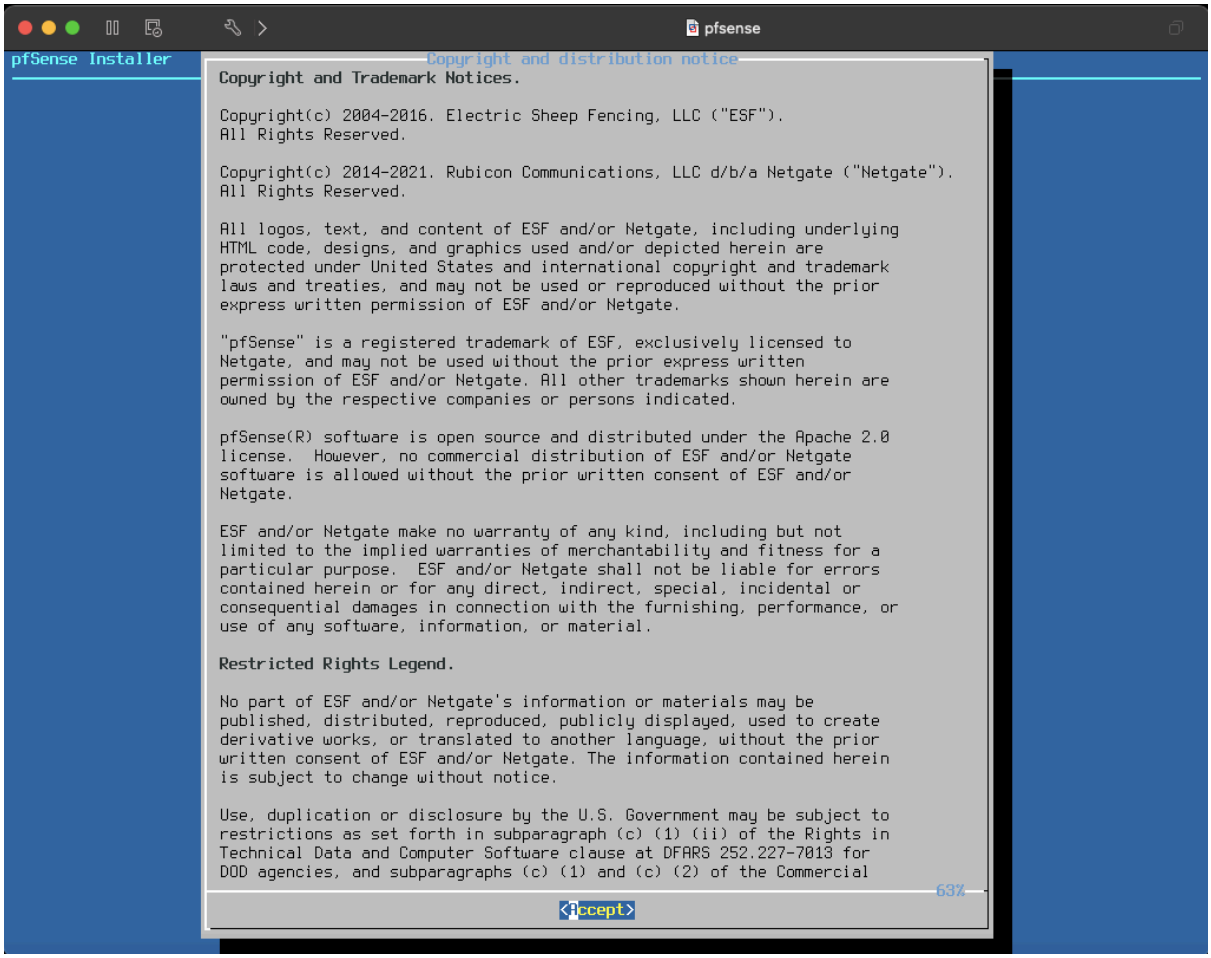
Cybersecurity Homelab for Detection and Monitoring

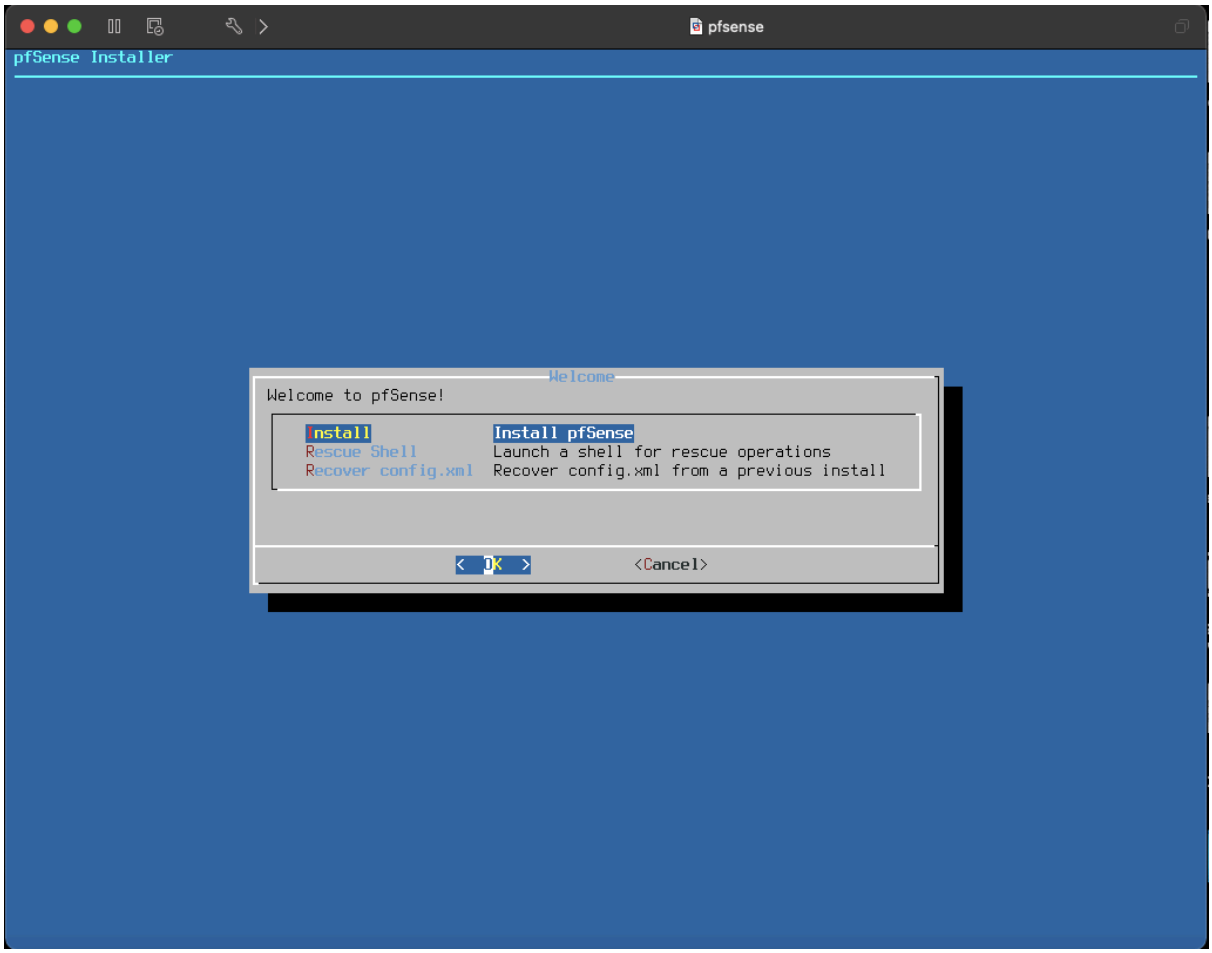
Configuring pfsense –

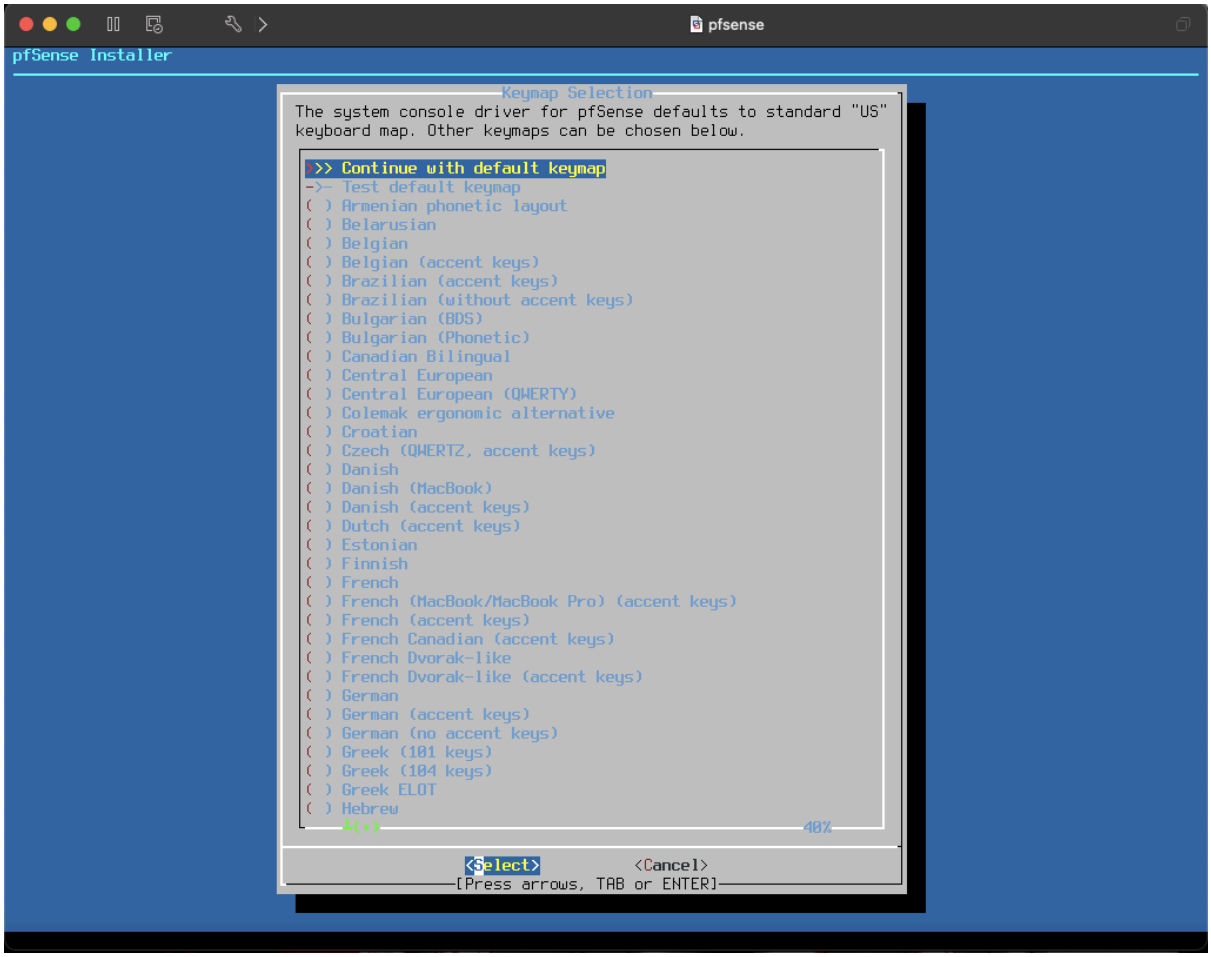
Pfsense will be configured as a firewall to segment our private homelab network and will be only accessible from our kali linux machine.
Download the iso file from https://www.pfsense.org/download/ and create a new VM on VMware Fusion. Select the recommended settings.

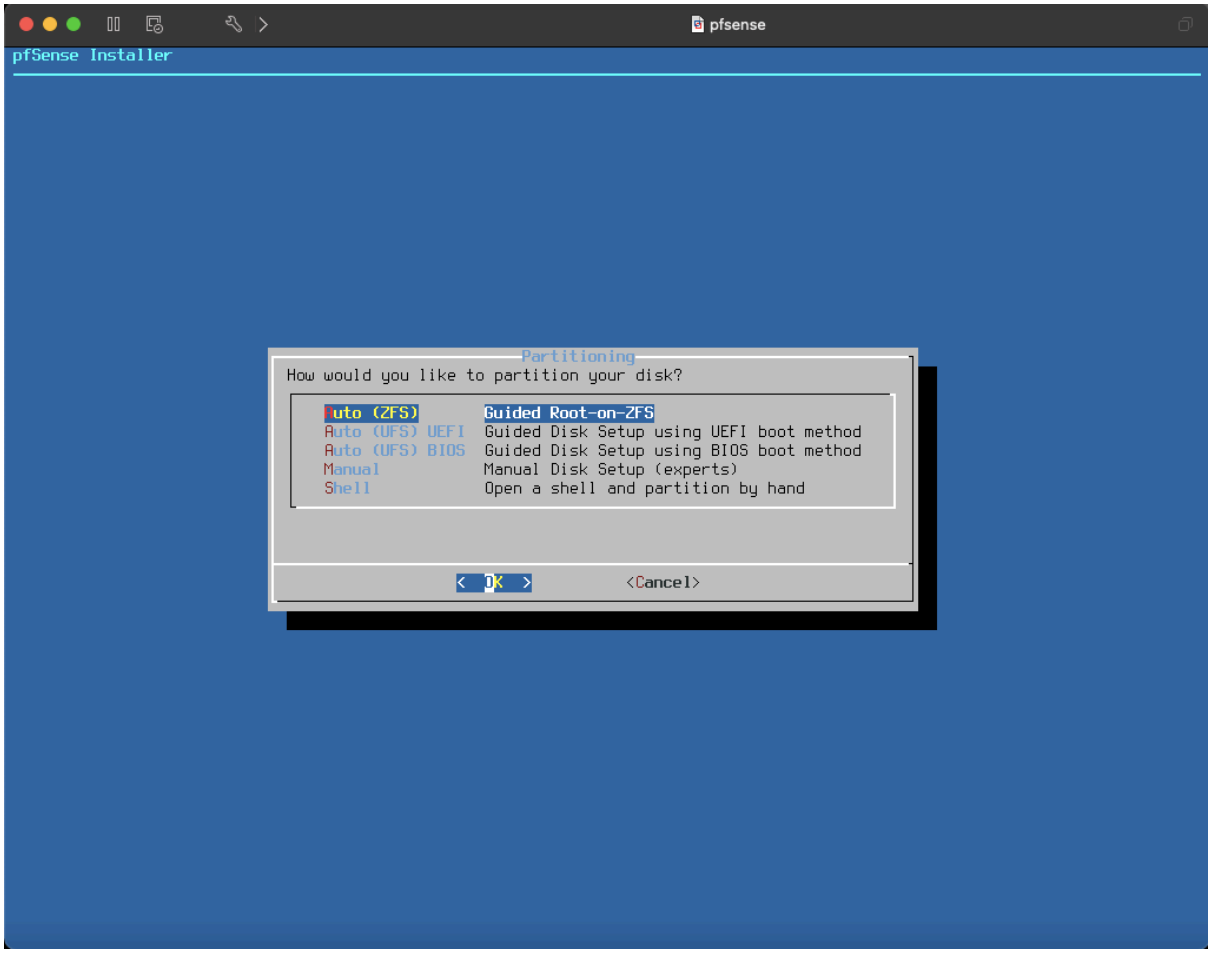
Add 5 network adapters and correspond them with a custom interface as show below.

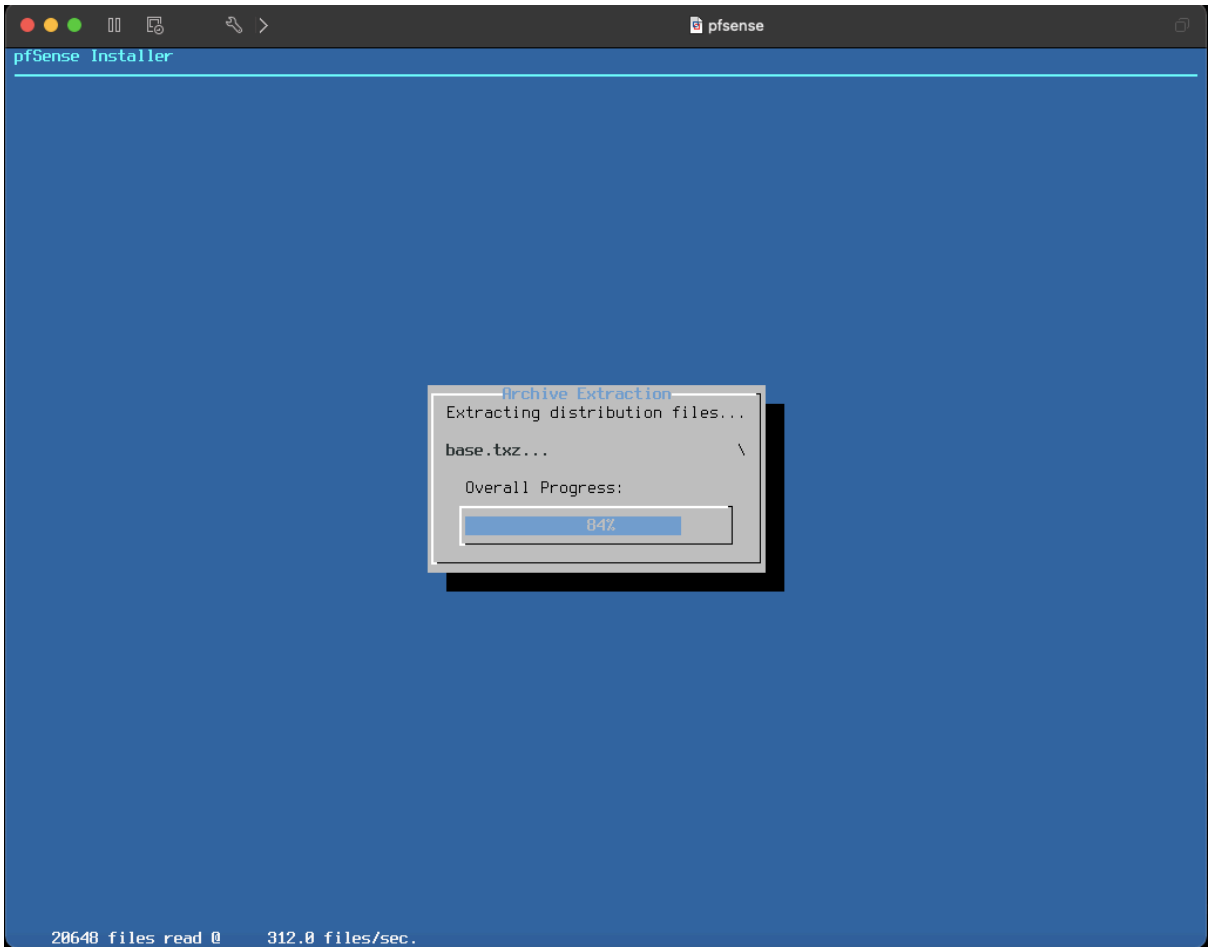
Accept all defaults when the pfsense machine powers on and wait for it to configure and reboot.

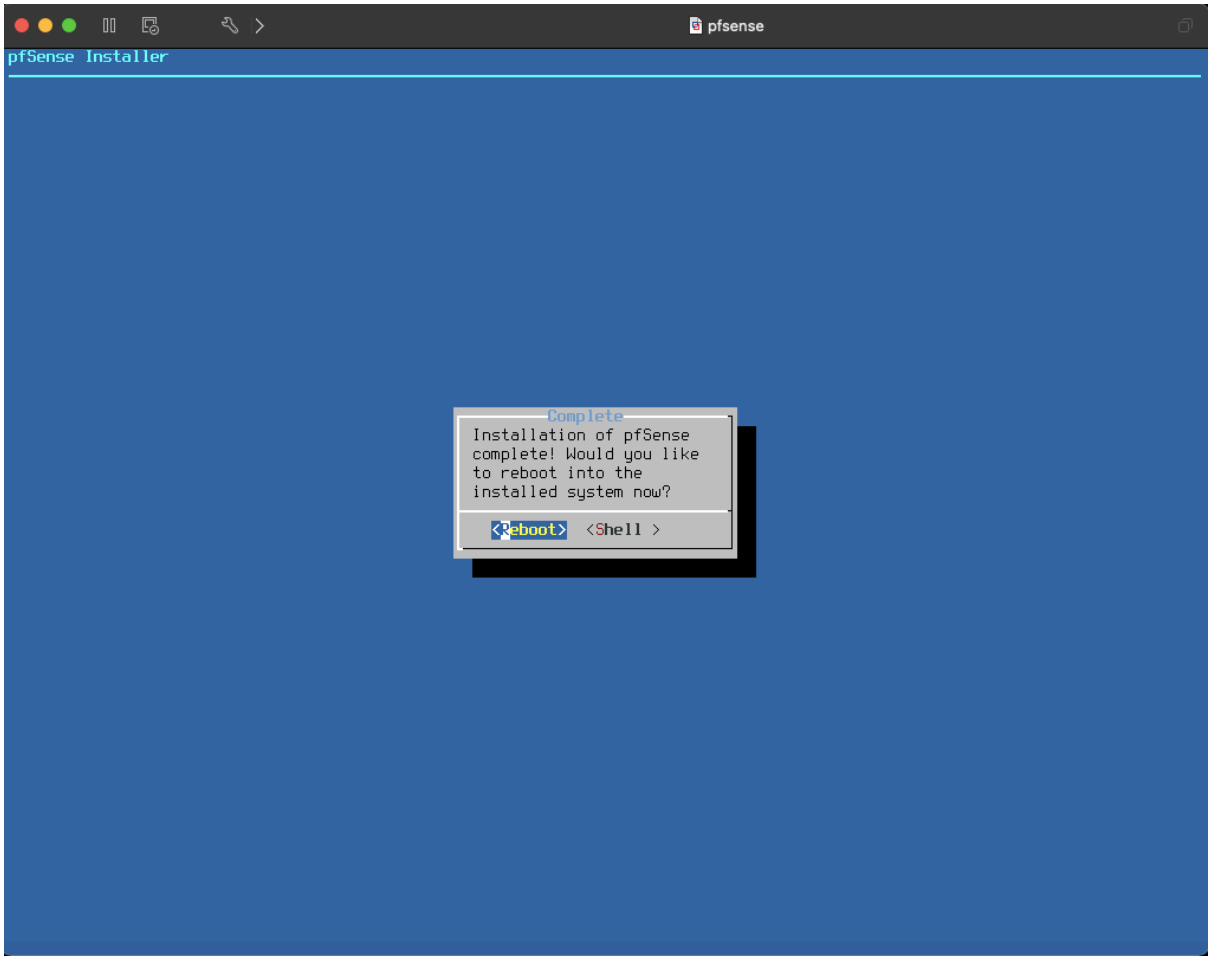


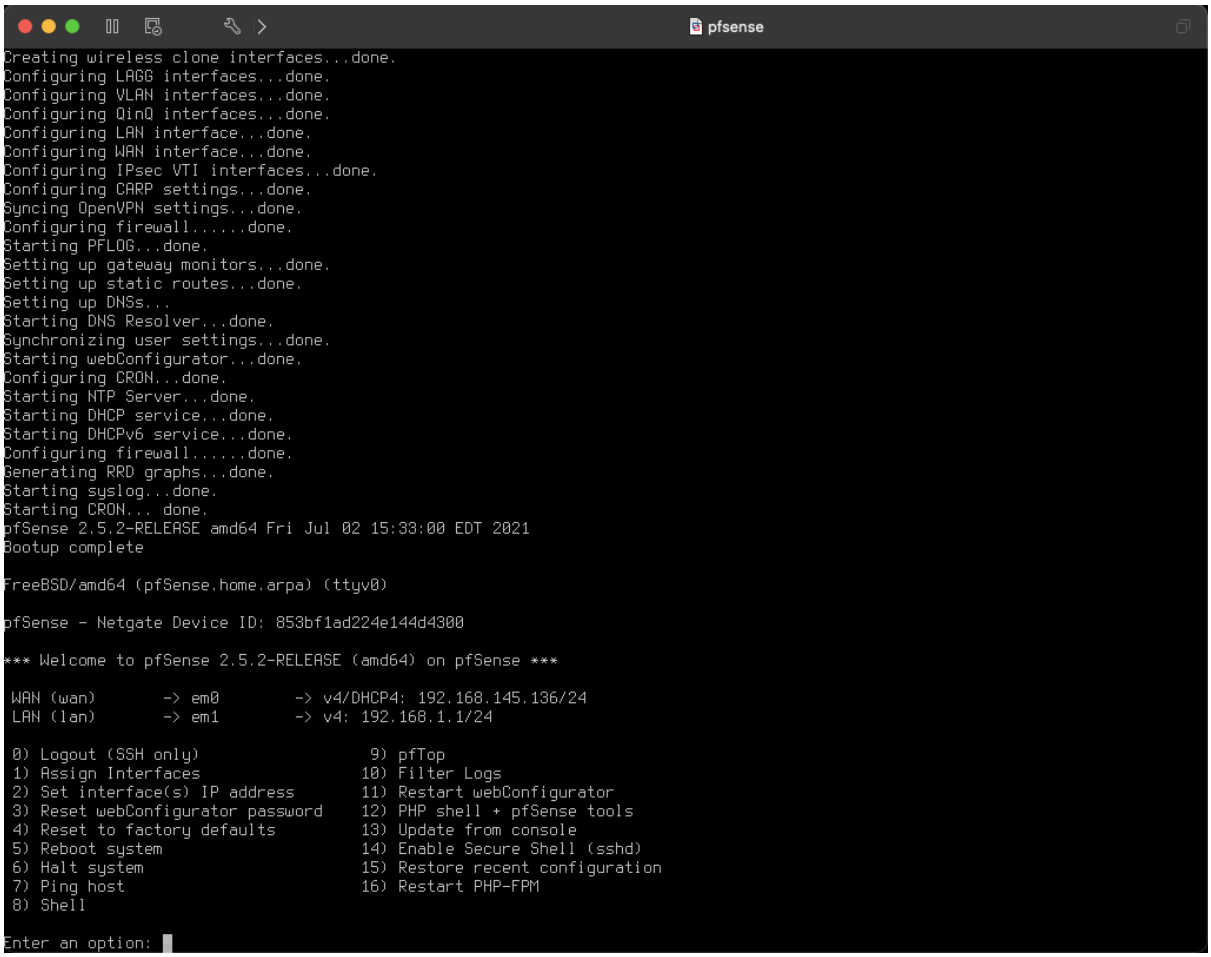

pfsense
pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
< OK >
<Cancel>


pfsense
pfSense Installer
Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.
>>> Continue with default keymap
-> Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
( ) Central European (QWERTY)
( ) Colemak ergonomic alternative
( ) Croatian
( ) Czech (QWERTZ, accent keys)
( ) Danish
( ) Danish (MacBook)
( ) Danish (accent keys)
( ) Dutch (accent keys)
( ) Estonian
( ) Finnish
( ) French
( ) French (MacBook/MacBook Pro) (accent keys)
( ) French (accent keys)
( ) French Canadian (accent keys)
( ) French Dvorak-like
( ) French Dvorak-like (accent keys)
( ) German
( ) German (accent keys)
( ) German (no accent keys)
( ) Greek (101 keys)
( ) Greek (104 keys)
( ) Greek ELOT
( ) Hebrew
40%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]

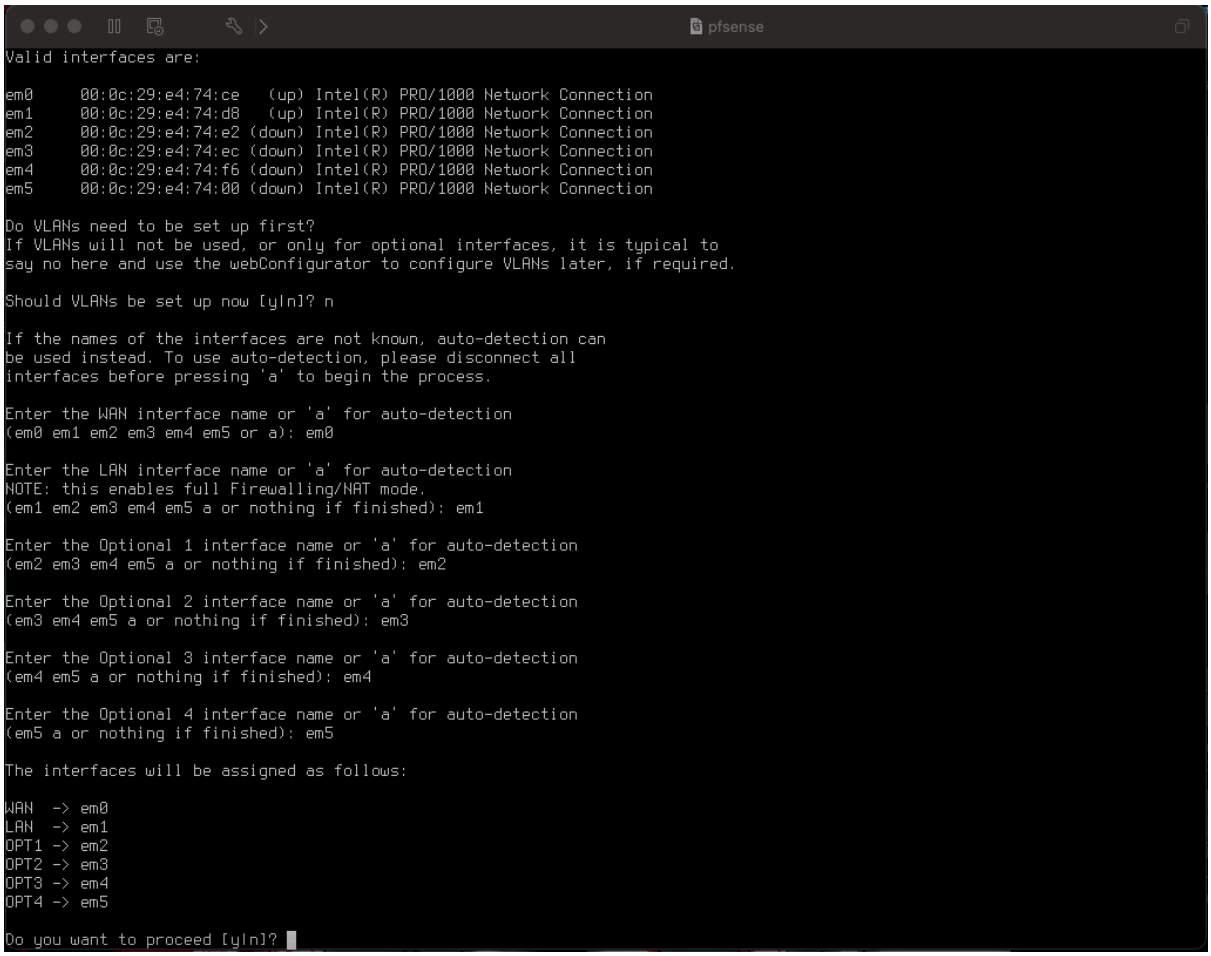

pfsense
pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) UEFI Guided Disk Setup using UEFI boot method
Auto (UFS) BIOS Guided Disk Setup using BIOS boot method
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>


pfsense
pfSense Installer
Archive Extraction
Extracting distribution files...
base.txz... \
Overall Progress:
84%
20648 files read @ 312.0 files/sec.

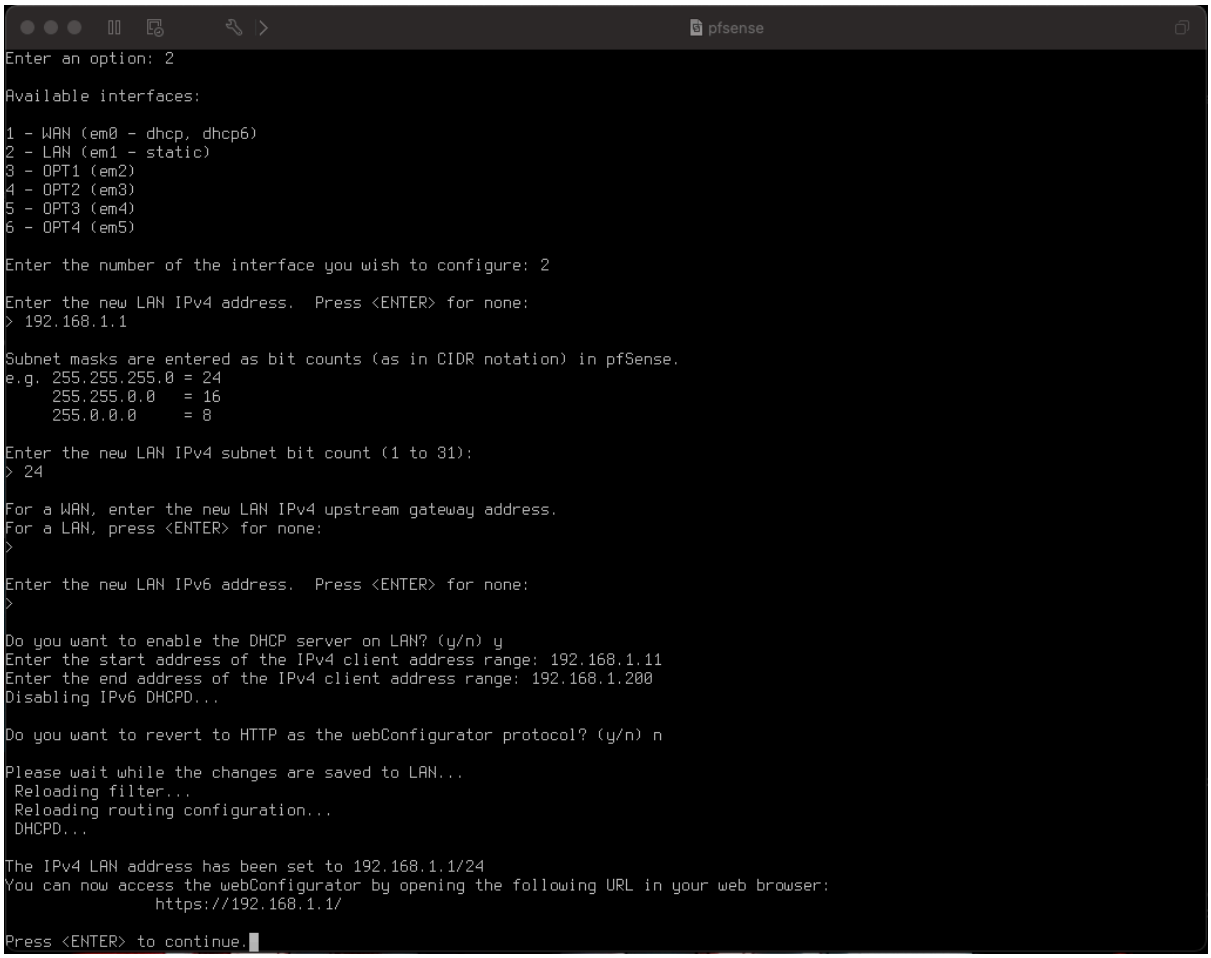

pfsense
pfSense Installer
Complete
Installation of pfSense
complete! Would you like
to reboot into the
installed system now?
<Reboot>
<Shell >


pfsense
Creating wireless clone interfaces...done.
Configuring LAGG interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring LAN interface...done.
Configuring WAN interface...done.
Configuring IPsec VTI interfaces...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Setting up static routes...done.
Setting up DNSs...
Starting DNS Resolver...done.
Synchronizing user settings...done.
Starting webConfigurator...done.
Configuring CRON...done.
Starting NTP Server...done.
Starting DHCP service...done.
Starting DHCPv6 service...done.
Configuring firewall.....done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
pfSense - Netgate Device ID: 853bf1ad224e144d4300
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.145.136/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

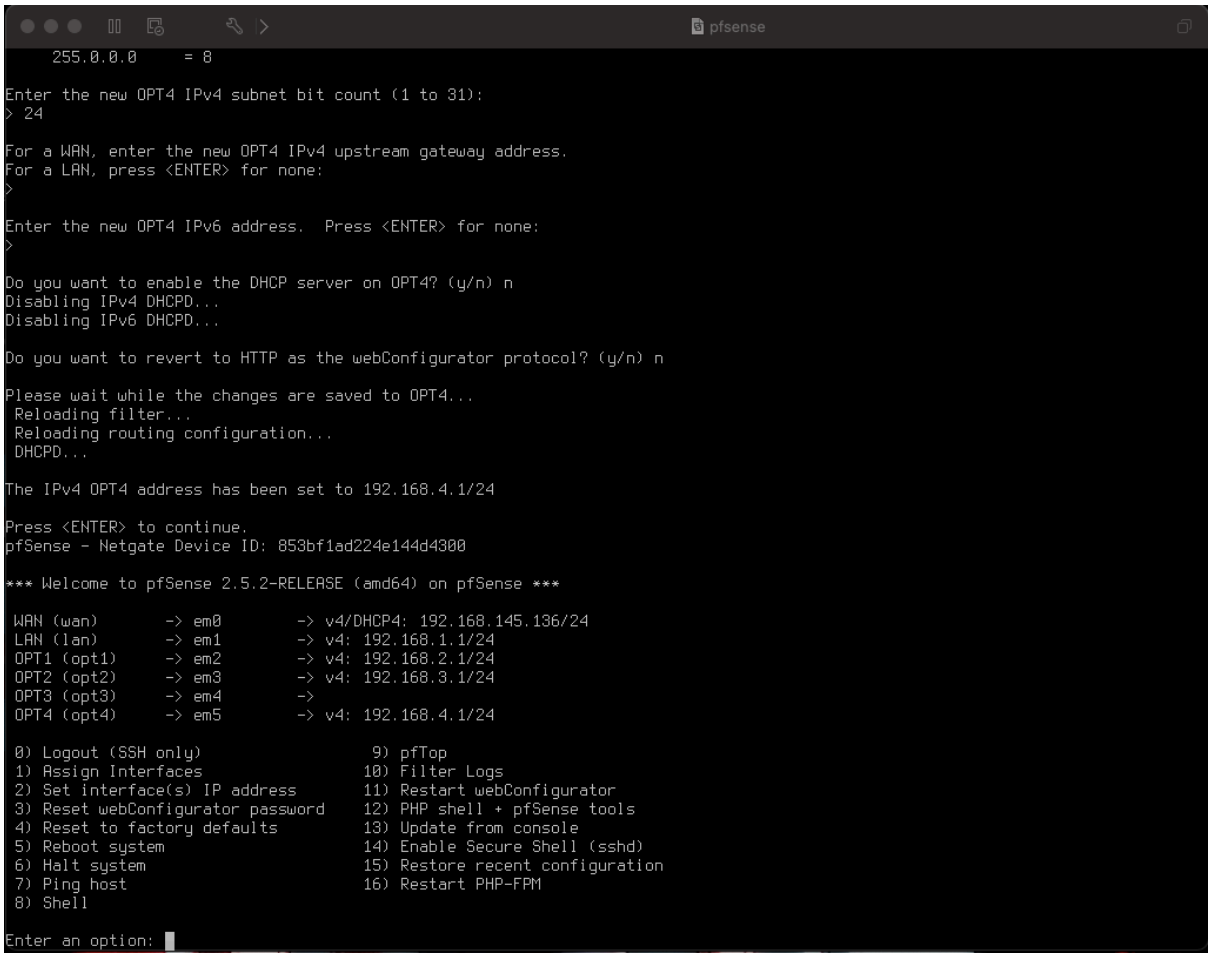
Enter option 1
Should VLANS be set up now
[y:n]?: n
Enter em0, em1, em2, em3, em4, and em5 respectively for each consecutive question
Do you want to proceed [y:n]?: y



Enter option 2
We will start with the LAN interface (2)
The IP address 192.168.1.1 will be used to access pfsense WebGUI via kali .
Use the following configuration for LAN interface.



Configuration for OPT1, OPT2,OPT3 and OPT4 can be done similarly as shown below
(OPT3 interface will have span port with traffic that security onion will be monitoring so leave it as blank without an IP)

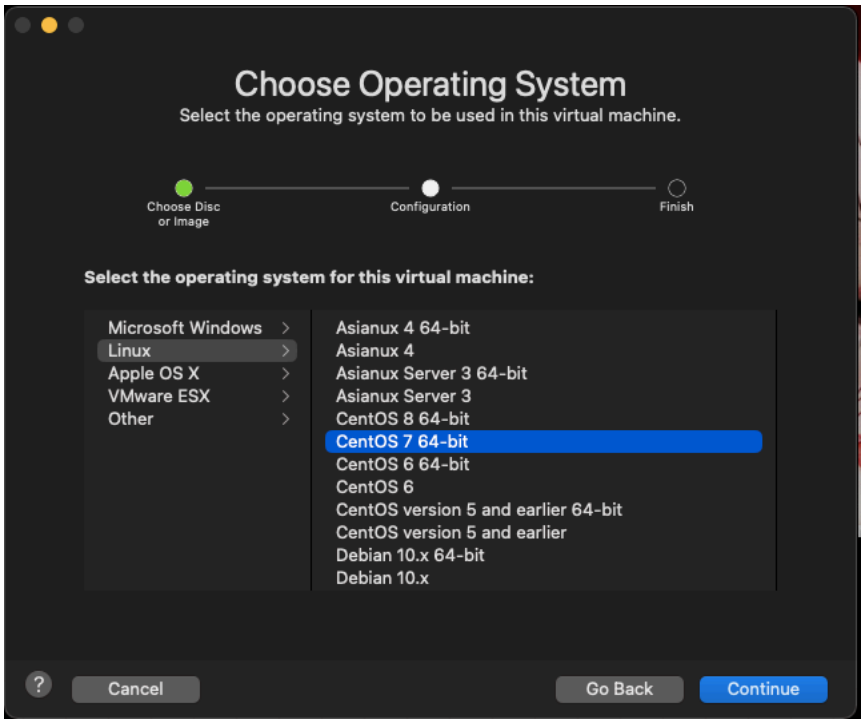


The rest of the configuration will be done via kali through webConfigurator.

Configure Security Onion –

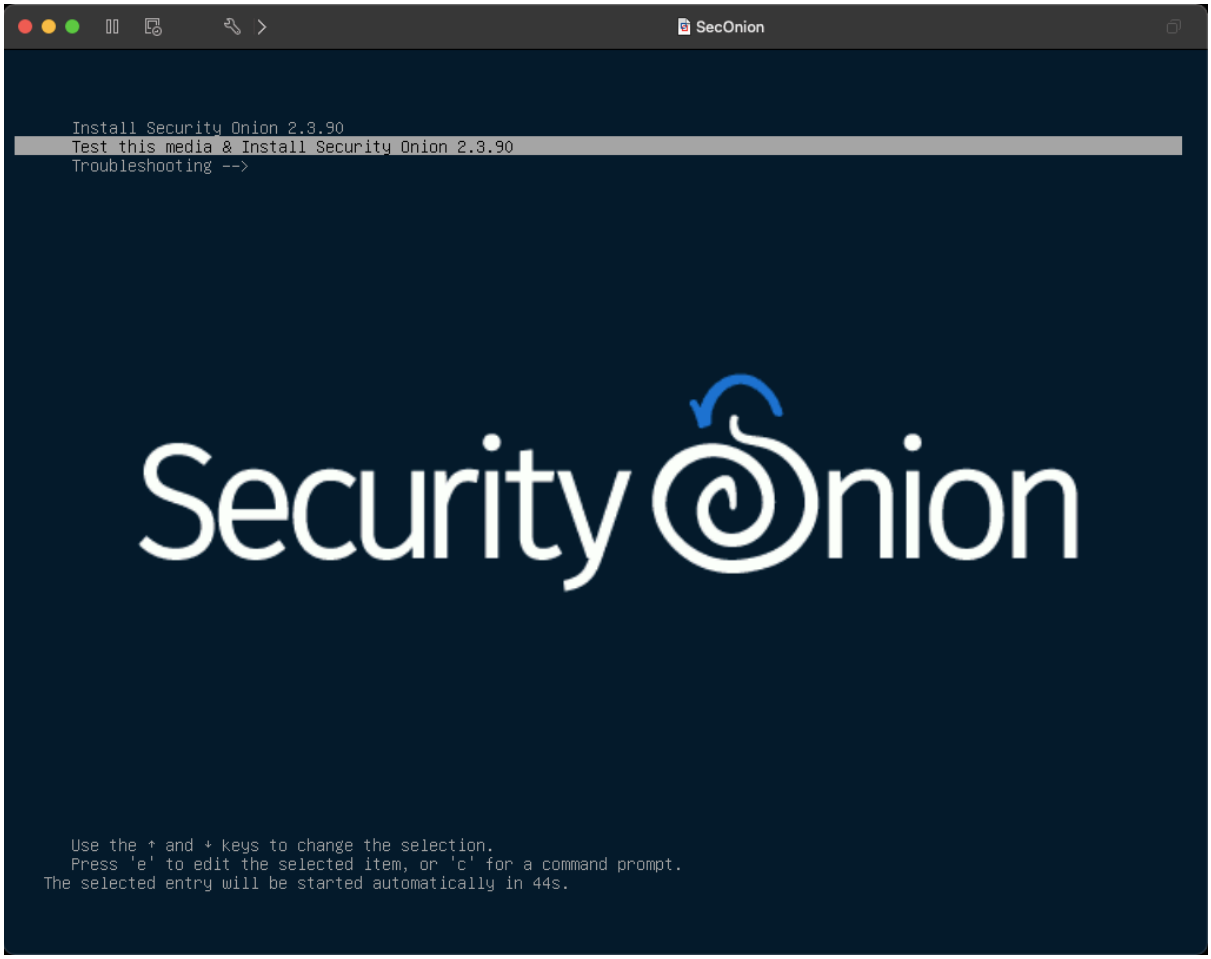
All in one Intrusion Detection System (IDS), security monitoring and log management solution.

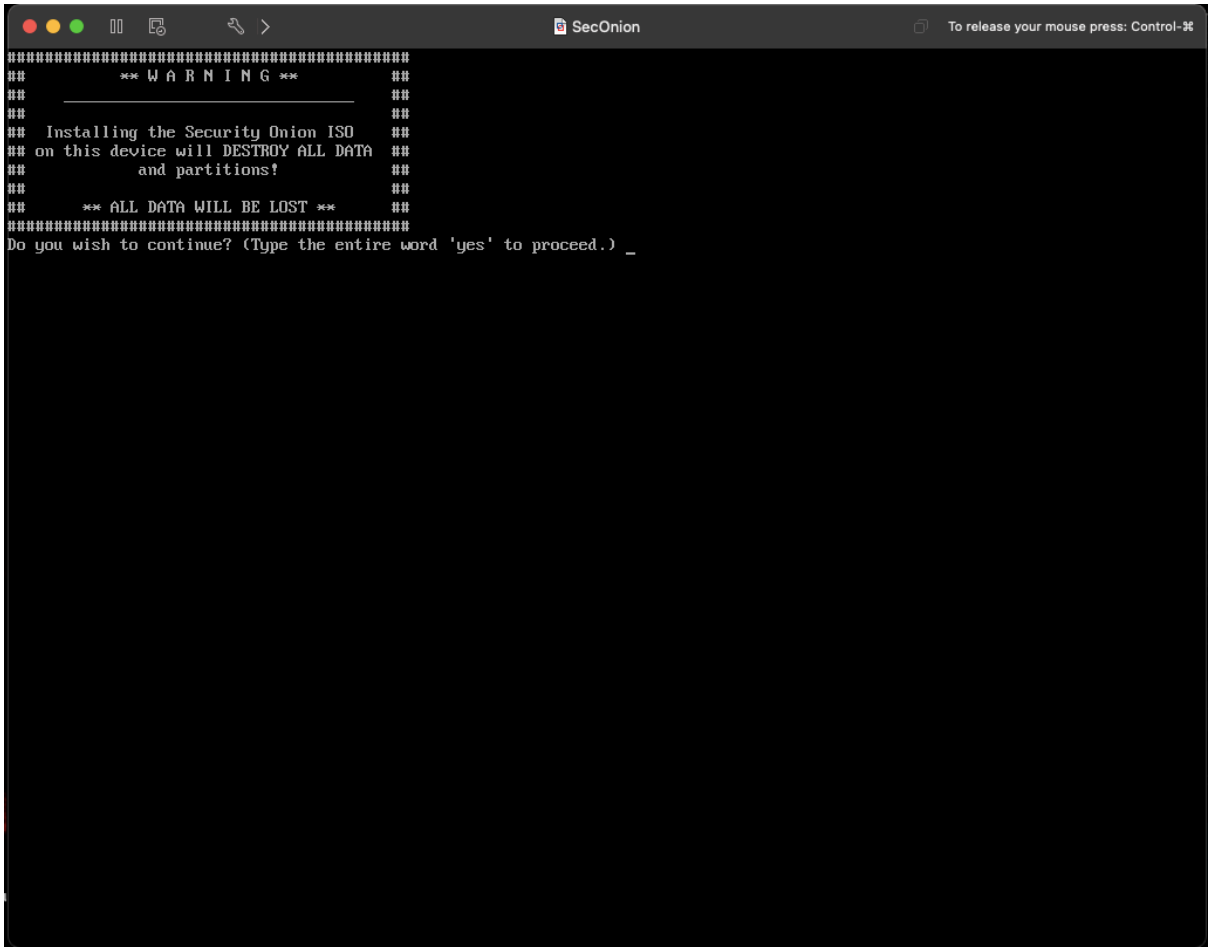
Download the iso file from https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md and install the VM
Add 2 network adapters and and assign them custom interfaces.

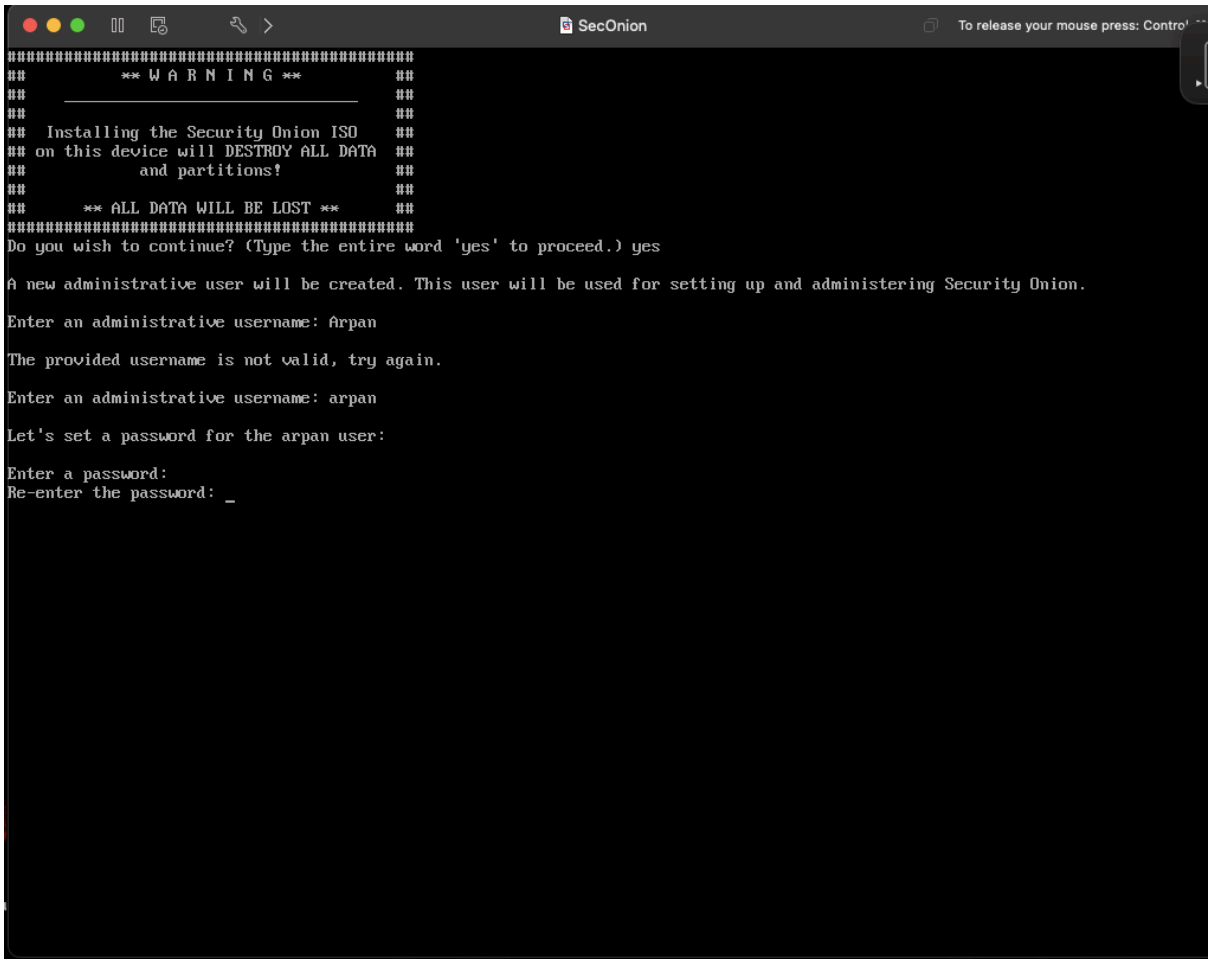



Show All
SecOnion: Settings
Add Device...
System Settings
General
Sharing
Keyboard & Mouse
Processors & Memory
Display
Removable Devices
Network Adapter
Network Adapter 2
Network Adapter 3
Hard Disk (SCSI)
CD/DVD (IDE)
Sound Card
USB & Bluetooth
Printer
Camera
Other
Startup Disk
Encryption
Compatibility
Isolation
Advanced

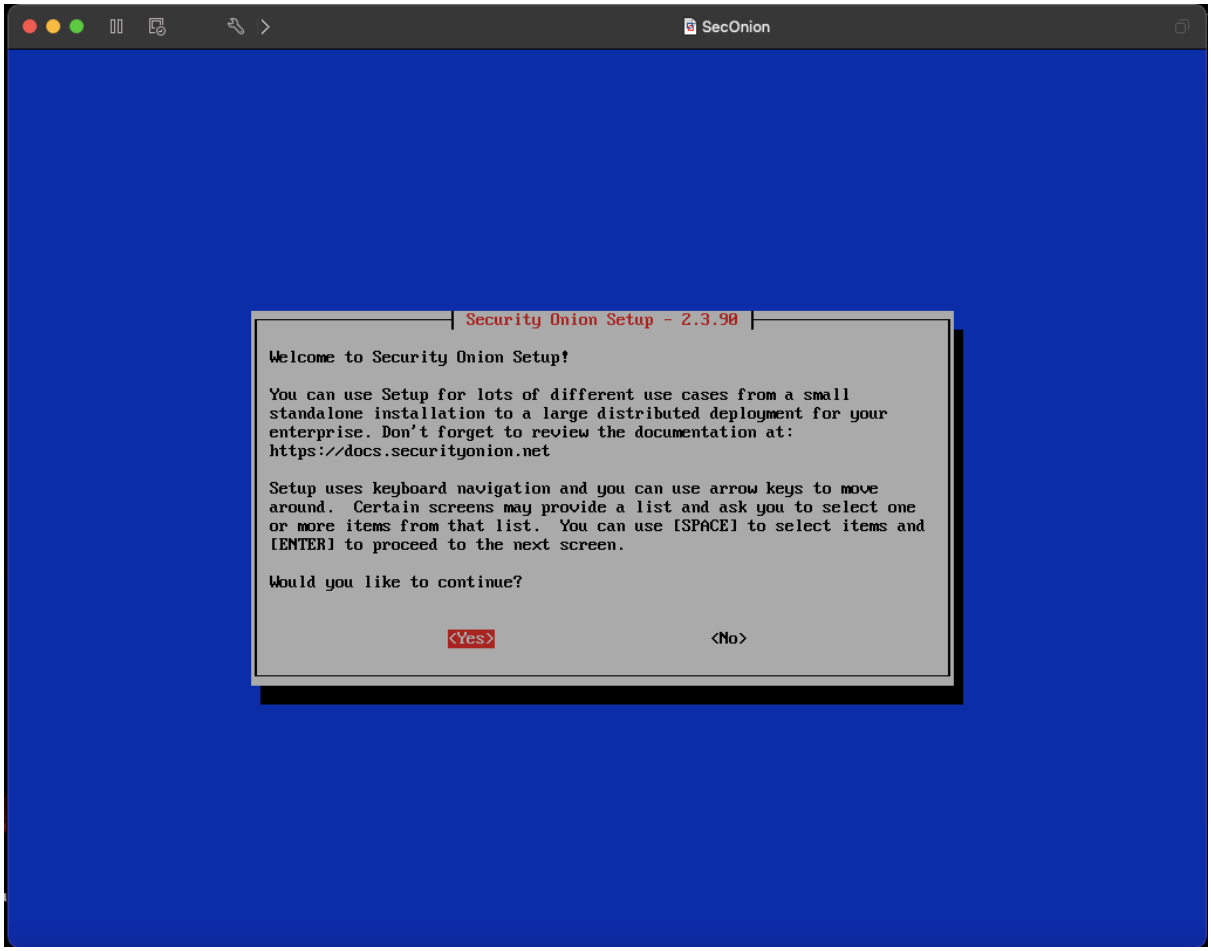
Follow the prompts as shown in the following screenshots.

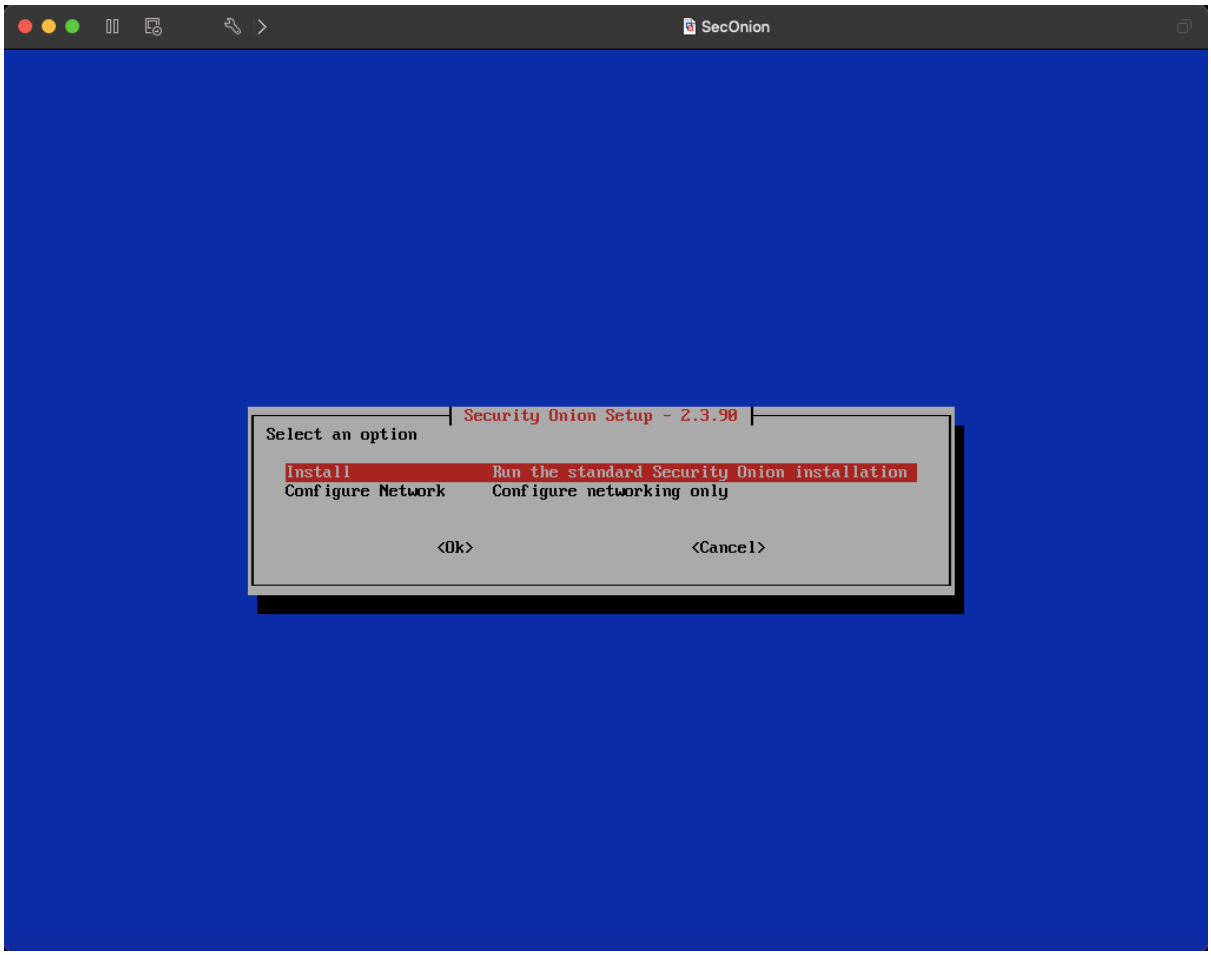


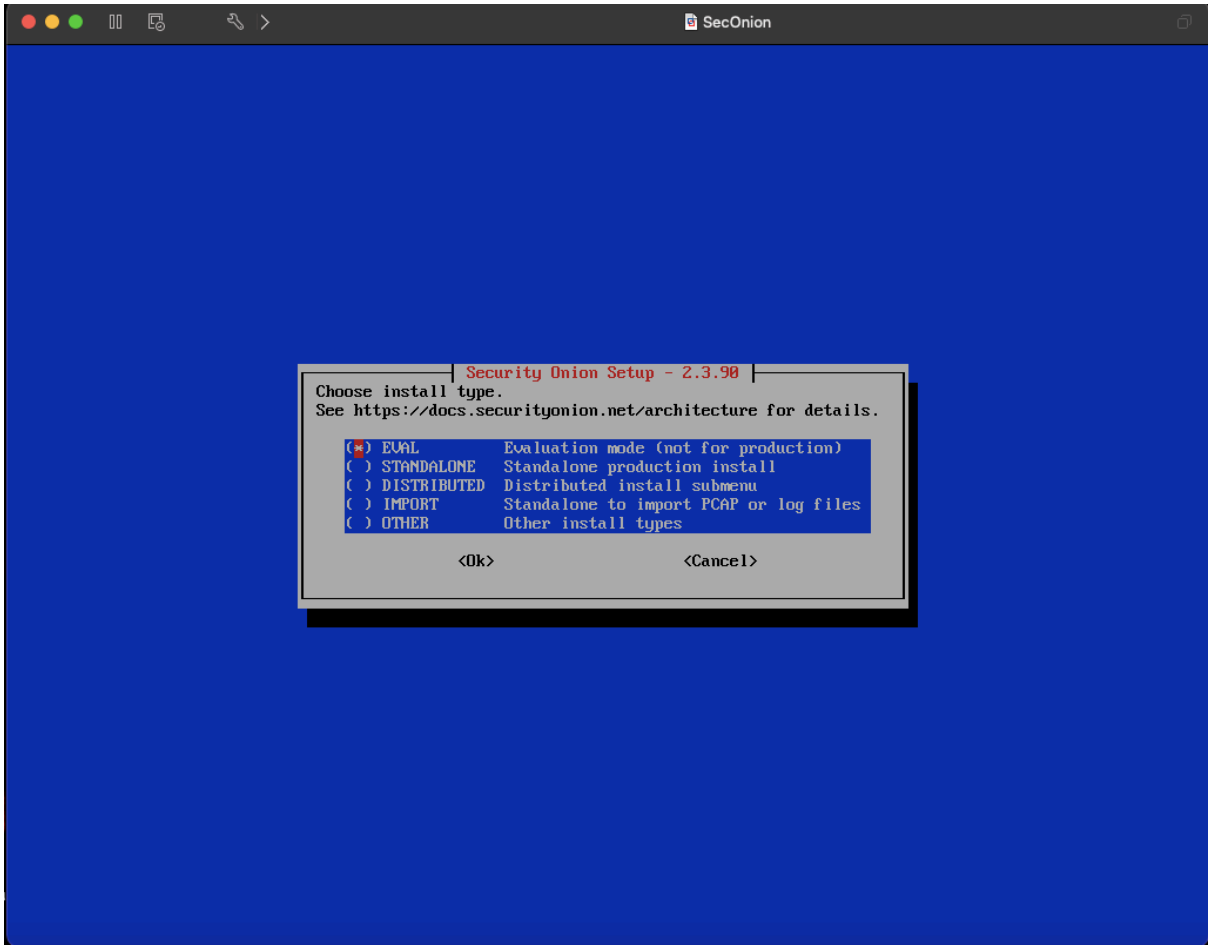

SecOnion
To release your mouse press: Control-⌘
##
** W A R N I N G **
____
##
Installing the Security Onion ISO
on this device will DESTROY ALL DATA
and partitions!
##
** ALL DATA WILL BE LOST **
##
Do you wish to continue? (Type the entire word 'yes' to proceed.) _

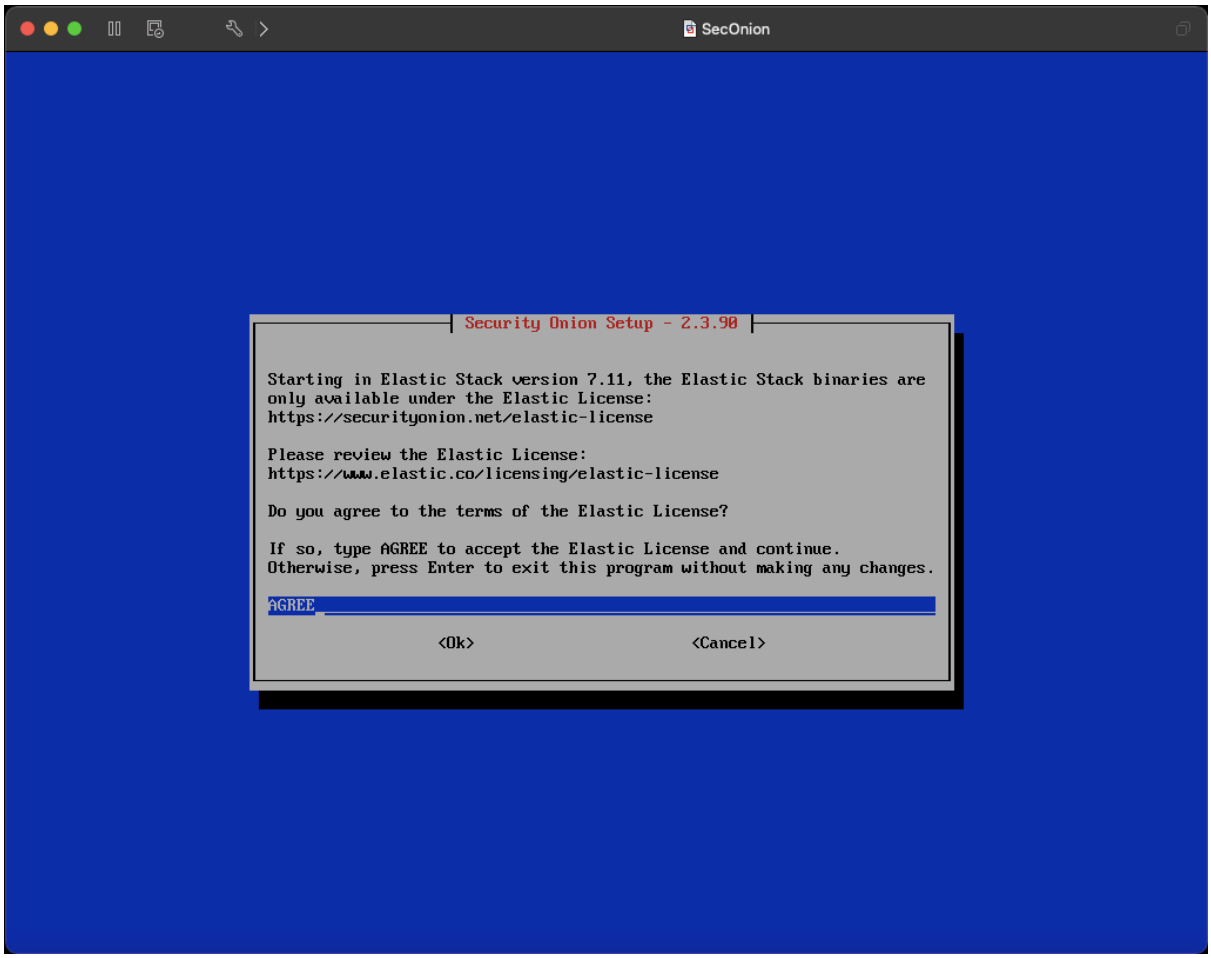

SecOnion
To release your mouse press: Contro
##
** W A R N I N G **

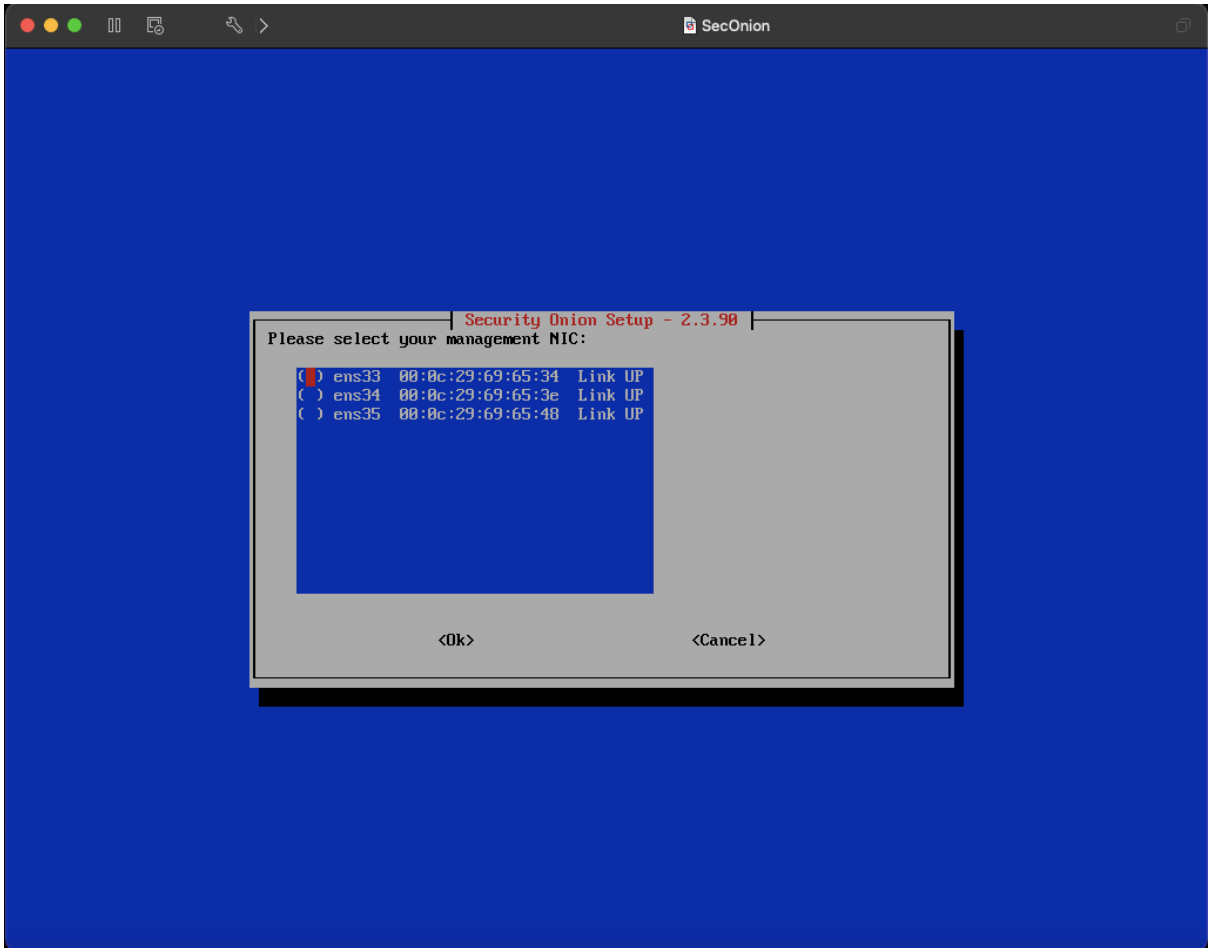
##
Installing the Security Onion ISO
on this device will DESTROY ALL DATA
and partitions!
##
** ALL DATA WILL BE LOST **
##
Do you wish to continue? (Type the entire word 'yes' to proceed.) yes
A new administrative user will be created. This user will be used for setting up and administering Security Onion.
Enter an administrative username: Arpan
The provided username is not valid, try again.
Enter an administrative username: arpan
Let's set a password for the arpan user:
Enter a password:
Re-enter the password: _

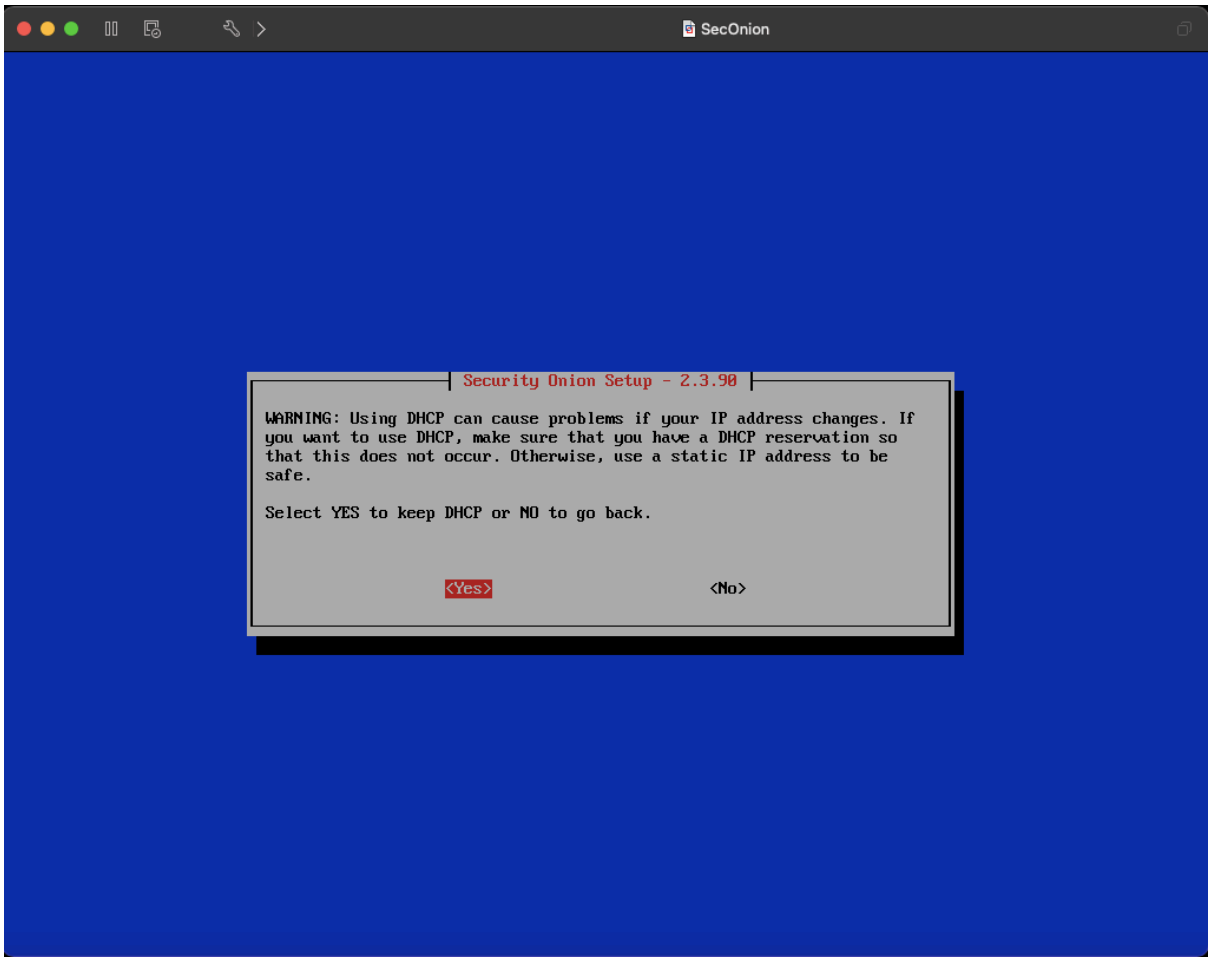

SecOnion
Security Onion Setup - 2.3.90
Welcome to Security Onion Setup!
You can use Setup for lots of different use cases from a small standalone installation to a large distributed deployment for your enterprise. Don't forget to review the documentation at: https://docs.securityonion.net
Setup uses 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?
<Yes>
<No>

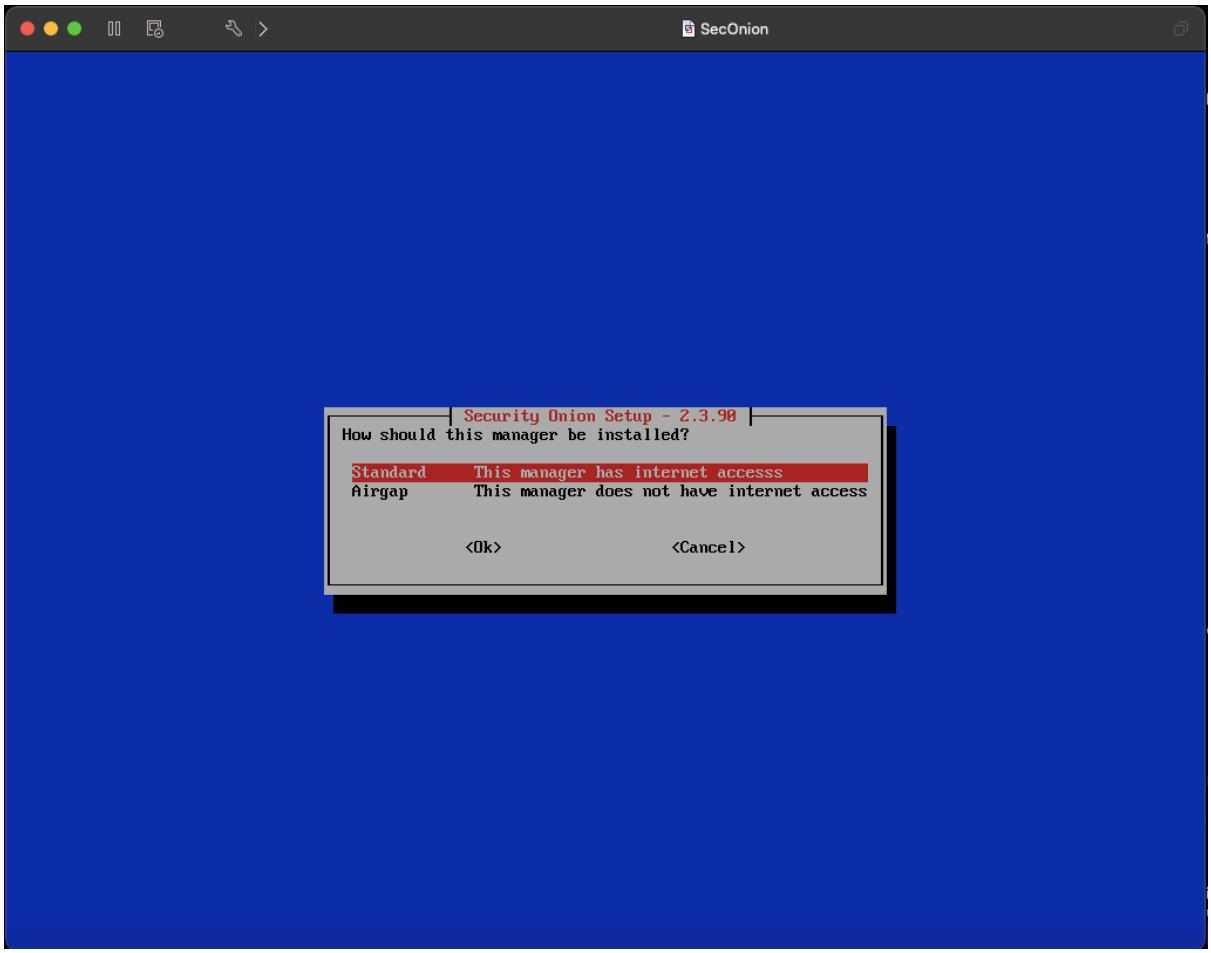

SecOnion
Security Onion Setup - 2.3.90
Select an option
Install
Run the standard Security Onion installation
Configure Network
Configure networking only
<Ok>
<Cancel>

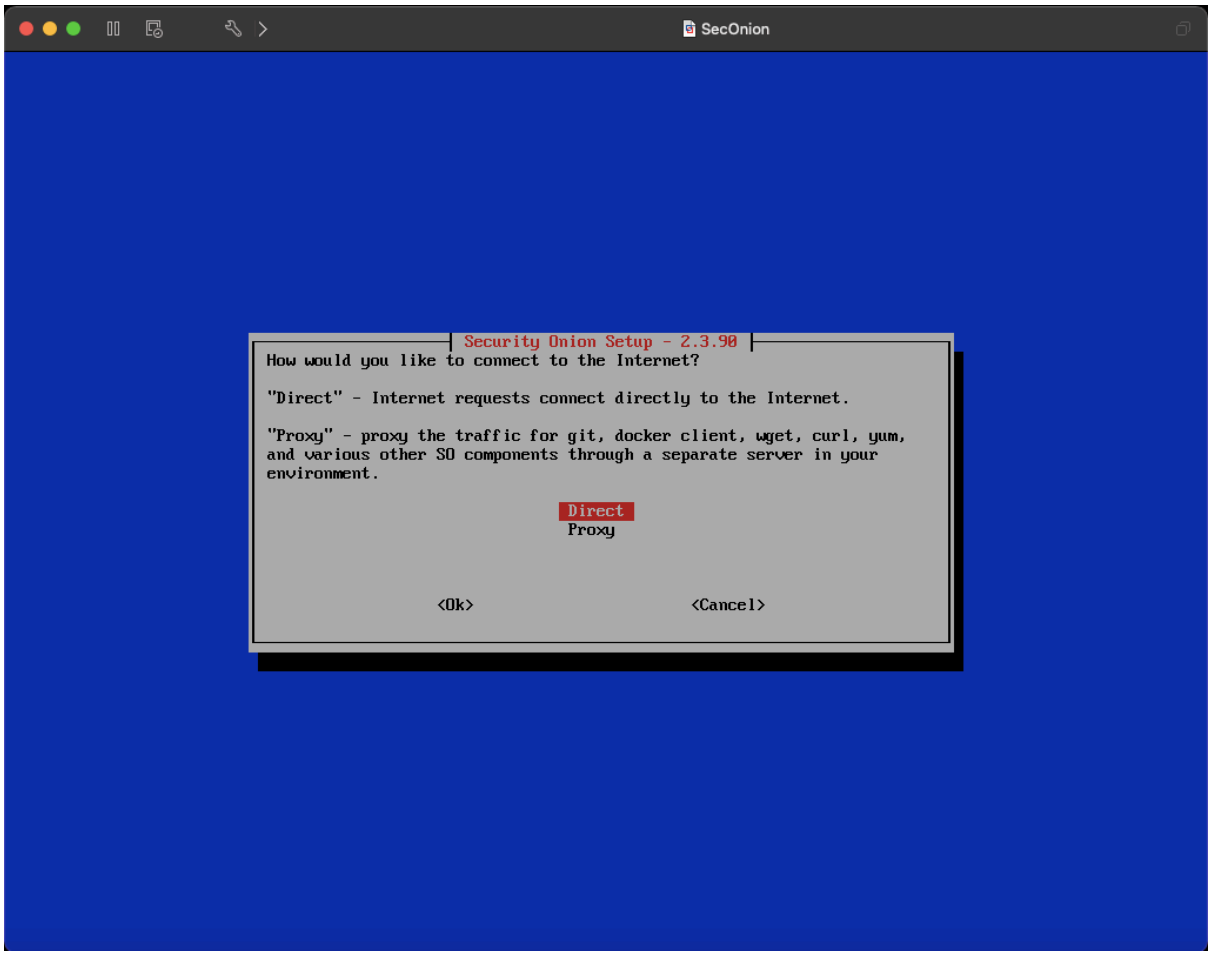

SecOnion
Security Onion Setup - 2.3.90
Choose install type.
See https://docs.securityonion.net/architecture for details.
(*) EVAL Evaluation mode (not for production)
( ) STANDALONE Standalone production install
( ) DISTRIBUTED Distributed install submenu
( ) IMPORT Standalone to import PCAP or log files
( ) OTHER Other install types
<Ok>
<Cancel>

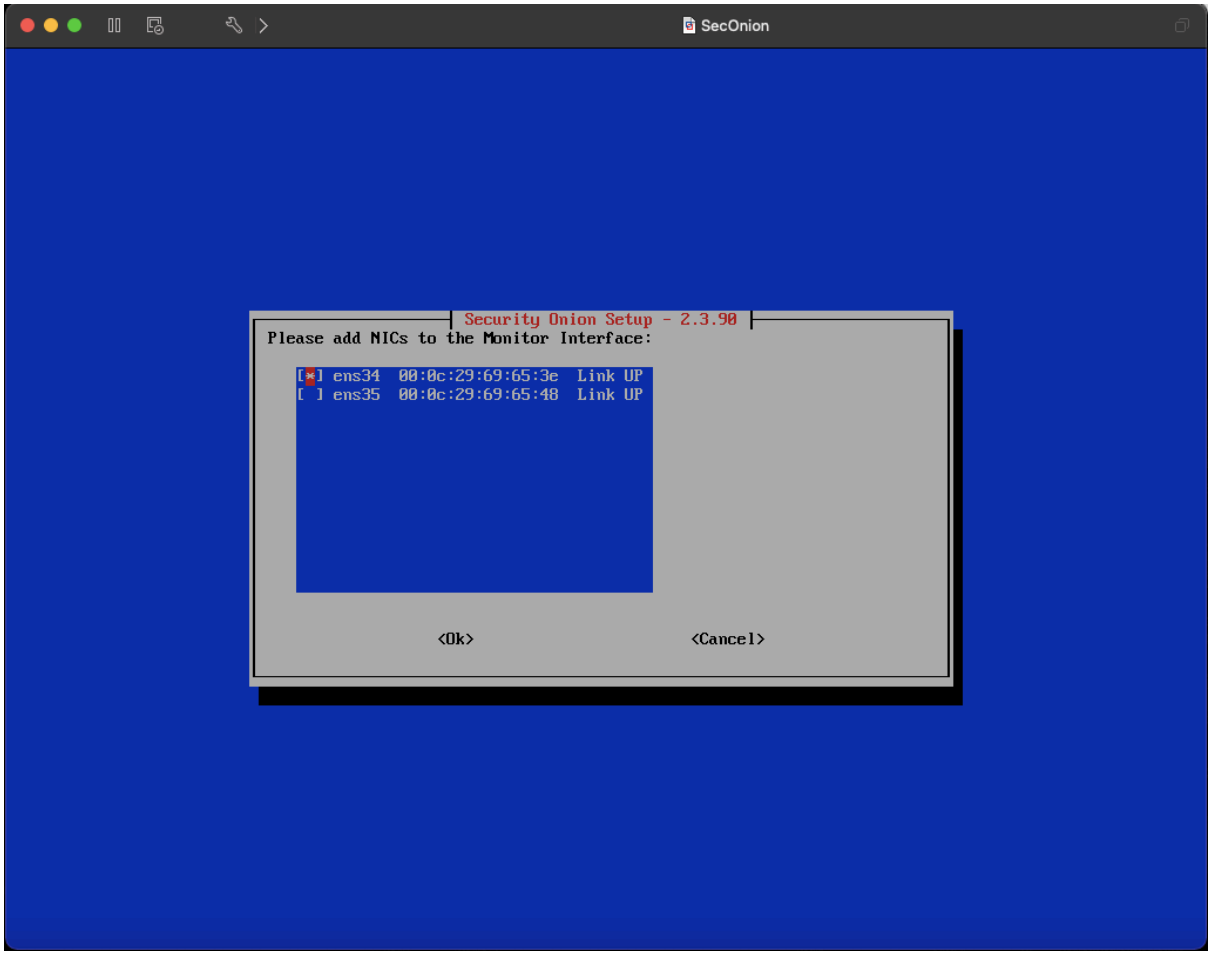

SecOnion
Security Onion Setup - 2.3.90
Starting in Elastic Stack version 7.11, the Elastic Stack binaries are
only available under the Elastic License:
https://securityonion.net/elastic-license
Please review the Elastic License:
https://www.elastic.co/licensing/elastic-license
Do you agree to the terms of the Elastic License?
If so, type AGREE to accept the Elastic License and continue.
Otherwise, press Enter to exit this program without making any changes.
AGREE
<Ok>
<Cancel>

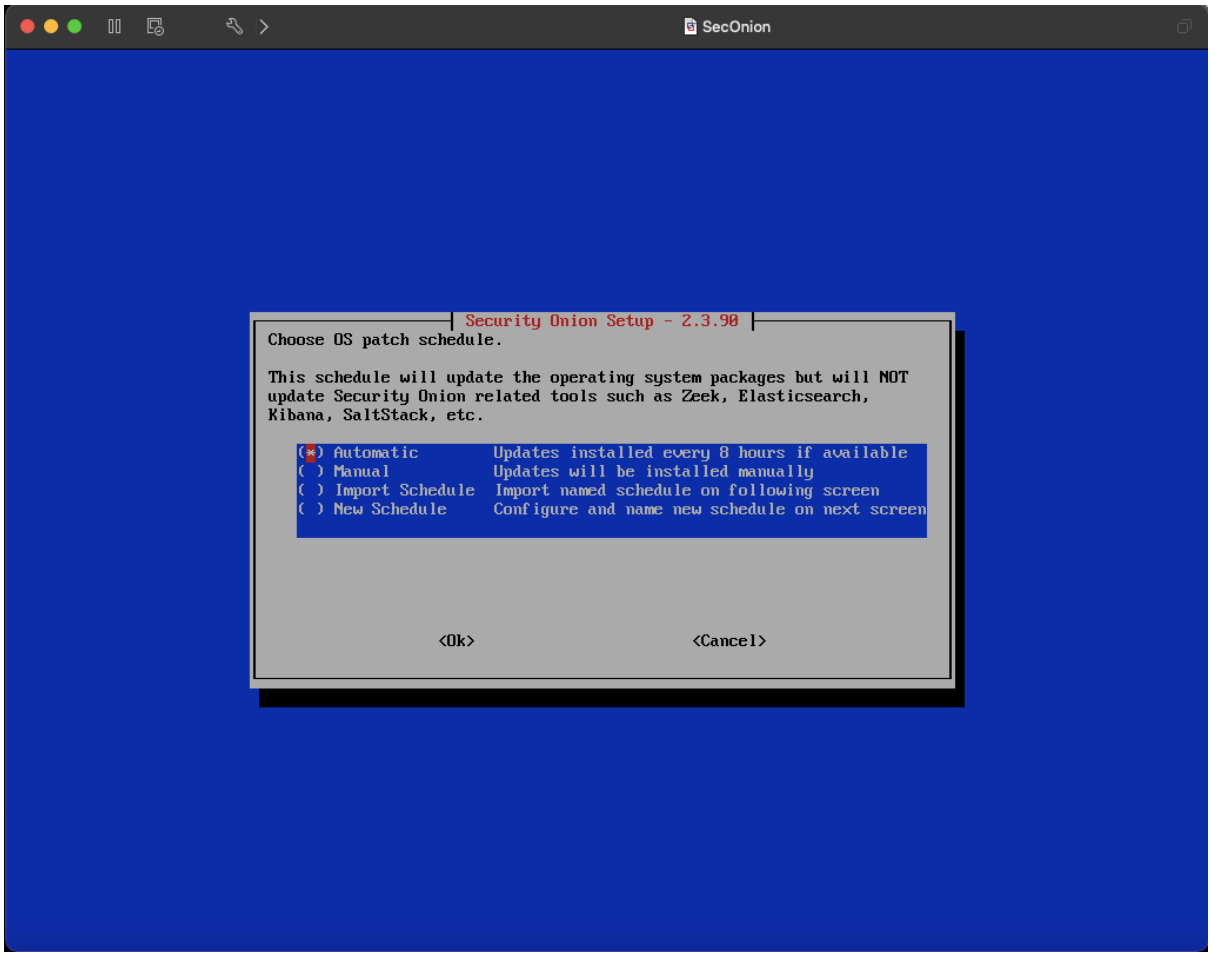

SecOnion
Security Onion Setup - 2.3.90
Please select your management NIC:
( ) ens33 00:0c:29:69:65:34 Link UP
( ) ens34 00:0c:29:69:65:3e Link UP
( ) ens35 00:0c:29:69:65:48 Link UP
<Ok>
<Cancel>

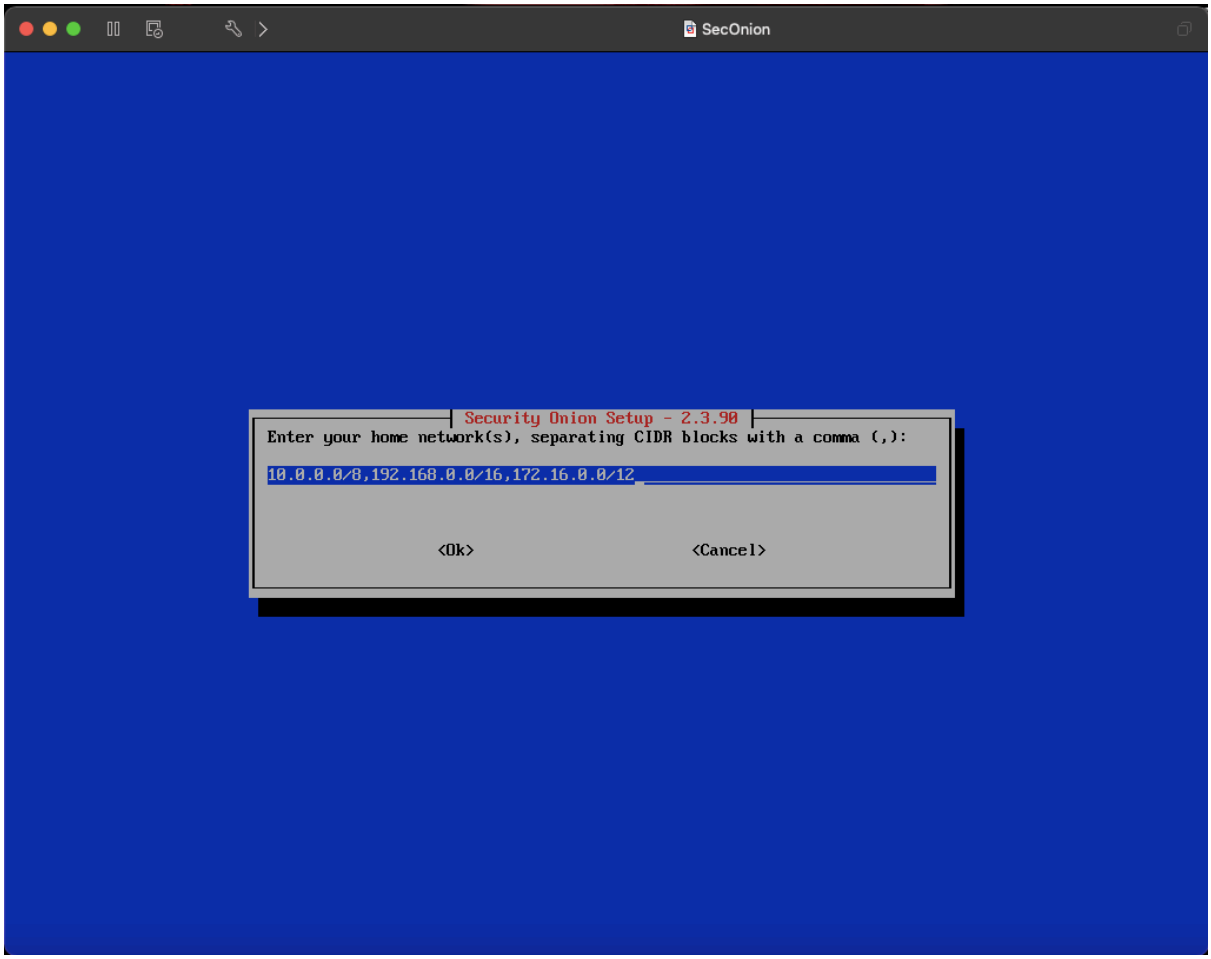

SecOnion
Security Onion Setup - 2.3.90
WARNING: Using DHCP can cause problems if your IP address changes. If you want to use DHCP, make sure that you have a DHCP reservation so that this does not occur. Otherwise, use a static IP address to be safe.
Select YES to keep DHCP or NO to go back.
<Yes>
<No>

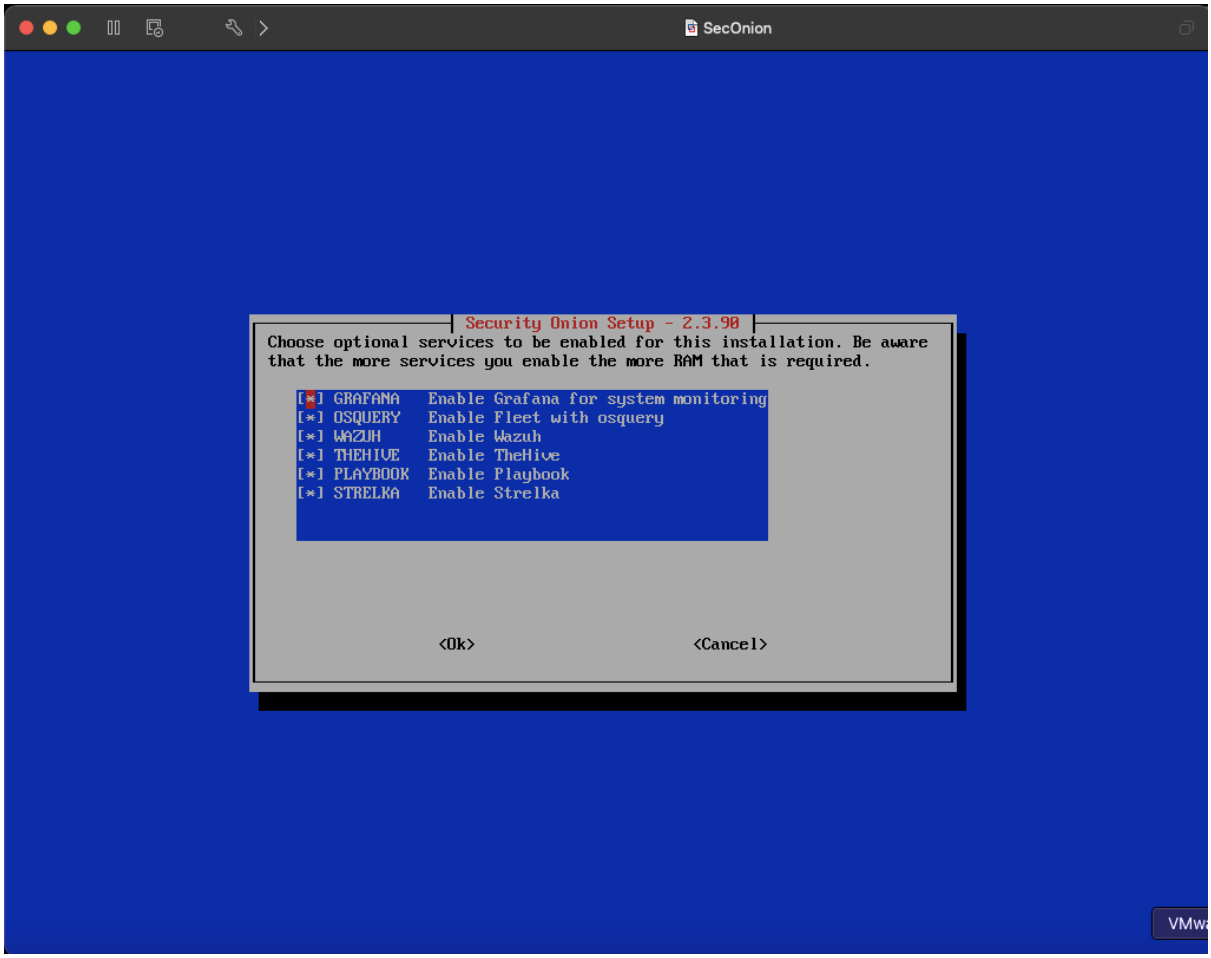

SecOnion
Security Onion Setup - 2.3.90
How should this manager be installed?
Standard This manager has internet accesss
Airgap This manager does not have internet access
<Ok>
<Cancel>

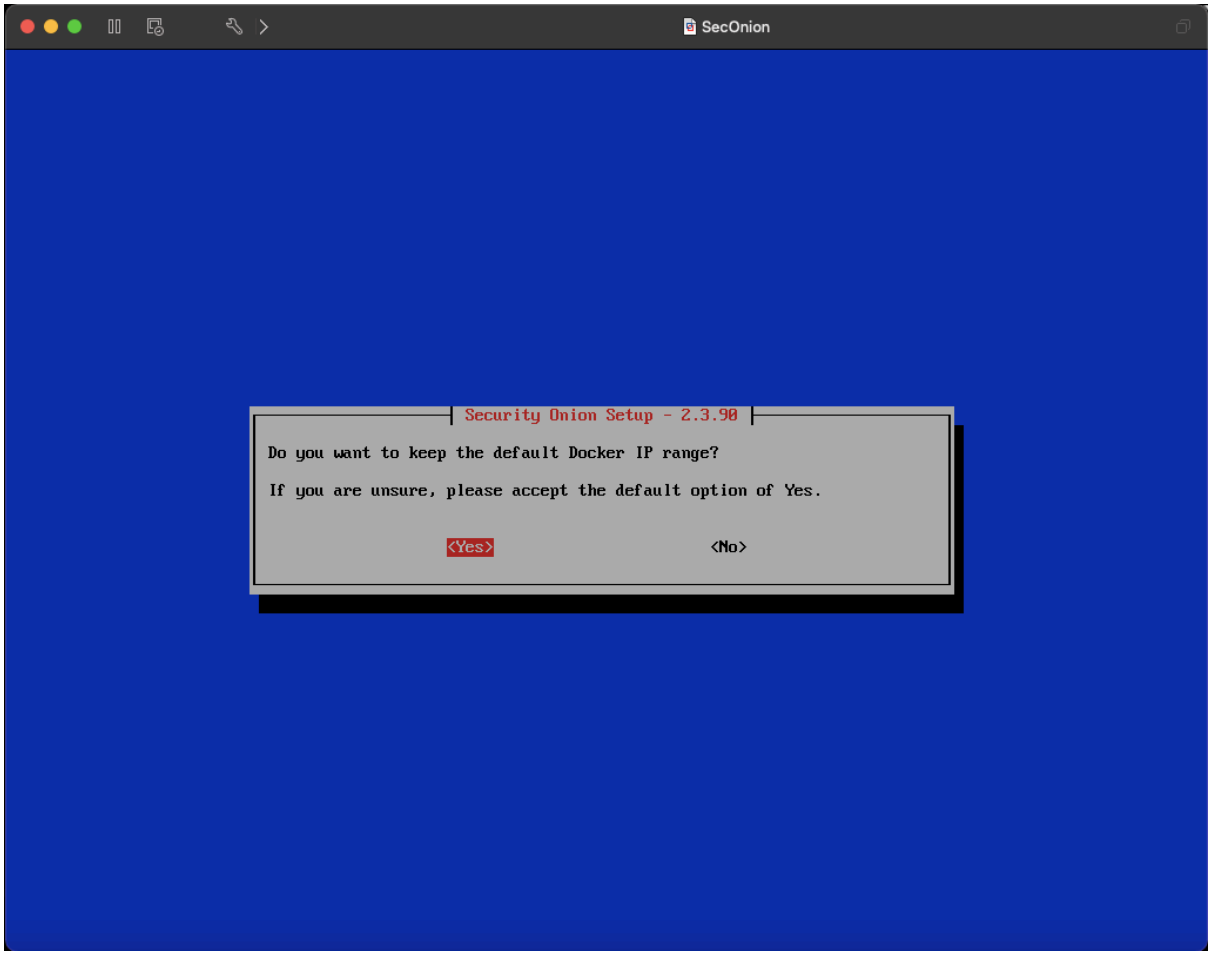

SecOnion
Security Onion Setup - 2.3.90
How would you like to connect to the Internet?
"Direct" - Internet requests connect directly to the Internet.
"Proxy" - proxy the traffic for git, docker client, wget, curl, yum, and various other SO components through a separate server in your environment.
Direct
Proxy
<Ok>
<Cancel>

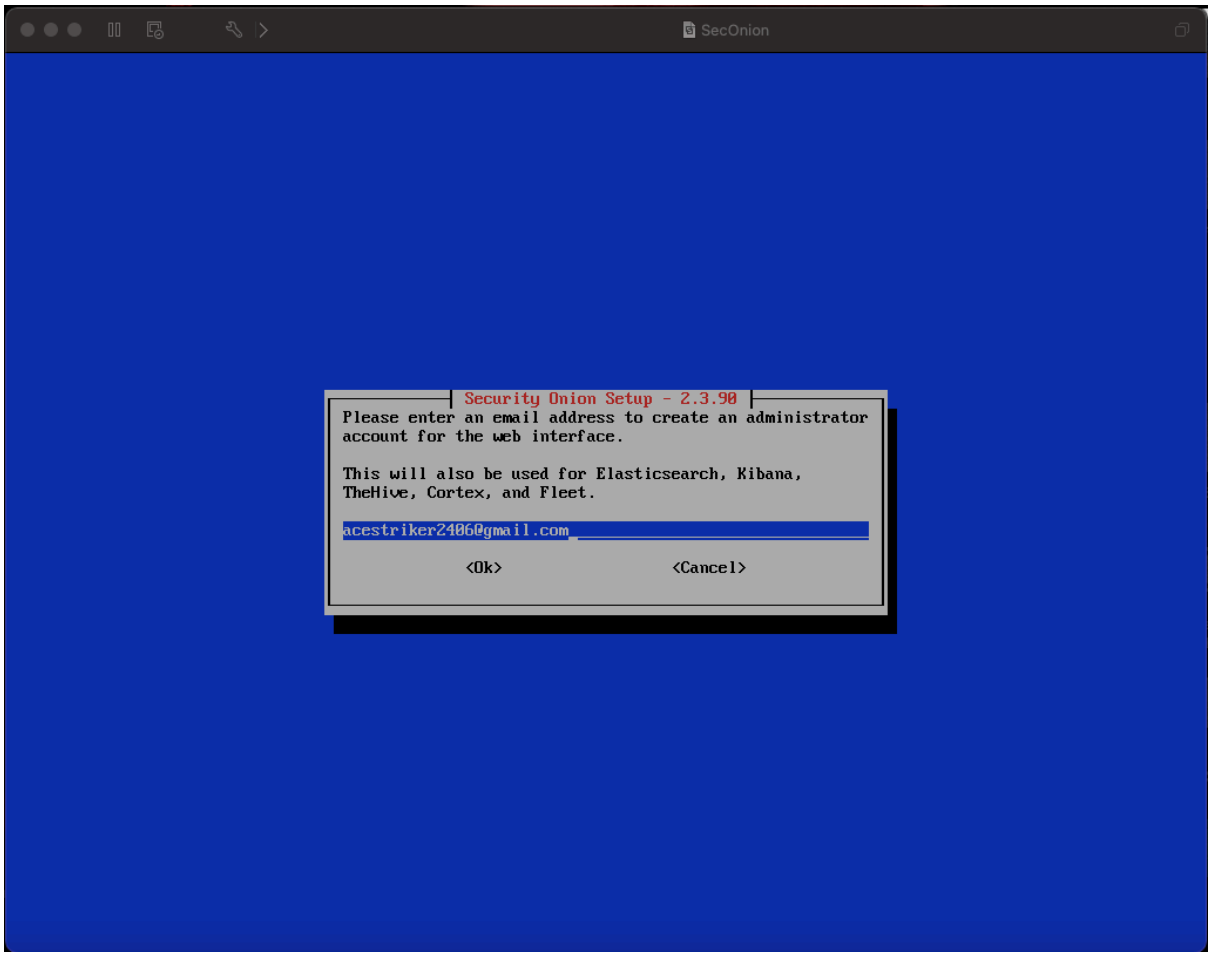

SecOnion
Security Onion Setup - 2.3.90
Please add NICs to the Monitor Interface:
[*] ens34 00:0c:29:69:65:3e Link UP
[ ] ens35 00:0c:29:69:65:48 Link UP
<Ok>
<Cancel>

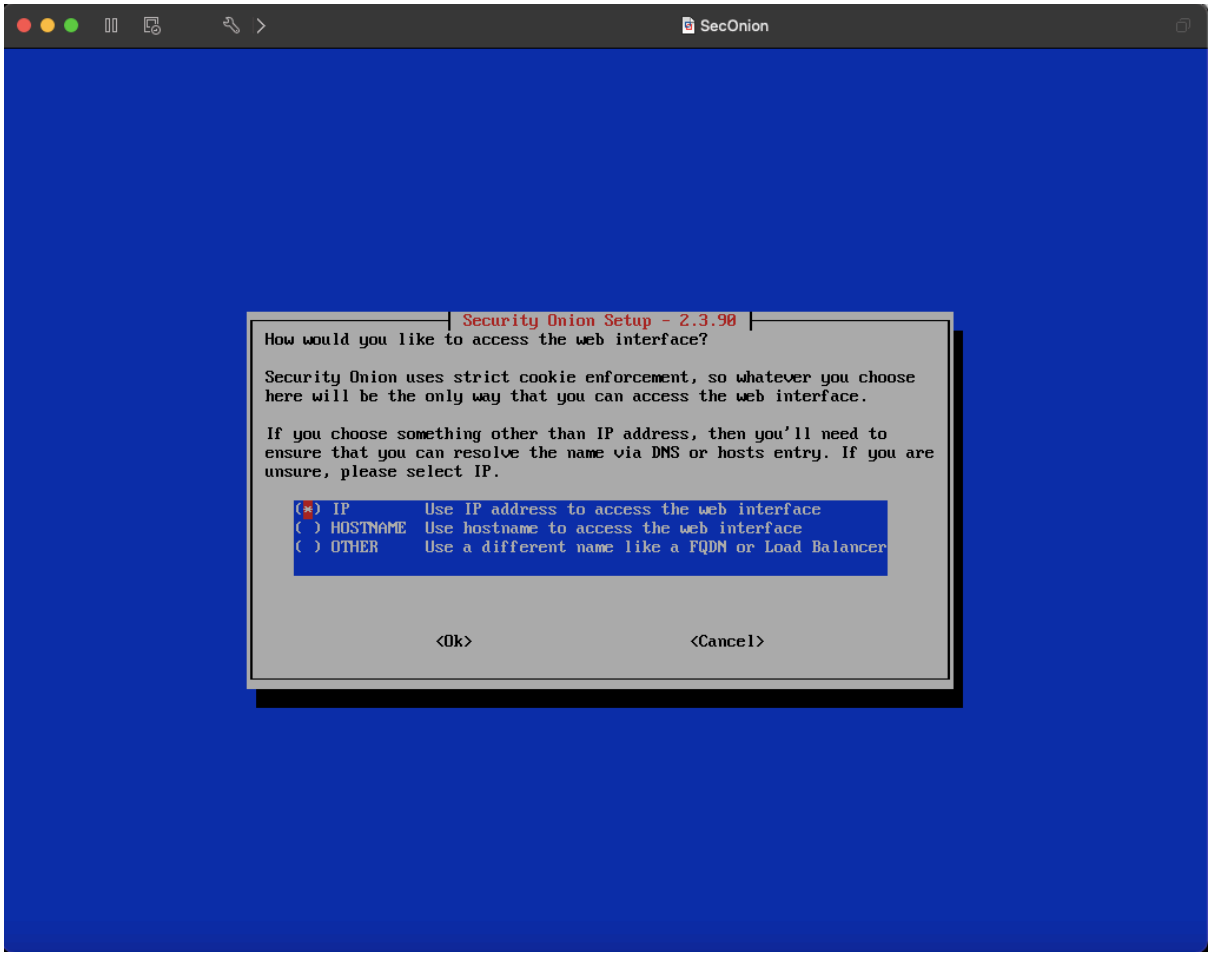

SecOnion
Security Onion Setup - 2.3.90
Choose OS patch schedule.
This schedule will update the operating system packages but will NOT update Security Onion related tools such as Zeek, Elasticsearch, Kibana, SaltStack, etc.
(*) Automatic Updates installed every 8 hours if available
( ) Manual Updates will be installed manually
( ) Import Schedule Import named schedule on following screen
( ) New Schedule Configure and name new schedule on next screen
<Ok>
<Cancel>

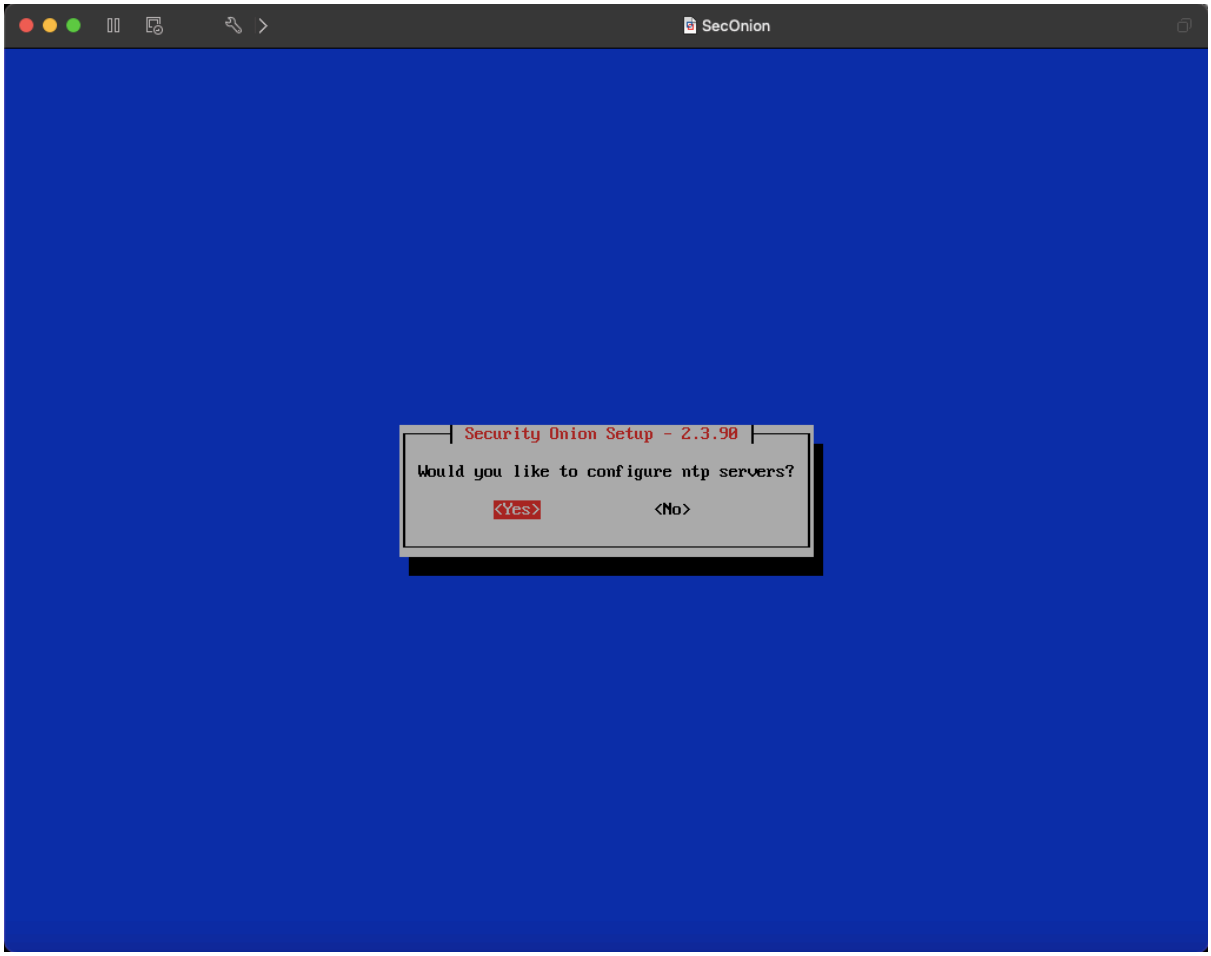

SecOnion
Security Onion Setup - 2.3.90
Enter your home network(s), separating CIDR blocks with a comma (,):
10.0.0.0/8,192.168.0.0/16,172.16.0.0/12
<Ok>
<Cancel>

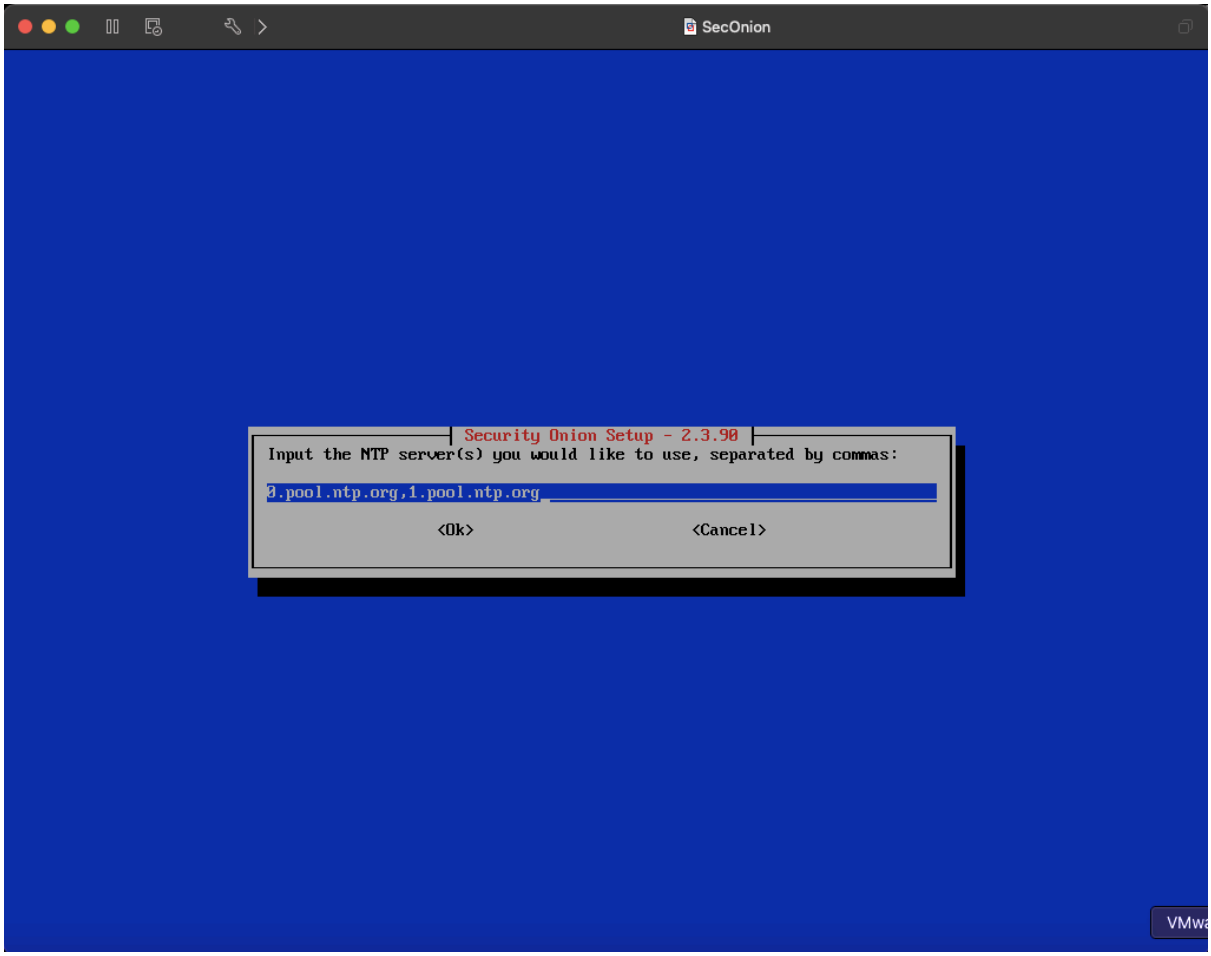

SecOnion
Security Onion Setup - 2.3.90
Choose optional services to be enabled for this installation. Be aware that the more services you enable the more RAM that is required.
[*] GRAFANA Enable Grafana for system monitoring
[*] OSQUERY Enable Fleet with osquery
[*] WAZUH Enable Wazuh
[*] THEHIVE Enable TheHive
[*] PLAYBOOK Enable Playbook
[*] STRELKA Enable Strelka
<Ok>
<Cancel>

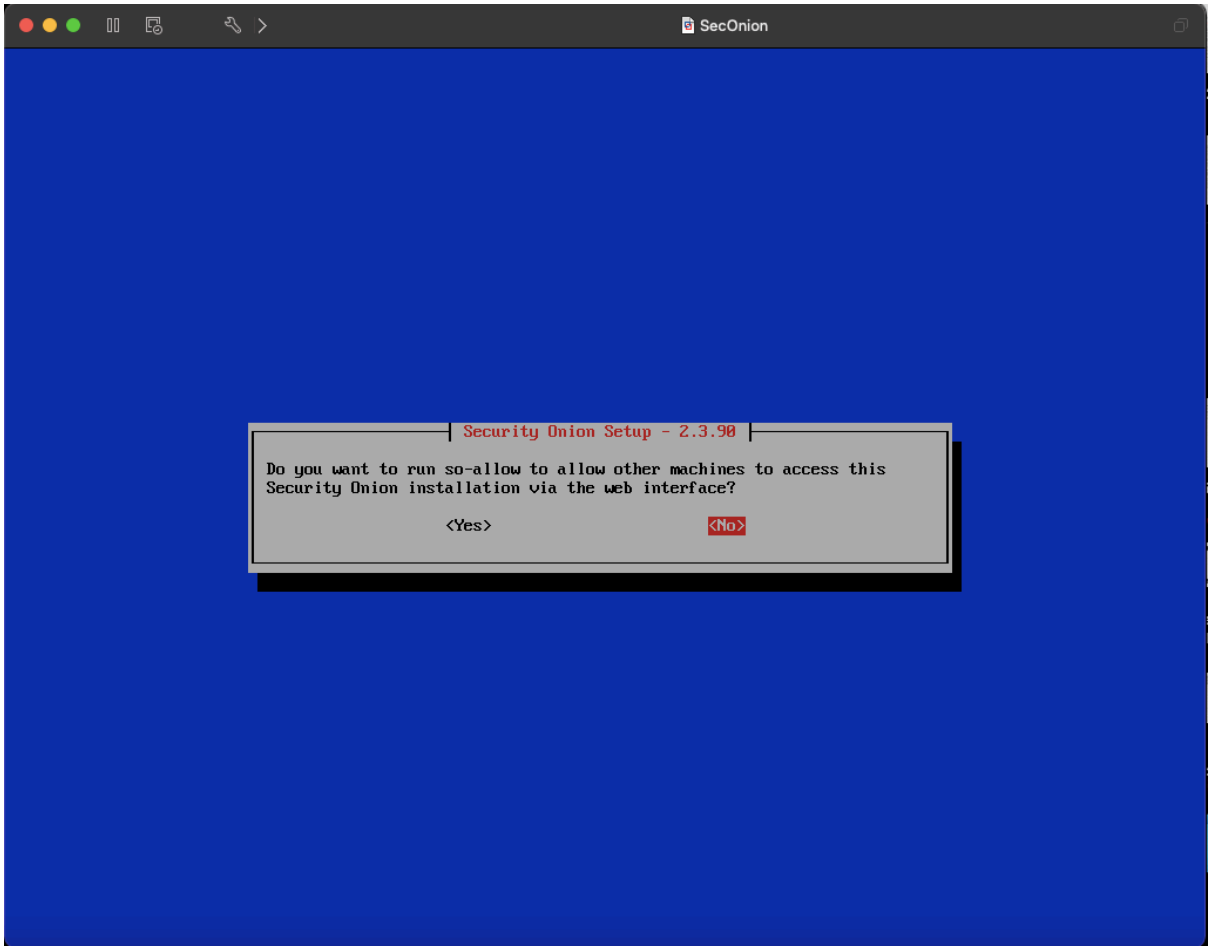

SecOnion
Security Onion Setup - 2.3.90
Do you want to keep the default Docker IP range?
If you are unsure, please accept the default option of Yes.
<Yes>
<No>

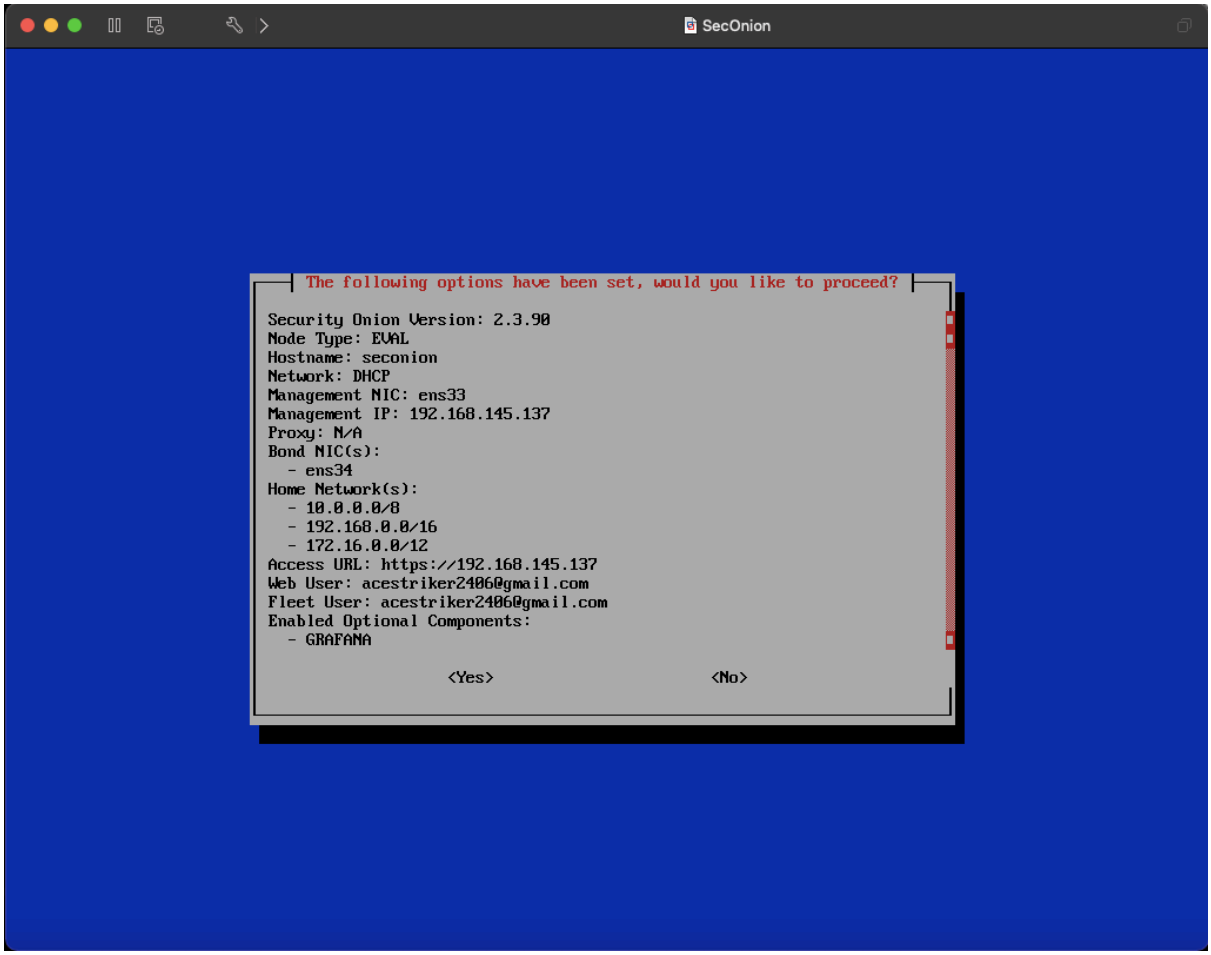

SecOnion
Security Onion Setup - 2.3.90
Please enter an email address to create an administrator
account for the web interface.
This will also be used for Elasticsearch, Kibana,
TheHive, Cortex, and Fleet.
acestriker2406@gmail.com
<Ok>
<Cancel>


SecOnion
Security Onion Setup - 2.3.90
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>


SecOnion
Security Onion Setup - 2.3.90
Would you like to configure ntp servers?
<Yes>
<No>


SecOnion
Security Onion Setup - 2.3.90
Input the NTP server(s) you would like to use, separated by commas:
0.pool.ntp.org,1.pool.ntp.org
<Ok>
<Cancel>
VMwa

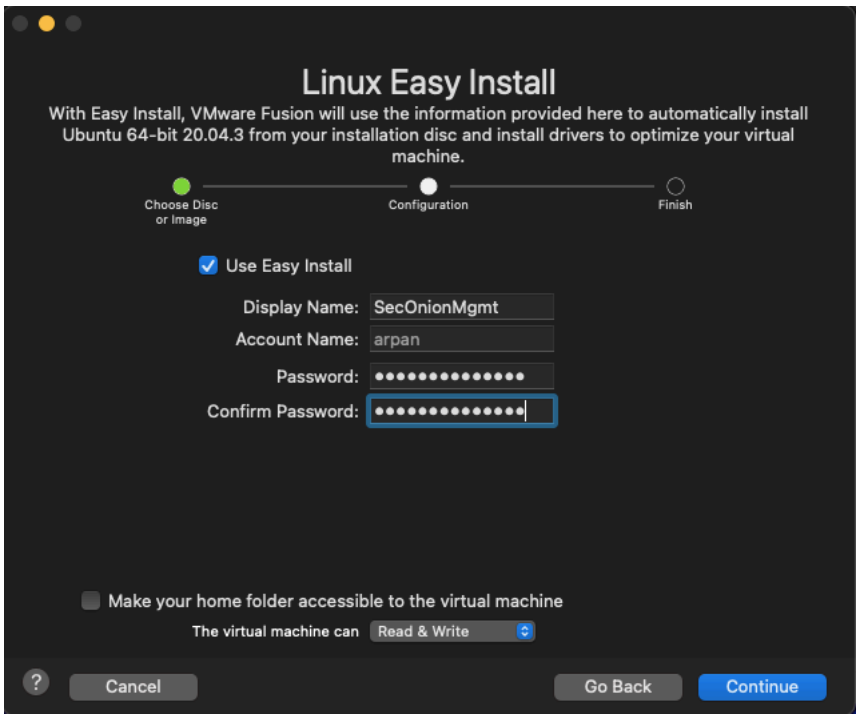

SecOnion
Security Onion Setup - 2.3.90
Do you want to run so-allow to allow other machines to access this Security Onion installation via the web interface?
<Yes>
<No>

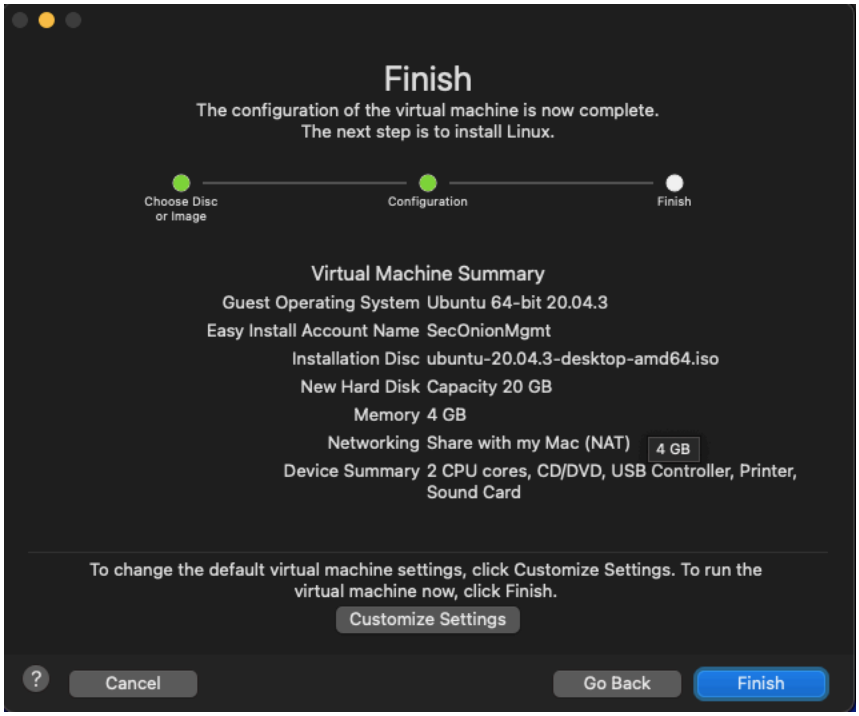

SecOnion
The following options have been set, would you like to proceed?
Security Onion Version: 2.3.90
Node Type: EVAL
Hostname: seconion
Network: DHCP
Management NIC: ens33
Management IP: 192.168.145.137
Proxy: N/A
Bond NIC(s):
- ens34
Home Network(s):
- 10.0.0.0/8
- 192.168.0.0/16
- 172.16.0.0/12
Access URL: https://192.168.145.137
Web User: acestriker2406@gmail.com
Fleet User: acestriker2406@gmail.com
Enabled Optional Components:
- GRAFANA
<Yes>
<No>

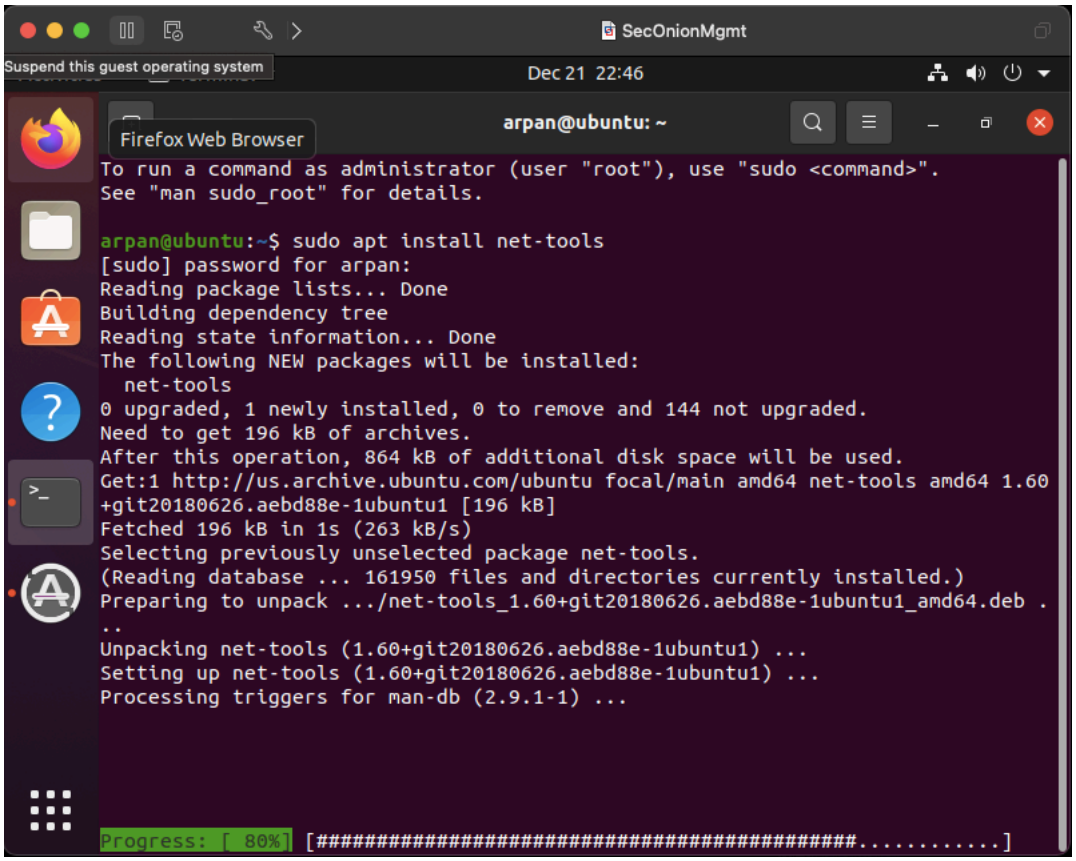
Security Onion Management/ Analyst machine –

After installing Security Onion, having access to the web interface will be done from an external Ubuntu desktop simulating a SOC/Security analyst accessing a SIEM or any other tool from their device.

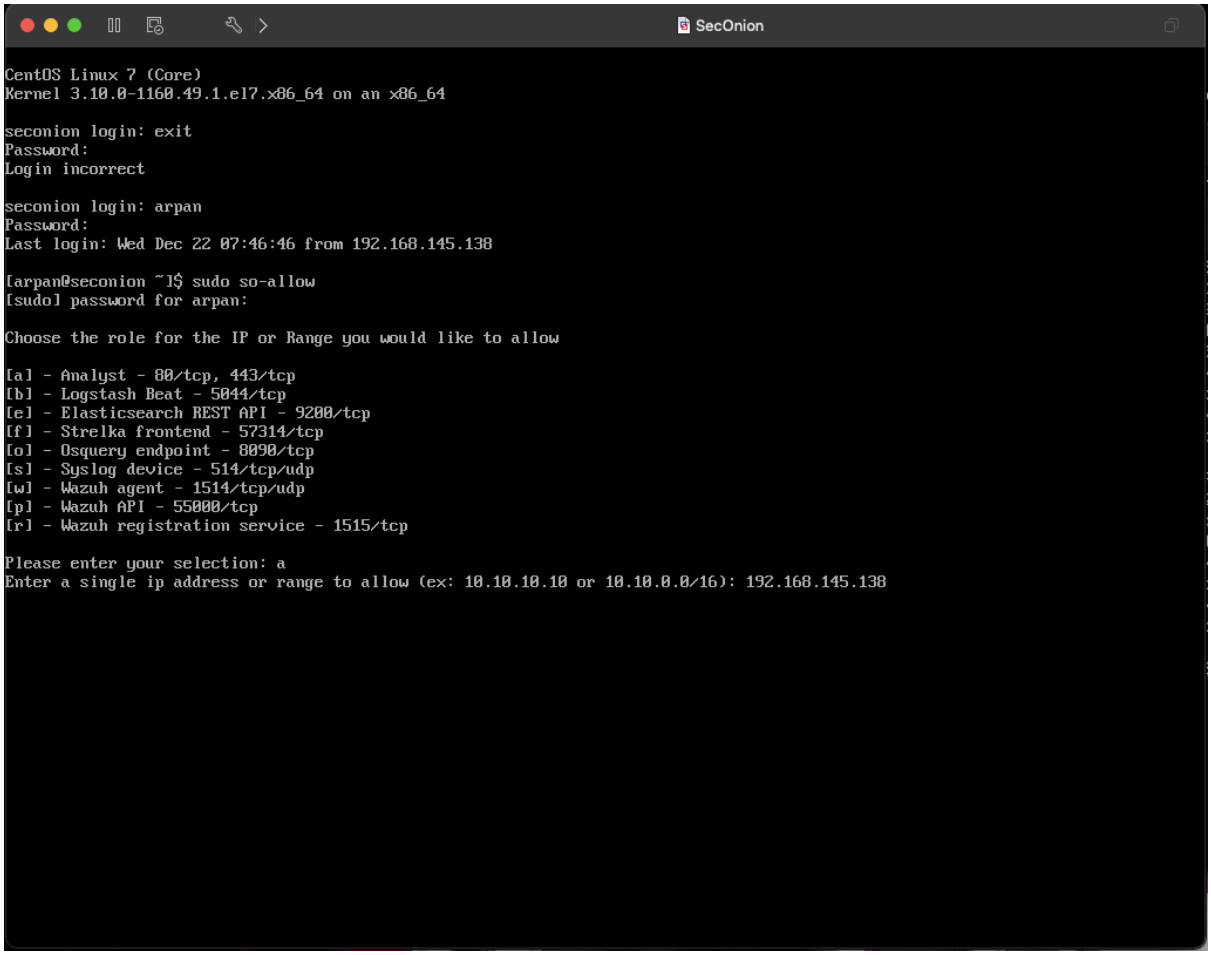
Configuring Ubuntu desktop –
Download the iso file from https://ubuntu.com/download/desktop and install the VM. Take not of the IP address by typing “ifconfig” on terminal.



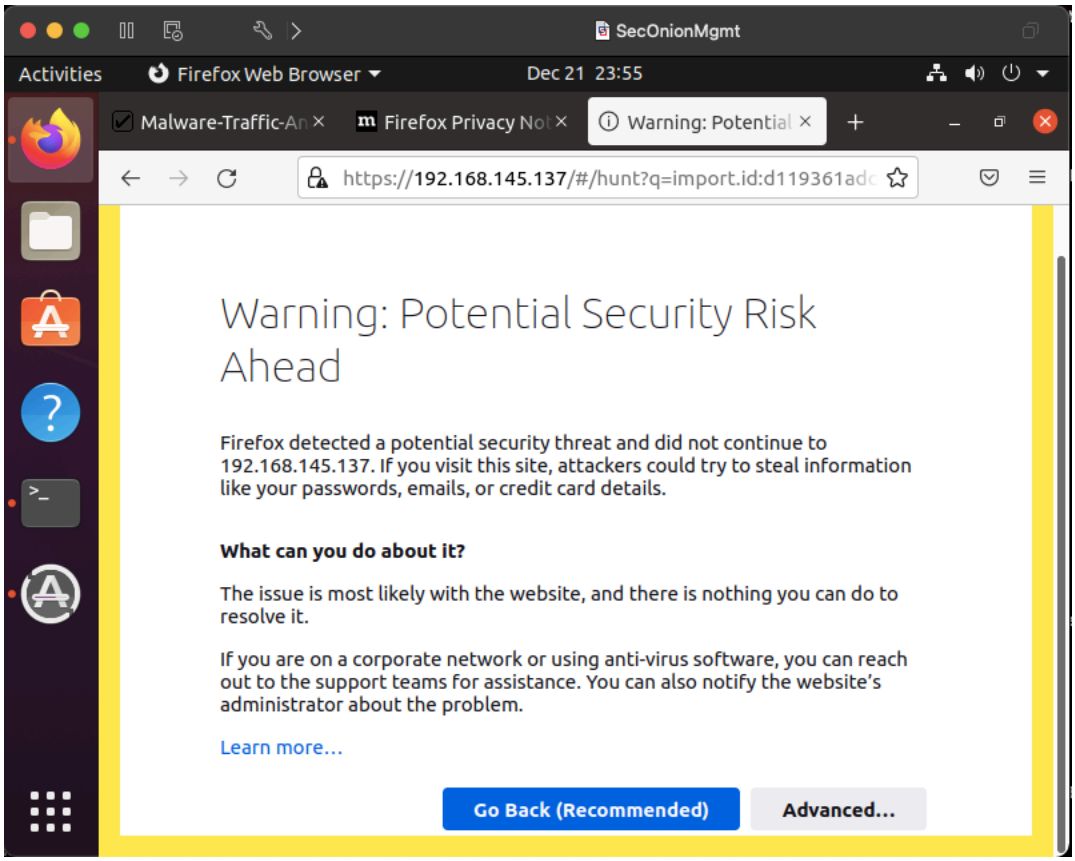

Finish
The configuration of the virtual machine is now complete.
The next step is to install Linux.
Choose Disc or Image
Configuration
Finish
Virtual Machine Summary
Guest Operating System Ubuntu 64-bit 20.04.3
Easy Install Account Name SecOnionMgmt
Installation Disc ubuntu-20.04.3-desktop-amd64.iso
New Hard Disk Capacity 20 GB
Memory 4 GB
Networking Share with my Mac (NAT)
4 GB
Device Summary 2 CPU cores, CD/DVD, USB Controller, Printer, Sound Card
To change the default virtual machine settings, click Customize Settings. To run the virtual machine now, click Finish.
Customize Settings
Cancel
Go Back
Finish

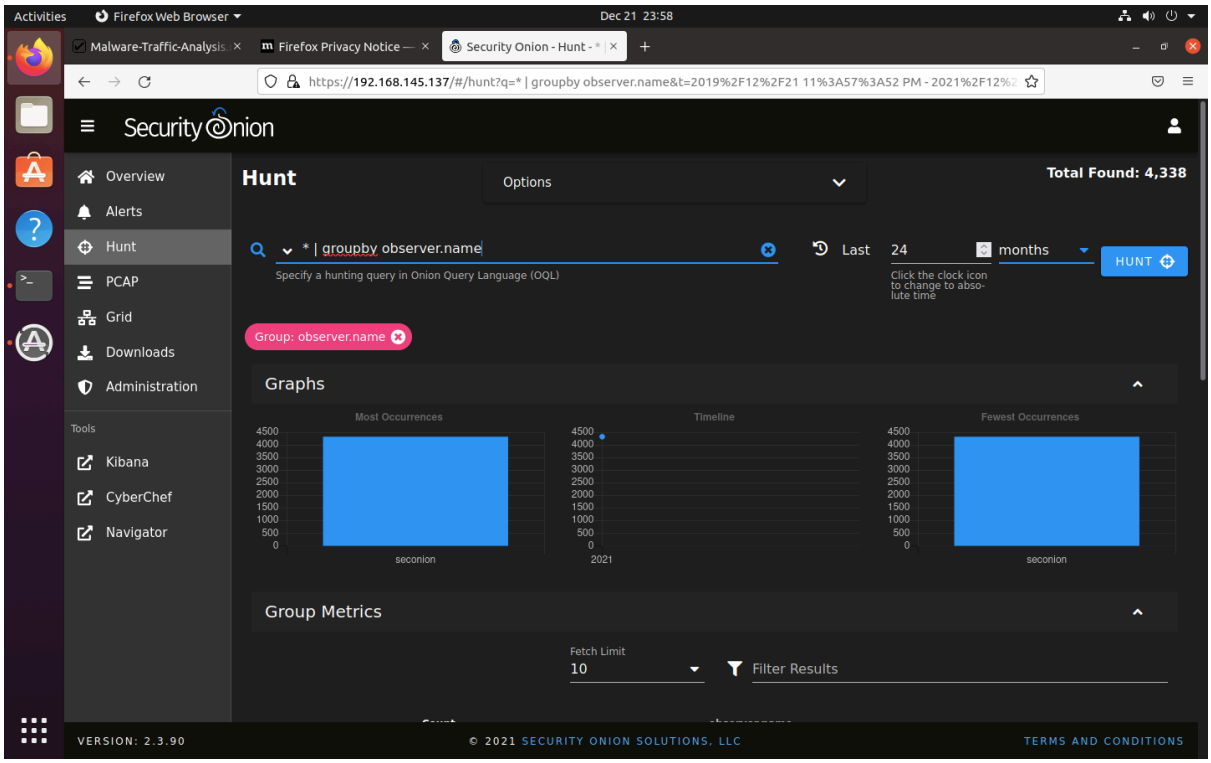

SecOnionMgmt
Suspend this guest operating system
Dec 21 22:46
Firefox Web Browser
arpan@ubuntu: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
arpan@ubuntu:~$ sudo apt install net-tools
[sudo] password for arpan:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
net-tools
0 upgraded, 1 newly installed, 0 to remove and 144 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60
+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 1s (263 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 161950 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb .
..
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
Progress: [80%] [##.....]

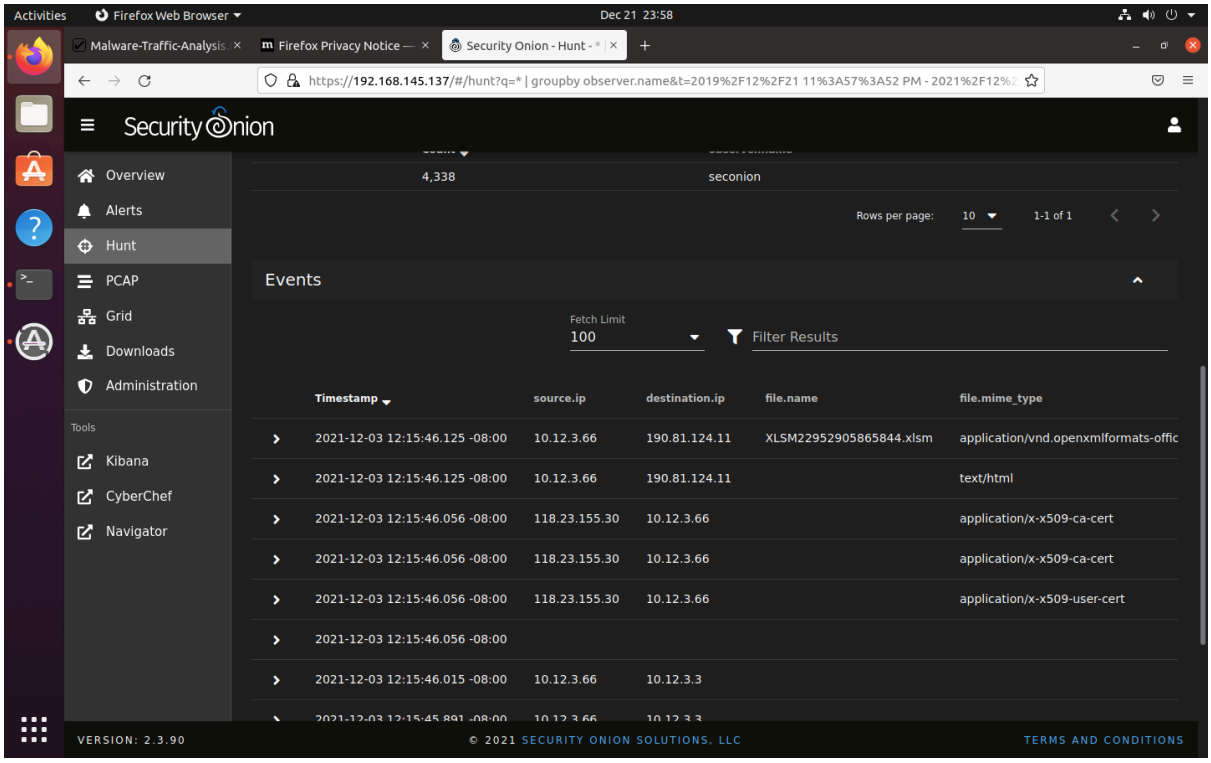
Head back to the Security Onion instance and run the following command – “sudo so-allow”
Enter password, type a and wait for the process to complete

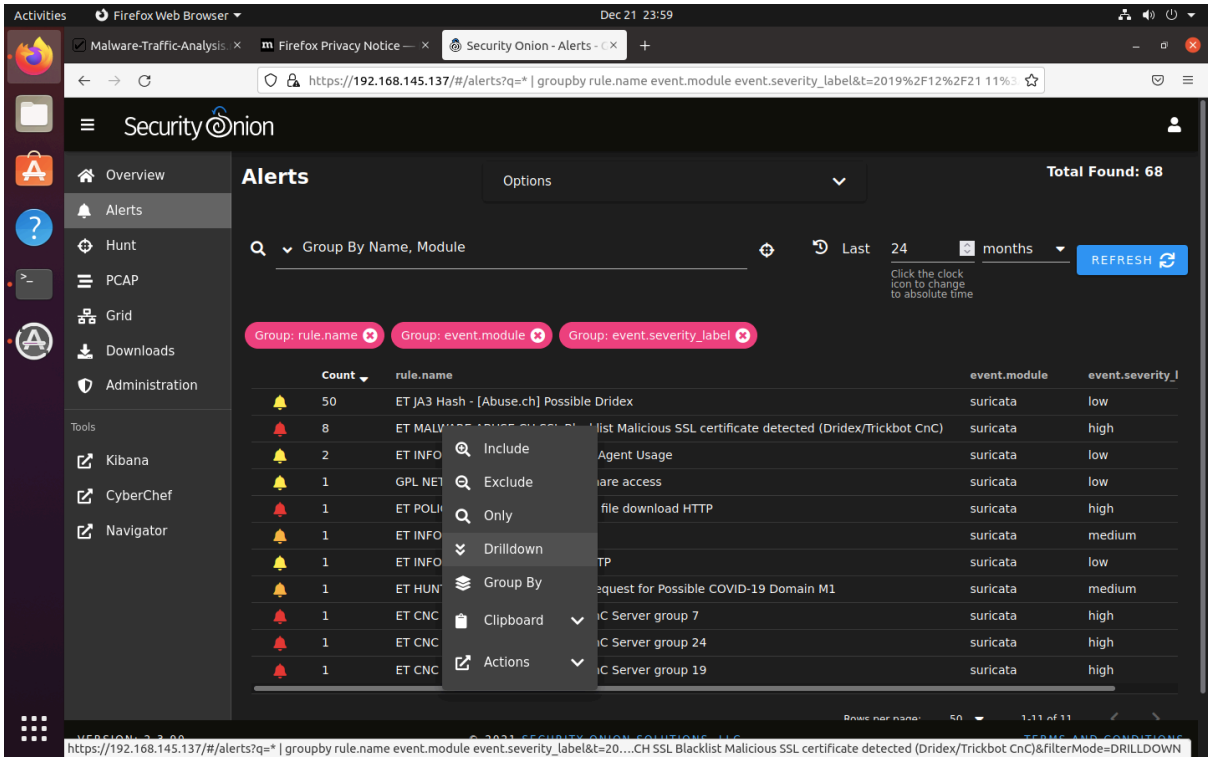


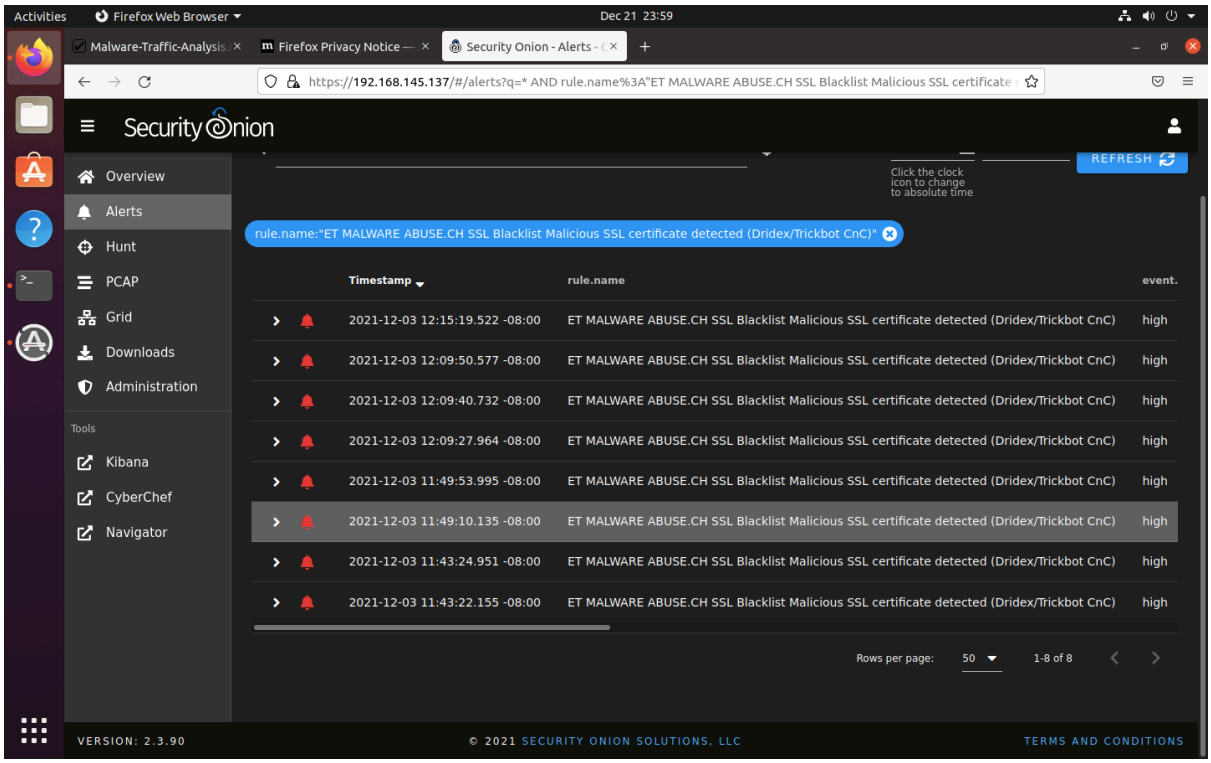
Type in the IP address from the Ubuntu desktop.
This will create a firewall rule on Security Onion that will allow you web access from the Ubuntu desktop.
Navigate to the Security Onion IP address on your Ubuntu desktop.

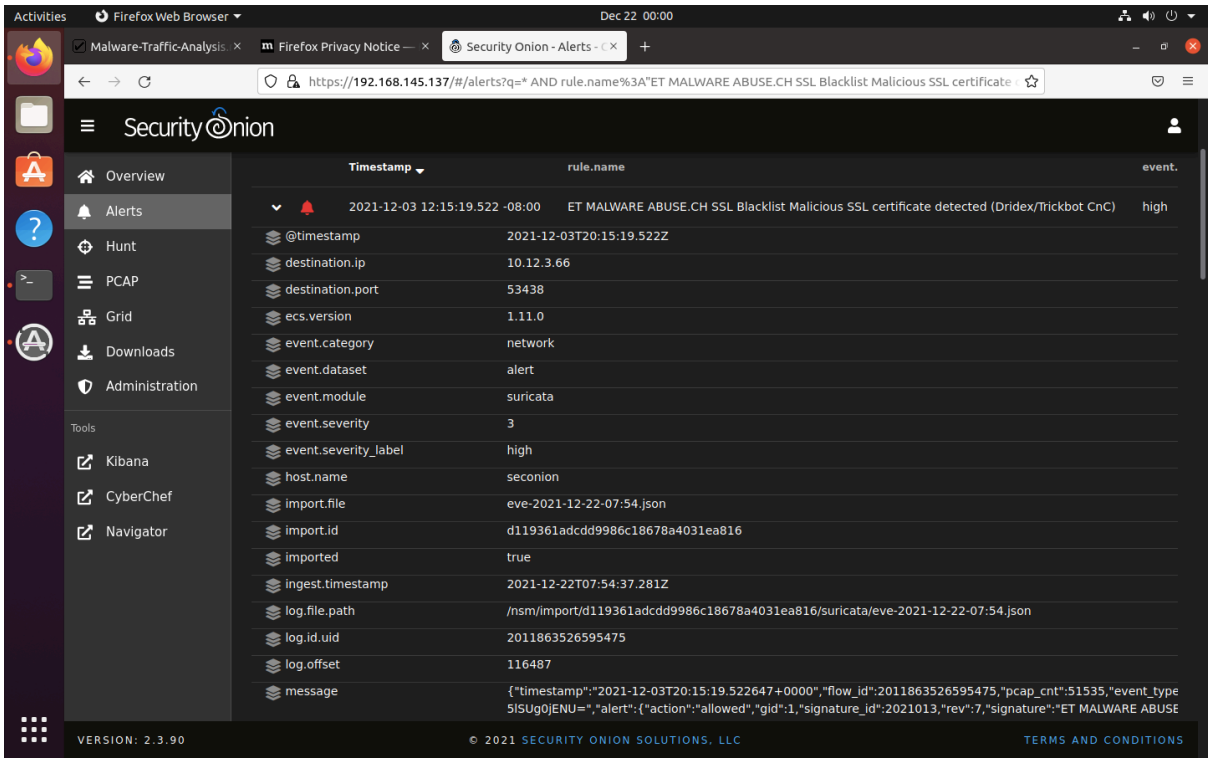



Activities
Firefox Web Browser
Dec 21 23:58
Malware-Traffic-Analysis
Firefox Privacy Notice —
Security Onion - Hunt -
https://192.168.145.137/#/hunt?q=* | groupby observer.name&t=2019%2F12%2F21 11%3A57%3A52 PM - 2021%2F12%2
Security Onion
Overview
Alerts
Hunt
PCAP
Grid
Downloads
Administration
Tools
Kibana
CyberChef
Navigator
Hunt
Options
Total Found: 4,338
* | groupby observer.name
Specify a hunting query in Onion Query Language (OQL)
Last
24
months
HUNT
Click the clock icon to change to absolute time
Group: observer.name
Graphs
Most Occurrences
Timeline
Fewest Occurrences
4500
4000
3500
3000
2500
2000
1500
1000
500
0
seconion
2021
Group Metrics
Fetch Limit
10
Filter Results
VERSION: 2.3.90
© 2021 SECURITY ONION SOLUTIONS, LLC
TERMS AND CONDITIONS


Activities
Firefox Web Browser
Dec 21 23:58
Malware-Traffic-Analysis
Firefox Privacy Notice
Security Onion - Hunt -
https://192.168.145.137/#/hunt?q=* | groupby observer.name&t=2019%2F12%2F21 11%3A57%3A52 PM - 2021%2F12%
Security Onion
Overview
Alerts
Hunt
PCAP
Grid
Downloads
Administration
Tools
Kibana
CyberChef
Navigator
4,338
seconion
Rows per page:
10
1-1 of 1
Events
Fetch Limit
100
Filter Results
Timestamp
source.ip
destination.ip
file.name
file.mime_type
2021-12-03 12:15:46.125 -08:00
10.12.3.66
190.81.124.11
XLSM22952905865844.xlsm
application/vnd.openxmlformats-offic
2021-12-03 12:15:46.125 -08:00
10.12.3.66
190.81.124.11
text/html
2021-12-03 12:15:46.056 -08:00
118.23.155.30
10.12.3.66
application/x-x509-ca-cert
2021-12-03 12:15:46.056 -08:00
118.23.155.30
10.12.3.66
application/x-x509-ca-cert
2021-12-03 12:15:46.056 -08:00
118.23.155.30
10.12.3.66
application/x-x509-user-cert
2021-12-03 12:15:46.056 -08:00
2021-12-03 12:15:46.015 -08:00
10.12.3.66
10.12.3.3
VERSION: 2.3.90
© 2021 SECURITY ONION SOLUTIONS, LLC
TERMS AND CONDITIONS


Activities
Firefox Web Browser
Dec 21 23:59
Malware-Traffic-Analysis
Firefox Privacy Notice —
Security Onion - Alerts -
https://192.168.145.137/#/alerts?q=* | groupby rule.name event.module event.severity_label&t=2019%2F12%2F21 11%3
Security Onion
Overview
Alerts
Hunt
PCAP
Grid
Downloads
Administration
Tools
Kibana
CyberChef
Navigator
Alerts
Options
Total Found: 68
Group By Name, Module
Last
24
months
REFRESH
Click the clock icon to change to absolute time
Group: rule.name
Group: event.module
Group: event.severity_label
Count
rule.name
event.module
event.severity_l
50
ET JA3 Hash - [Abuse.ch] Possible Dridex
suricata
low
8
suricata
high
2
suricata
low
1
suricata
low
1
suricata
high
1
suricata
medium
1
suricata
low
1
suricata
medium
1
suricata
high
1
suricata
high
1
suricata
high
Include
Exclude
Only
Drilldown
Group By
Clipboard
Actions
Rows per page:
50
1-11 of 11
https://192.168.145.137/#/alerts?q=* | groupby rule.name event.module event.severity_label&t=20....CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)&filterMode=DRILLDOWN


Activities
Firefox Web Browser
Dec 21 23:59
Malware-Traffic-Analysis
Firefox Privacy Notice
Security Onion - Alerts
https://192.168.145.137/#/alerts?q=* AND rule.name%3A"ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate
Security Onion
Overview
Alerts
Hunt
PCAP
Grid
Downloads
Administration
Tools
Kibana
CyberChef
Navigator
REFRESH
Click the clock icon to change to absolute time
rule.name:"ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)"
Timestamp
rule.name
event.
2021-12-03 12:15:19.522 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
2021-12-03 12:09:50.577 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
2021-12-03 12:09:40.732 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
2021-12-03 12:09:27.964 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
2021-12-03 11:49:53.995 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
2021-12-03 11:49:10.135 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
2021-12-03 11:43:24.951 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
2021-12-03 11:43:22.155 -08:00 ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) high
Rows per page: 50
1-8 of 8
VERSION: 2.3.90
© 2021 SECURITY ONION SOLUTIONS, LLC
TERMS AND CONDITIONS

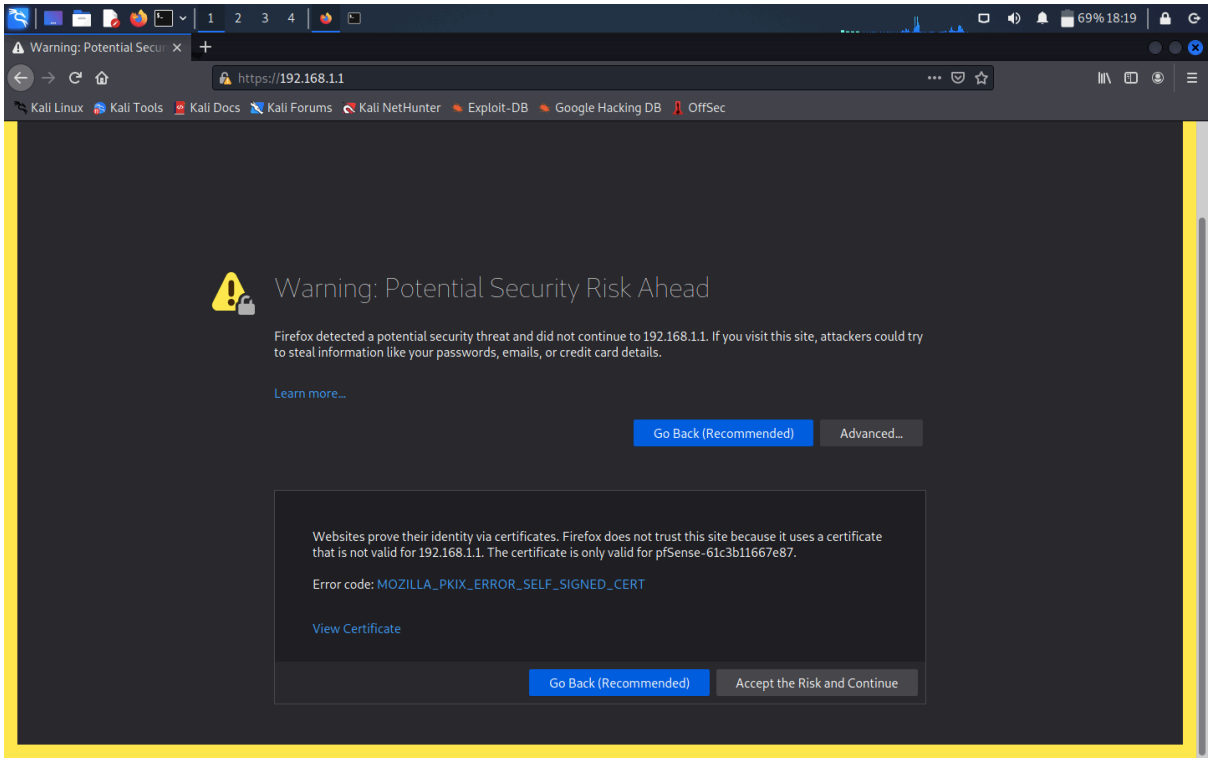

Activities
Firefox Web Browser
Dec 22 00:00
Malware-Traffic-Analysis
Firefox Privacy Notice —
Security Onion - Alerts -
https://192.168.145.137/#/alerts?q=* AND rule.name%3A"ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate
Security Onion
Overview
Alerts
Hunt
PCAP
Grid
Downloads
Administration
Tools
Kibana
CyberChef
Navigator
Timestamp
rule.name
event.
2021-12-03 12:15:19.522 -08:00
ET MALWARE ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)
high
@timestamp 2021-12-03T20:15:19.522Z
destination.ip 10.12.3.66
destination.port 53438
ecs.version 1.11.0
event.category network
event.dataset alert
event.module suricata
event.severity 3
event.severity_label high
host.name seconion
import.file eve-2021-12-22-07:54.json
import.id d119361adcdd9986c18678a4031ea816
imported true
ingest.timestamp 2021-12-22T07:54:37.281Z
log.file.path /nsm/import/d119361adcdd9986c18678a4031ea816/suricata/eve-2021-12-22-07:54.json
log.id.uid 2011863526595475
log.offset 116487
message {"timestamp":"2021-12-03T20:15:19.522647+0000","flow_id":2011863526595475,"pcap_cnt":51535,"event_type
5lSUg0jENU=","alert":{"action":"allowed","gid":1,"signature_id":2021013,"rev":7,"signature":"ET MALWARE ABUSE
VERSION: 2.3.90
© 2021 SECURITY ONION SOLUTIONS, LLC
TERMS AND CONDITIONS

Installing kali linux –

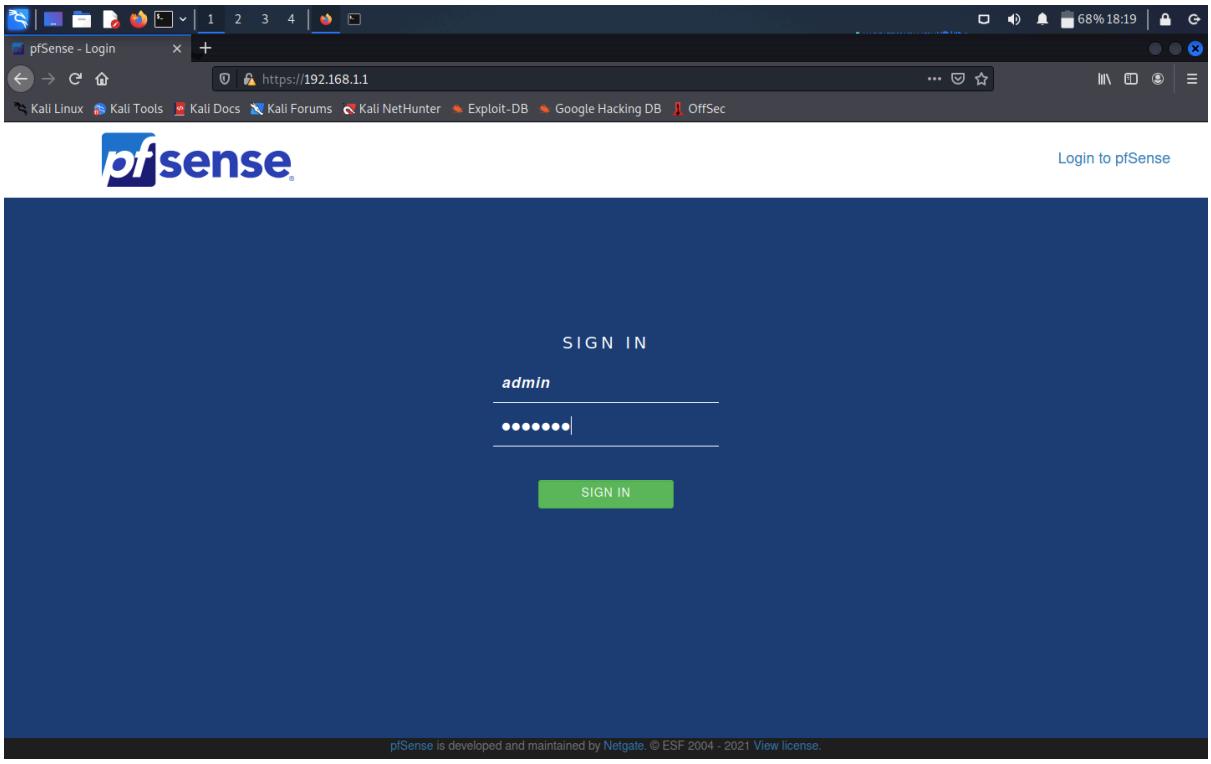
Install Kali linux machine in the similar manner, accept all the defaults and finish.
https://www.kali.org/get-kali/

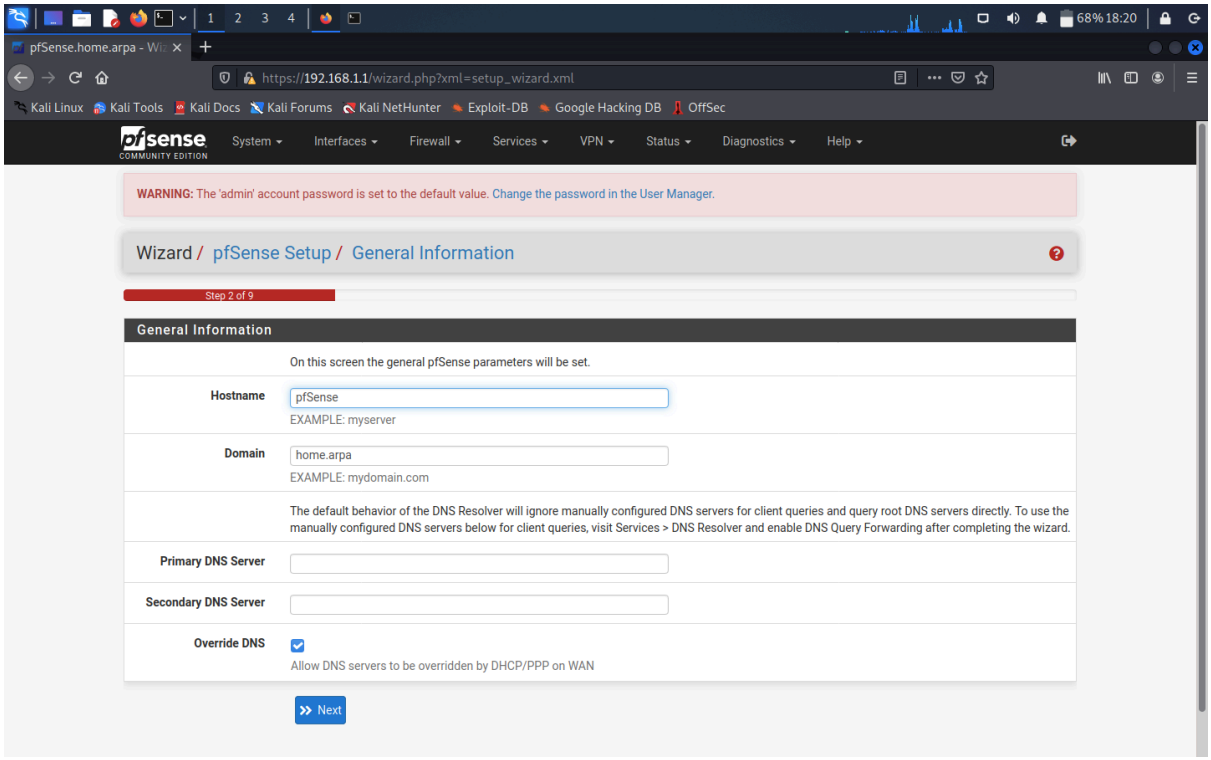
pfsense Interfaces and Rules –

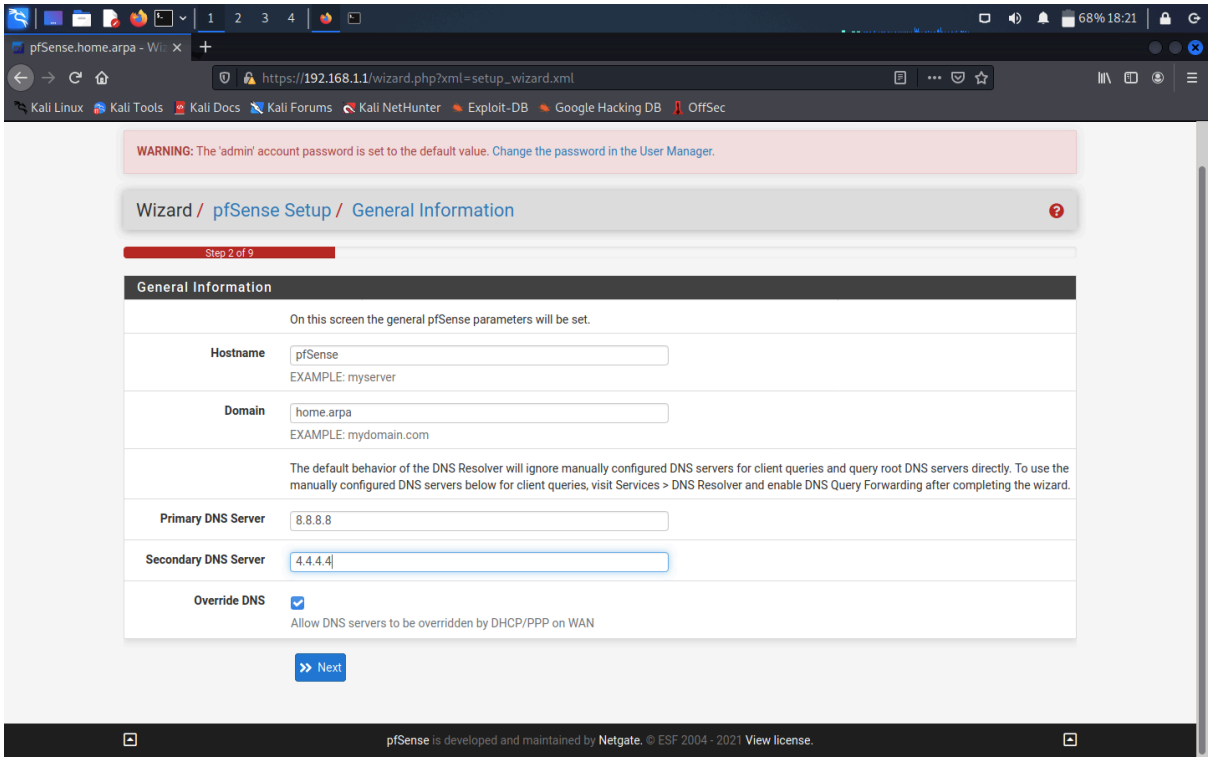
The psfsense webConfigurator can be accessed in order to make changes to pfsense interfaces and firewall rules.
Navigate to the web browser and search for 192.168.1.1
Select advanced and accept the risk.



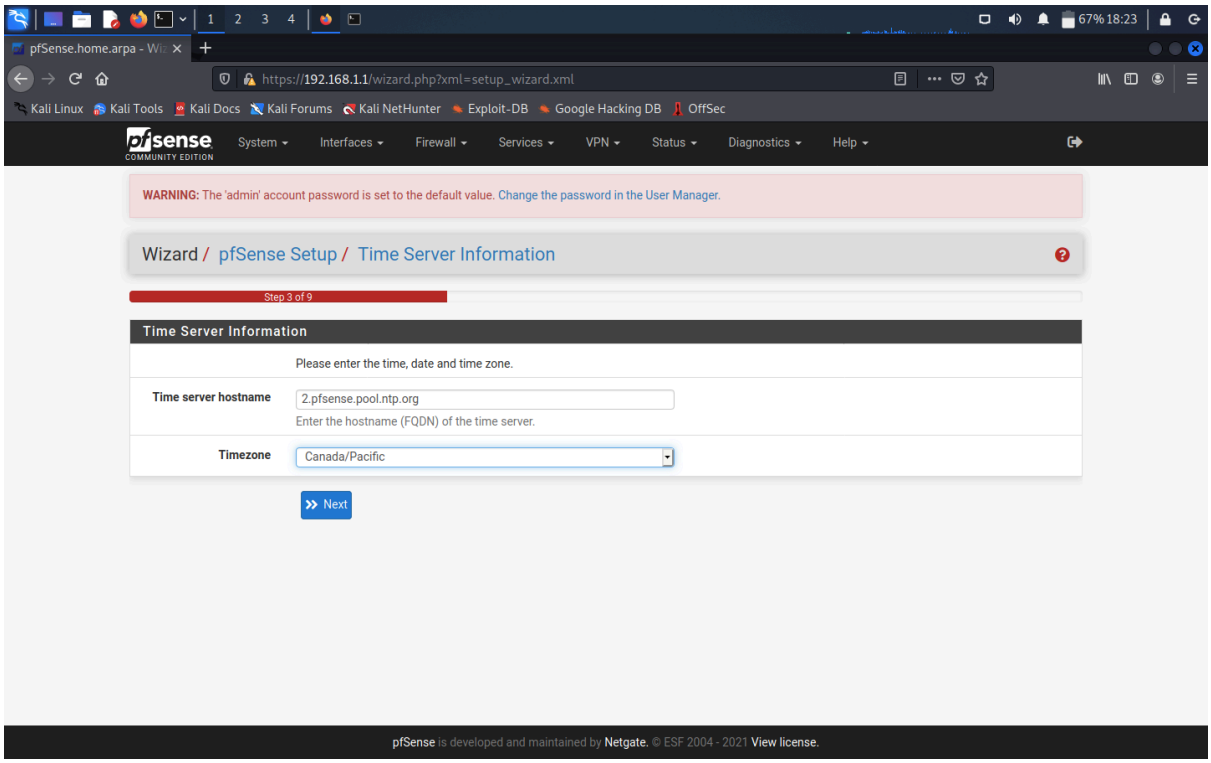
Sign in to pfsense using default credentials “admin” and “pfsense”
We will see the “Wizard/pfsense/Setup/“ page. Click next till you get to step 2 of 9.
Add 8.8.8.8 as Primary DNS Server and 4.4.4.4 as Secondary DNS Server and click next.

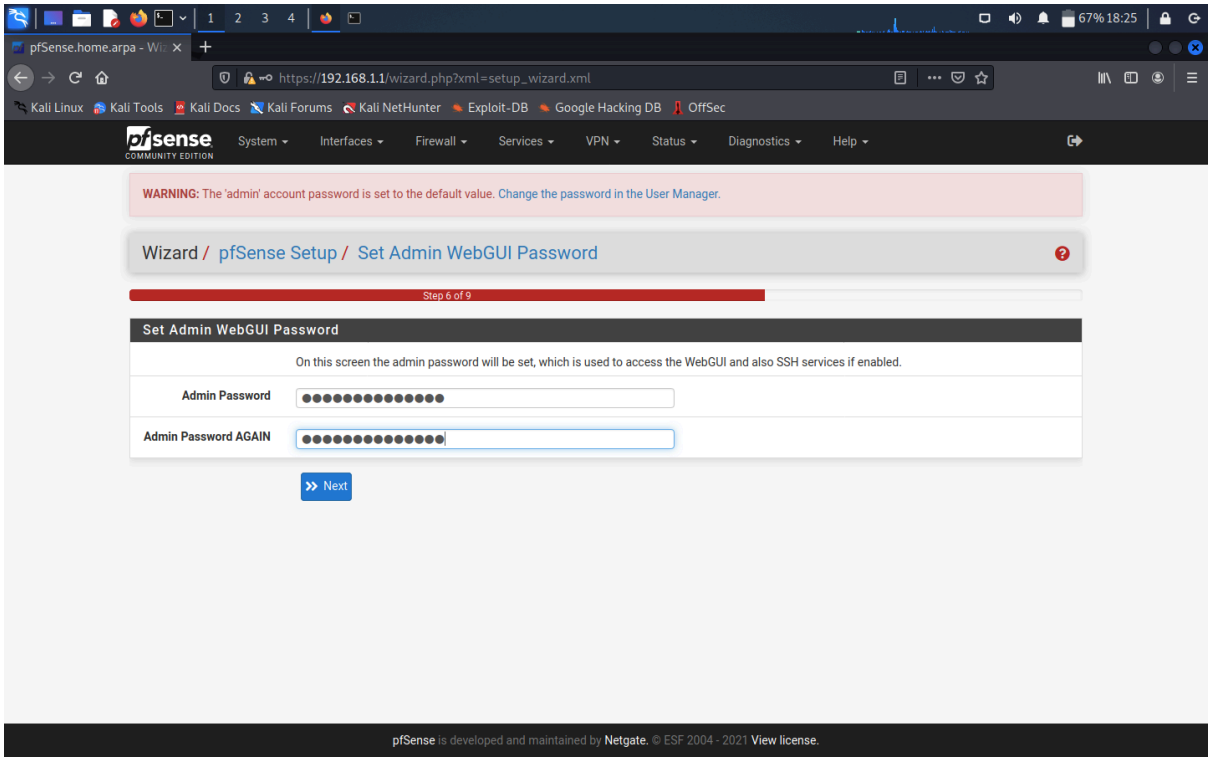


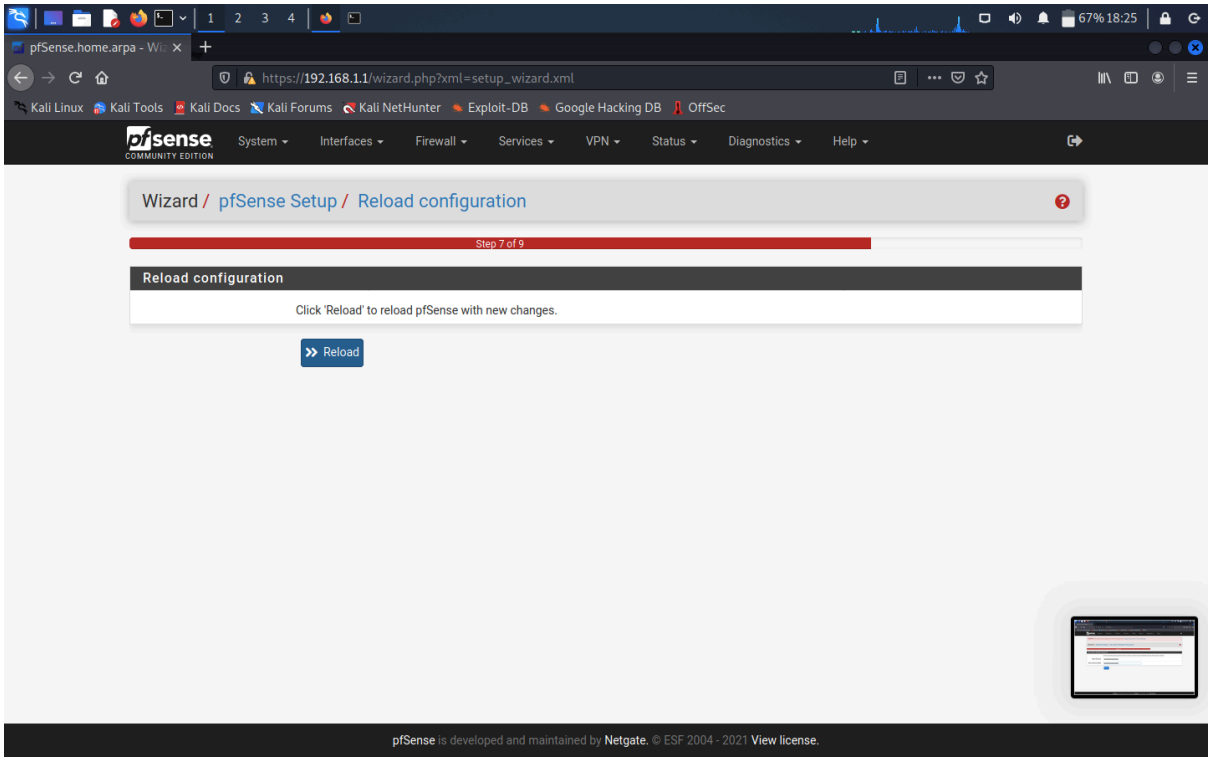

pfSense.home.arpa - Wiz
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / General Information
Step 2 of 9
General Information
On this screen the general pfSense parameters will be set.
Hostname
pfSense
EXAMPLE: myserver
Domain
home.arpa
EXAMPLE: mydomain.com
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server
Secondary DNS Server
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN
Next

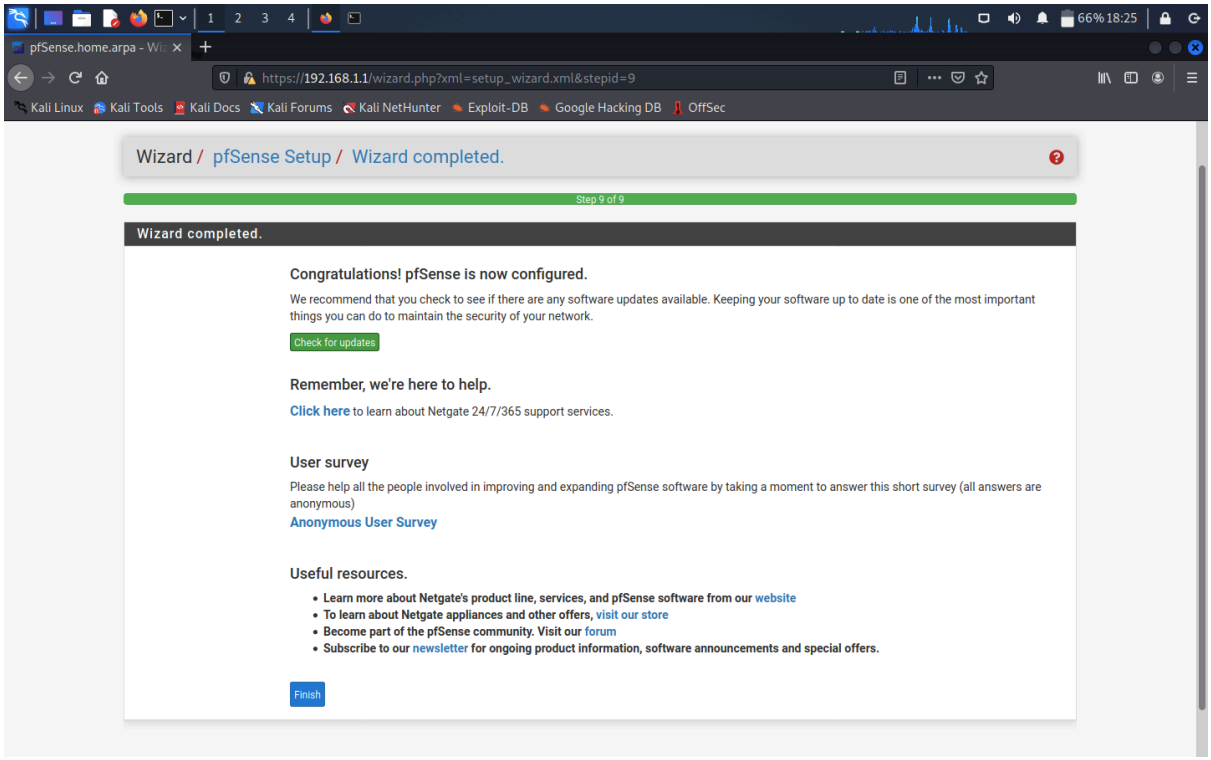

pfSense.home.arpa - Wi
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / General Information
Step 2 of 9
General Information
On this screen the general pfSense parameters will be set.
Hostname
pfSense
EXAMPLE: myserver
Domain
home.arpa
EXAMPLE: mydomain.com
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server
8.8.8.8
Secondary DNS Server
4.4.4.4
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

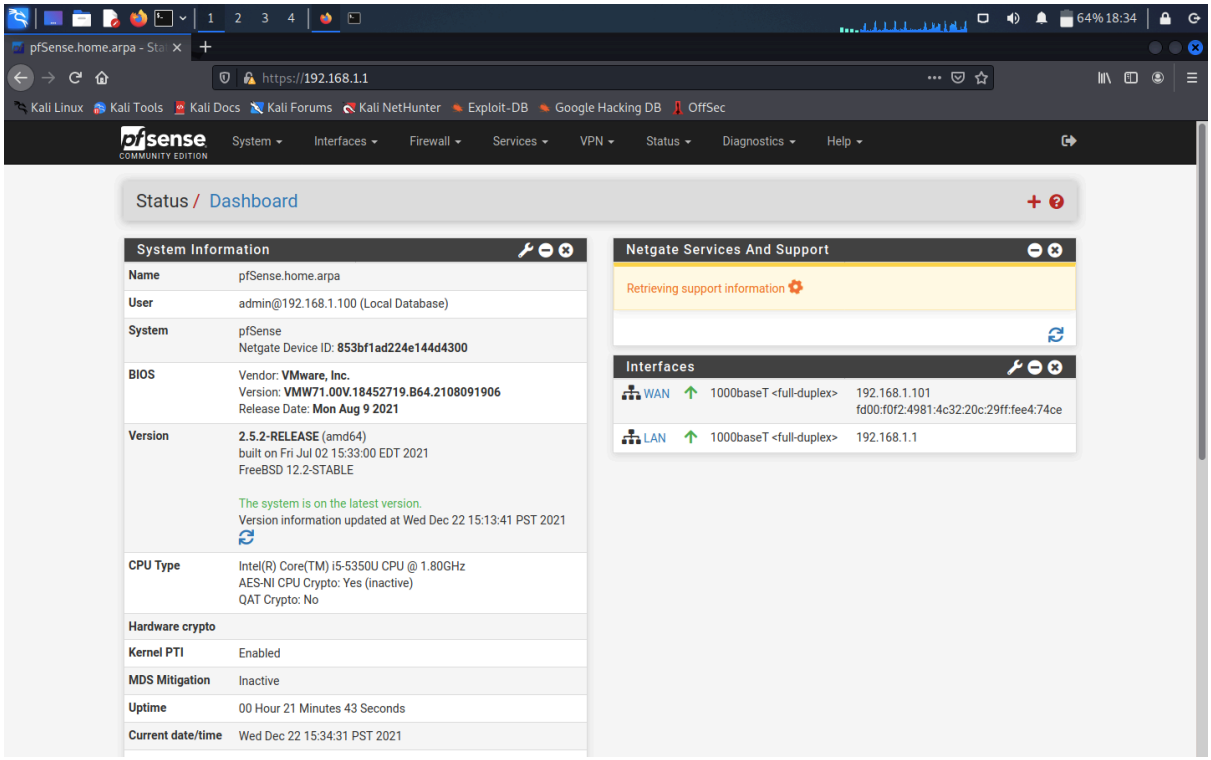
Select the following steps as show in the screenshots below and click on finish.



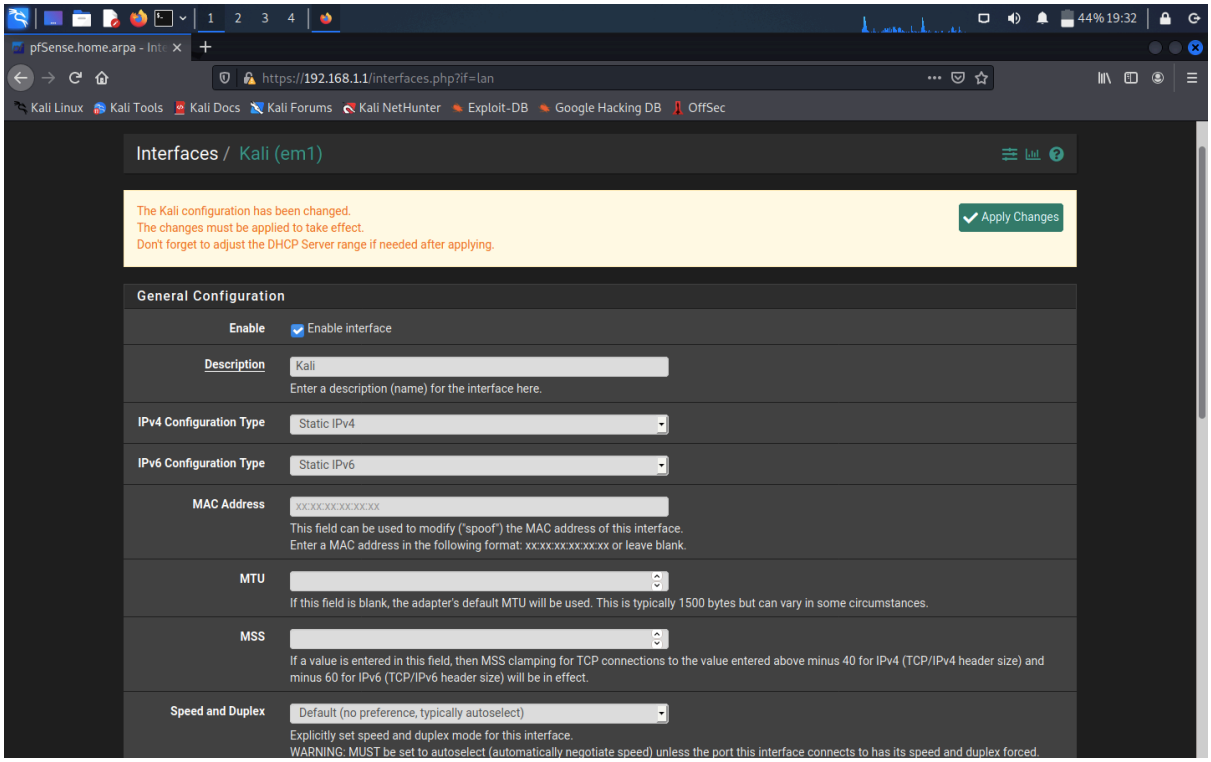

pfSense.home.arpa - Wi
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / Set Admin WebGUI Password
Step 6 of 9
Set Admin WebGUI Password
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.
Admin Password
Admin Password AGAIN
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

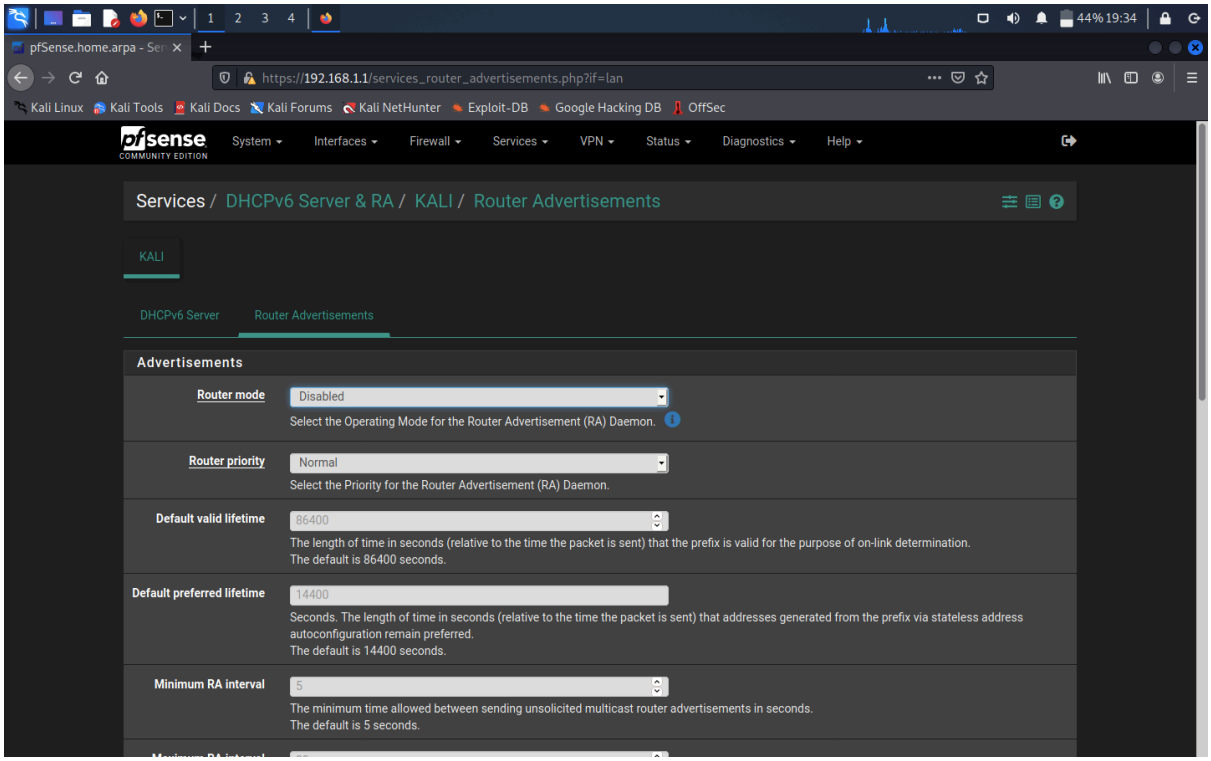

pfSense.home.arpa - Wi
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Reload configuration
Step 7 of 9
Reload configuration
Click 'Reload' to reload pfSense with new changes.
Reload
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

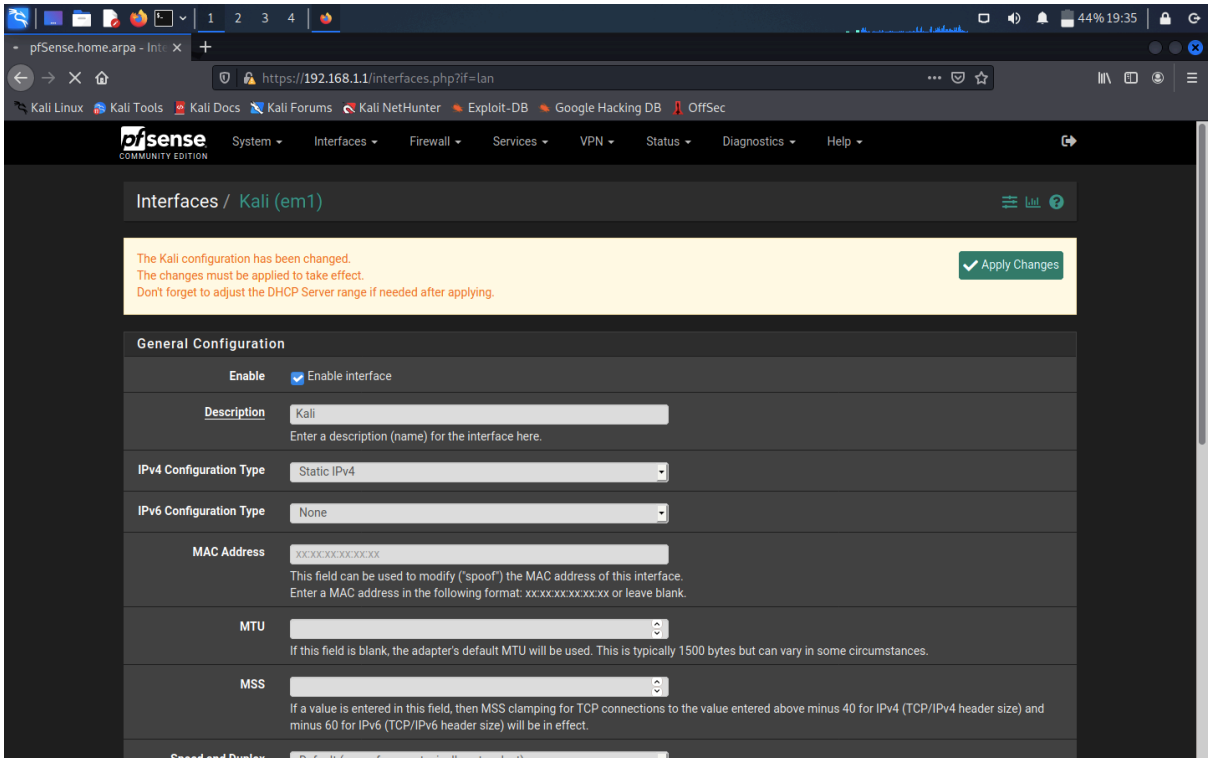

pfSense.home.arpa - Wiz
https://192.168.1.1/wizard.php?xml=setup_wizard.xml&stepid=9
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Wizard / pfSense Setup / Wizard completed.
Step 9 of 9
Wizard completed.
Congratulations! pfSense is now configured.
We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.
Check for updates
Remember, we're here to help.
Click here to learn about Netgate 24/7/365 support services.
User survey
Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)
Anonymous User Survey
Useful resources.
Learn more about Netgate's product line, services, and pfSense software from our website
To learn about Netgate appliances and other offers, visit our store
Become part of the pfSense community. Visit our forum
Subscribe to our newsletter for ongoing product information, software announcements and special offers.
Finish

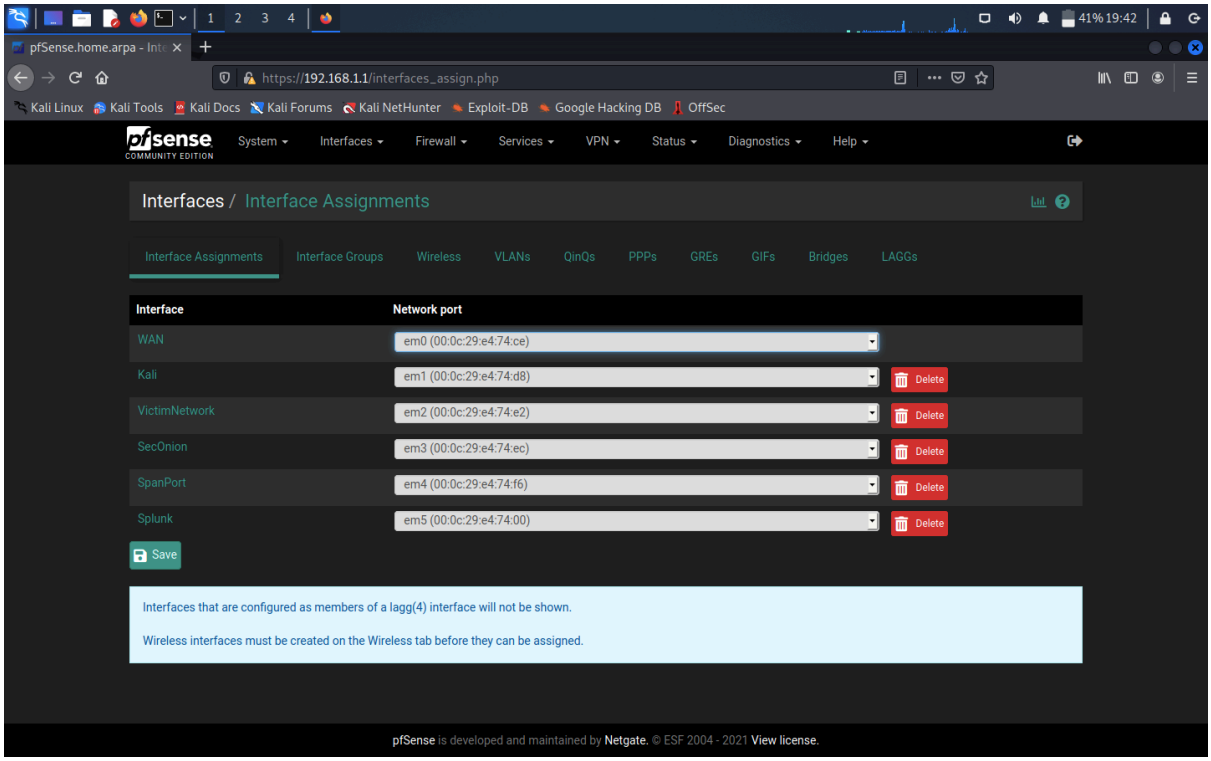

pfSense.home.arpa - Sta
https://192.168.1.1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name
pfSense.home.arpa
User
admin@192.168.1.100 (Local Database)
System
pfSense
Netgate Device ID: 853bf1ad224e144d4300
BIOS
Vendor: VMware, Inc.
Version: VMW71.00V.18452719.B64.2108091906
Release Date: Mon Aug 9 2021
Version
2.5.2-RELEASE (amd64)
built on Fri Jul 02 15:33:00 EDT 2021
FreeBSD 12.2-STABLE
The system is on the latest version.
Version information updated at Wed Dec 22 15:13:41 PST 2021
CPU Type
Intel(R) Core(TM) i5-5350U CPU @ 1.80GHz
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto
Kernel PTI
Enabled
MDS Mitigation
Inactive
Uptime
00 Hour 21 Minutes 43 Seconds
Current date/time
Wed Dec 22 15:34:31 PST 2021
Netgate Services And Support
Retrieving support information
Interfaces
WAN
1000baseT <full-duplex>
192.168.1.101
fd00:f0f2:4981:4c32:20c:29ff:fee4:74ce
LAN
1000baseT <full-duplex>
192.168.1.1

Click on Interfaces and select LAN. For “Description” change change LAN to Kali as this is the kali interface. Scroll down and click on save. Follow the steps as show below and do the same for the rest of the interfaces.

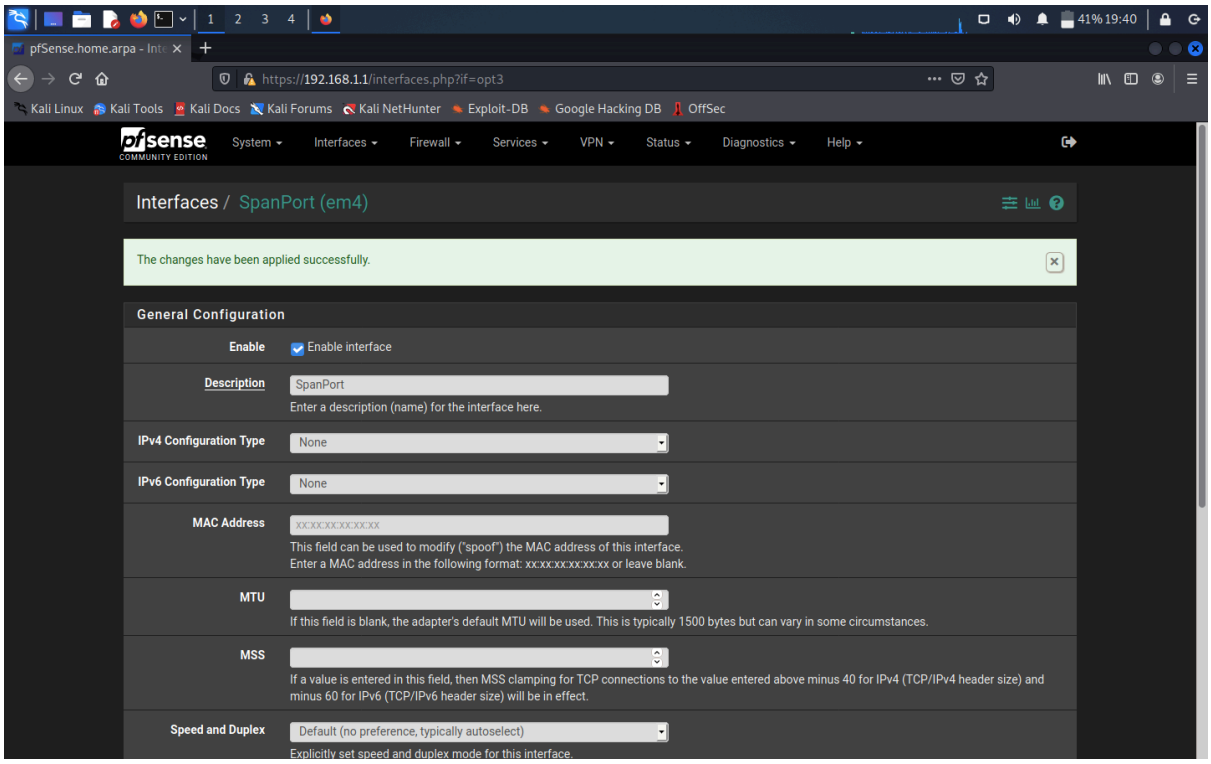



pfSense.home.arpa - Ser
https://192.168.1.1/services_router_advertisements.php?if=lan
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / DHCPv6 Server & RA / KALI / Router Advertisements
KALI
DHCPv6 Server
Router Advertisements
Advertisements
Router mode
Disabled
Select the Operating Mode for the Router Advertisement (RA) Daemon.
Router priority
Normal
Select the Priority for the Router Advertisement (RA) Daemon.
Default valid lifetime
86400
The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination.
The default is 86400 seconds.
Default preferred lifetime
14400
Seconds. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred.
The default is 14400 seconds.
Minimum RA interval
5
The minimum time allowed between sending unsolicited multicast router advertisements in seconds.
The default is 5 seconds.


pfSense.home.arpa - Int
https://192.168.1.1/interfaces.php?if=lan
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / Kali (em1)
The Kali configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.
Apply Changes
General Configuration
Enable
Enable interface
Description
Kali
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

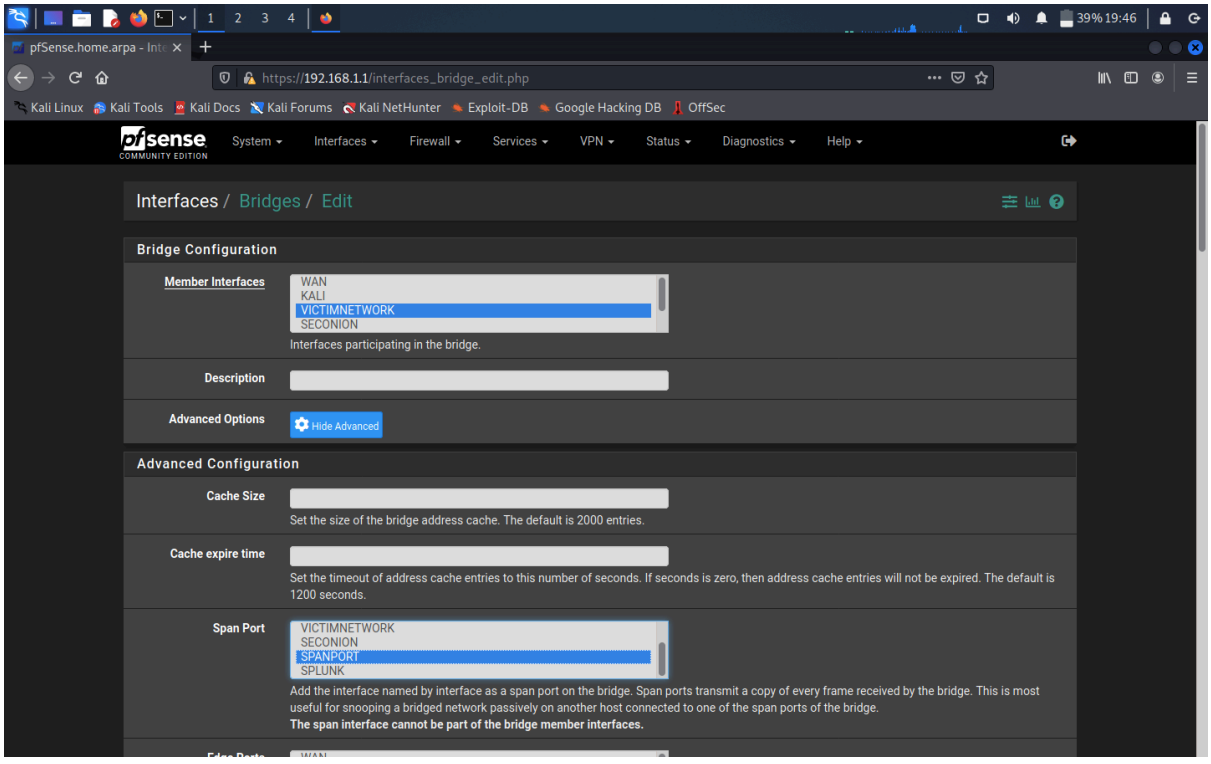

pfSense.home.arpa - Inte
https://192.168.1.1/interfaces_assign.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / Interface Assignments
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (00:0c:29:e4:74:ce)
Kali
em1 (00:0c:29:e4:74:d8)
Delete
VictimNetwork
em2 (00:0c:29:e4:74:e2)
Delete
SecOnion
em3 (00:0c:29:e4:74:ec)
Delete
SpanPort
em4 (00:0c:29:e4:74:f6)
Delete
Splunk
em5 (00:0c:29:e4:74:00)
Delete
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

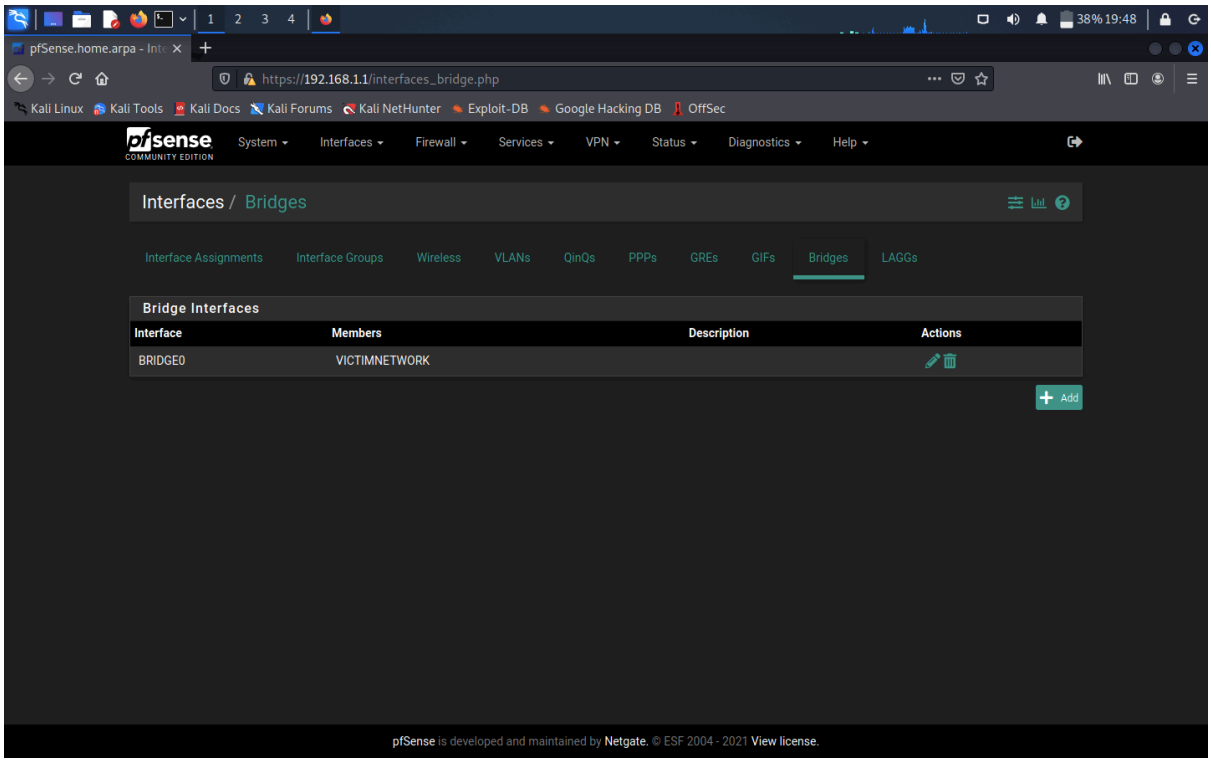
For OPT3 enable the interface as show below.



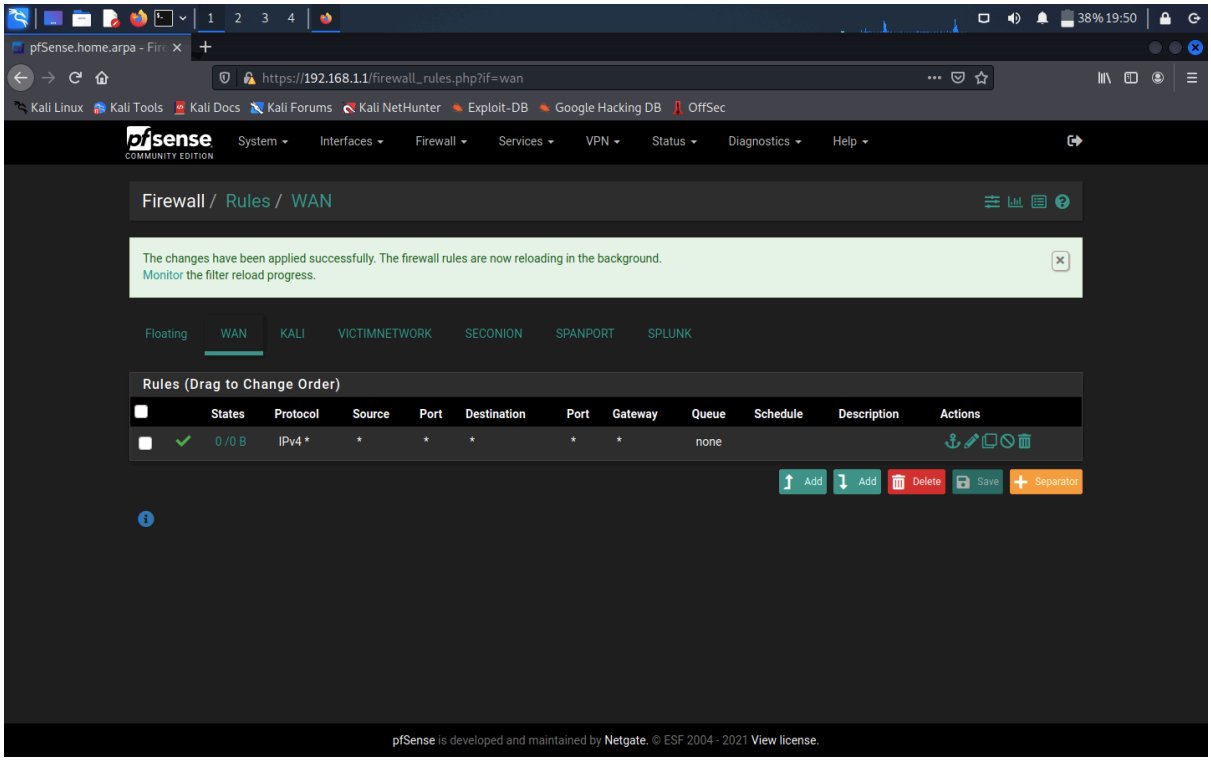
Go back to Interfaces Assignment and select Bridges.
Click Add
Select VictimNetwork as the Member interface

Then select Display Advanced under Advanced Configuration for Span Port, select “SPANPORT” and scroll down and click on save.




pfSense.home.arpa - Int
https://192.168.1.1/interfaces_bridge.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / Bridges
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Bridge Interfaces
Interface
Members
Description
Actions
BRIDGE0
VICTIMNETWORK
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

Click Firewall >> Rules
Add a rule by clicking Add button with a downward arrow. Under “edit Firewall Rule” for Protocol select Any. Scroll down and save.

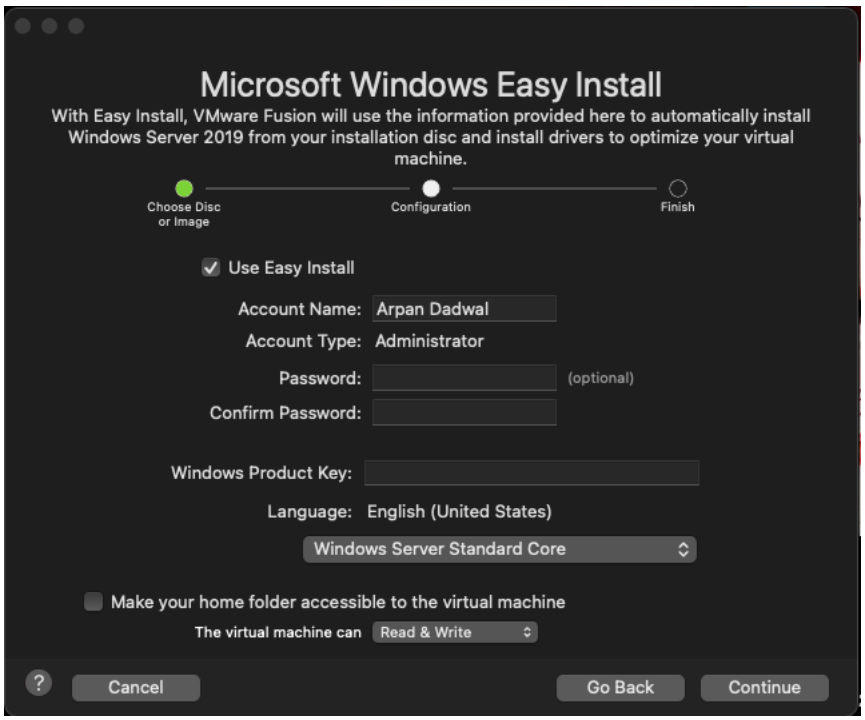


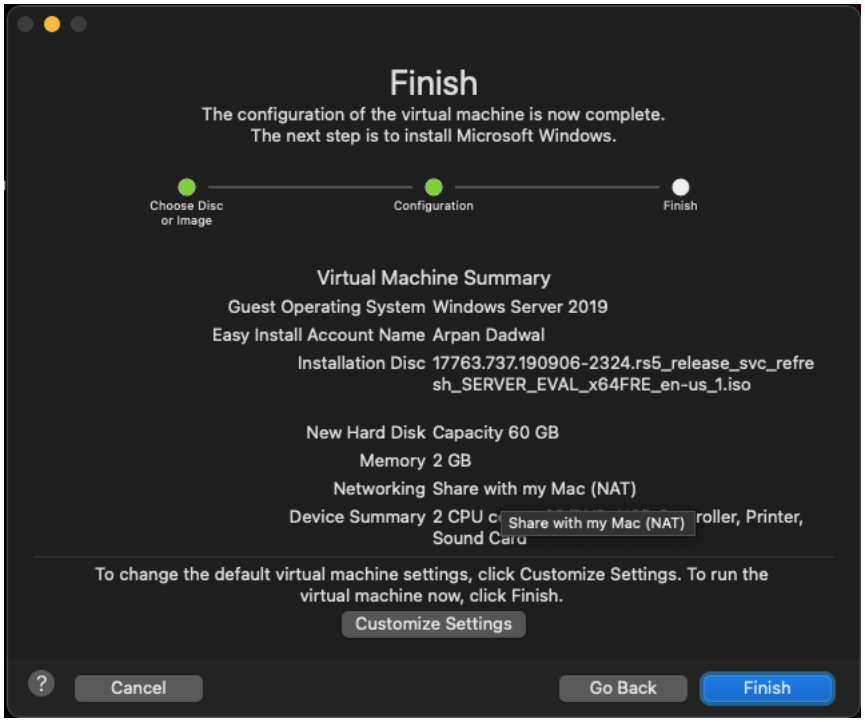
This concludes the necessary firewall configuration for pfsense..

Configuring Windows Server as a Domain Controller

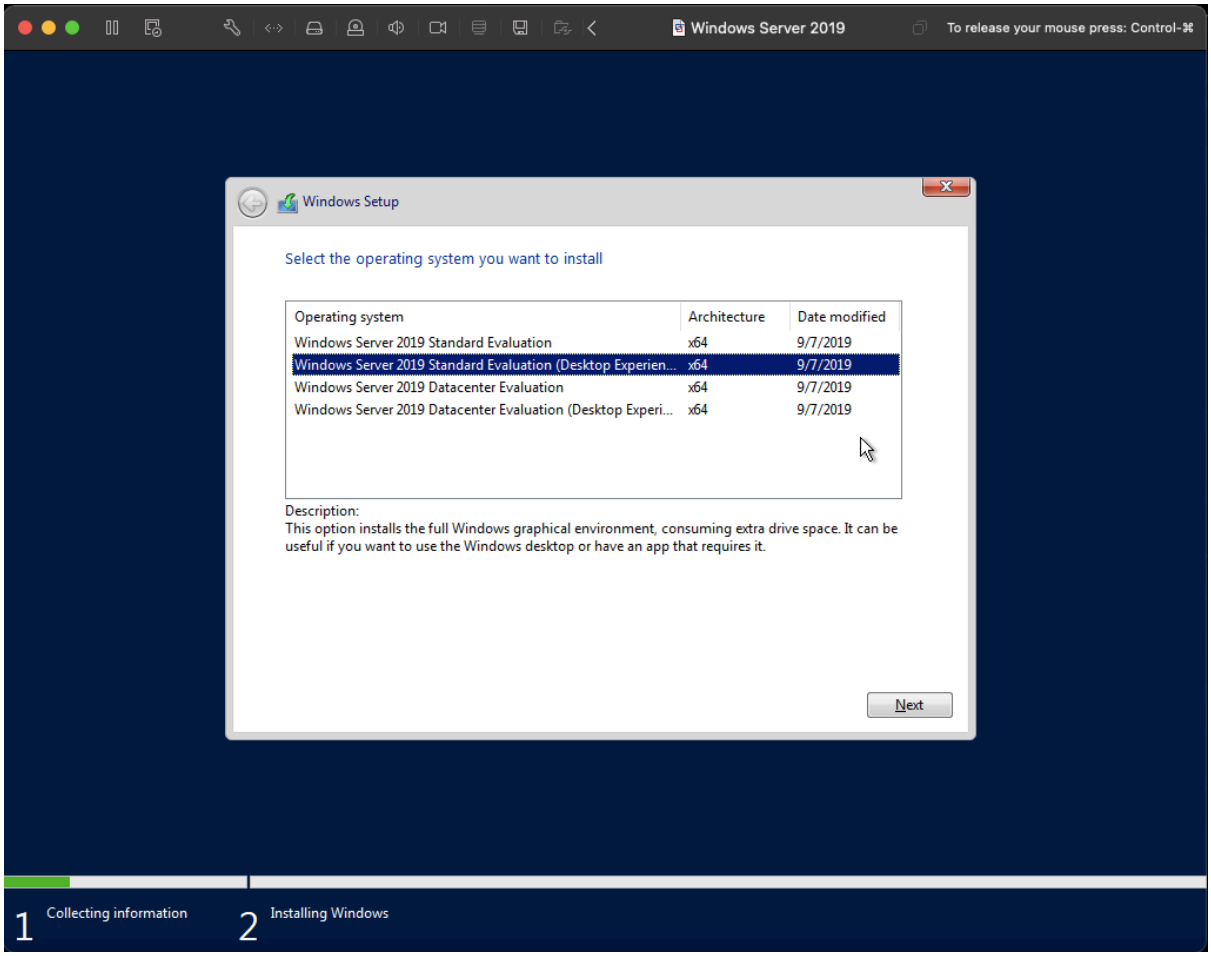
We will be setting up an Active Directory domain with a Windows 2019 server as the Domain Controller and a Windows 10 machine.

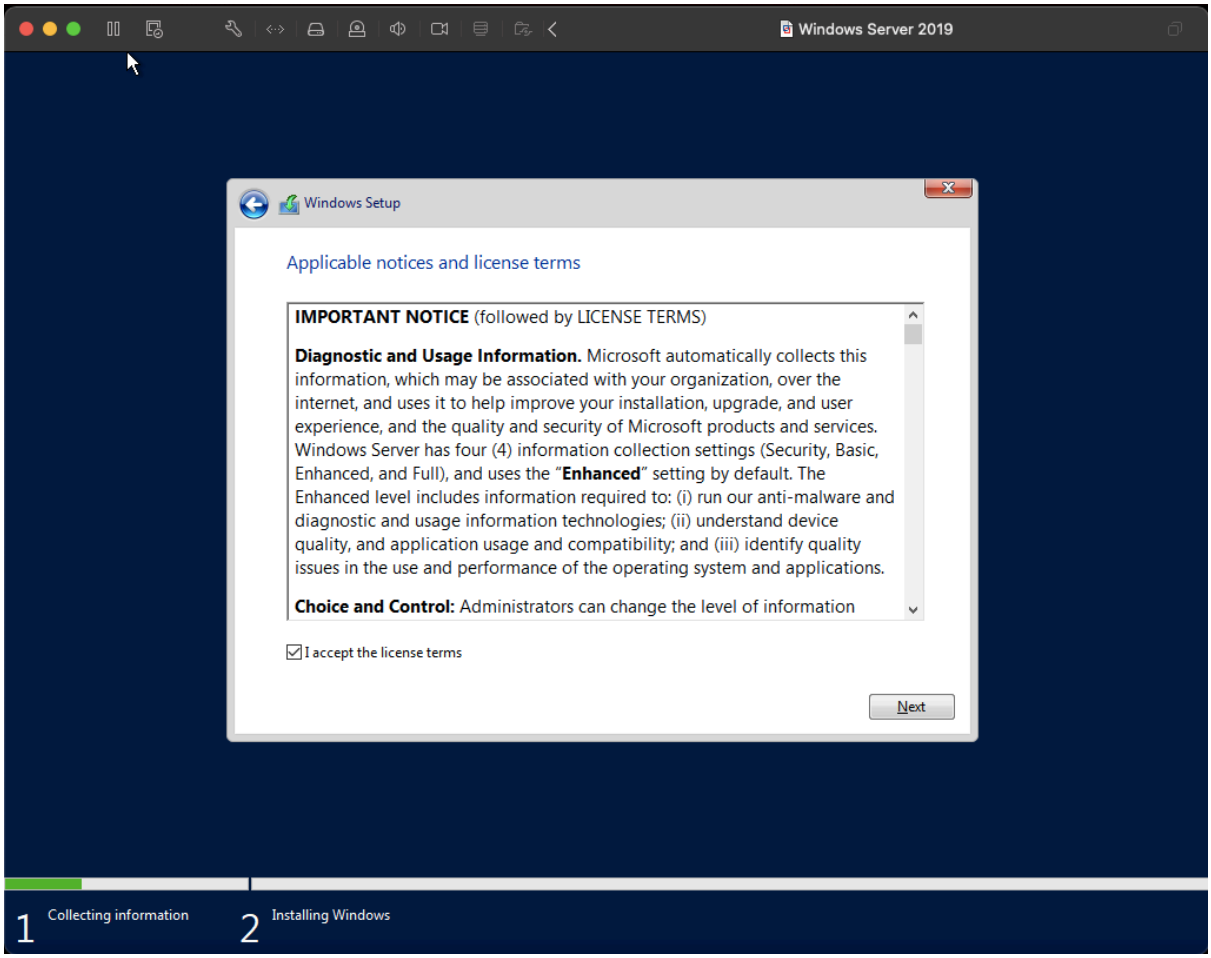
Download Windows 2019 server evaluation copy from https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019 and install the VM with defaults as shown below.

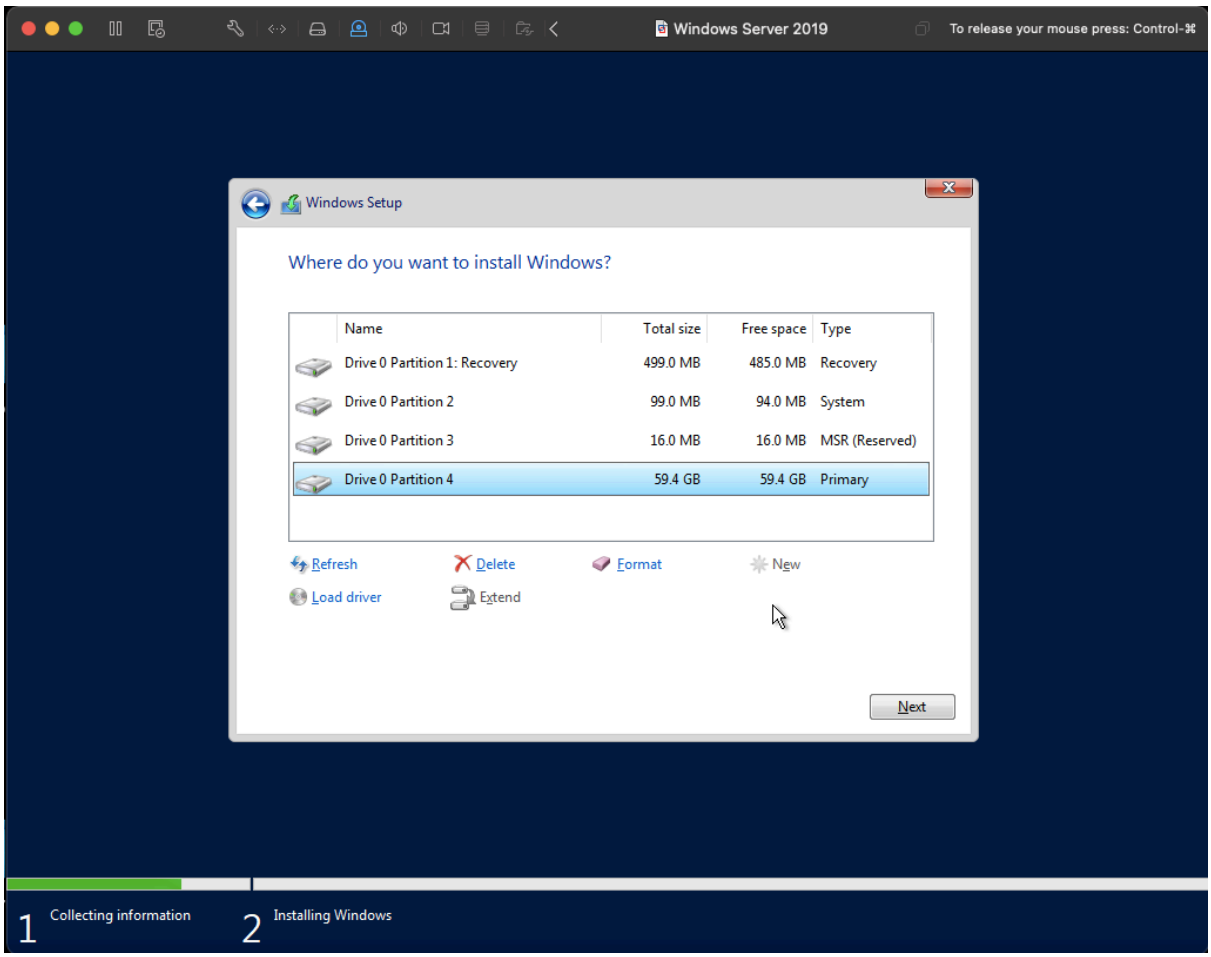



Finish
The configuration of the virtual machine is now complete.
The next step is to install Microsoft Windows.
Choose Disc or Image
Configuration
Finish
Virtual Machine Summary
Guest Operating System Windows Server 2019
Easy Install Account Name Arpan Dadwal
Installation Disc 17763.737.190906-2324.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_en-us_1.iso
New Hard Disk Capacity 60 GB
Memory 2 GB
Networking Share with my Mac (NAT)
Device Summary 2 CPU c roller, Printer, Sound Card
Share with my Mac (NAT)
To change the default virtual machine settings, click Customize Settings. To run the virtual machine now, click Finish.
Customize Settings
Cancel
Go Back
Finish

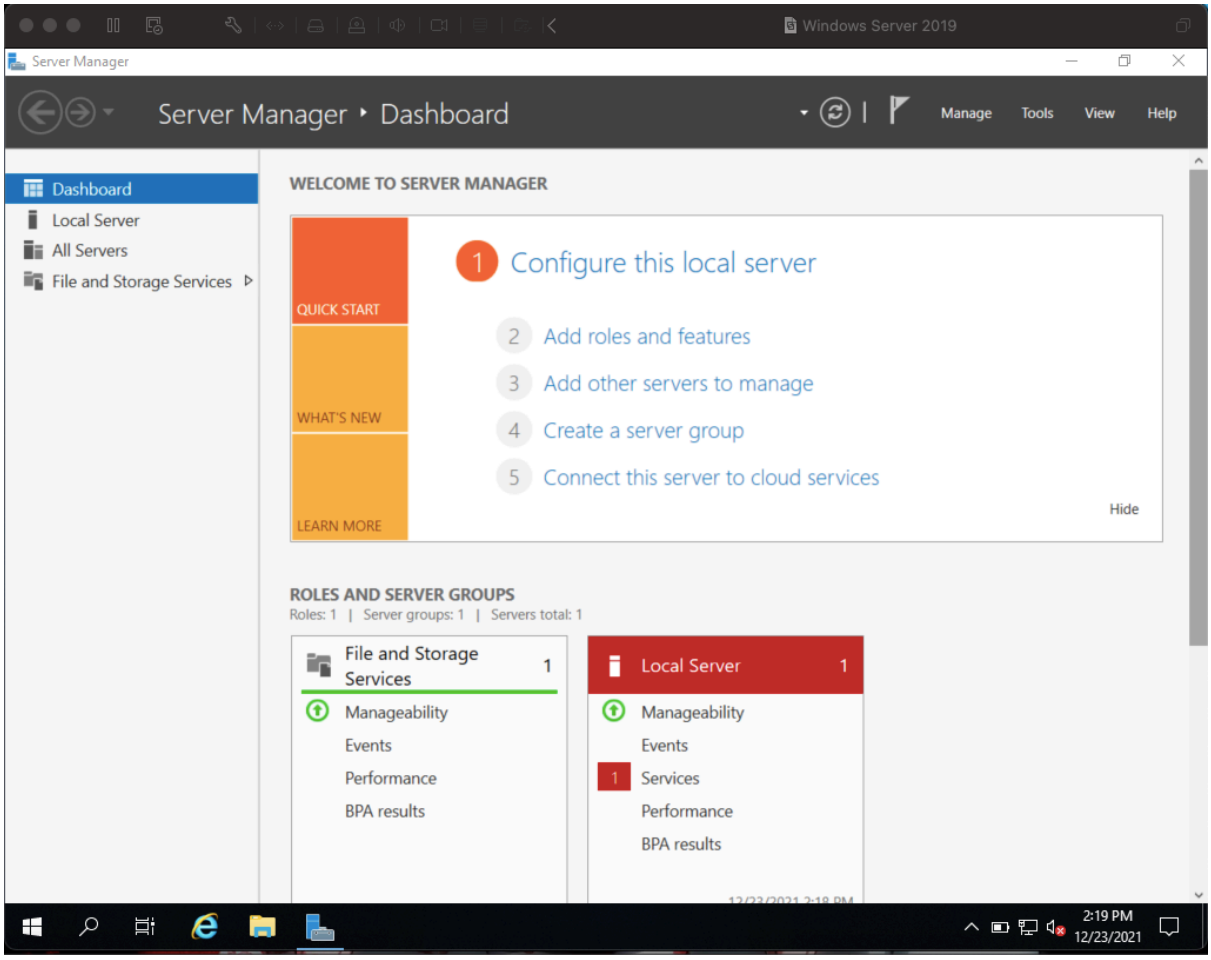
Power on the machine and select the following options –



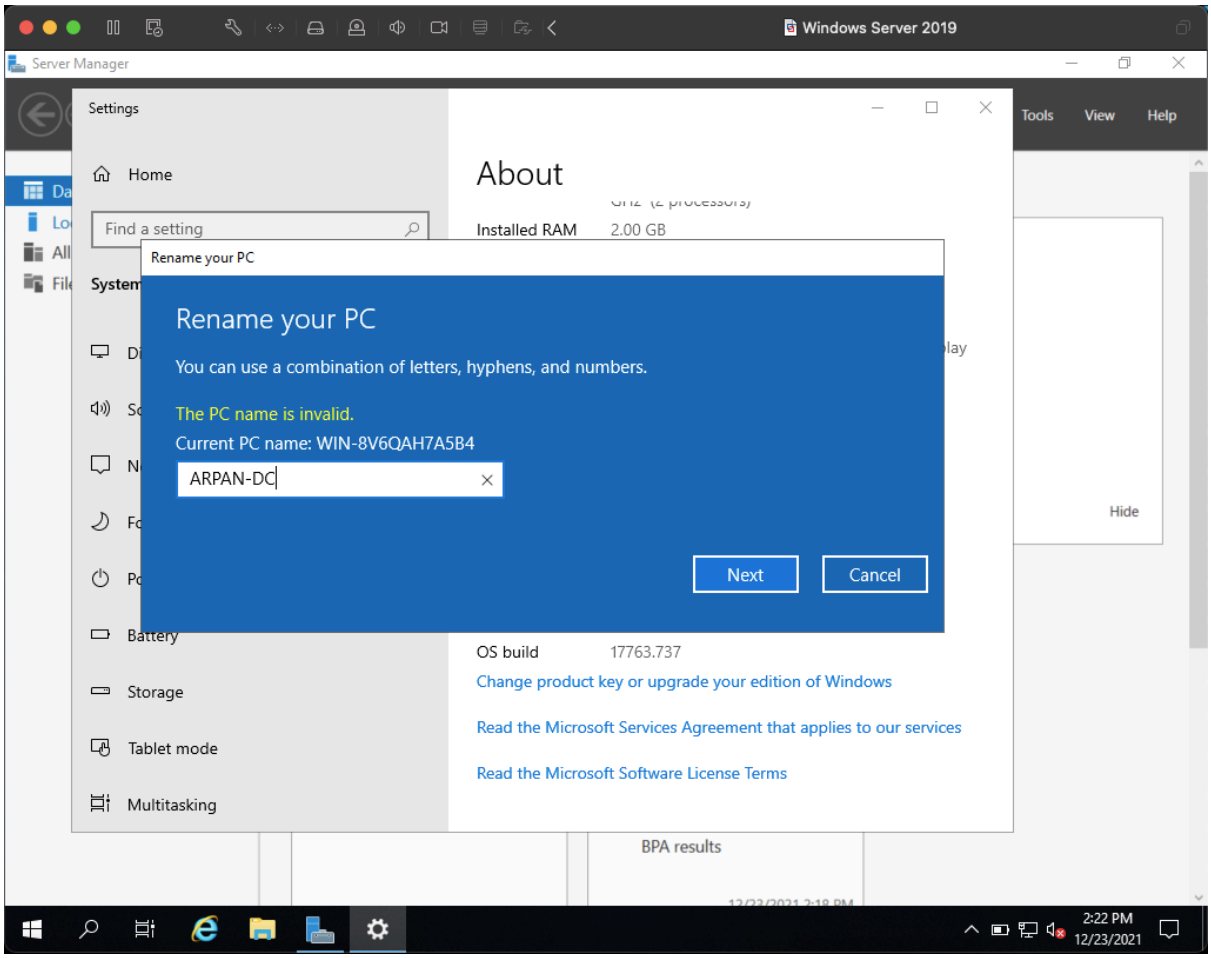

Windows Server 2019
Windows Setup
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information, which may be associated with your organization, over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Windows Server has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. The Enhanced level includes information required to: (i) run our anti-malware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
Choice and Control: Administrators can change the level of information
I accept the license terms
Next
1 Collecting information
2 Installing Windows


Windows Server 2019
To release your mouse press: Control-⌘
Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Partition 1: Recovery
499.0 MB
485.0 MB
Recovery
Drive 0 Partition 2
99.0 MB
94.0 MB
System
Drive 0 Partition 3
16.0 MB
16.0 MB
MSR (Reserved)
Drive 0 Partition 4
59.4 GB
59.4 GB
Primary
Refresh
Delete
Format
New
Load driver
Extend
Next
1
Collecting information
2
Installing Windows

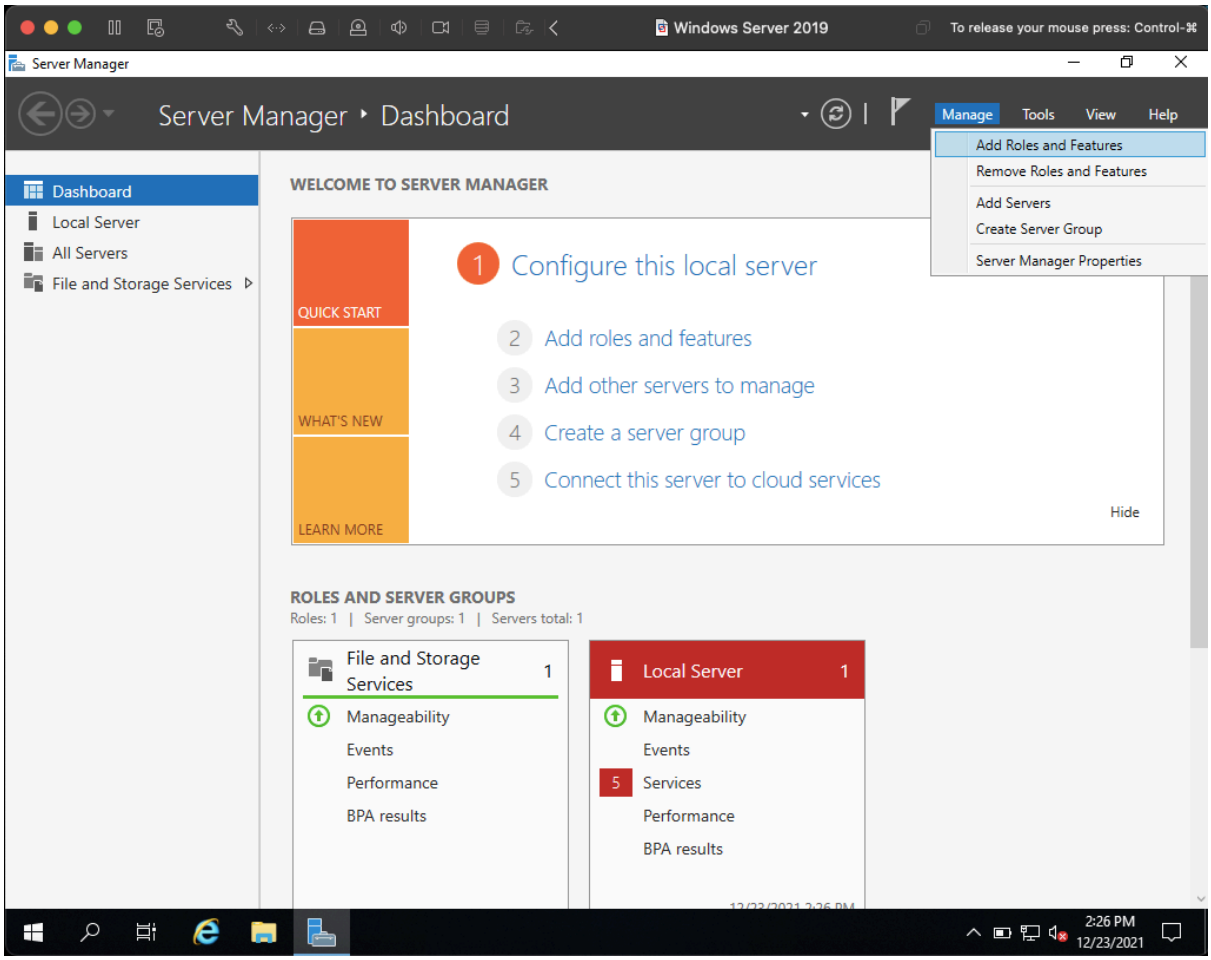
After installation we will end up with this screen-

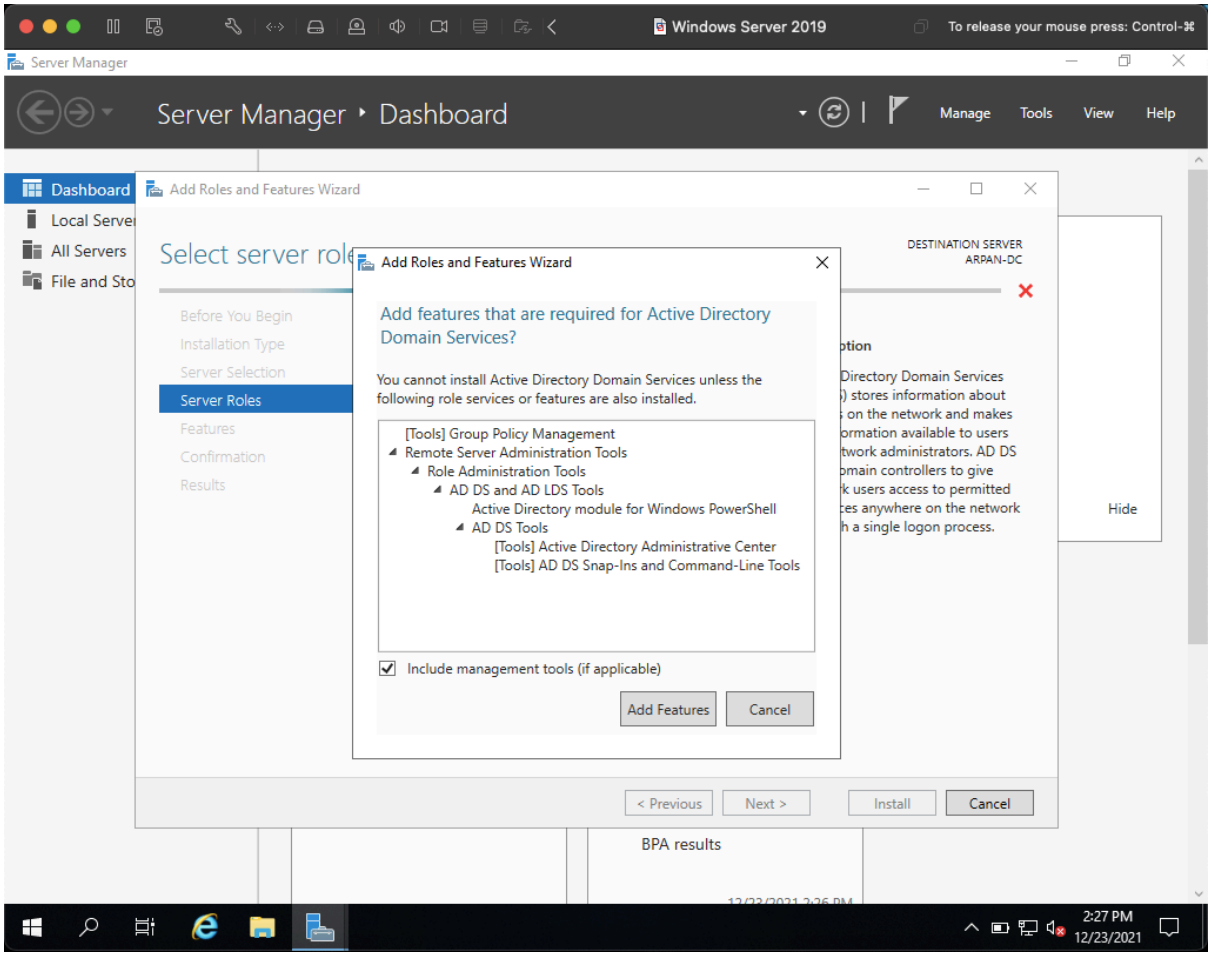


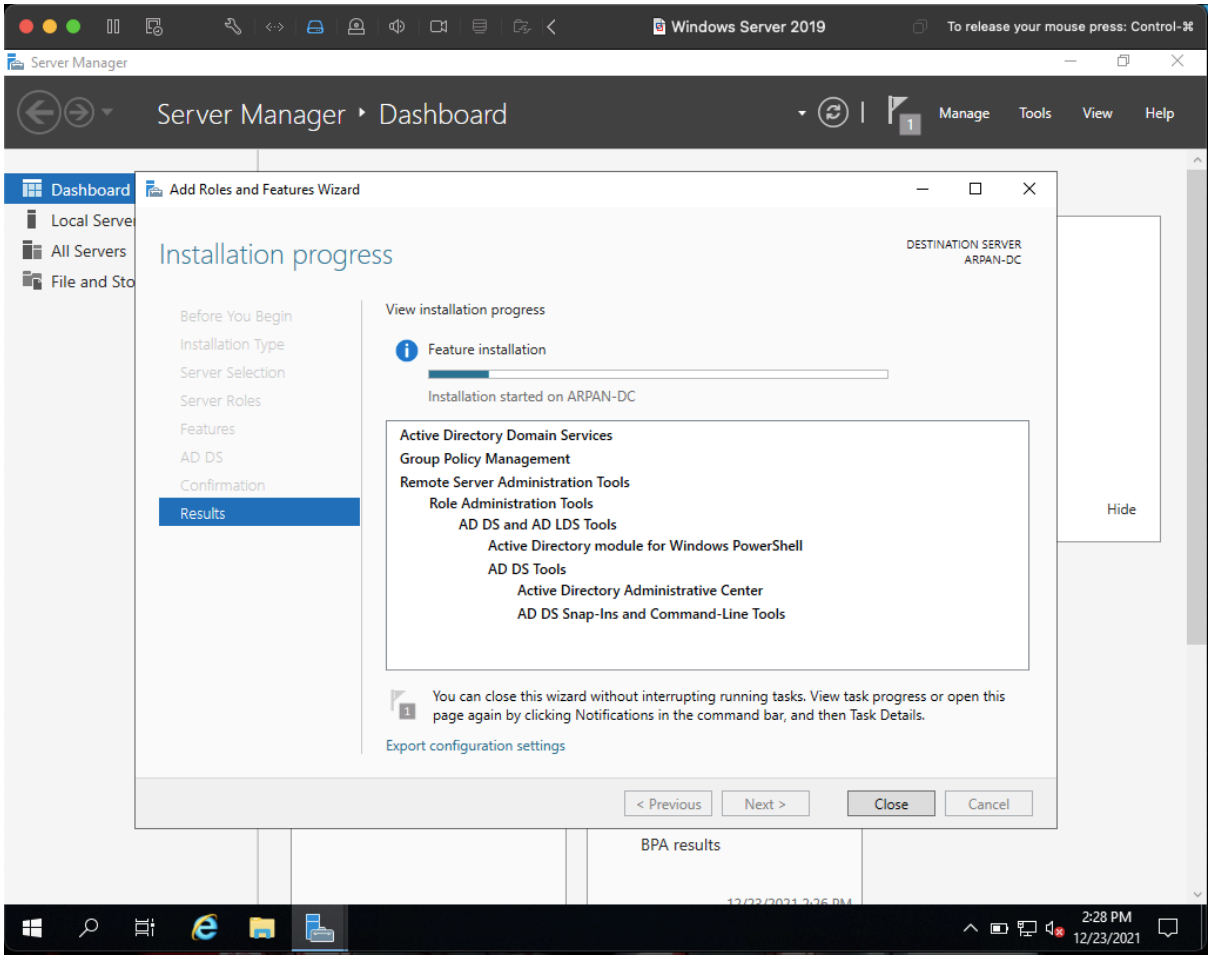
Rename the Domain Controller –
Navigate to settings in search bar.
Search for settings in search bar.
Search for “pc name” and select Rename PC and rename it.
Select Restart Now.



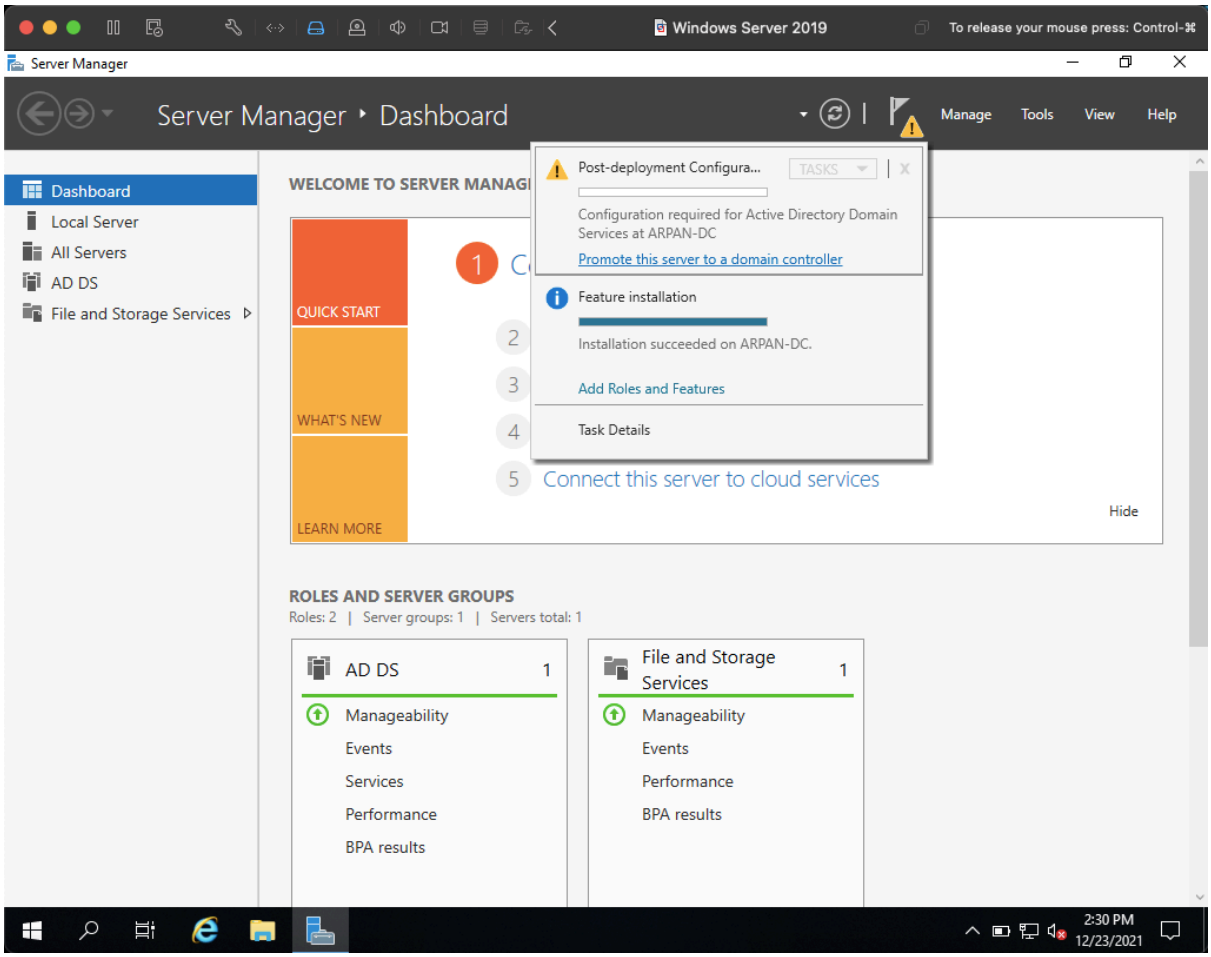
After reboot, on the Server Manager Dashboard, click Manage >> Add Roles and Features
Keep clicking Next till you get to the Server Roles menu
Select Active Directory Domain Services
Select “Add Features”
Click Next till the Confirmation menu and then click Install.

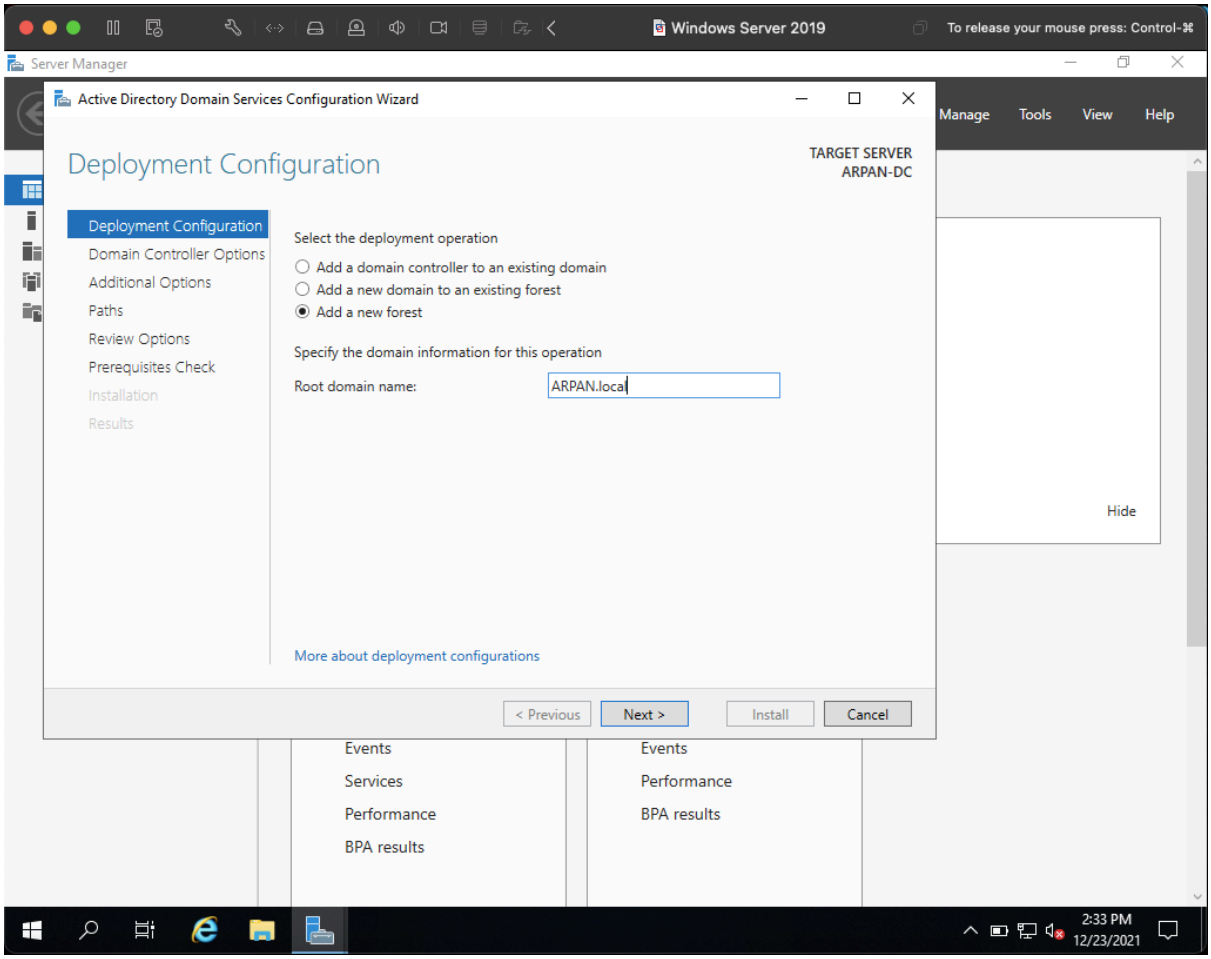


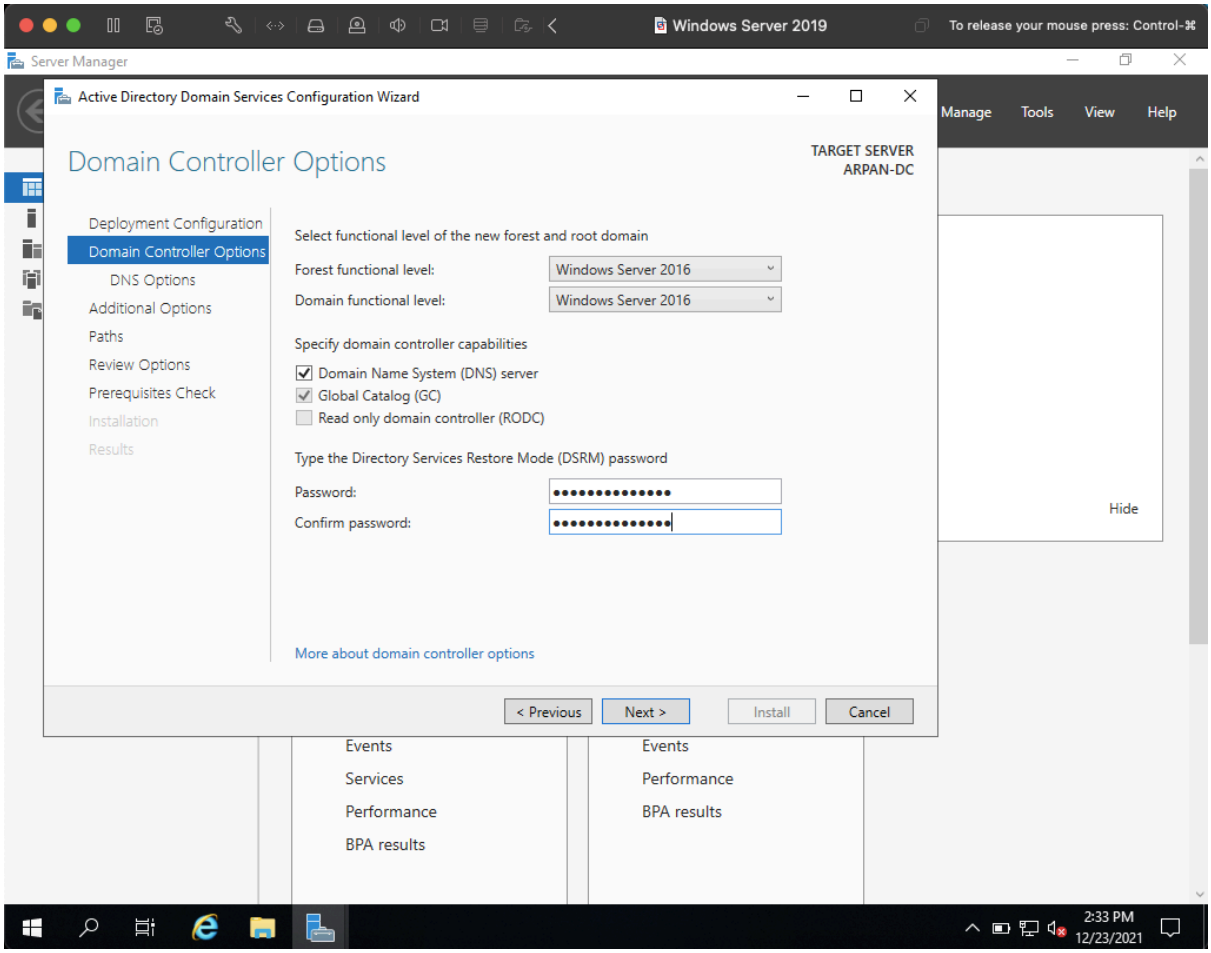

Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Sto
Add Roles and Features Wizard
Select server role
DESTINATION SERVER
ARPAN-DC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
Directory Domain Services
stores information about
on the network and makes
ormation available to users
twork administrators. AD DS
omain controllers to give
k users access to permitted
es anywhere on the network
h a single logon process.
Hide
< Previous
Next >
Install
Cancel
BPA results
2:27 PM
12/23/2021


Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Sto
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
ARPAN-DC
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
View installation progress
Feature installation
Installation started on ARPAN-DC
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel
Hide
BPA results
2:28 PM
12/23/2021

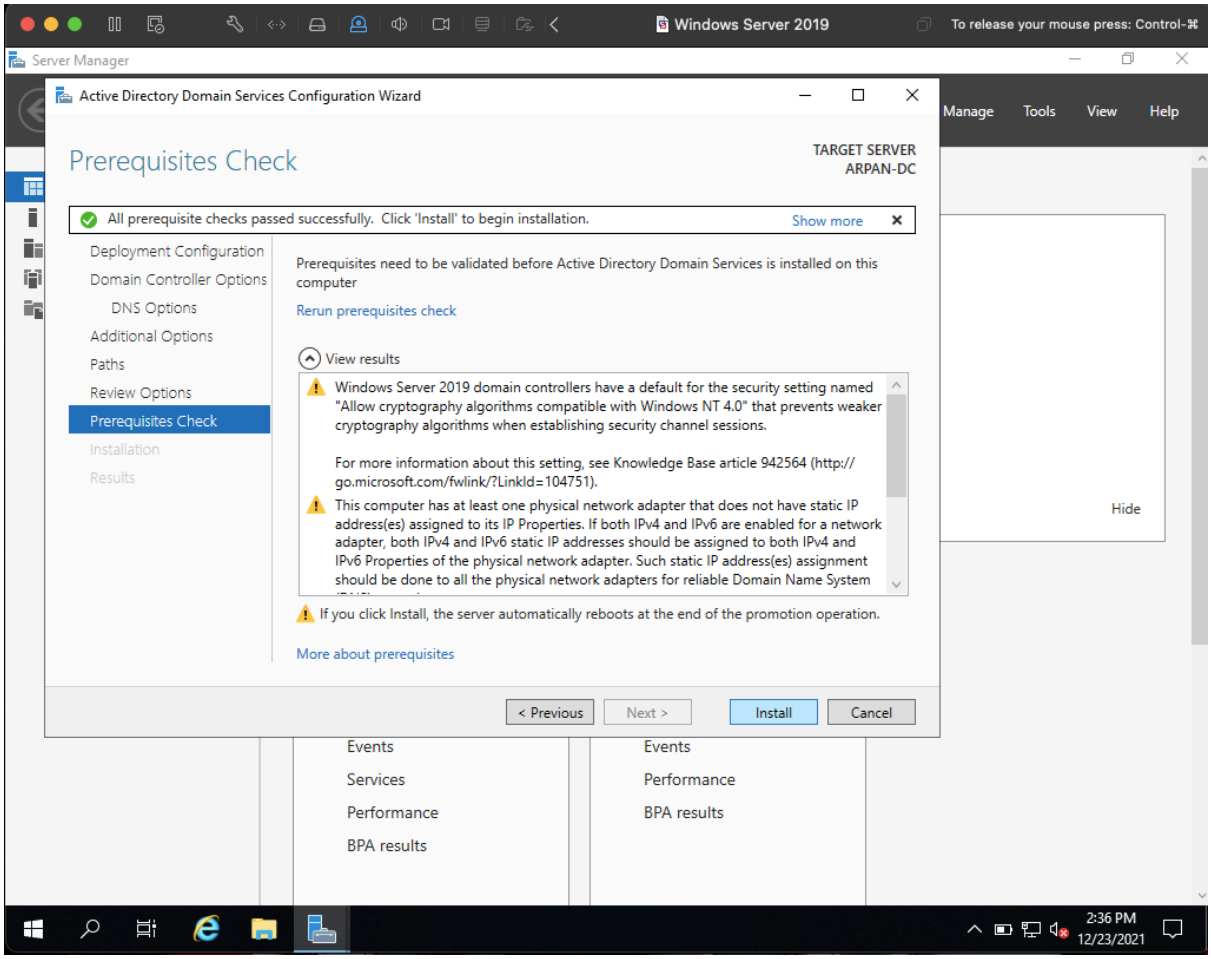
After install click Close
Click on the flag with a yellow caution triangle
Select “Promote this server to a domain controller”
Select Add a new forest
Specify domain name and click Next
Set a Password




Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Manage
Tools
View
Help
Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
ARPAN-DC
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
ARPAN.local
More about deployment configurations
< Previous
Next >
Install
Cancel
Hide
Events
Services
Performance
BPA results
Events
Performance
BPA results
2:33 PM
12/23/2021

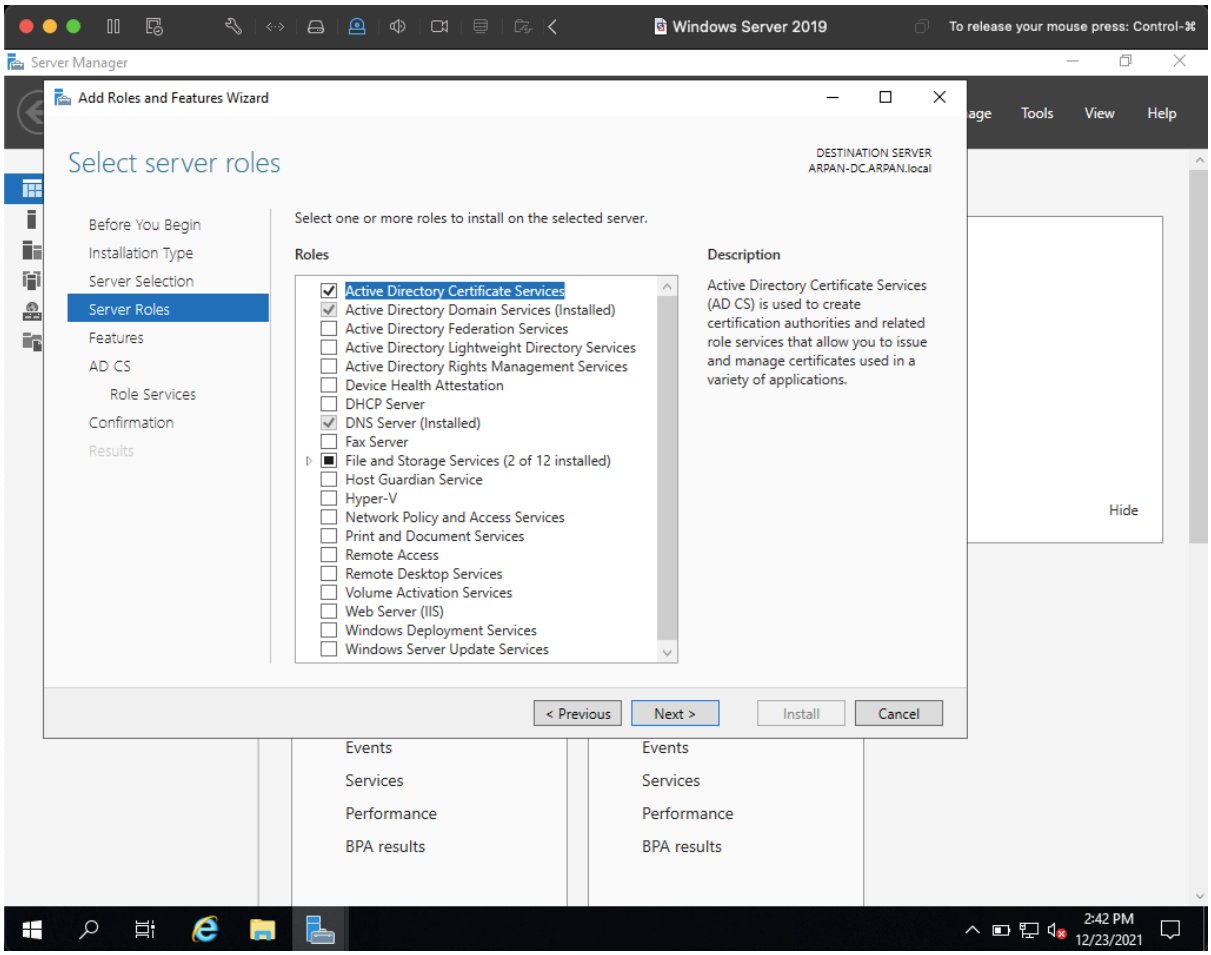

Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
ARPAN-DC
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel
Manage
Tools
View
Help
Hide
Events
Services
Performance
BPA results
Events
Performance
BPA results
2:33 PM
12/23/2021

Click Next till the Prerequisites Check menu and click Install.
Wait for reboot.

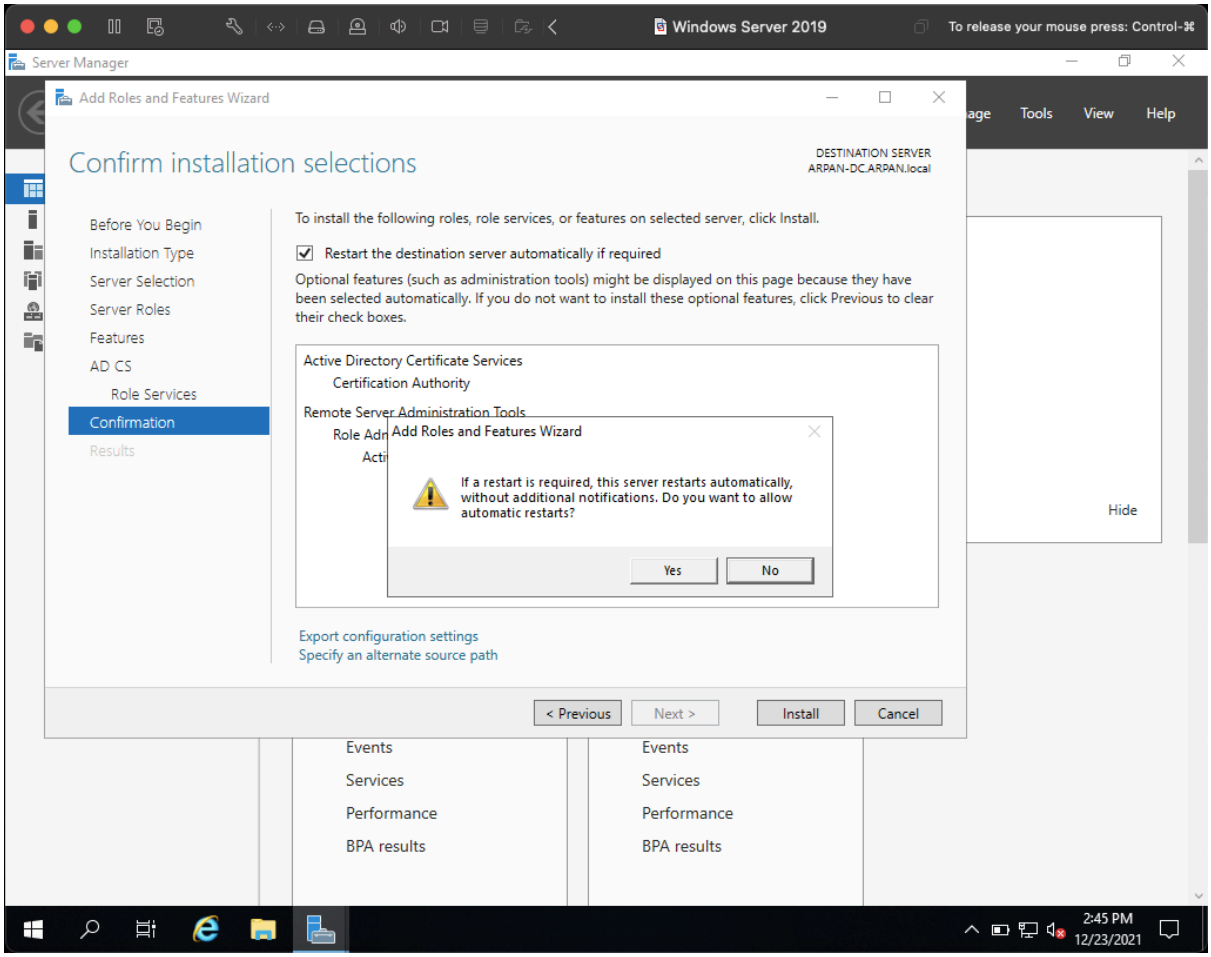


After the reboot, Log back in
Select Manage >> Add roles and features again on the Server Manager.
Click Next till you get to the Server Roles

Select Active Directory Certificate Services
Select Add Features

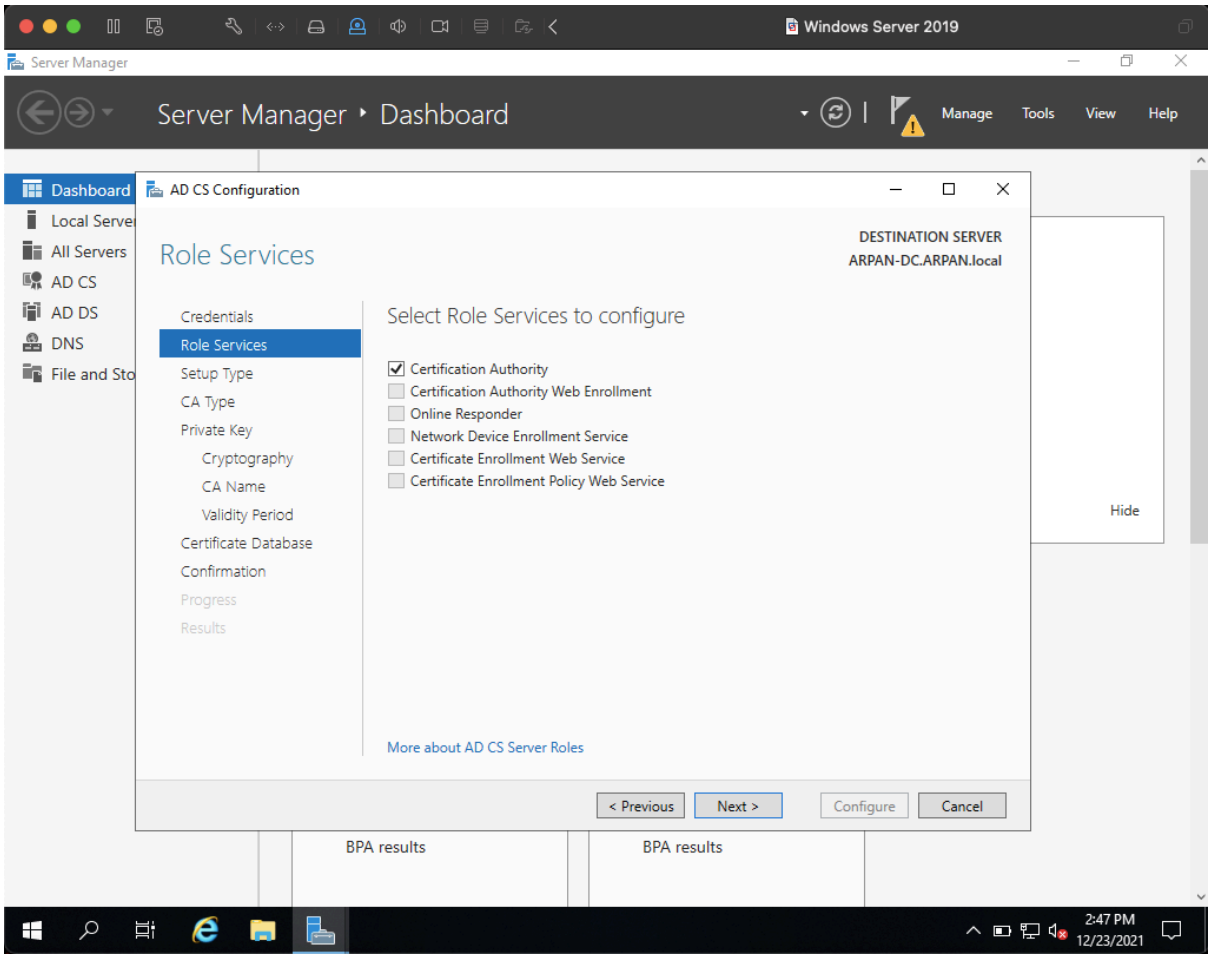


Click Next till the Confirmation menu
After installation click Close

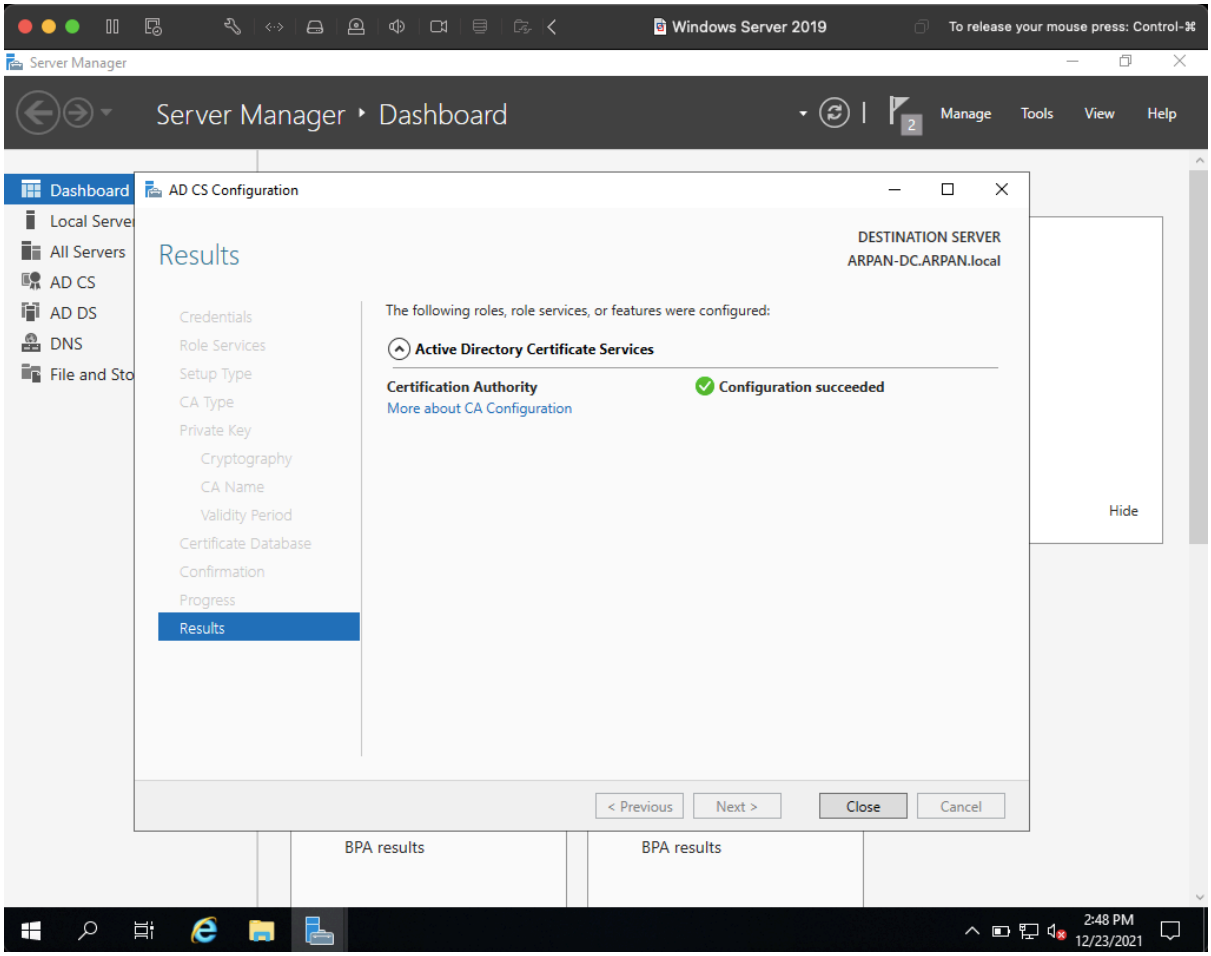


Click the flag with a yellow caution triangle and select “Configure Active Directory Certificate Services on the destination server”

Click next and on Role Services menu, check Certification Authority



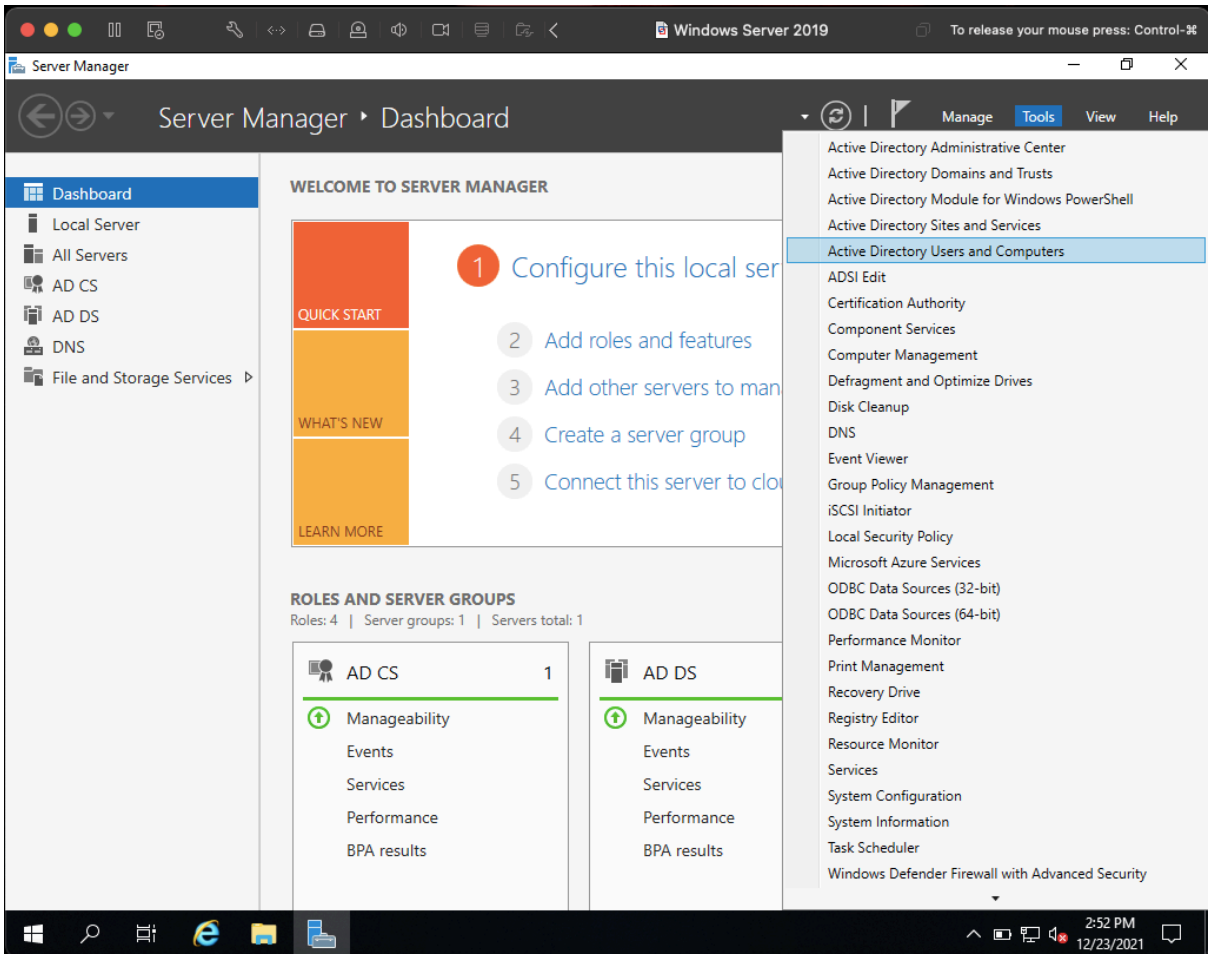
Click Next and configure

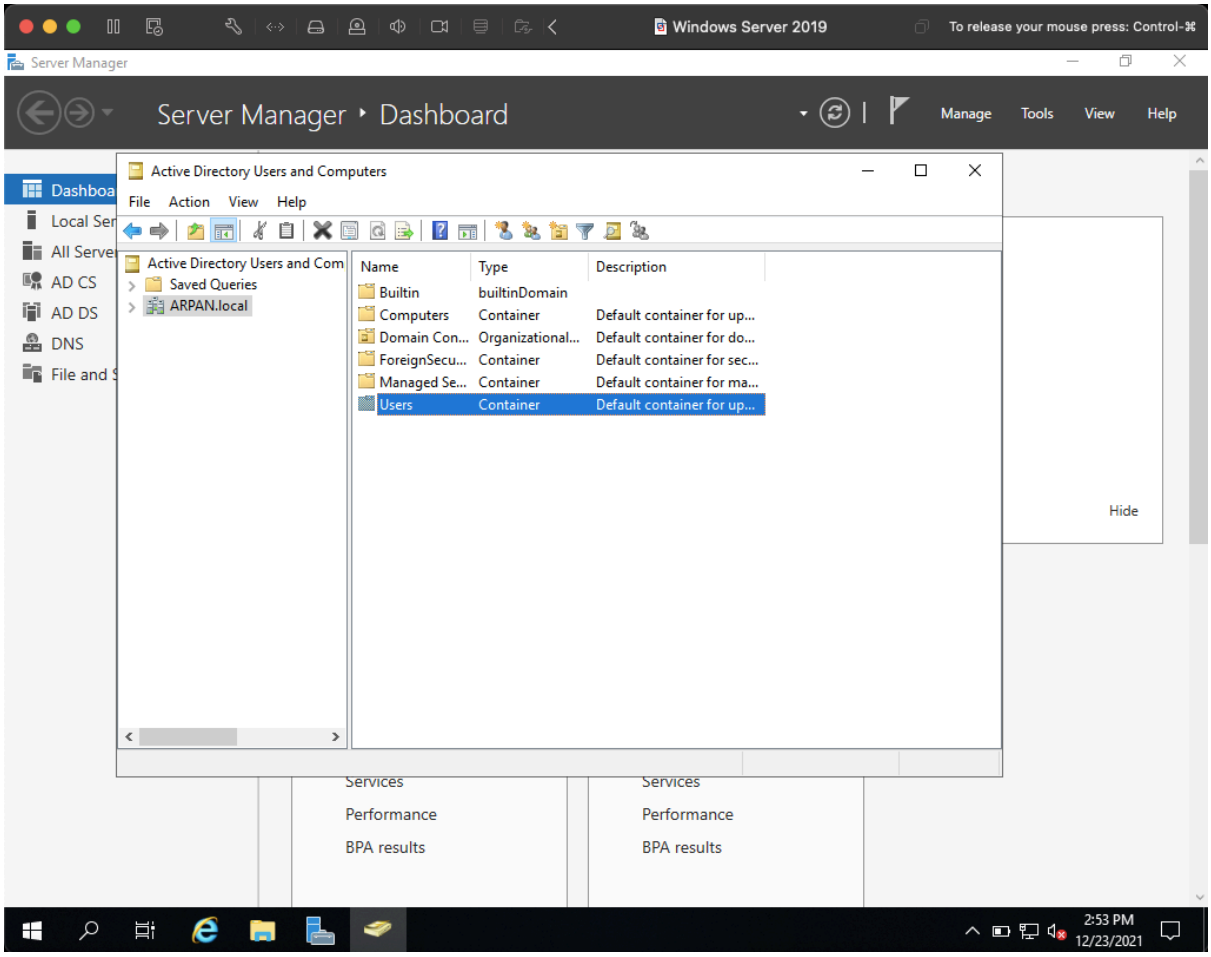


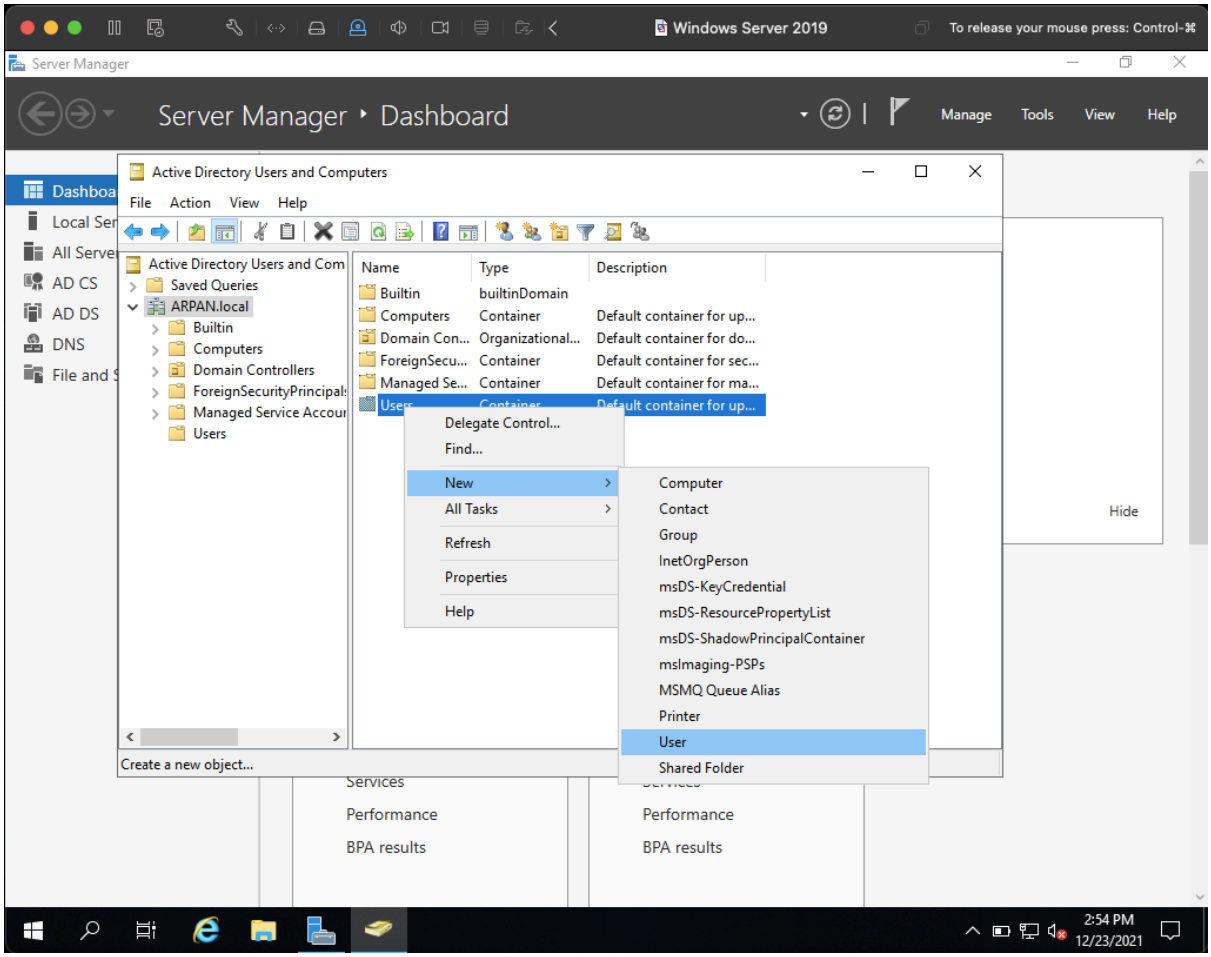
Manually restart the server in order for the settings to take effect

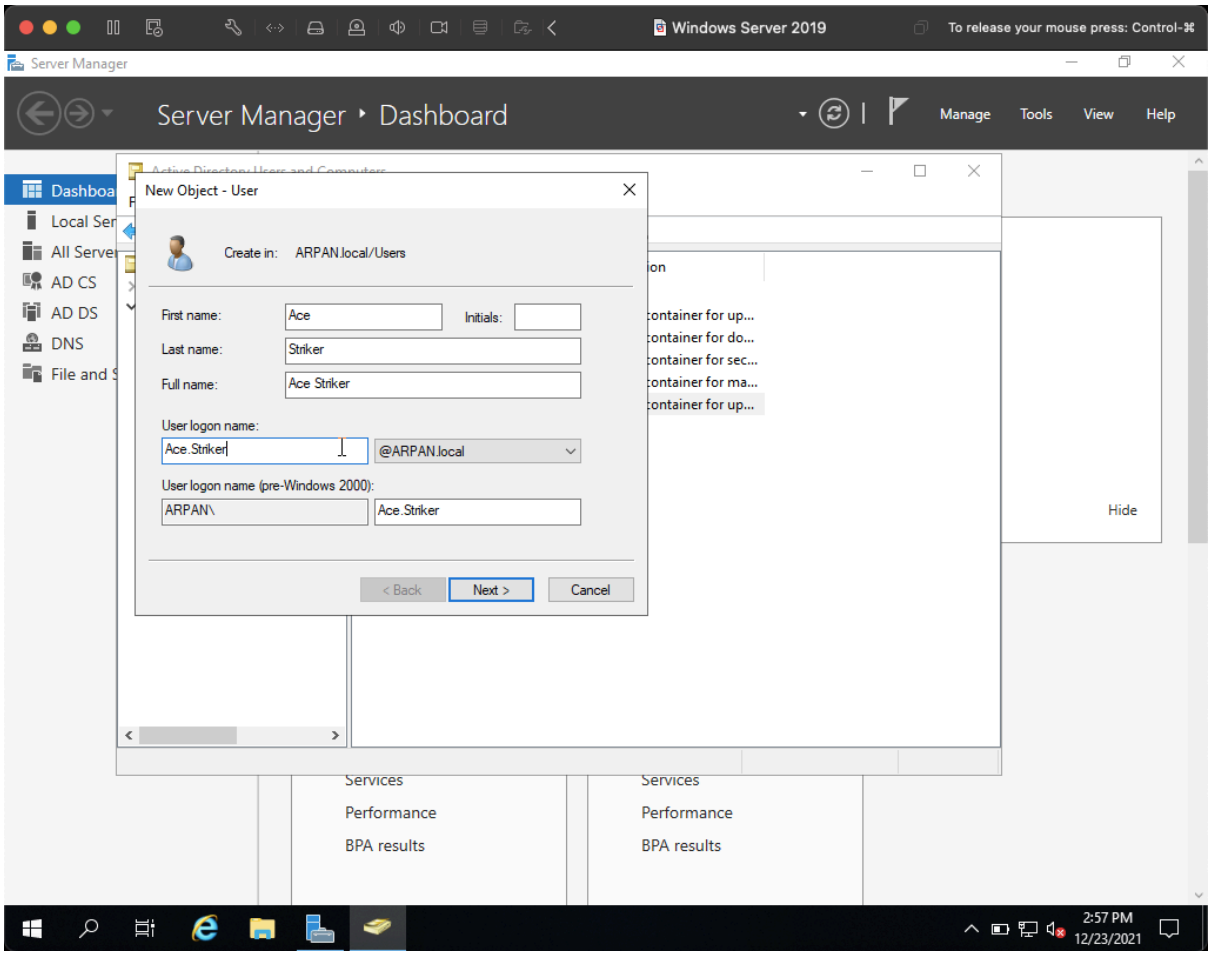
Now we will add users

Back at the Server Manager select Tools > Active Directory Users and Computers
Select your Domain Name > Users, right click and select New > User.
Enter a suitable logon name for the user
Set a password and select Finish.

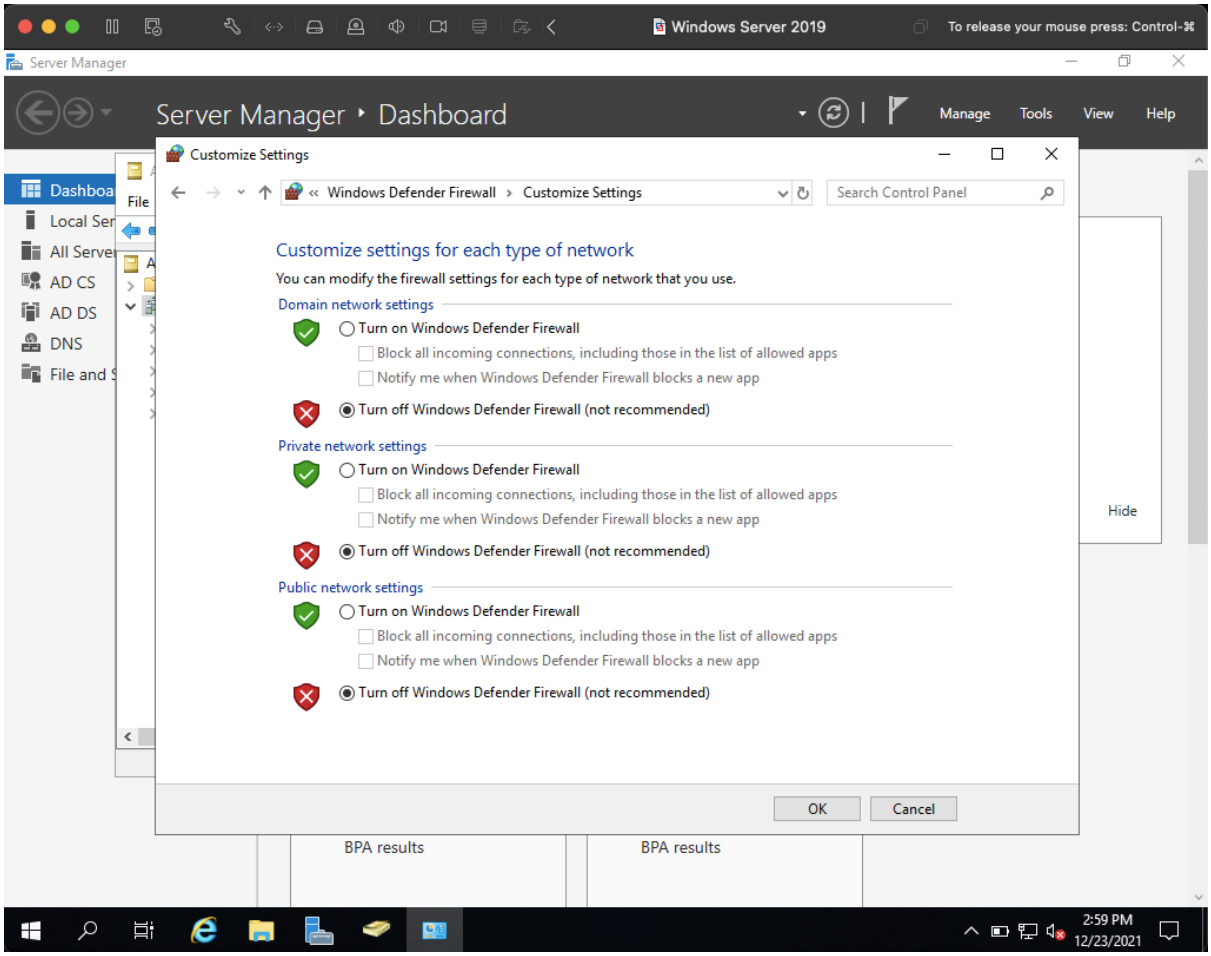



Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
ARPAN.local
Name
Type
Description
Builtin
builtinDomain
Computers
Container
Default container for up...
Domain Con...
Organizational...
Default container for do...
ForeignSecu...
Container
Default container for sec...
Managed Se...
Container
Default container for ma...
Users
Container
Default container for up...
Hide
Services
Performance
BPA results
Services
Performance
BPA results
2:53 PM
12/23/2021

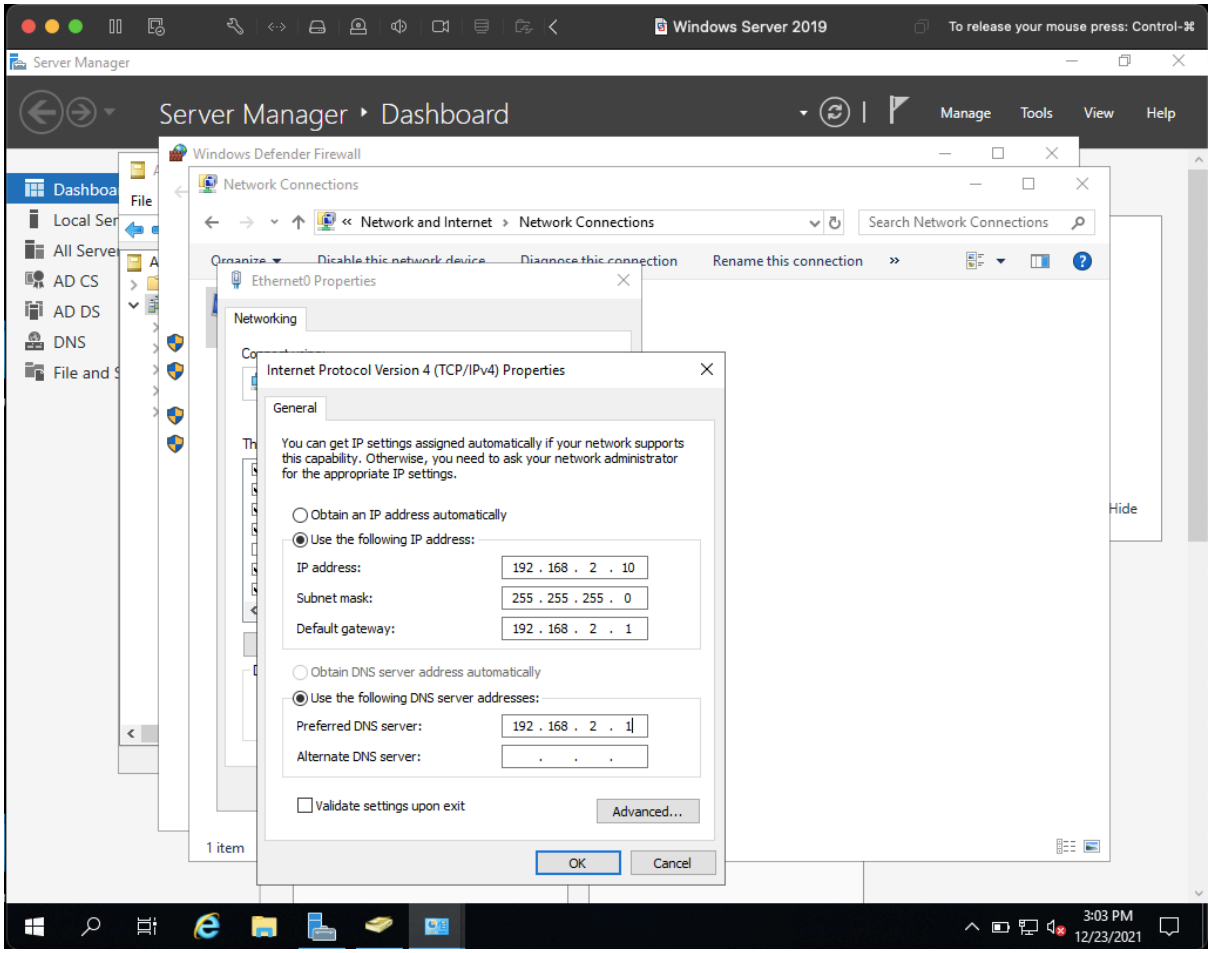

Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
ARPAN.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Name
Type
Description
Builtin
builtinDomain
Computers
Container
Default container for up...
Domain Con...
Organizational...
Default container for do...
ForeignSecu...
Container
Default container for sec...
Managed Se...
Container
Default container for ma...
Users
Container
Default container for up...
Delegate Control...
Find...
New
All Tasks
Refresh
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder
Create a new object...
Hide
Services
Performance
BPA results
Performance
BPA results
2:54 PM
12/23/2021


Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboa
Local Ser
All Server
AD CS
AD DS
DNS
File and S
New Object - User
Create in: ARPAN.local/Users
First name:
Ace
Initials:
Last name:
Striker
Full name:
Ace Striker
User logon name:
Ace.Striker
@ARPAN.local
User logon name (pre-Windows 2000):
ARPAN\
Ace.Striker
< Back
Next >
Cancel
container for up...
container for do...
container for sec...
container for ma...
container for up...
Hide
Services
Performance
BPA results
Services
Performance
BPA results
2:57 PM
12/23/2021

Search for Windows Defender Firewall > Turn Windows Defender Firewall on or off.
Turn off the firewall for all networks.



Now use pfsense as default gateway for the Domain Controller
Navigate to Control Panel > Network and Internet > Network Connections and configure as shown below.



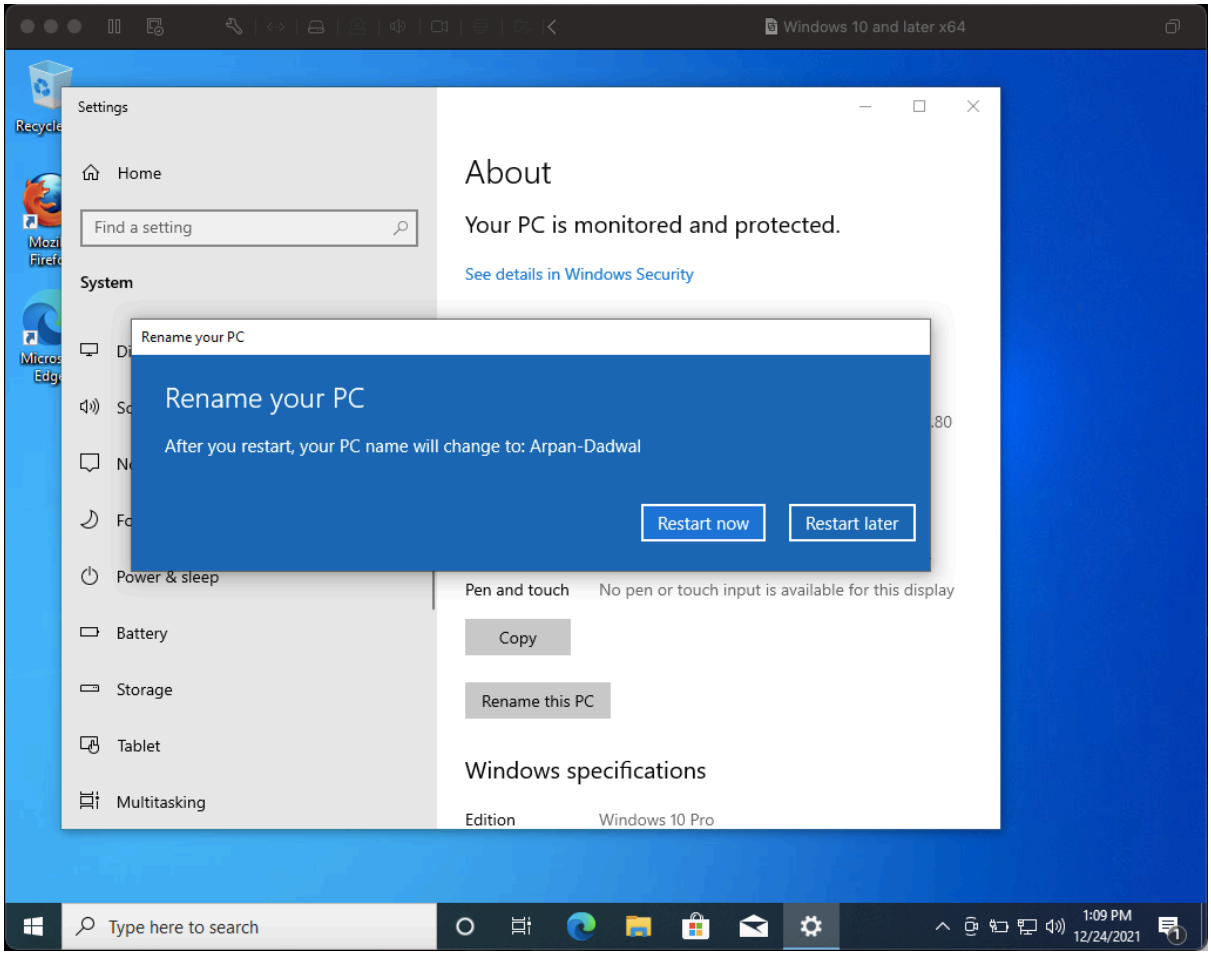
This marks the end of Domain Controller configuration.

Configuring Windows 10 Desktop and Adding a User to the AD Domain

We will be adding a Windows 10 desktop to the Domain and complete the active directory lab.

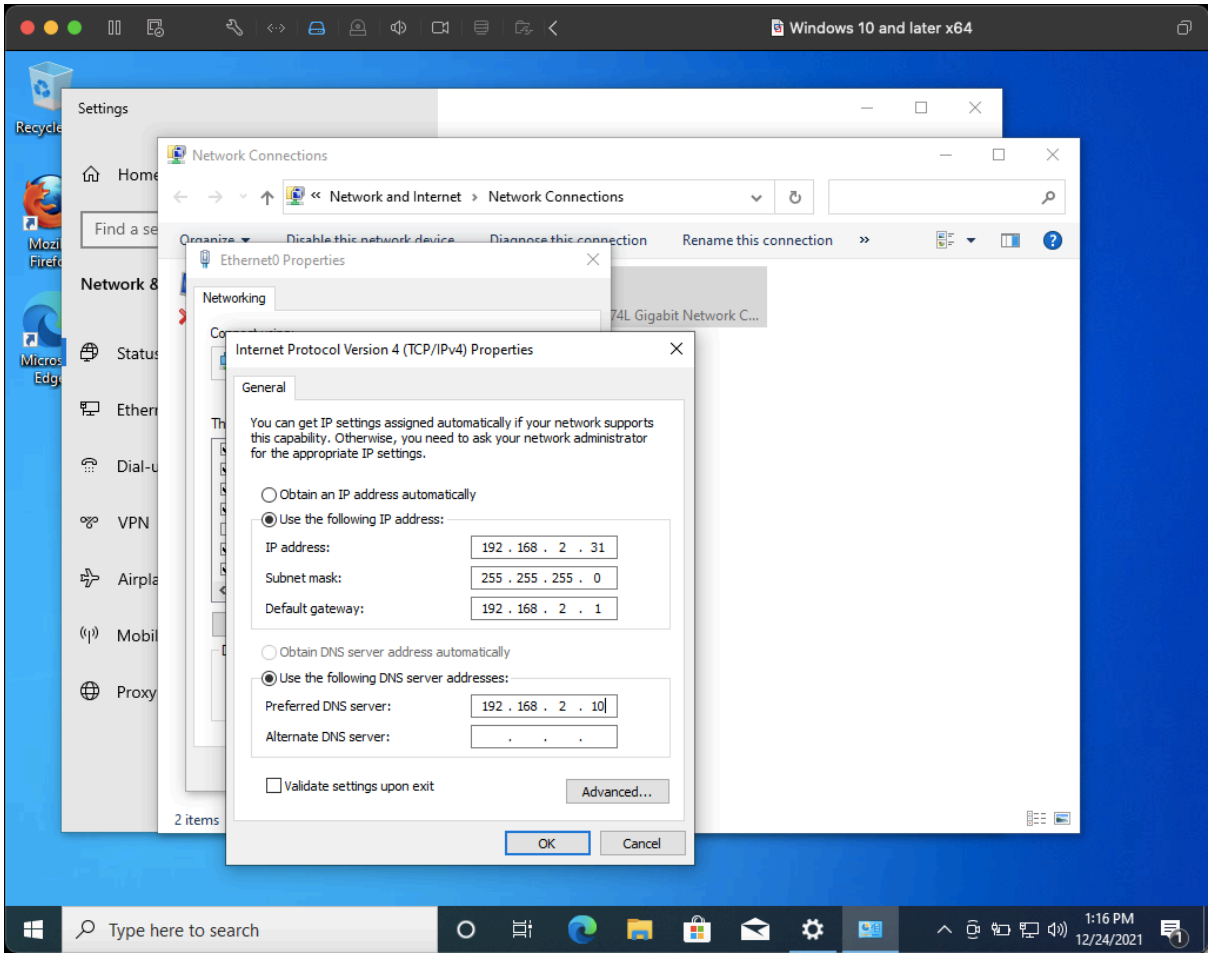
Download Windows 10 iso from the link
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise

Install the VM as usual with defaults and follow the steps as shown –
Uncheck all privacy settings and select Accept.
Search “pc name” and change the PC Name according to the designated user.
Restart the PC.



Joining the PC to the Domain –

Navigate to Network Adapter settings
Right-click on Ethernet0 and select properties
Select IPV4
Add IP address (192.168.2.21) and use 192.168.2.1 as the default gateway
Use 192.168.2.10 (VictimNetwork) as the DNS Server

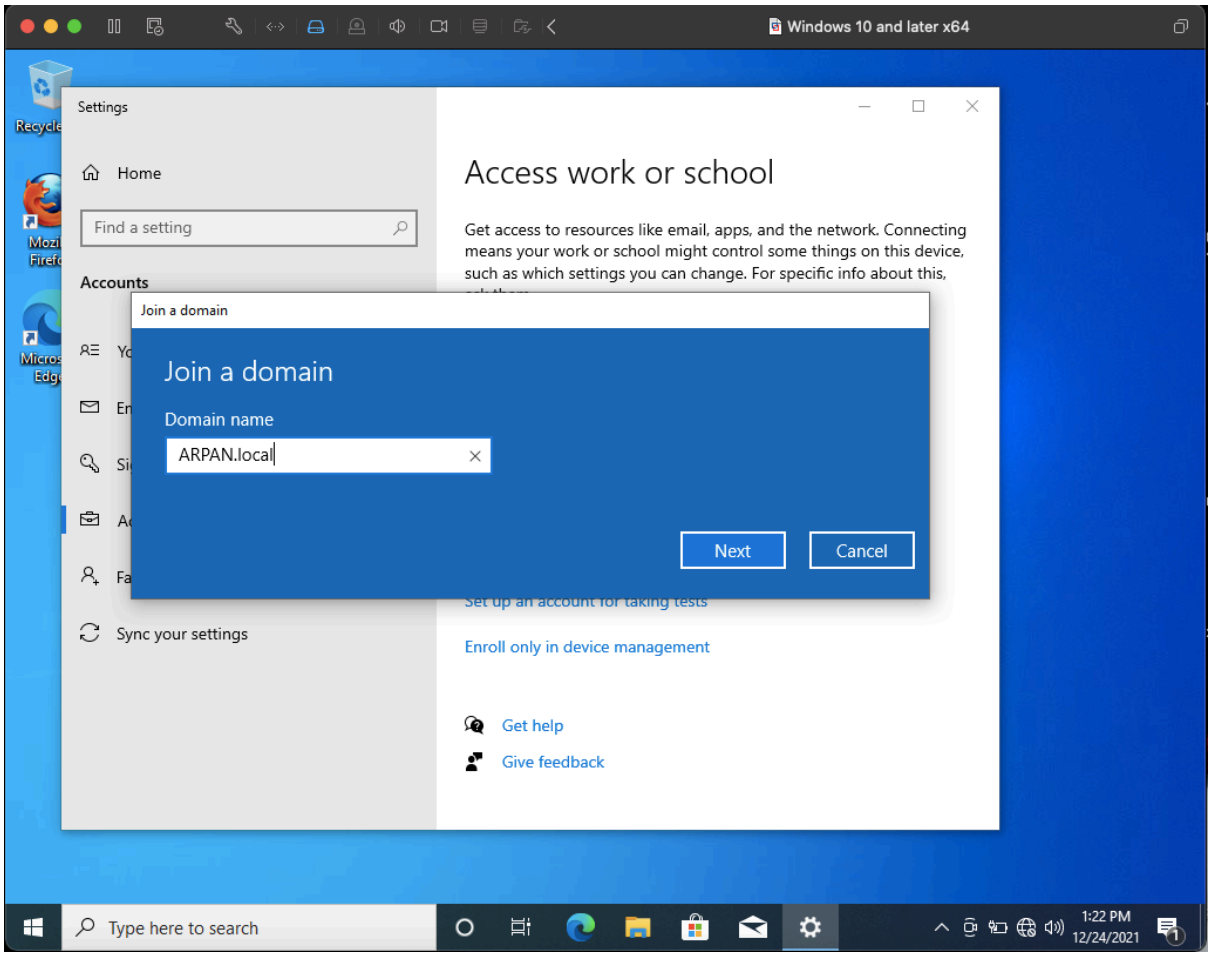


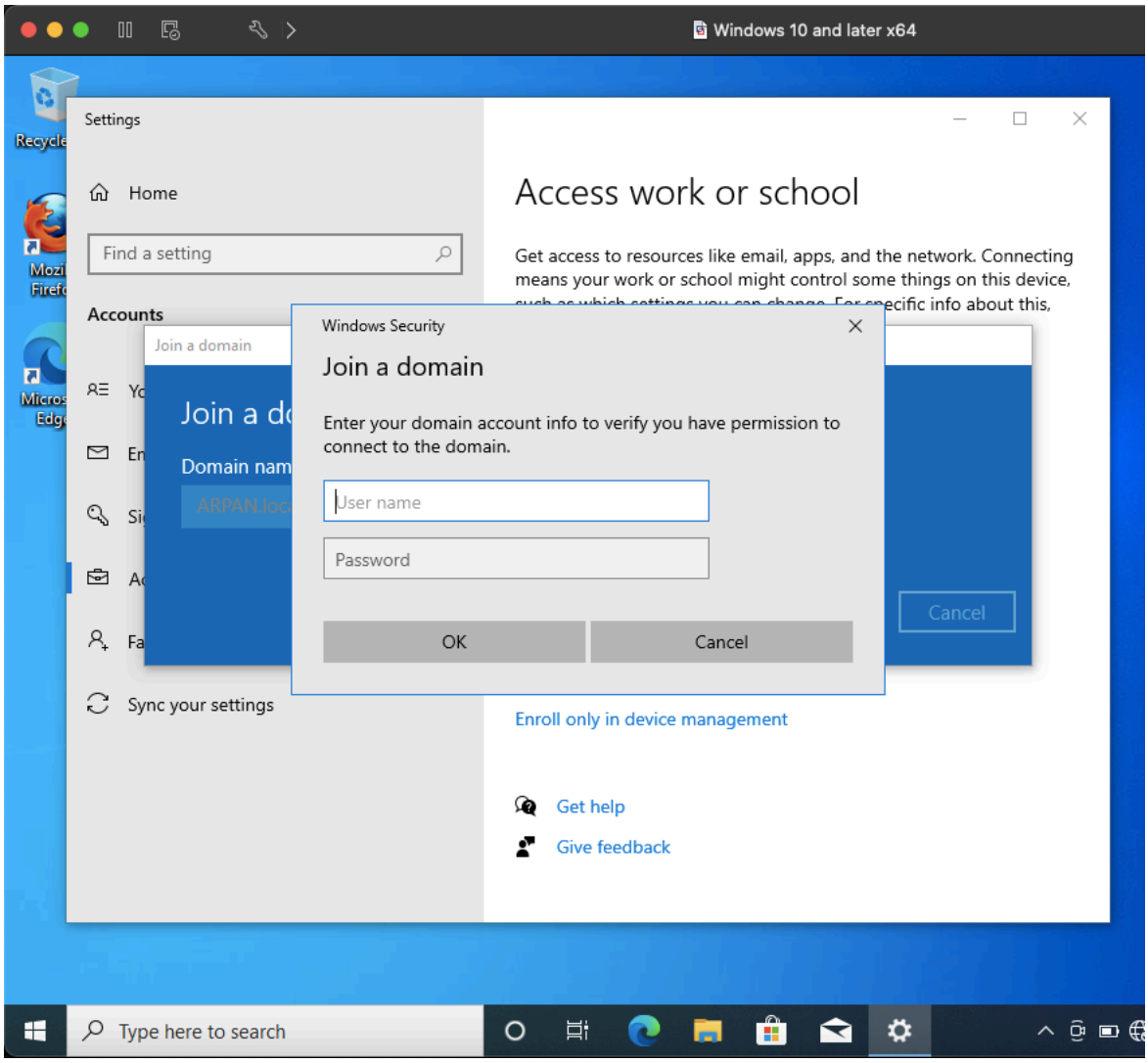
Head over to pfsense

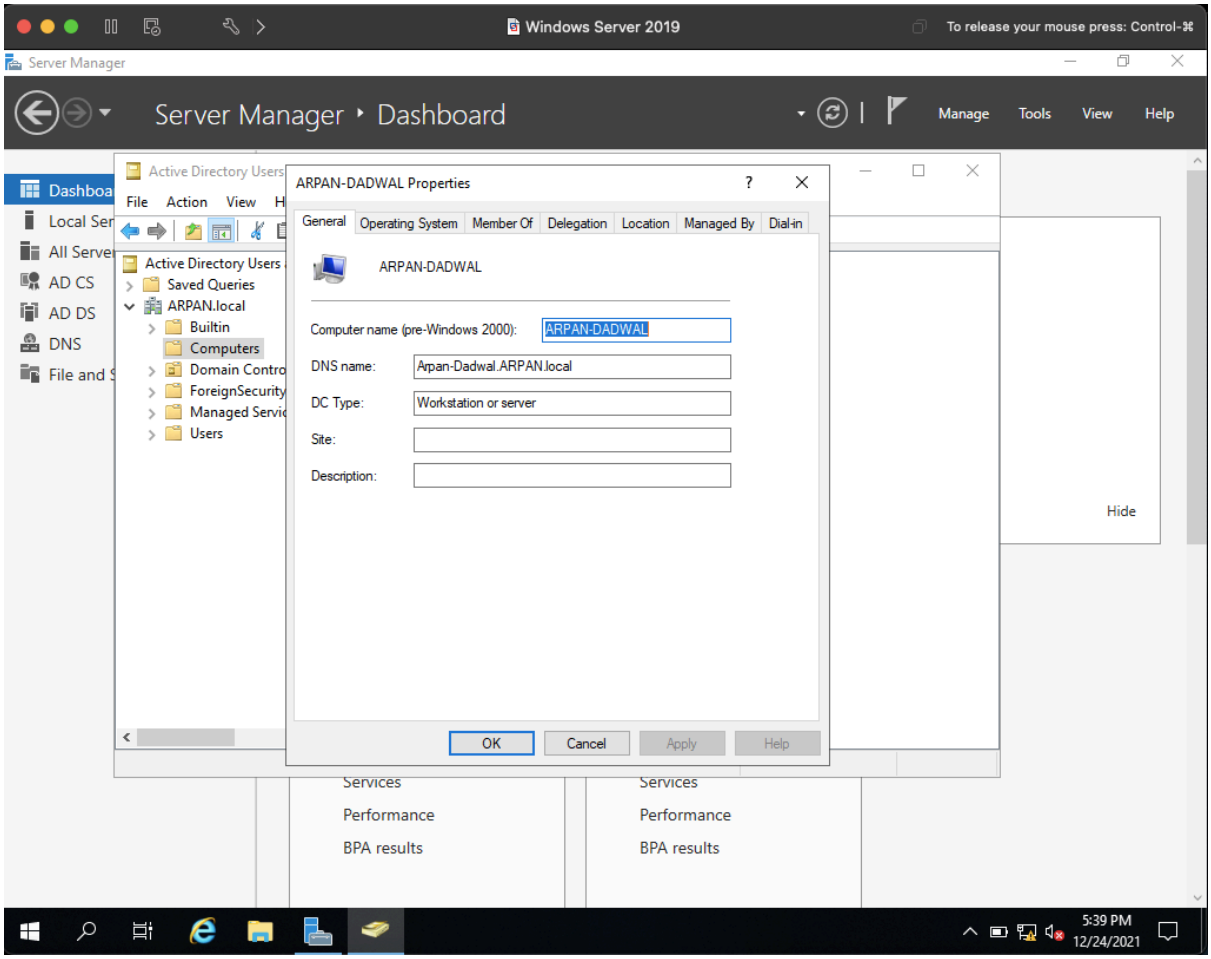
At Services > DHCP Server > VICTIMNETWORK > DMS Server – type the IP of your domain controller (192.168.2.10)
Scroll down to Other Options > Domain Name – type your domain name.local

Search “domain” and select Access work or school
Select Connect > join this to local Active Directory Domain
Enter you domain name.local

Enter Username: Administrator and password
Of your DC, select skip and Restart



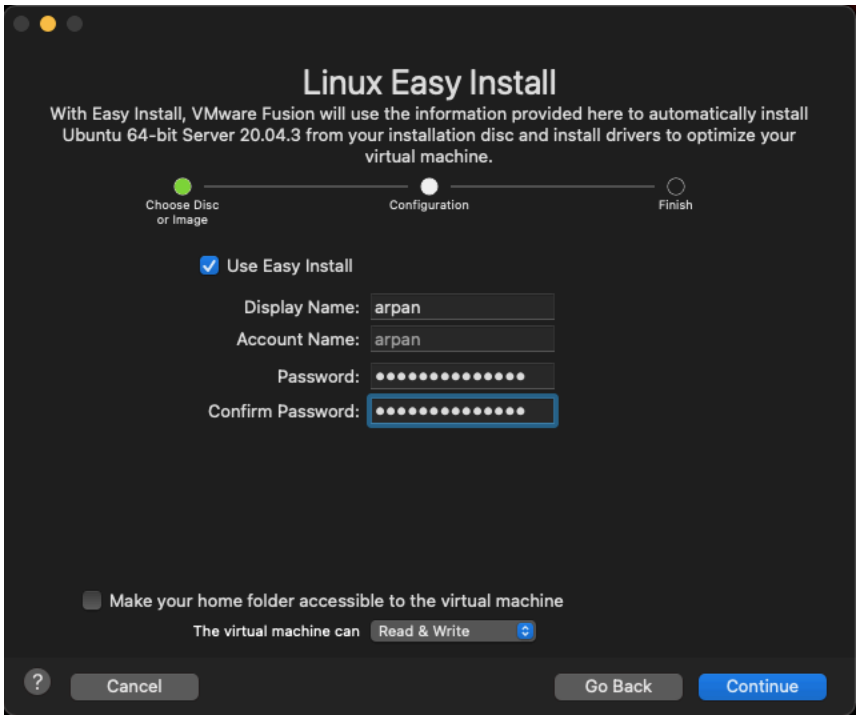

Windows 10 and later x64
Settings
Home
Find a setting
Accounts
Sync your settings
Access work or school
Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device,
Enroll only in device management
Get help
Give feedback
Join a domain
Windows Security
Join a domain
Enter your domain account info to verify you have permission to connect to the domain.
User name
Password
OK
Cancel
Cancel
Type here to search

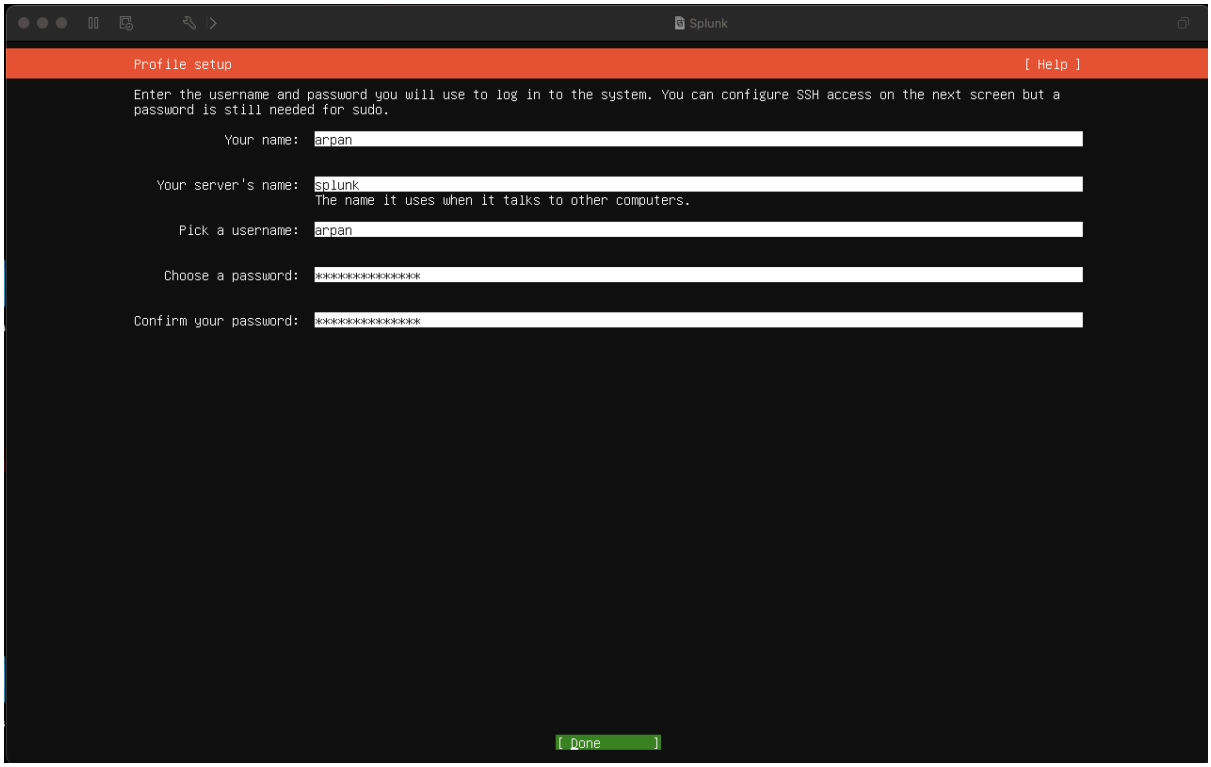

Windows Server 2019
To release your mouse press: Control-⌘
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users
File
Action
View
Active Directory Users
Saved Queries
ARPAN.local
Builtin
Computers
Domain Contro
ForeignSecurity
Managed Servic
Users
ARPAN-DADWAL Properties
General
Operating System
Member Of
Delegation
Location
Managed By
Dial-in
ARPAN-DADWAL
Computer name (pre-Windows 2000):
ARPAN-DADWAL
DNS name:
Arpan-Dadwal.ARPAN.local
DC Type:
Workstation or server
Site:
Description:
OK
Cancel
Apply
Help
Hide
Services
Performance
BPA results
Services
Performance
BPA results
5:39 PM
12/24/2021

Installing Splunk on a Ubuntu Server –

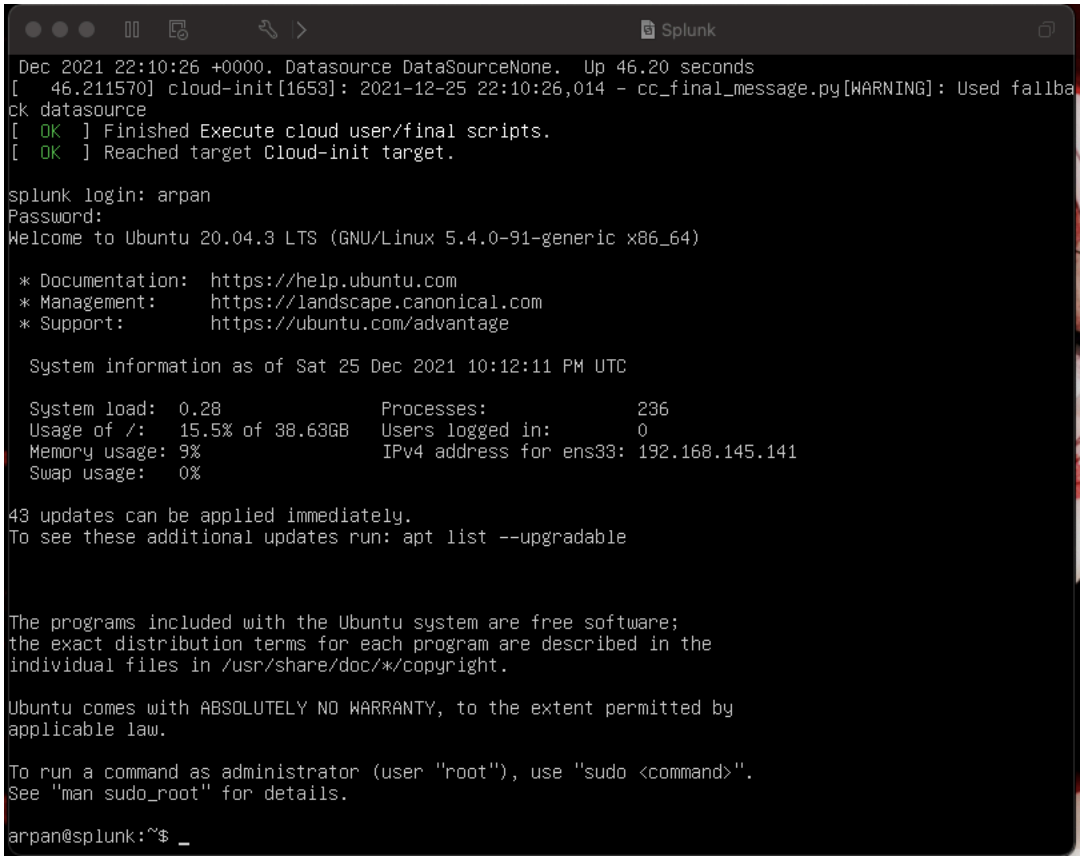
Splunk is one of the most widely used SIEMs in the Cybersecurity industry. Splunk essentially aggregates logs and datasets from various data sources and correlates all the information for easy searching, parsing and indexing.

First we will be downloading Ubuntu Server for our Splunk instance. After downloading, create a VM with the following settings.
Install the server with default settings and create a profile.




Splunk
Profile setup
[Help]
Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.
Your name: arpan
Your server's name: splunk
The name it uses when it talks to other computers.
Pick a username: arpan
Choose a password: ***************
Confirm your password: ***************
[Done]

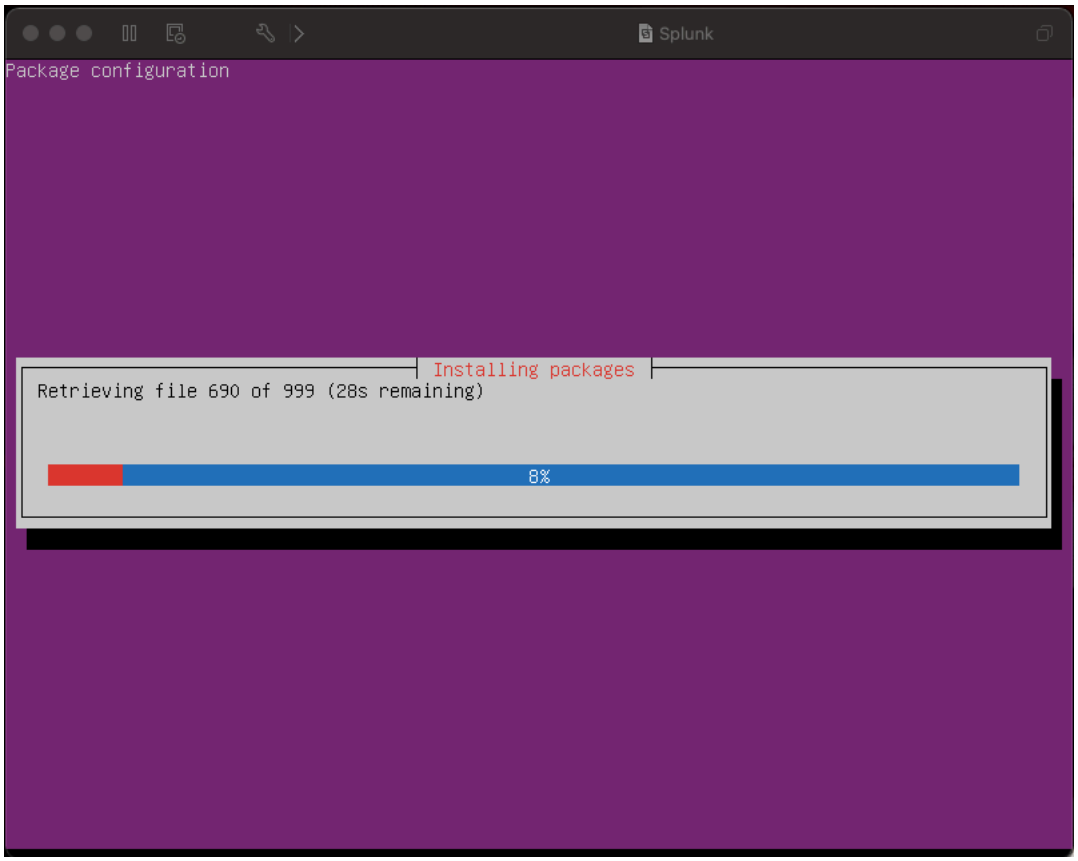
Install an OpenSSH server and add other services according to your preference. After reboot, your sign in screen will be like this –



Now we will be installing a GUI on Ubuntu Server using the following steps
On terminal type the following commands –

sudo apt install tasksel

sudo tasksel install ubuntu-desktop



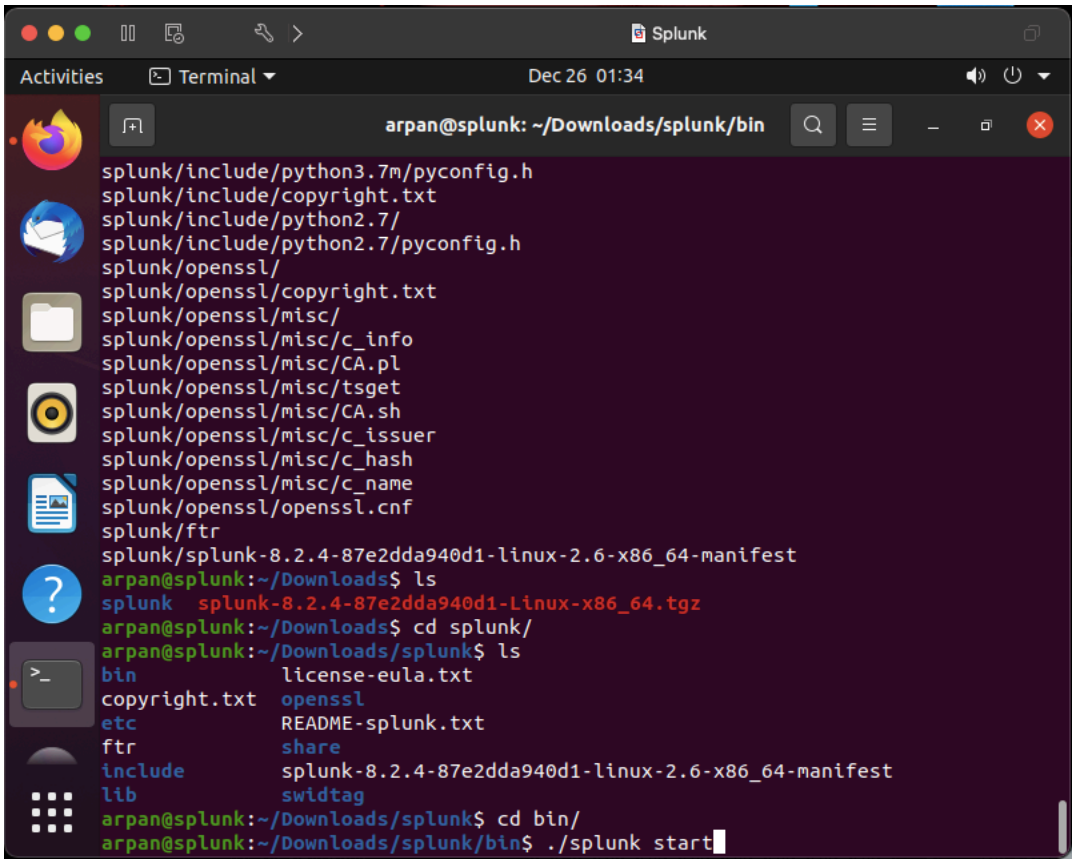
Reboot the VM with “reboot” command

Installing Splunk –

On Ubuntu Server, navigate to splunk.com and click on free splunk
Create an account, select the Linux package and download the .tgz file

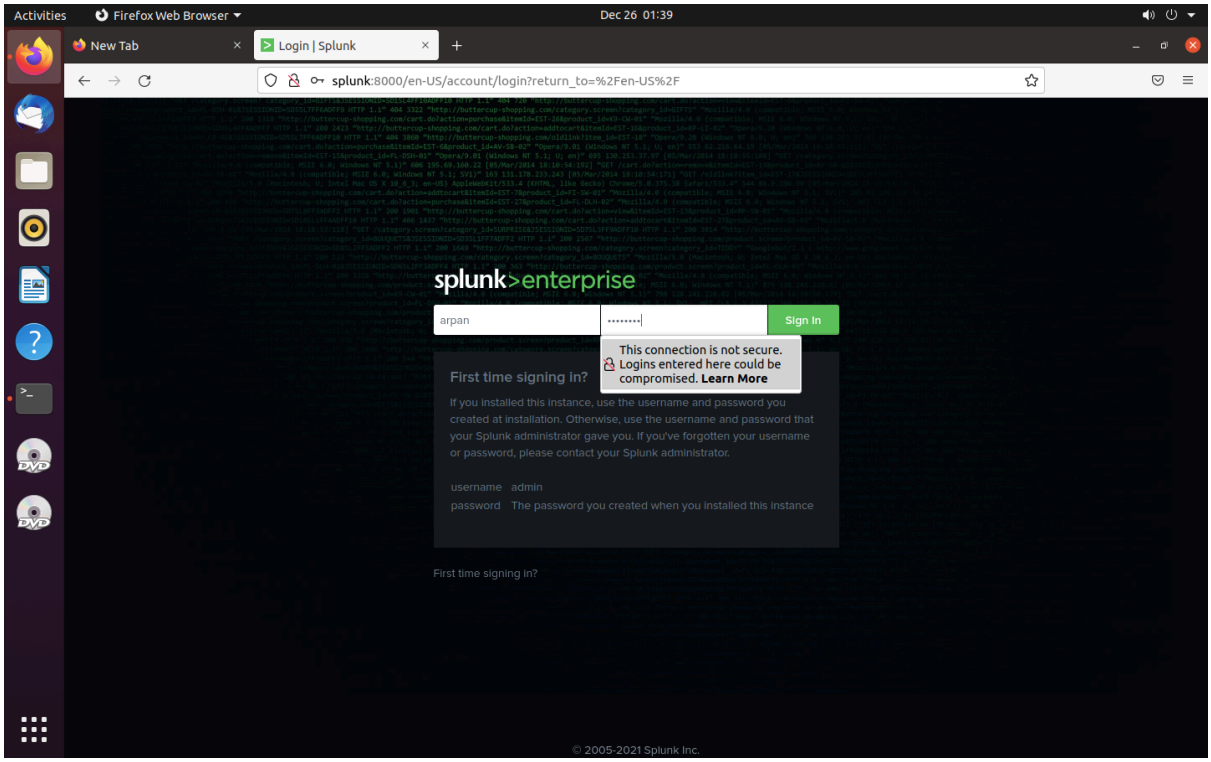
Open terminal, navigate to the Downloads directory and untar the file using command tar xvzf “splunk package”

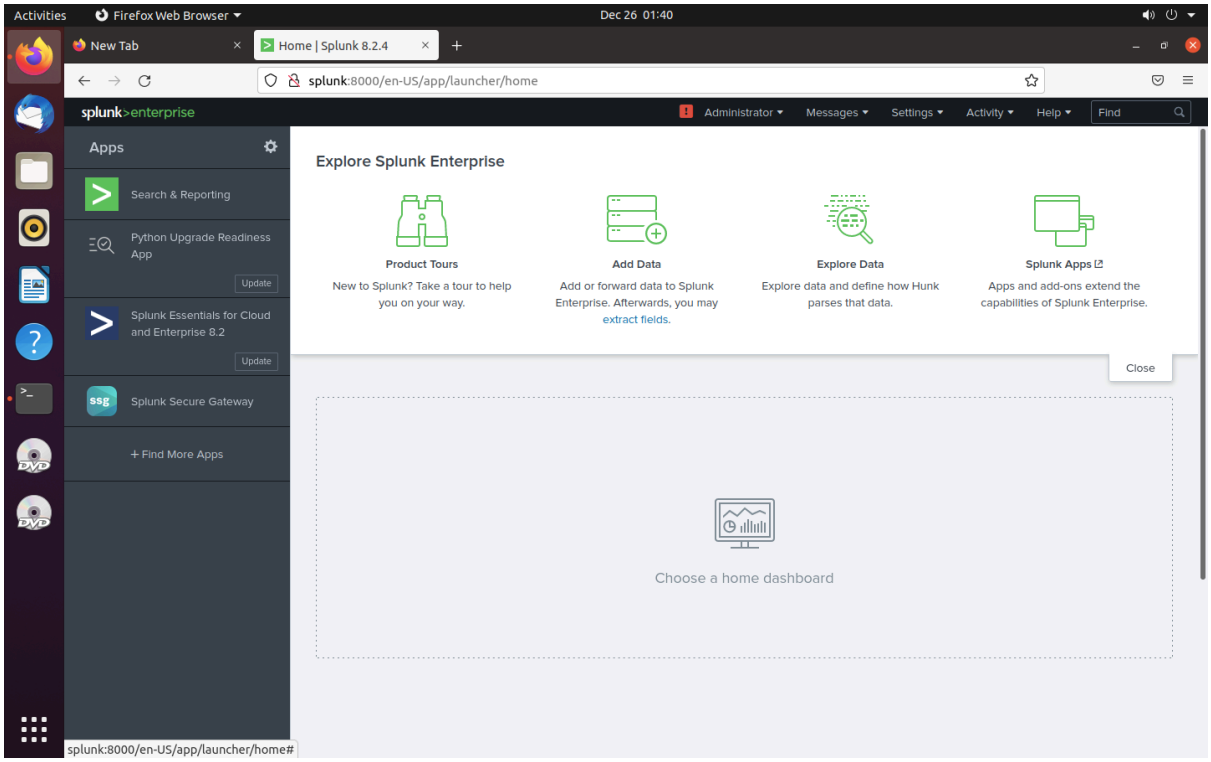
Now start the Splunk instance by using command ./splunk start



Enter admin username and password of your choice.

Navigate to http://splunk:8000 on your browser and log in using the username and password you configured in the previous step.



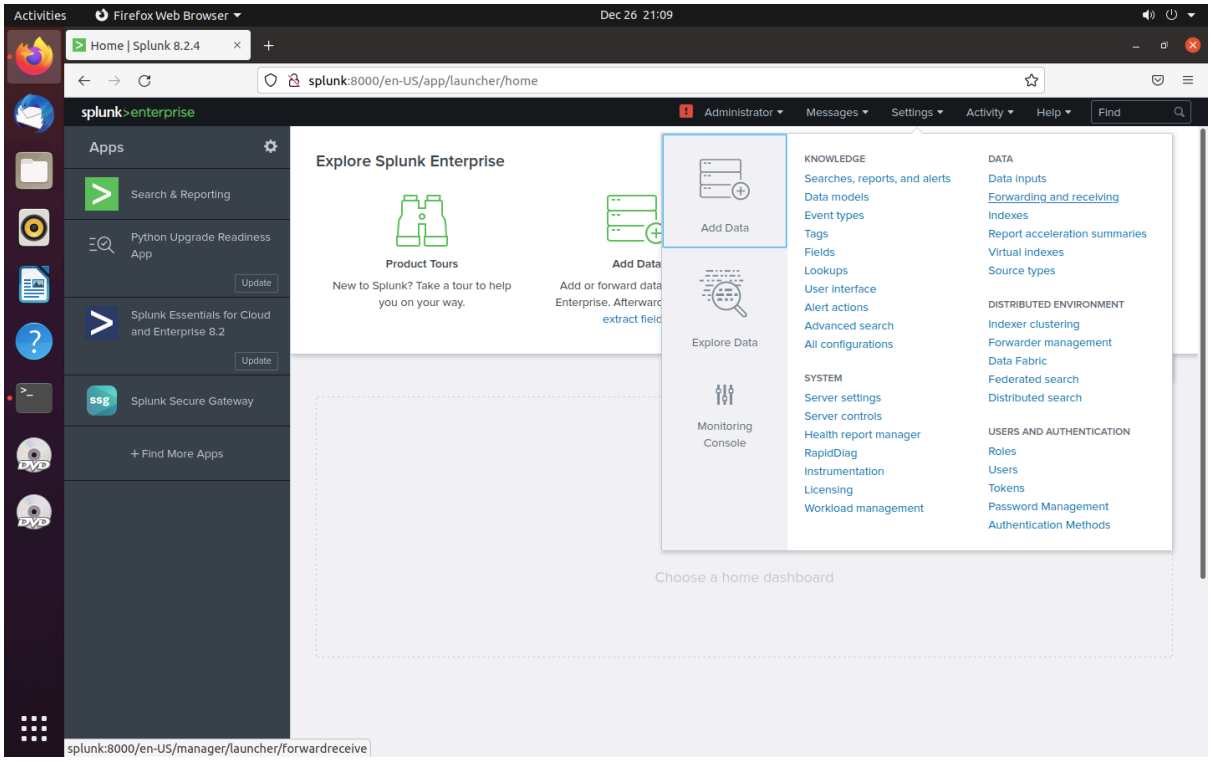

Activities
Firefox Web Browser
Dec 26 01:40
New Tab
Home | Splunk 8.2.4
splunk:8000/en-US/app/launcher/home
splunk>enterprise
Administrator
Messages
Settings
Activity
Help
Find
Apps
Search & Reporting
Python Upgrade Readiness App
Update
Splunk Essentials for Cloud and Enterprise 8.2
Update
Splunk Secure Gateway
+ Find More Apps
Explore Splunk Enterprise
Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.
Explore Data
Explore data and define how Hunk parses that data.
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.
Close
Choose a home dashboard
splunk:8000/en-US/app/launcher/home#

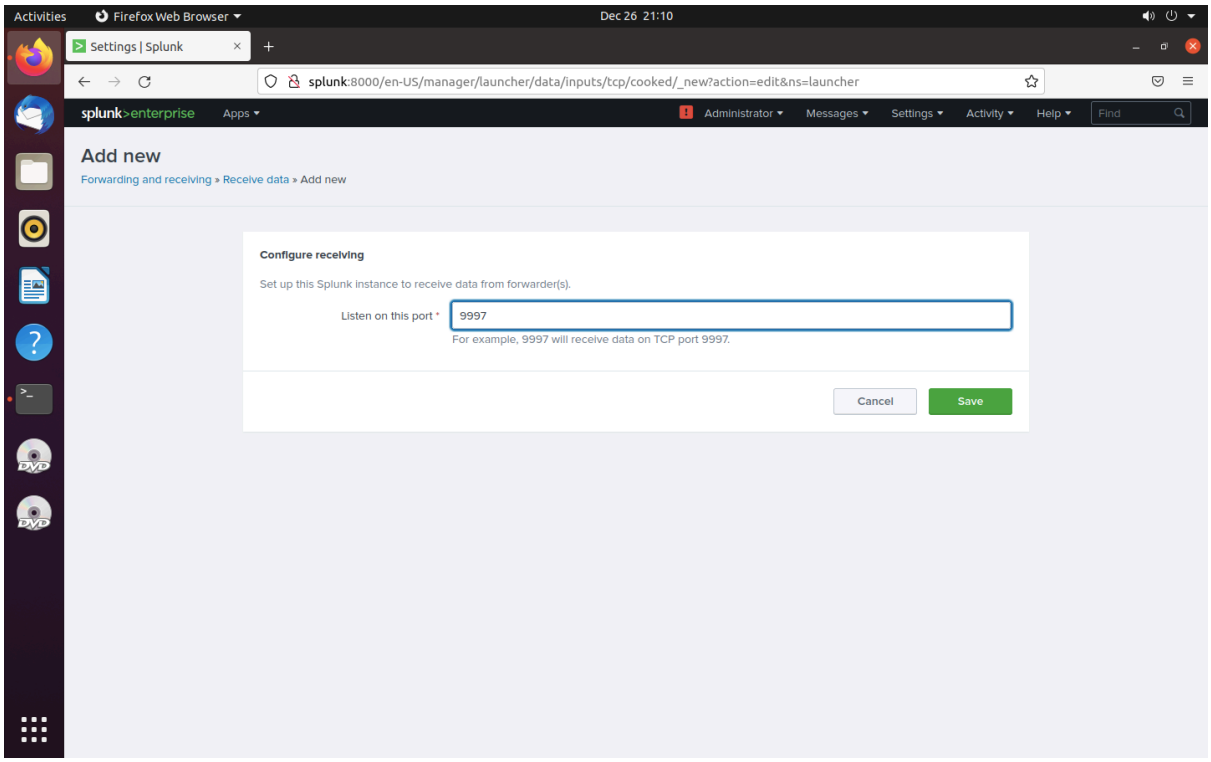
Installing Universal Forwarder on Windows Server

In order to log the activities on endpoints, Splunk uses a mechanism called Universal Forwarder. The Universal Forwarder can be installed on Windows, *nix and mac agents to forward logs to your Splunk instance.

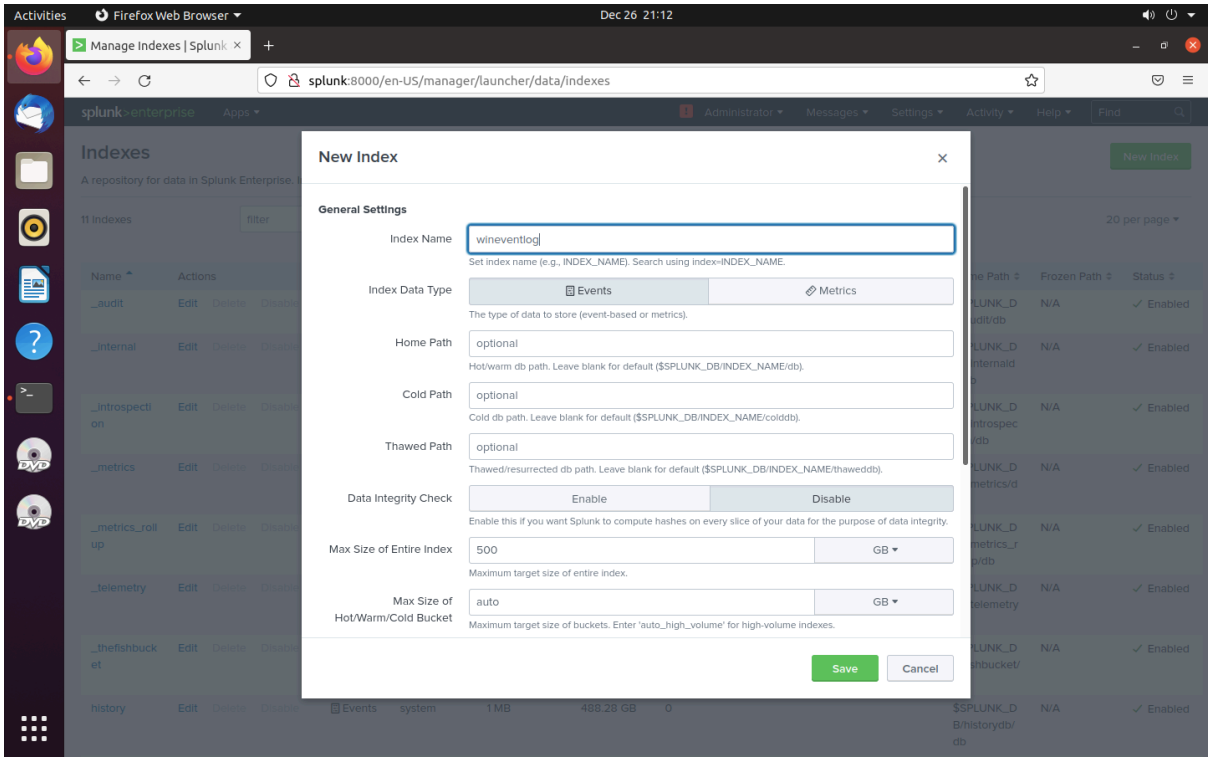
Set up “Receiving” on your Splunk Server.
Navigate to Settings >> Forwarding and Receiving >> New receiving Port

Enter port 9997 and save



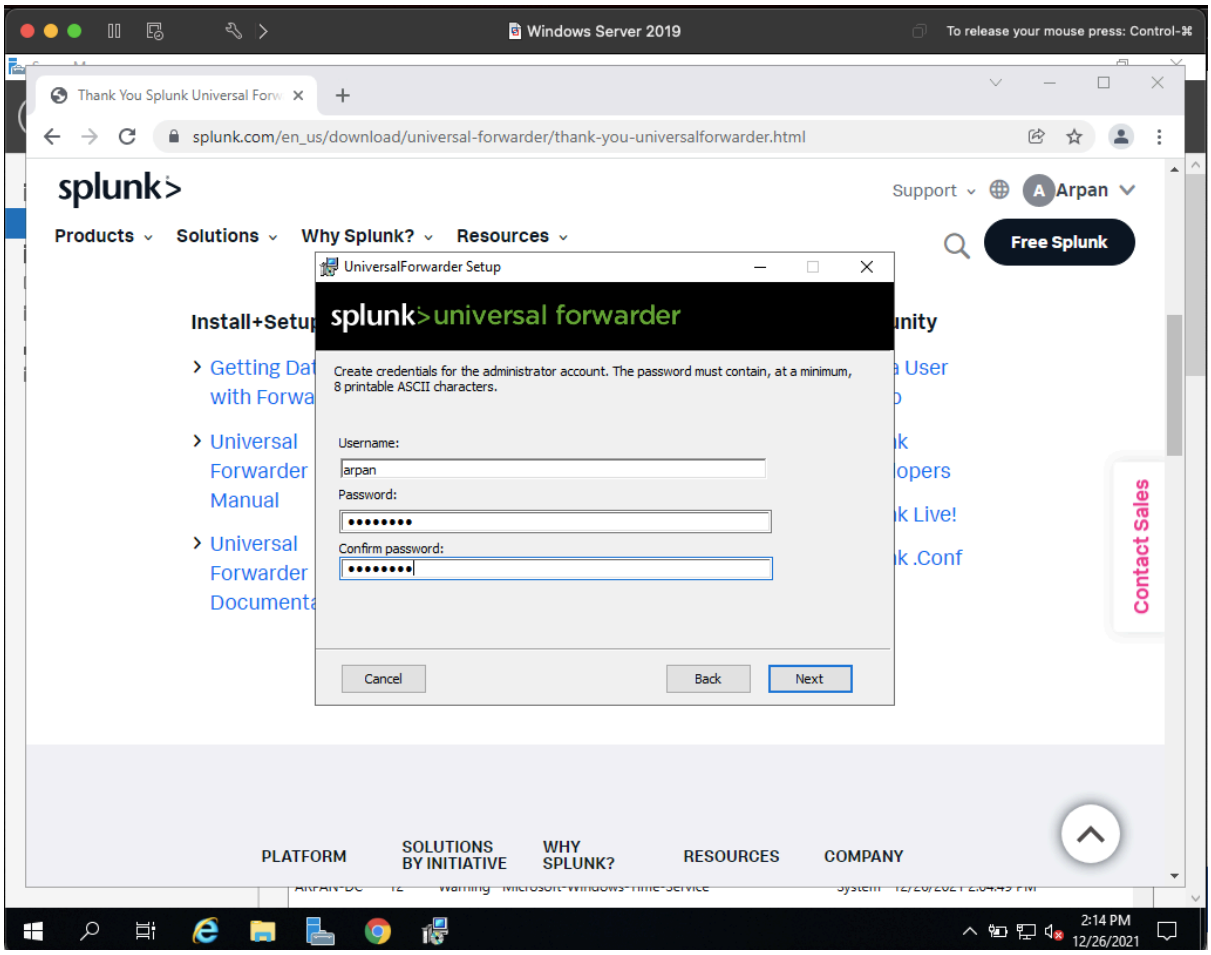

Activities
Firefox Web Browser
Dec 26 21:10
Settings | Splunk
splunk:8000/en-US/manager/launcher/data/inputs/tcp/cooked/_new?action=edit&ns=launcher
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add new
Forwarding and receiving » Receive data » Add new
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).
Listen on this port *
9997
For example, 9997 will receive data on TCP port 9997.
Cancel
Save

Navigate to Settings >> Indexes >> New Index
Name it “wineventlog” and save



On Windows Server, Download Universal Forwarder and install

Accept License and Agreement and click next
Create a suitable username and password
Enter the IP address of your Splunk server and default ports as prompted.

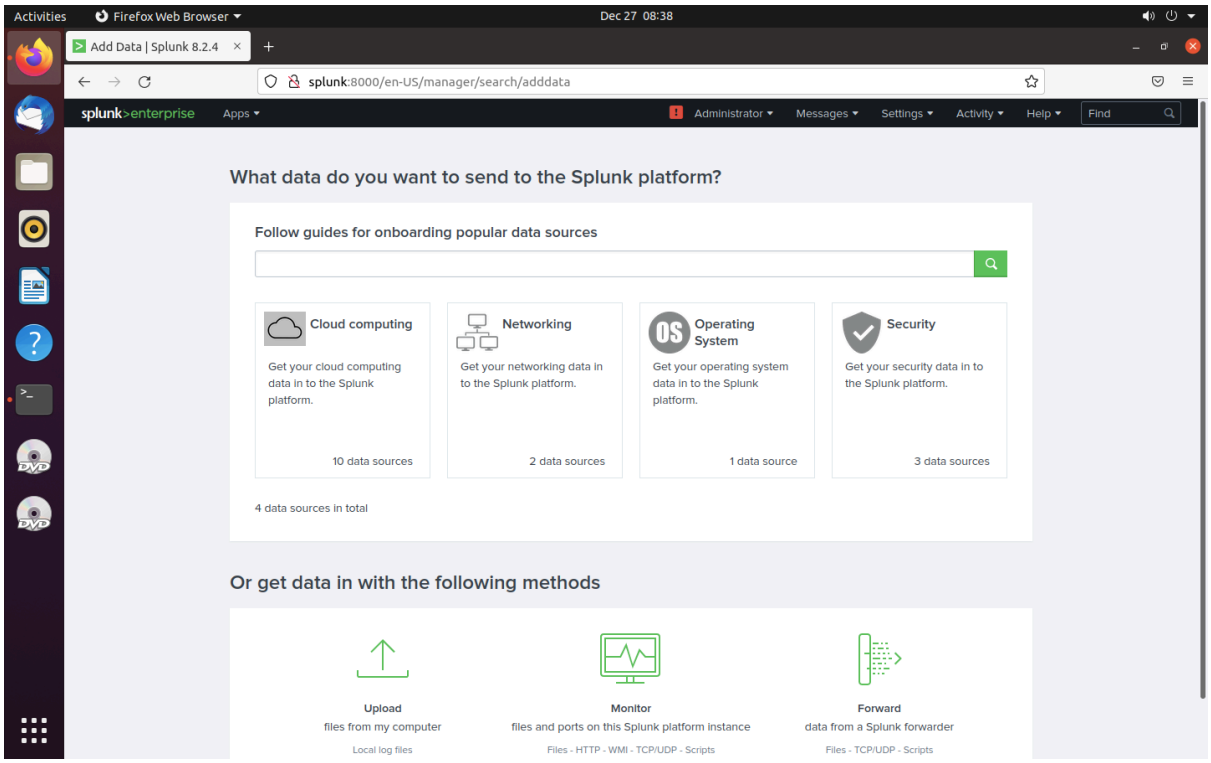


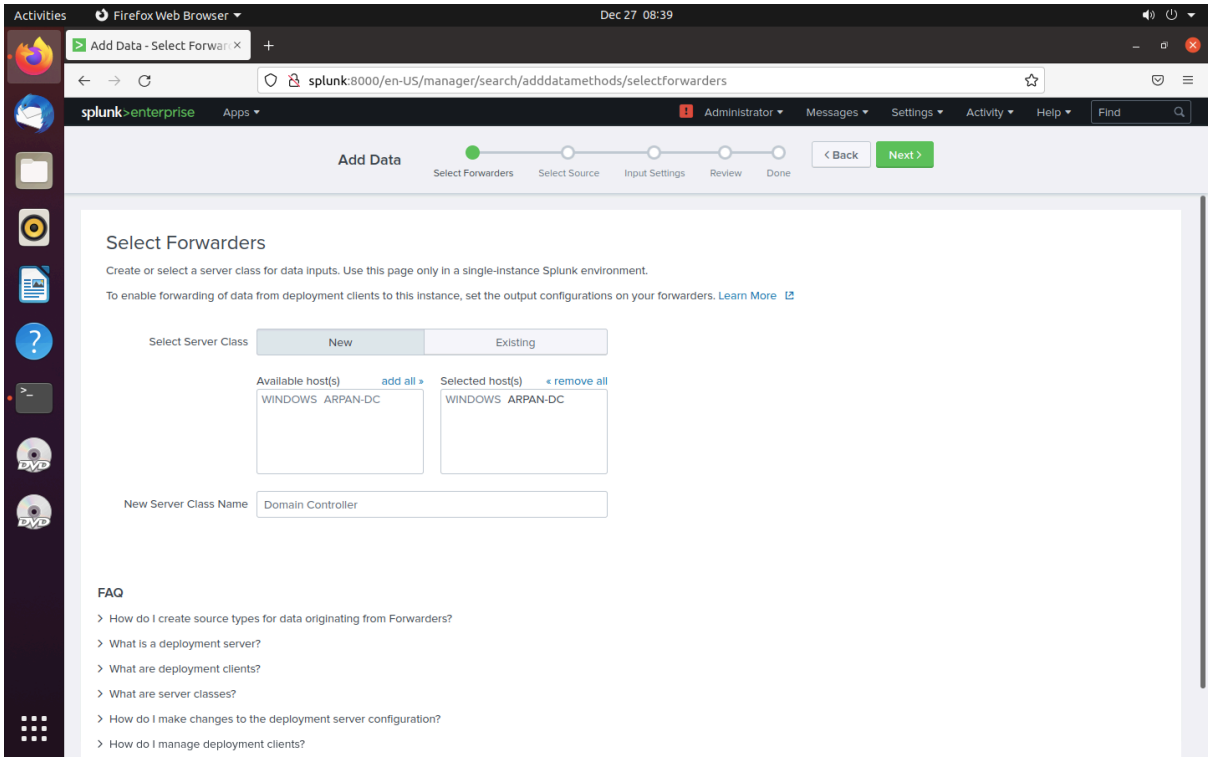
Navigate back to your Splunk instance >> Settings >> Add Data Select “Forward”

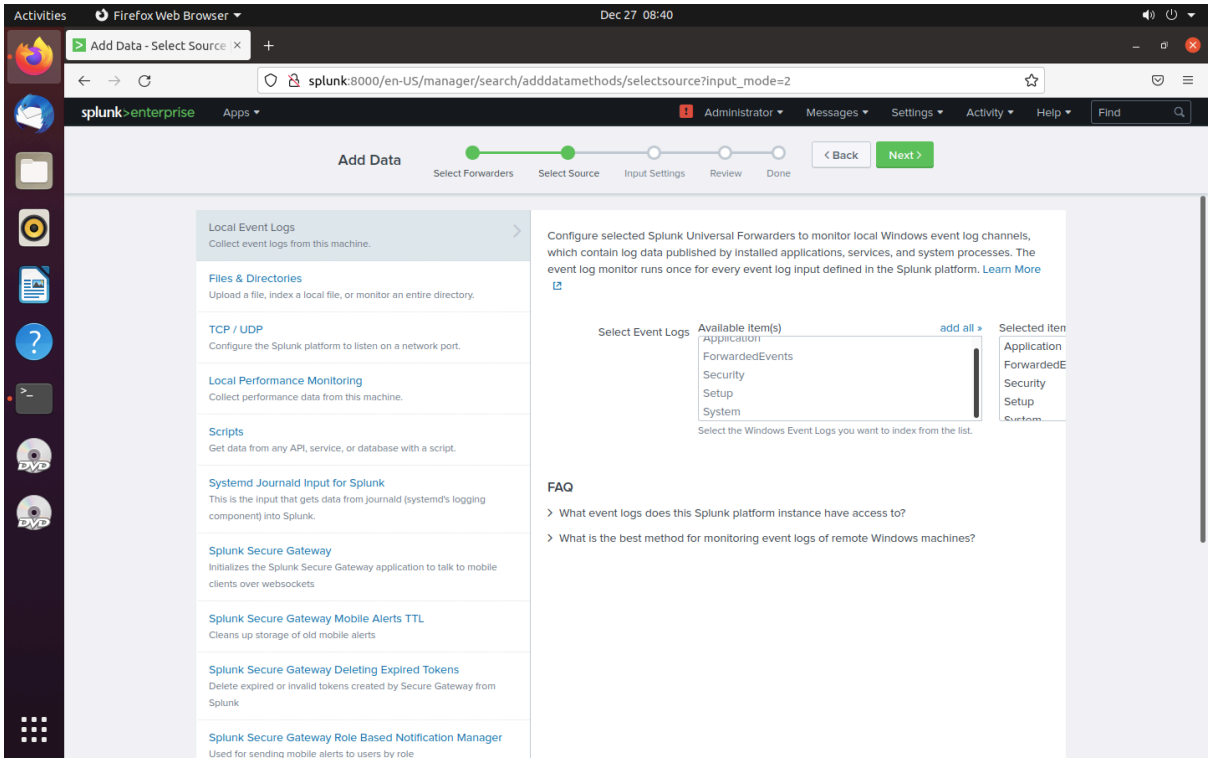
Select the Domain Controller (Windows Server) >> Enter a Server Class Name >> Next

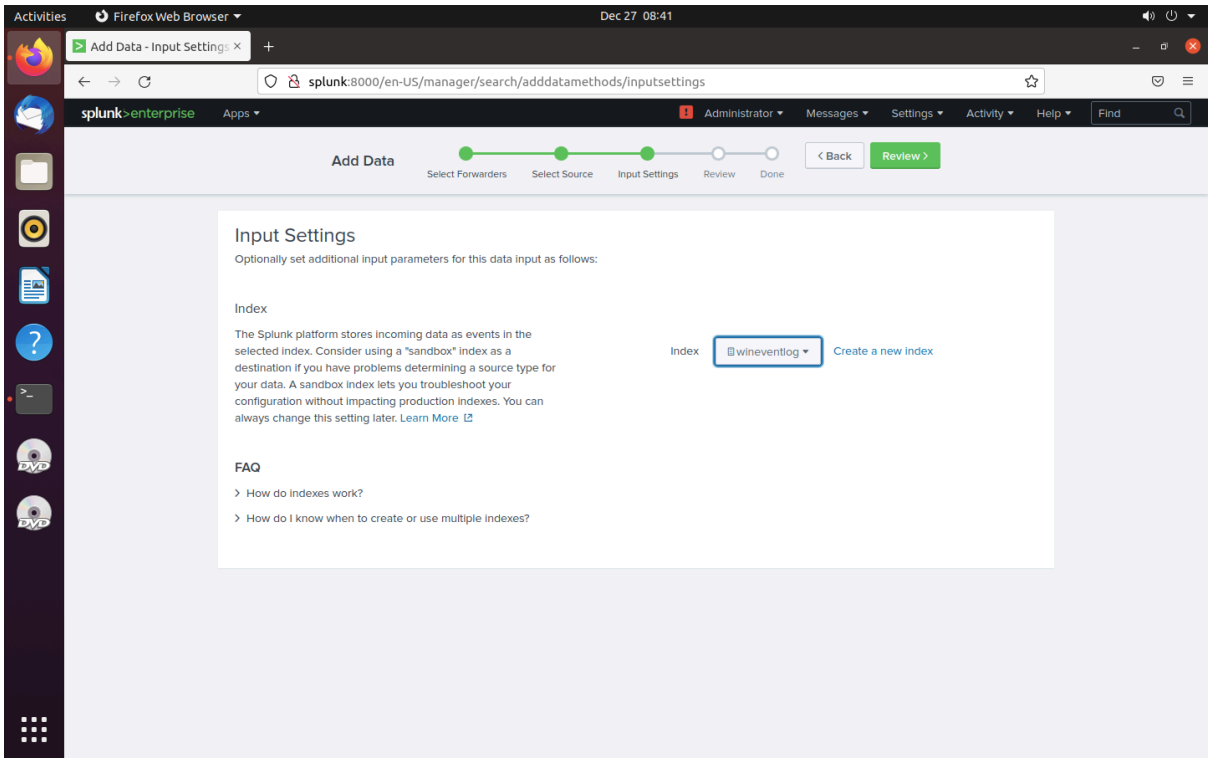
Select Local Events Logs and choose your desired event log >> Next

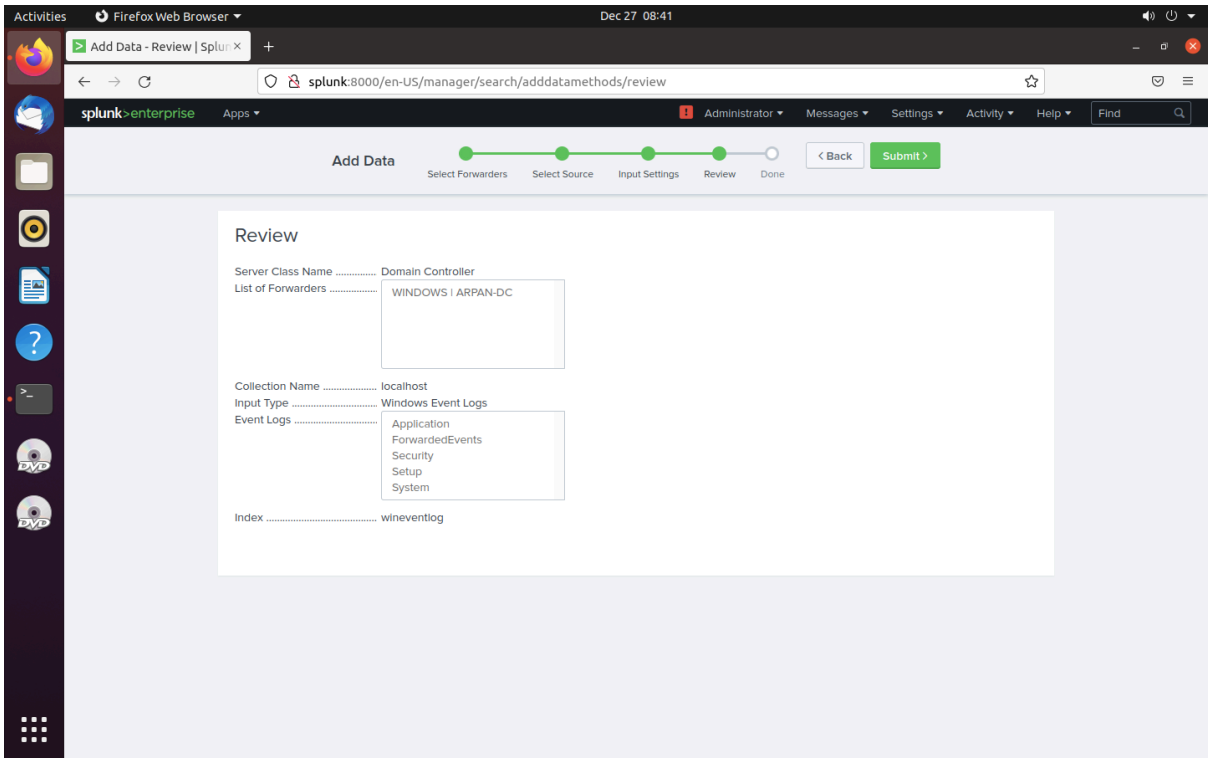
Select “wineventlog” as the Index >> Review >> Submit




Activities
Firefox Web Browser
Dec 27 08:39
Add Data - Select Forwar
splunk:8000/en-US/manager/search/adddatamethods/selectforwarders
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Forwarders
Select Source
Input Settings
Review
Done
Back
Next
Select Forwarders
Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.
To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. Learn More
Select Server Class
New
Existing
Available host(s)
add all »
WINDOWS ARPAN-DC
Selected host(s)
« remove all
WINDOWS ARPAN-DC
New Server Class Name
Domain Controller
FAQ
How do I create source types for data originating from Forwarders?
What is a deployment server?
What are deployment clients?
What are server classes?
How do I make changes to the deployment server configuration?
How do I manage deployment clients?


Activities
Firefox Web Browser
Dec 27 08:40
Add Data - Select Source
splunk:8000/en-US/manager/search/adddatamethods/selectsource?input_mode=2
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Forwarders
Select Source
Input Settings
Review
Done
Back
Next
Local Event Logs
Collect event logs from this machine.
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Local Performance Monitoring
Collect performance data from this machine.
Scripts
Get data from any API, service, or database with a script.
Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.
Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets
Splunk Secure Gateway Mobile Alerts TTL
Cleans up storage of old mobile alerts
Splunk Secure Gateway Deleting Expired Tokens
Delete expired or invalid tokens created by Secure Gateway from Splunk
Splunk Secure Gateway Role Based Notification Manager
Used for sending mobile alerts to users by role
Configure selected Splunk Universal Forwarders to monitor local Windows event log channels, which contain log data published by installed applications, services, and system processes. The event log monitor runs once for every event log input defined in the Splunk platform. Learn More
Select Event Logs
Available item(s)
add all »
Selected item
ForwardedEvents
Security
Setup
System
Application
Select the Windows Event Logs you want to index from the list.
FAQ
What event logs does this Splunk platform instance have access to?
What is the best method for monitoring event logs of remote Windows machines?


Activities
Firefox Web Browser
Dec 27 08:41
Add Data - Input Settings
splunk:8000/en-US/manager/search/adddatamethods/inputsettings
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Forwarders
Select Source
Input Settings
Review
Done
Back
Review
Input Settings
Optionally set additional input parameters for this data input as follows:
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More
Index
wineventlog
Create a new index
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?



This concludes the end of our homelab setup.