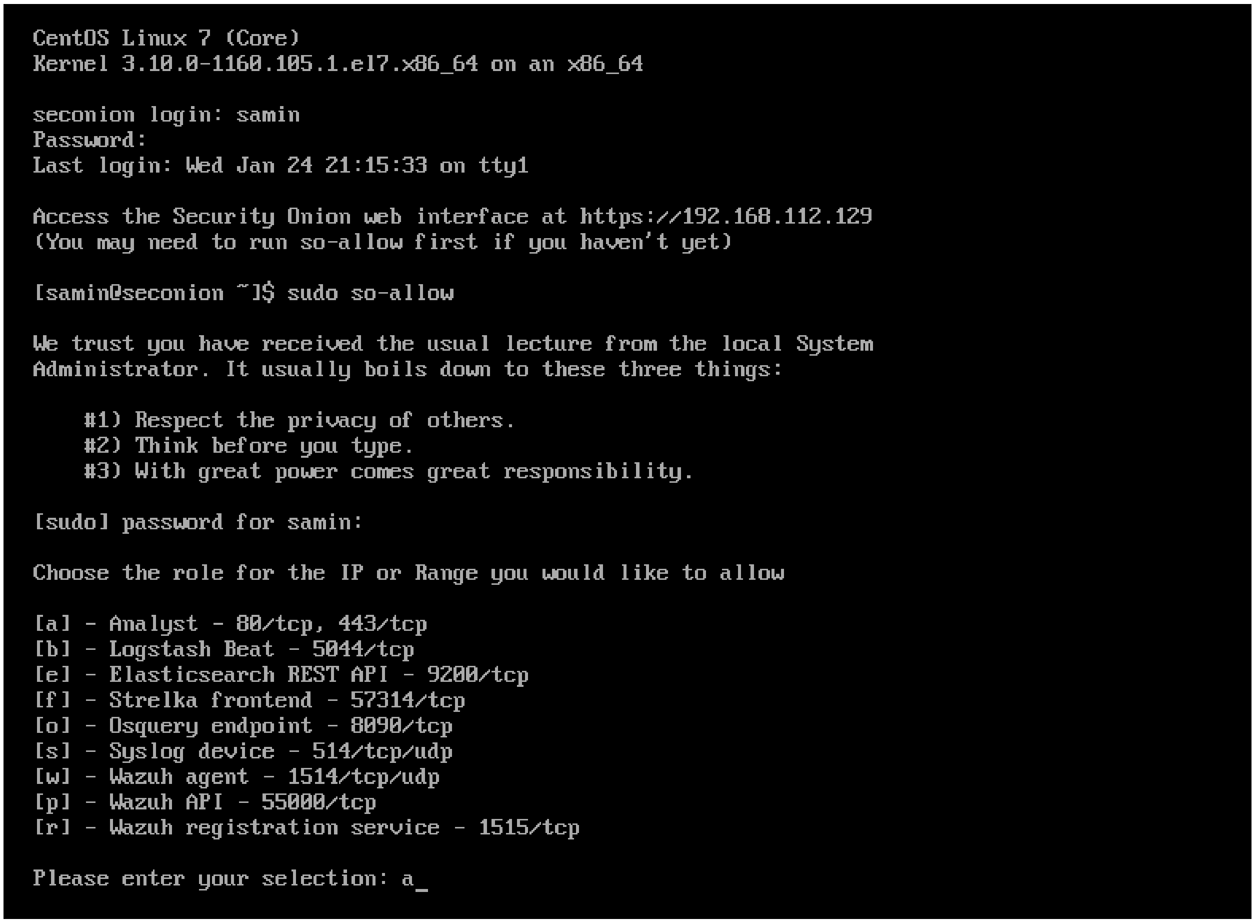
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

seconionmgmt@SecOnionMgmt:~$ sudo apt install net-tools
[sudo] password for seconionmgmt:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 191 not upgraded.
Need to get 204 kB of archives.
After this operation, 819 kB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+
git20181103.0eebece-1ubuntu5 [204 kB]
Fetched 204 kB in 0s (533 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 199422 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ..
.
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-1) ...
seconionmgmt@SecOnionMgmt:~$ SS
```

Run “ifconfig” next and then note the following IP address:



```
.
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-1) ...
seconionmgmt@SecOnionMgmt:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.112.130  netmask 255.255.255.0  broadcast 192.168.112.255
        inet6 fe80::b010:a5d7:104b:22bc  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2c:3d:9a  txqueuelen 1000  (Ethernet)
        RX packets 1296  bytes 1595807 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 646  bytes 65419 (65.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 181  bytes 16216 (16.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 181  bytes 16216 (16.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

seconionmgmt@SecOnionMgmt:~$
```

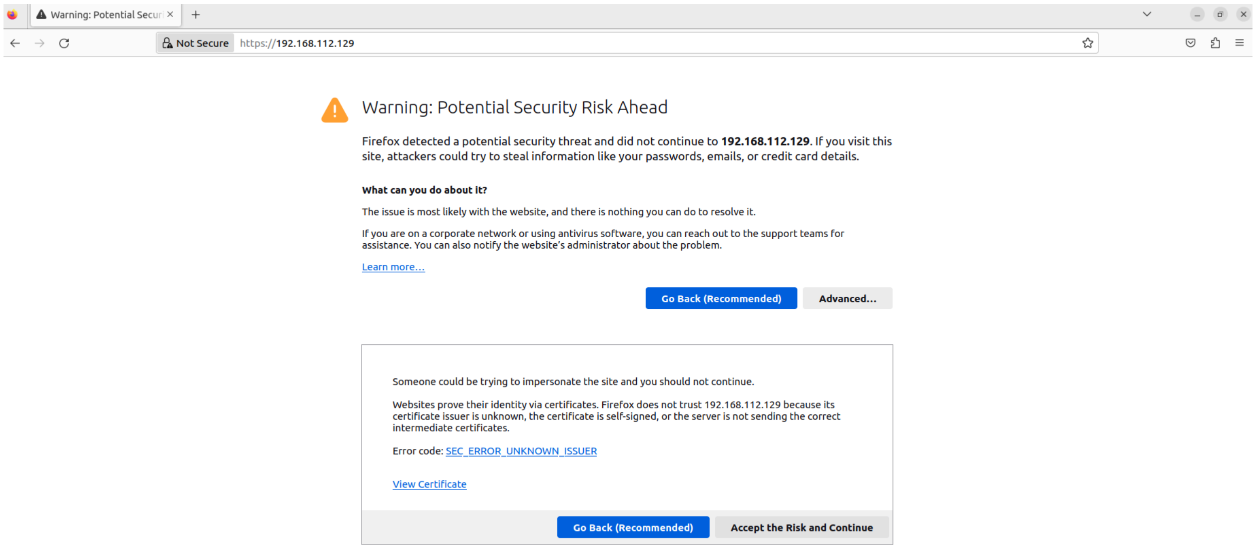
Now, log into the Sec Onion machine and enter “sudo so-allow”, then enter “a”:



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.105.1.el7.x86_64 on an x86_64

seconion login: samin
Password:
Last login: Wed Jan 24 21:15:33 on tty1

Access the Security Onion web interface at https://192.168.112.129
(You may need to run so-allow first if you haven't yet)

[samin@seconion ~]$ sudo so-allow

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for samin:

Choose the role for the IP or Range you would like to allow

[a] - Analyst - 80/tcp, 443/tcp
[b] - Logstash Beat - 5044/tcp
[e] - Elasticsearch REST API - 9200/tcp
[f] - Strelka frontend - 57314/tcp
[o] - Osquery endpoint - 8090/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection: a_
```

When prompted, enter in the the IP address of the Ubuntu Desktop noted above (this will allow traffic from your Ubuntu machine through to the Security Onion web instance).

Now navigate to the access URL of the Security Onion machine noted previously from the Ubuntu Desktop. You will be warned about a potential security risk, but you can ignore that and continue to the login page where you will be prompted to login with the email and password you defined earlier on:



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **192.168.112.129**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

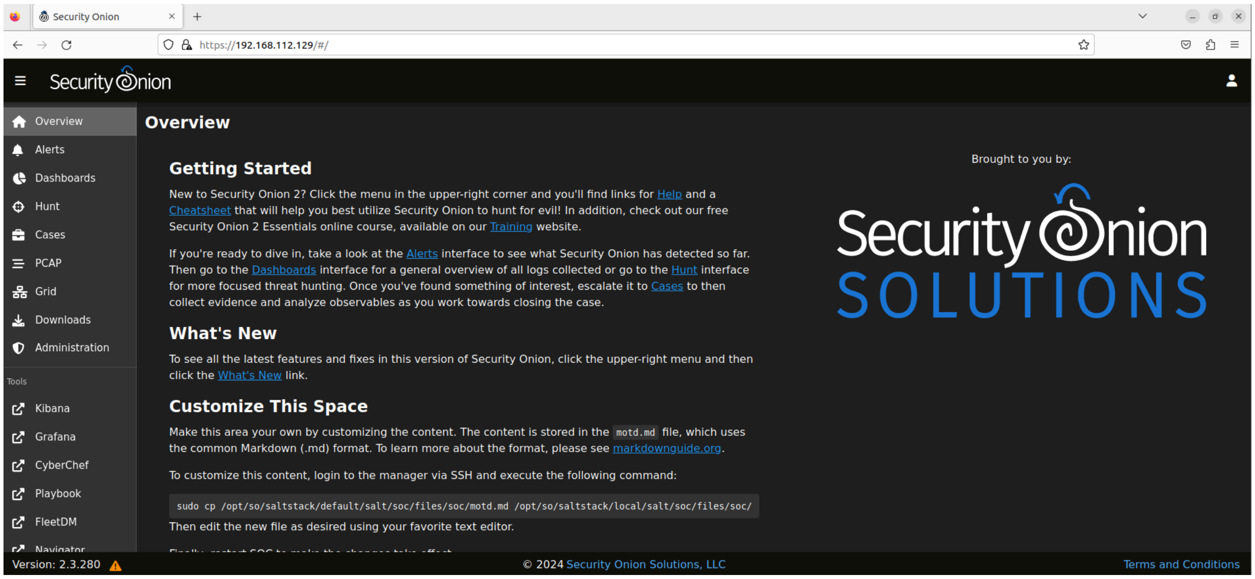
Learn more…

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.112.129 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate



Overview

Getting Started

New to Security Onion 2? Click the menu in the upper-right corner and you'll find links for Help and a Cheatsheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion 2 Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. Then go to the Dashboards interface for a general overview of all logs collected or go to the Hunt interface for more focused threat hunting. Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

What's New

To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

Customize This Space

Make this area your own by customizing the content. The content is stored in the `motd.md` file, which uses the common Markdown (.md) format. To learn more about the format, please see markdownguide.org.

To customize this content, login to the manager via SSH and execute the following command:

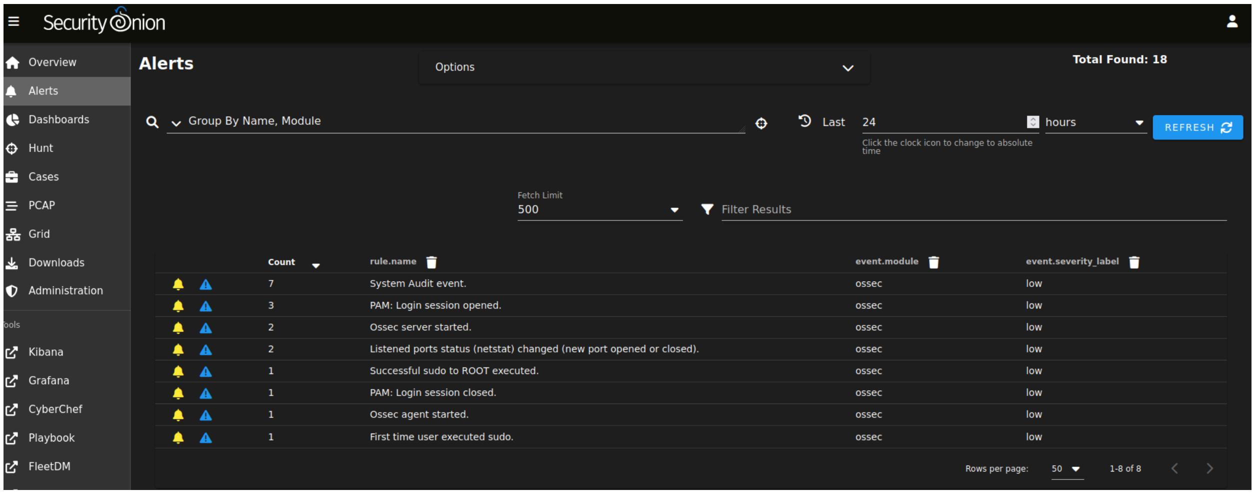
```
sudo cp /opt/so/saltstack/default/salt/soc/files/soc/motd.md /opt/so/saltstack/local/salt/soc/files/soc/
```

Then edit the new file as desired using your favorite text editor.

Finally, restart SOC to make the changes take effect.

Version: 2.3.280 ⚠ © 2024 Security Onion Solutions, LLC Terms and Conditions

From here, you navigate between the tabs on the left side to see the “Alerts”, “Dashboards”, and “Hunt” pages, among others; tools like Kibana and Grafana can also be opened from this sidebar (you may be prompted to log in with your email again when opening up tools like Kibana):



Alerts

Total Found: 18

Group By Name, Module

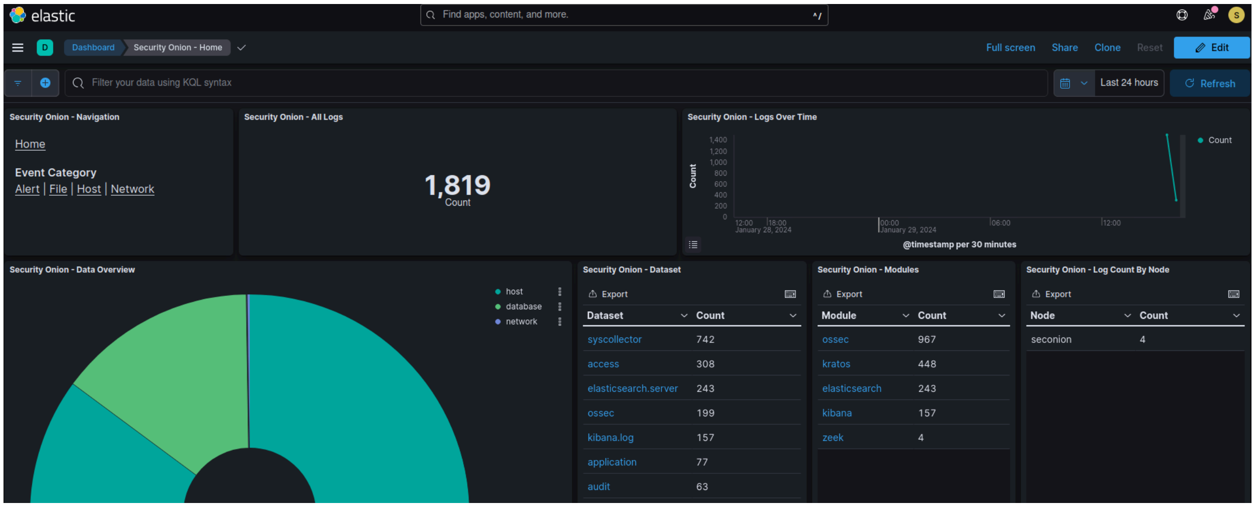
Last 24 hours

Fetch Limit 500

Filter Results

Count	rule.name	event.module	event.severity_label
7	System Audit event.	ossec	low
3	PAM: Login session opened.	ossec	low
2	Ossec server started.	ossec	low
2	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
1	Successful sudo to ROOT executed.	ossec	low
1	PAM: Login session closed.	ossec	low
1	Ossec agent started.	ossec	low
1	First time user executed sudo.	ossec	low

Rows per page: 50 1-8 of 8



Security Onion - Navigation

Home

Event Category

Alert | File | Host | Network

Security Onion - All Logs

1,819
Count

Security Onion - Logs Over Time

Security Onion - Data Overview

Security Onion - Dataset

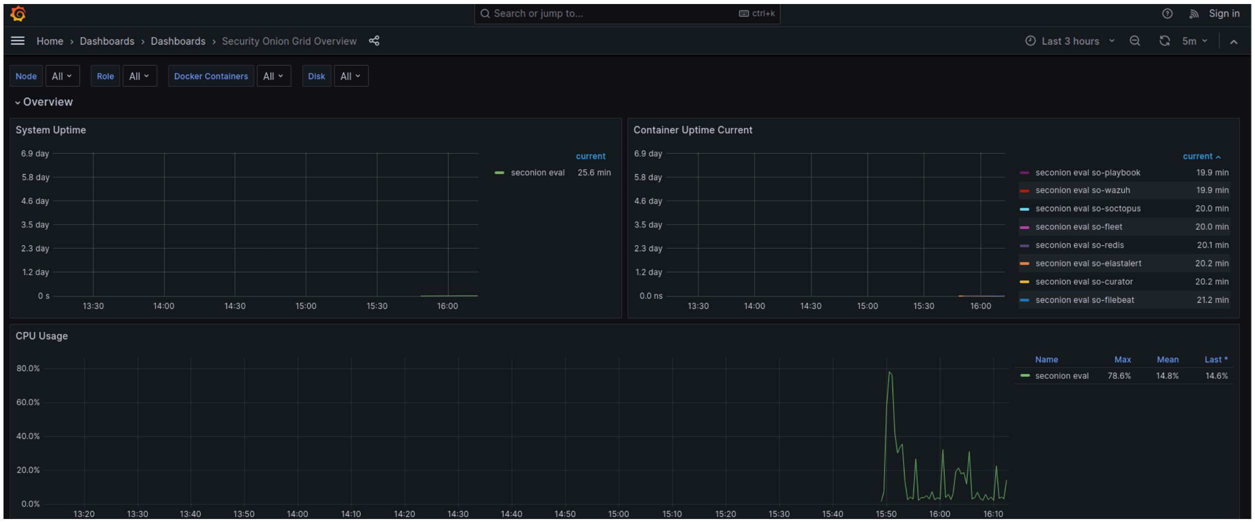
Dataset	Count
syscollector	742
access	308
elasticsearch.server	243
ossec	199
kibana.log	157
application	77
audit	63

Security Onion - Modules

Module	Count
ossec	967
kratos	448
elasticsearch	243
kibana	157
zeek	4

Security Onion - Log Count By Node

Node	Count
seconion	4



Home › Dashboards › Dashboards › Security Onion Grid Overview

Node: All   Role: All   Docker Containers: All   Disk: All

Overview

System Uptime

	current
seconion eval	25.6 min

Container Uptime Current

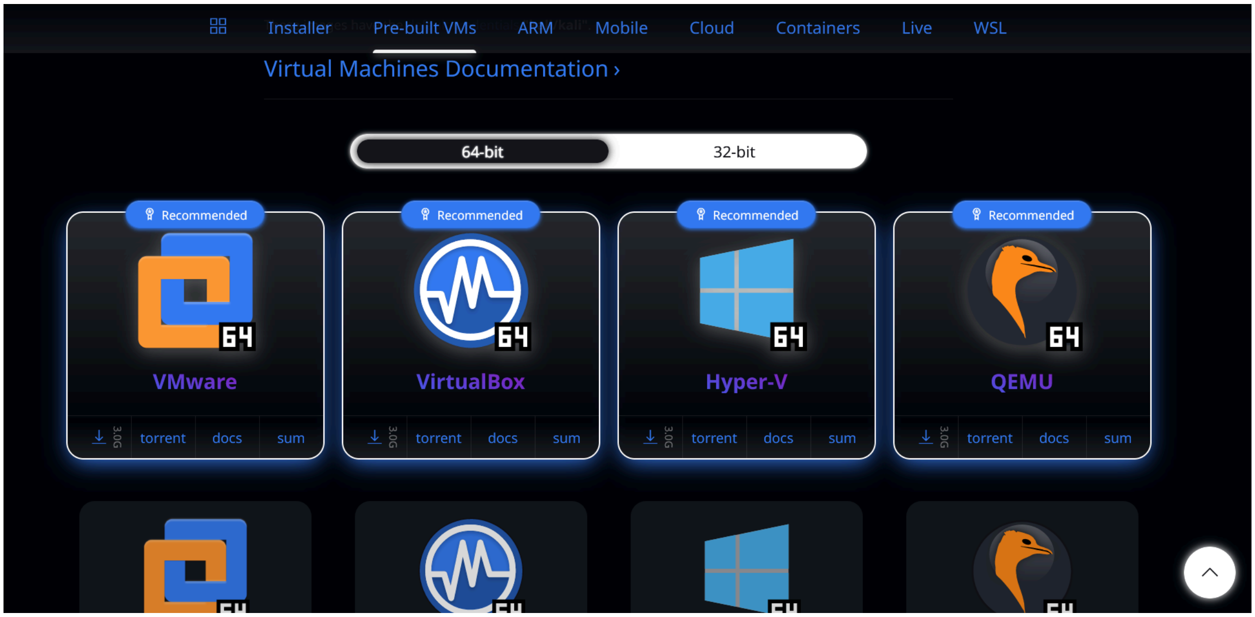
	current
seconion eval so-playbook	19.9 min
seconion eval so-wazuh	19.9 min
seconion eval so-soctopus	20.0 min
seconion eval so-fleet	20.0 min
seconion eval so-redis	20.1 min
seconion eval so-elastalert	20.2 min
seconion eval so-curator	20.2 min
seconion eval so-filebeat	21.2 min

CPU Usage

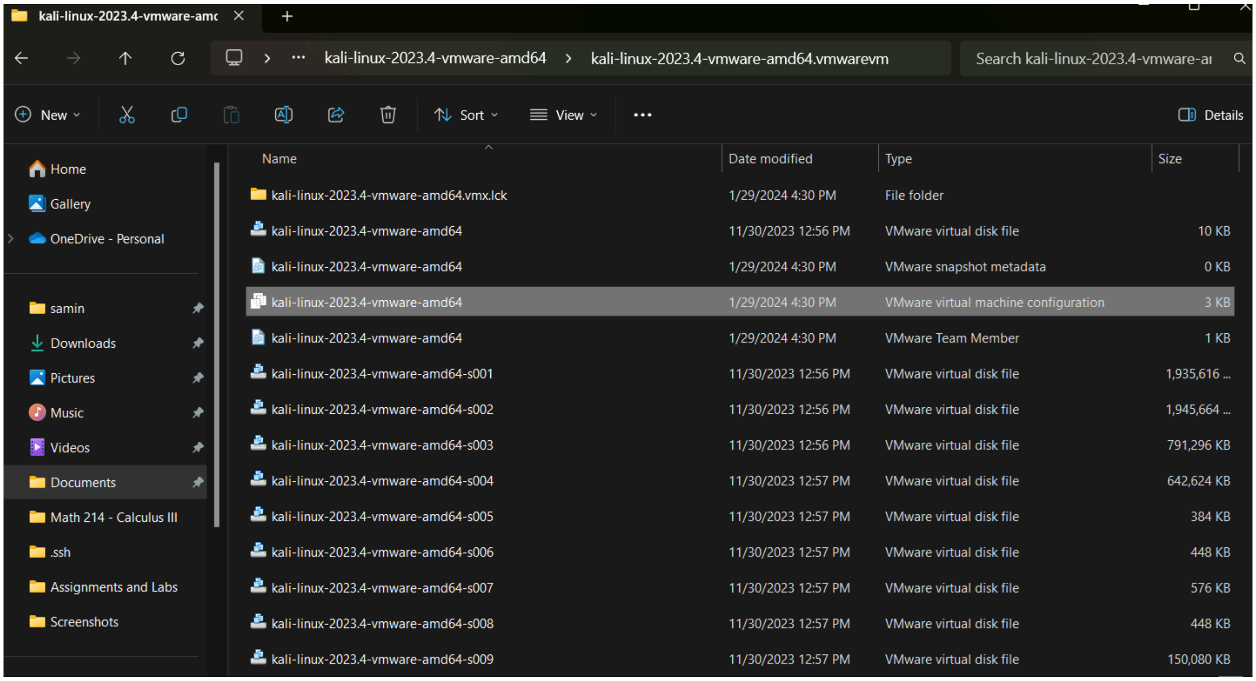
Name	Max	Mean	Last *
seconion eval	78.6%	14.8%	14.6%

Configuring Kali as the Attack Box

First we will need to download the Kali image, which can be found on their website. For this lab, we will be downloading the VMware 64 bit version:

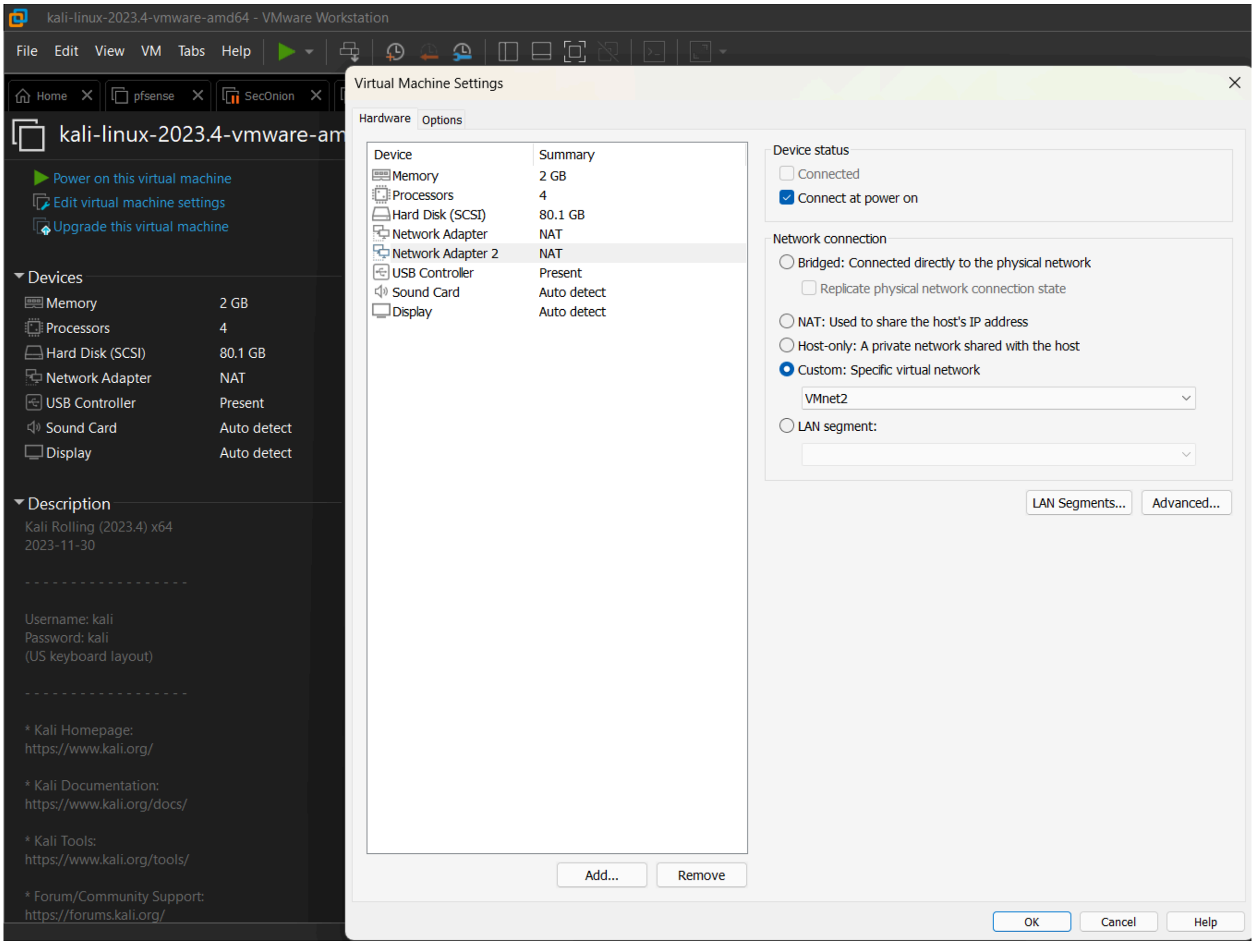


Once downloaded, extract the file to where you would like it to be, and then search for the file ending in .vmx (alternatively, look for the "VMware virtual machine configuration" file) and open it. It should open up the machine in VMware



Name	Date modified	Type	Size
kali-linux-2023.4-vmware-amd64.vmx.lck	1/29/2024 4:30 PM	File folder	
kali-linux-2023.4-vmware-amd64	11/30/2023 12:56 PM	VMware virtual disk file	10 KB
kali-linux-2023.4-vmware-amd64	1/29/2024 4:30 PM	VMware snapshot metadata	0 KB
kali-linux-2023.4-vmware-amd64	1/29/2024 4:30 PM	VMware virtual machine configuration	3 KB
kali-linux-2023.4-vmware-amd64	1/29/2024 4:30 PM	VMware Team Member	1 KB
kali-linux-2023.4-vmware-amd64-s001	11/30/2023 12:56 PM	VMware virtual disk file	1,935,616 ...
kali-linux-2023.4-vmware-amd64-s002	11/30/2023 12:56 PM	VMware virtual disk file	1,945,664 ...
kali-linux-2023.4-vmware-amd64-s003	11/30/2023 12:56 PM	VMware virtual disk file	791,296 KB
kali-linux-2023.4-vmware-amd64-s004	11/30/2023 12:57 PM	VMware virtual disk file	642,624 KB
kali-linux-2023.4-vmware-amd64-s005	11/30/2023 12:57 PM	VMware virtual disk file	384 KB
kali-linux-2023.4-vmware-amd64-s006	11/30/2023 12:57 PM	VMware virtual disk file	448 KB
kali-linux-2023.4-vmware-amd64-s007	11/30/2023 12:57 PM	VMware virtual disk file	576 KB
kali-linux-2023.4-vmware-amd64-s008	11/30/2023 12:57 PM	VMware virtual disk file	448 KB
kali-linux-2023.4-vmware-amd64-s009	11/30/2023 12:57 PM	VMware virtual disk file	150,080 KB

Edit the virtual machine settings to add another Network Adapter and map it to VMnet2:


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
pfsense
SecOnion
kali-linux-2023.4-vmware-am
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Virtual Machine Settings
Hardware
Options
Add...
Remove
LAN Segments...
Advanced...
OK
Cancel
Help

Devices

Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

Kali Rolling (2023.4) x64
2023-11-30

- - - - - - - - - - - - - - - - -

Username: kali
Password: kali
(US keyboard layout)

- - - - - - - - - - - - - - - - -

* Kali Homepage:
https://www.kali.org/

* Kali Documentation:
https://www.kali.org/docs/

* Kali Tools:
https://www.kali.org/tools/

* Forum/Community Support:
https://forums.kali.org/

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	NAT
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

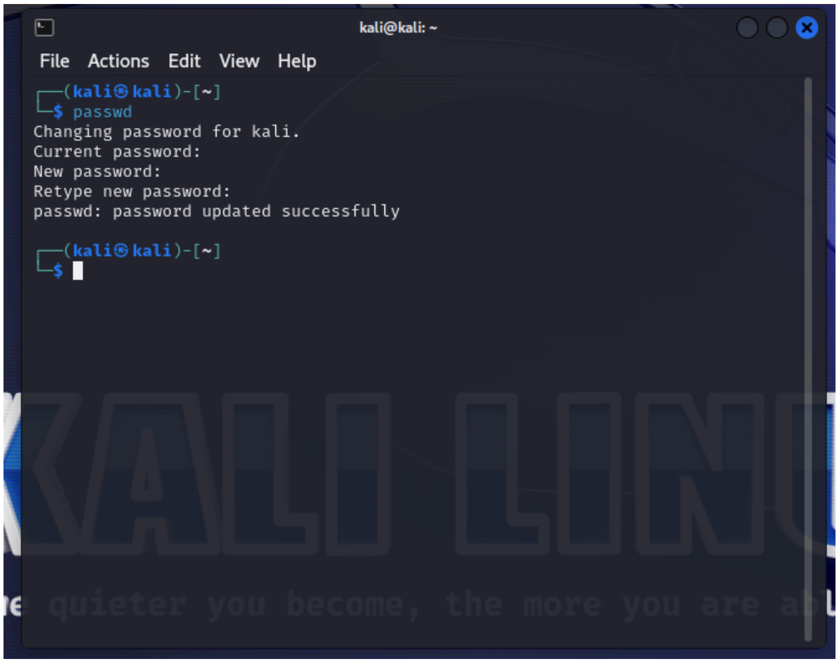
☐ Connected
☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network
☐ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet2
○ LAN segment:

You can now boot up the machine and login with the default credentials (username and password are both “kali”)

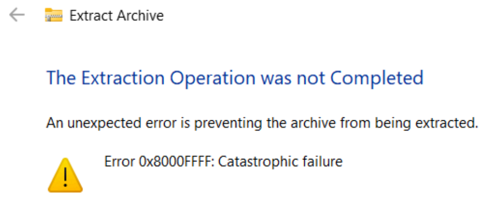
You can change the password by running “passwd” on the terminal, where you will be prompted to enter the current password (“kali”) before you set the new password:



```
┌──(kali㉿kali)-[~]
└─$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$ 
```

Troubleshooting

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



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/).