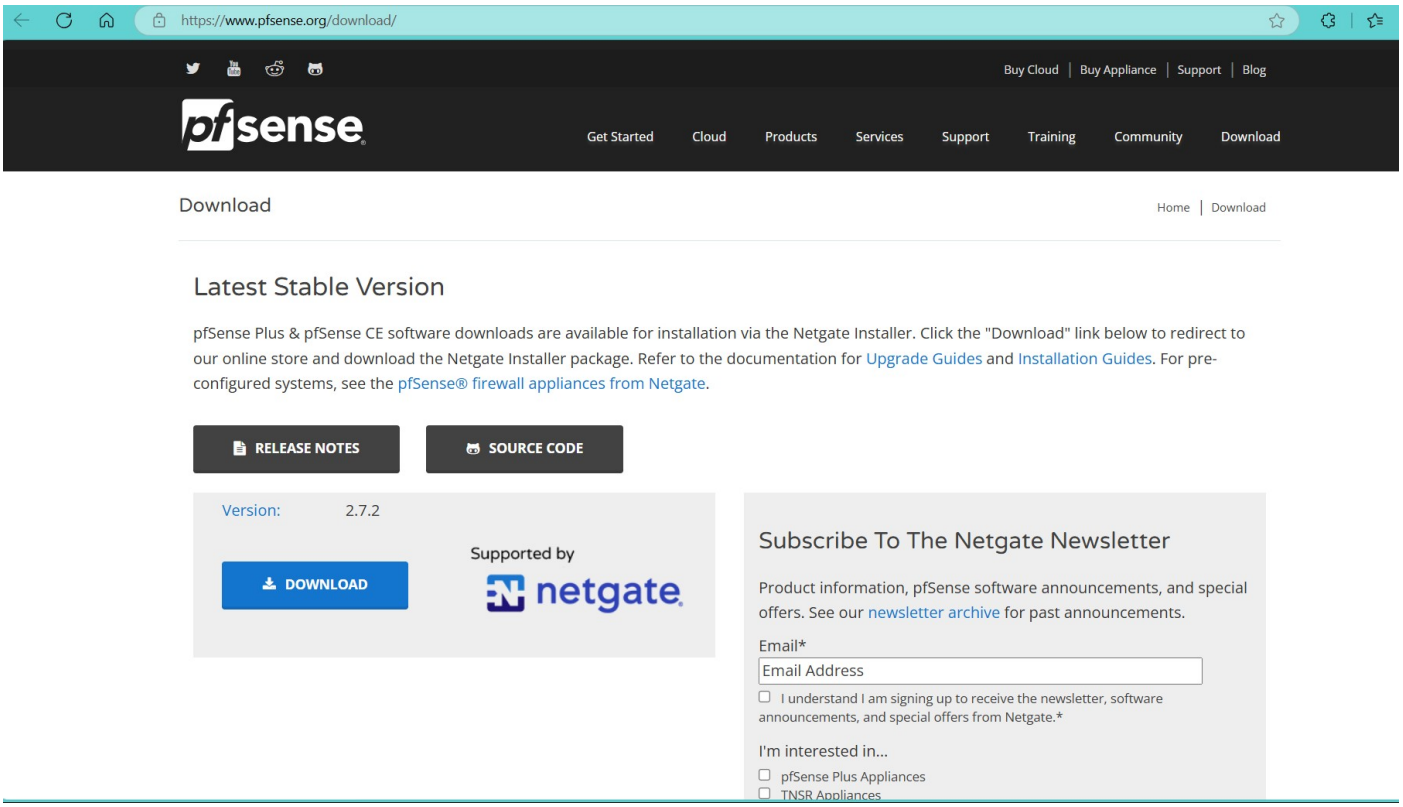
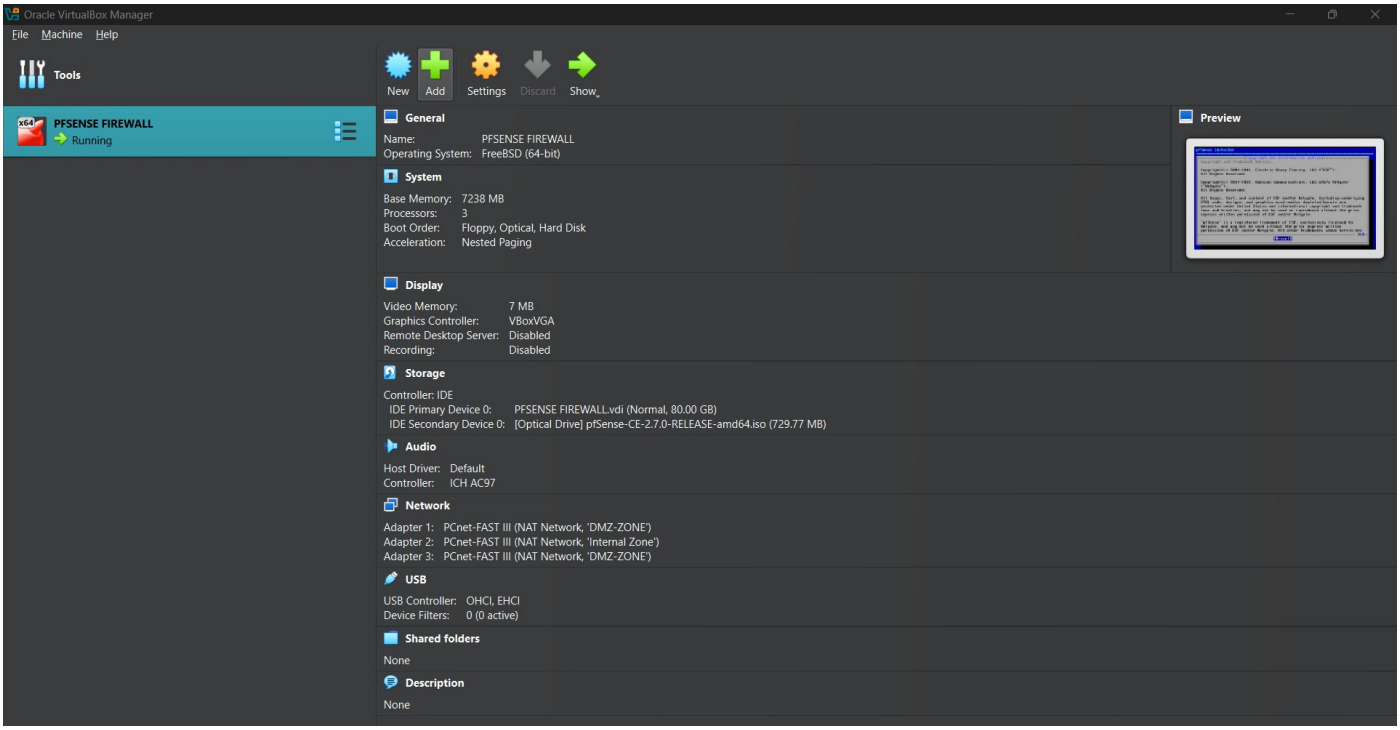
pfSense Firewall Configuration

Objective 1: Deploying the pfSense VM

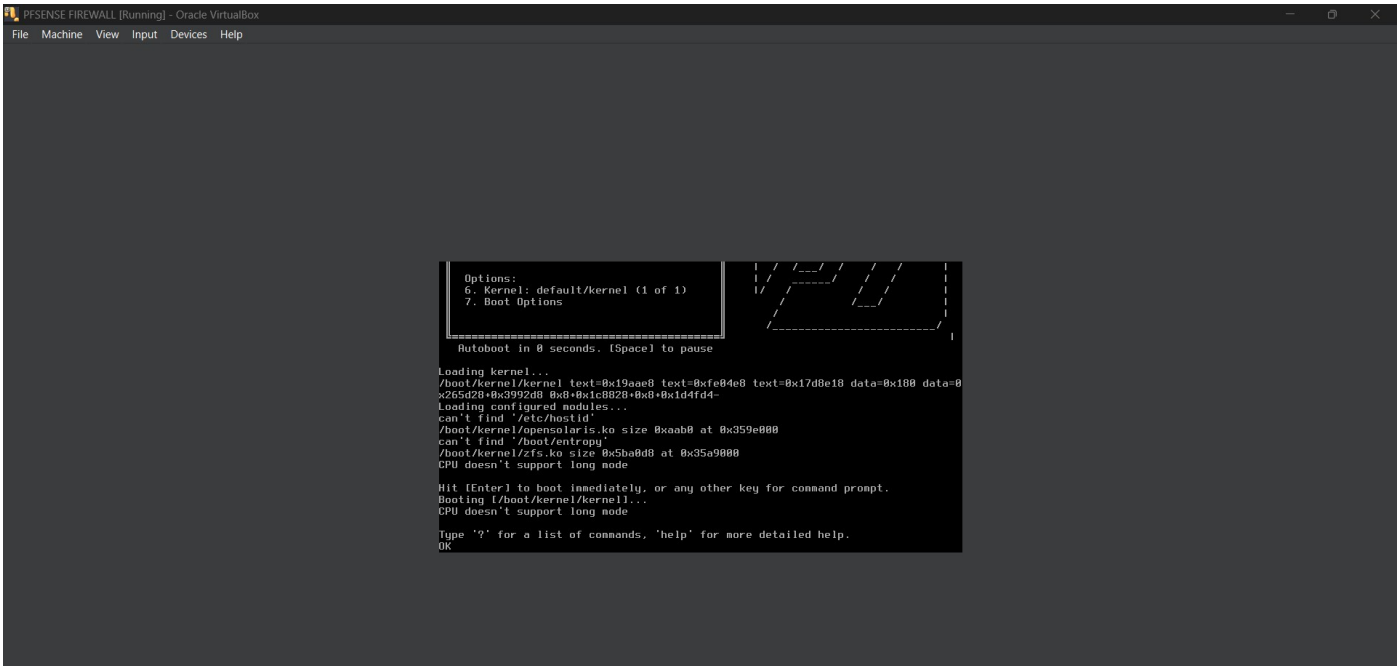
- Downloaded the latest pfSense install ISO file from the official website.

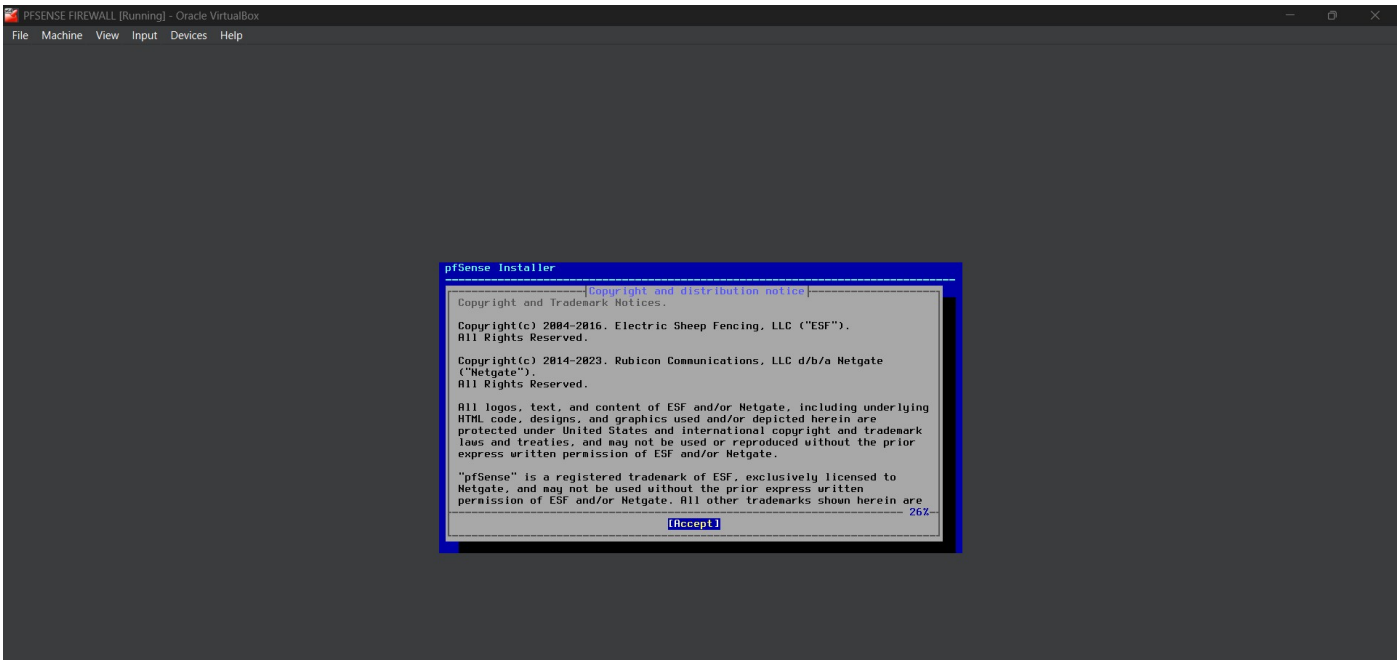


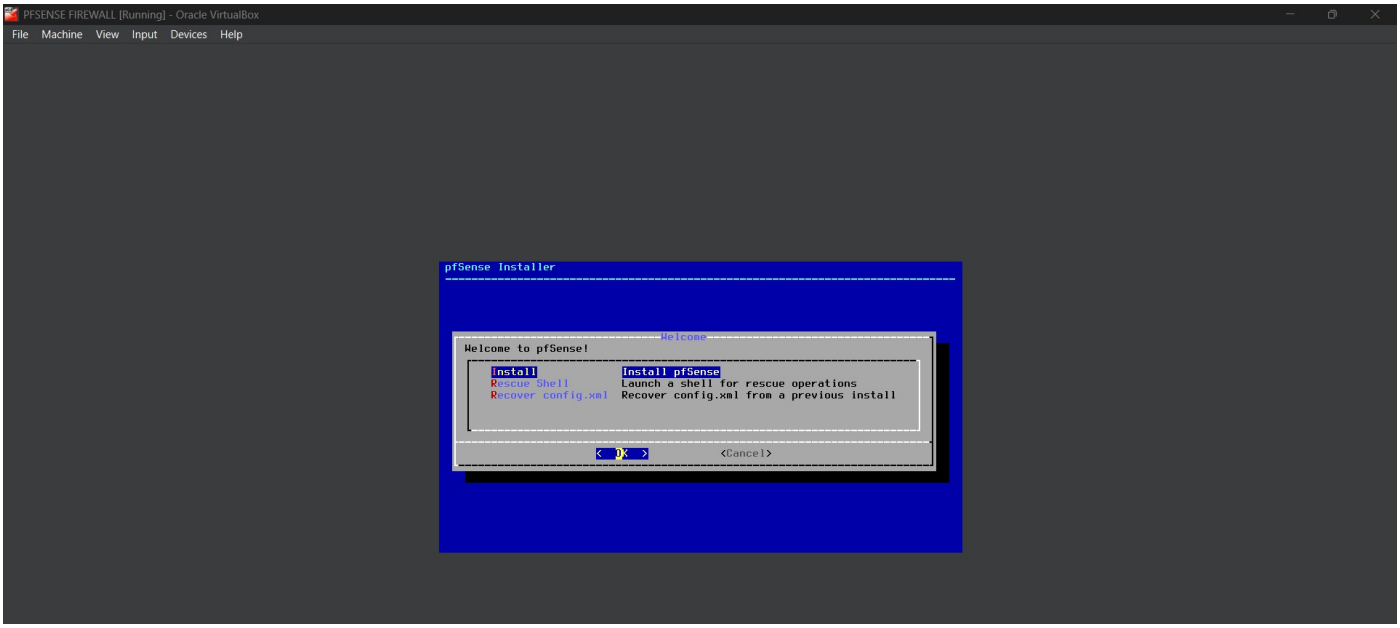
- Created a new virtual machine in Oracle VirtualBox and attached the downloaded ISO image for installation.Named the VM and configured hardware settings, ensuring three network interfaces were set up as required. Powered on the VM, initiating the pfSense Installer.



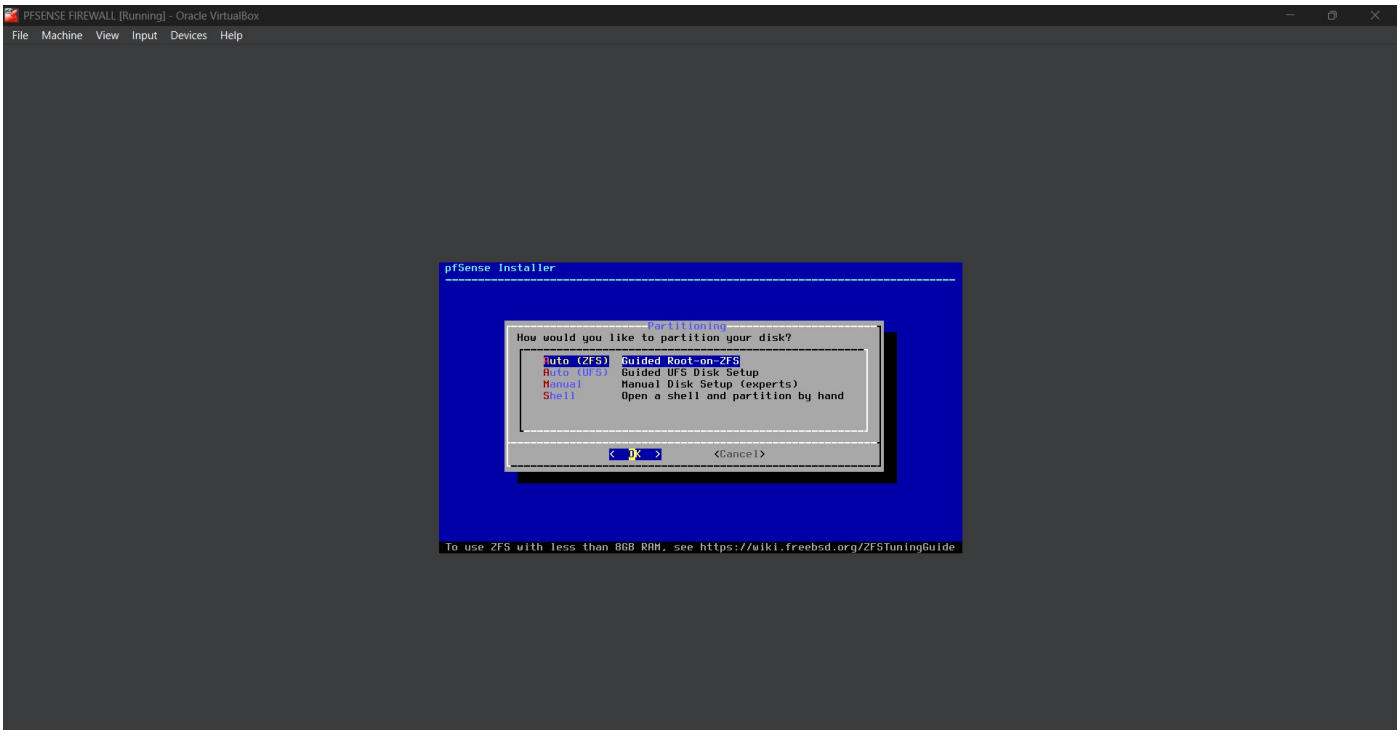
- Accepted the initial installation prompts and confirmed the default keymap selection.

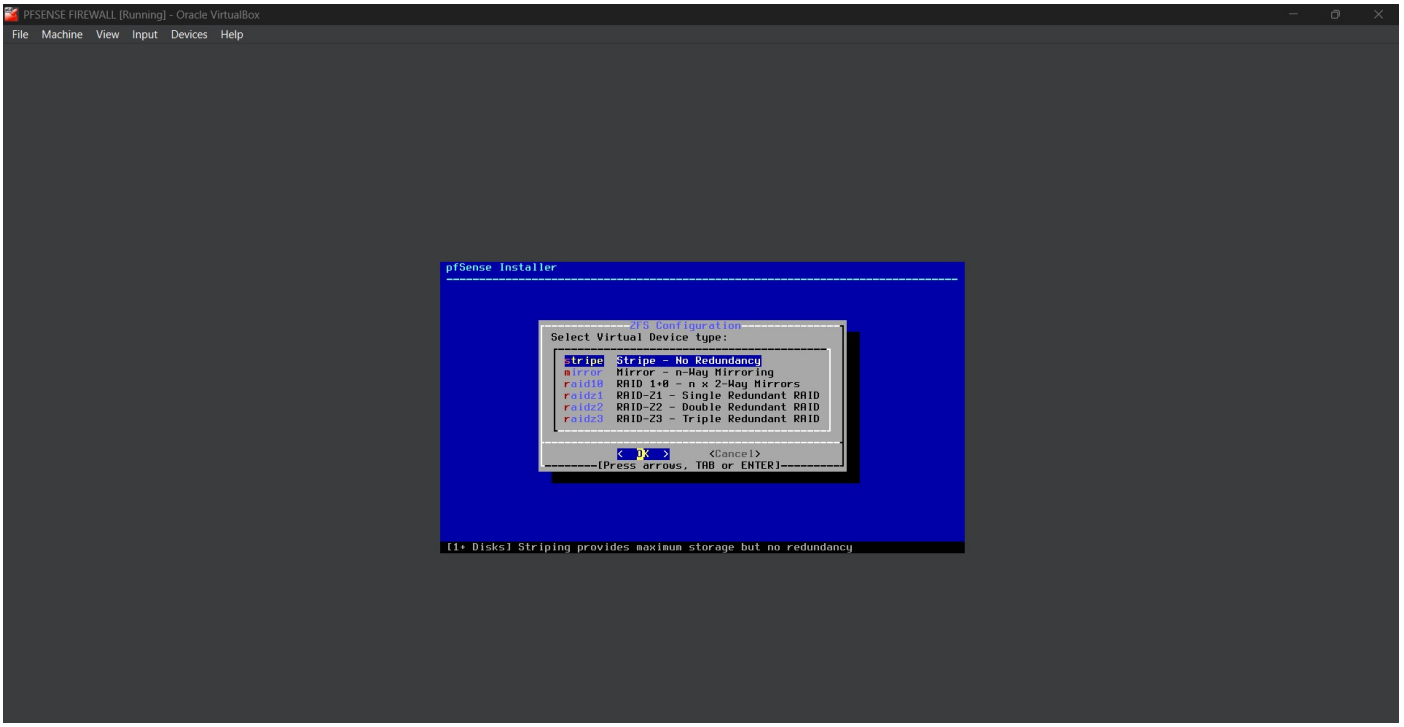


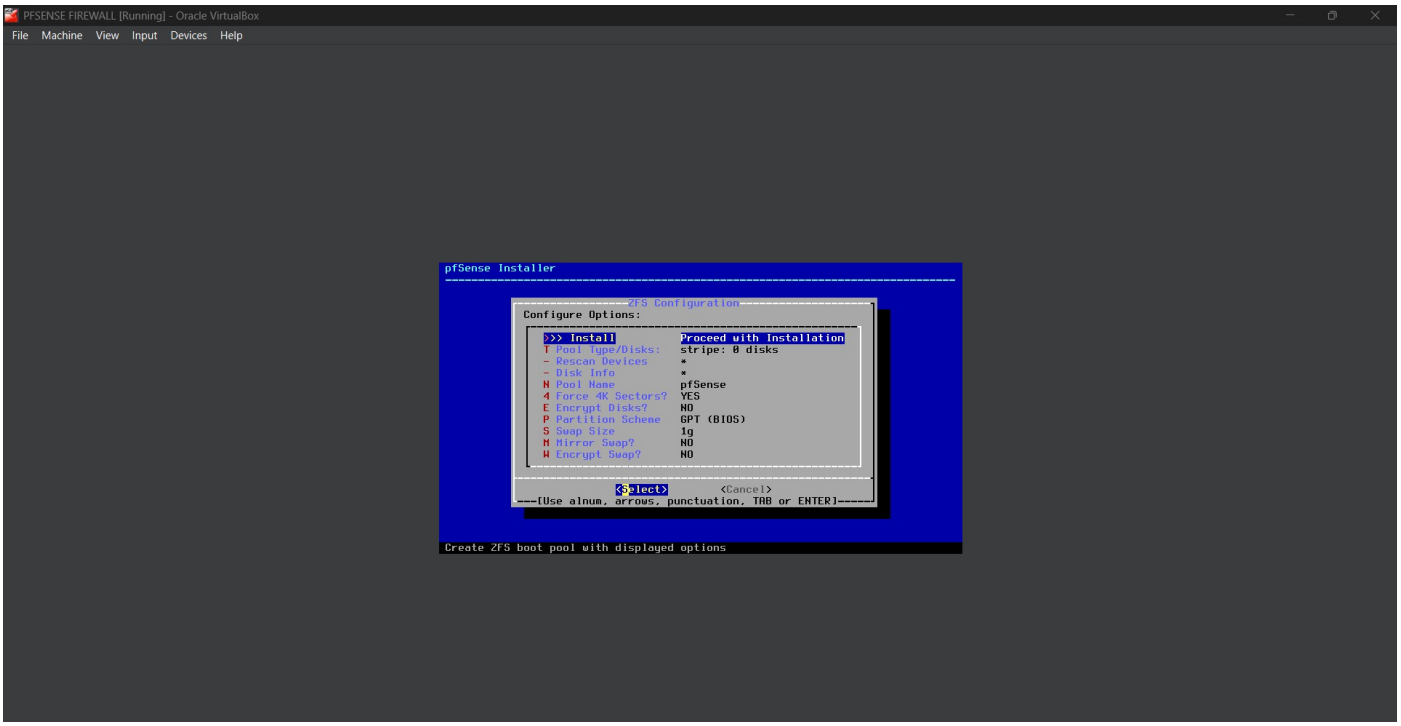


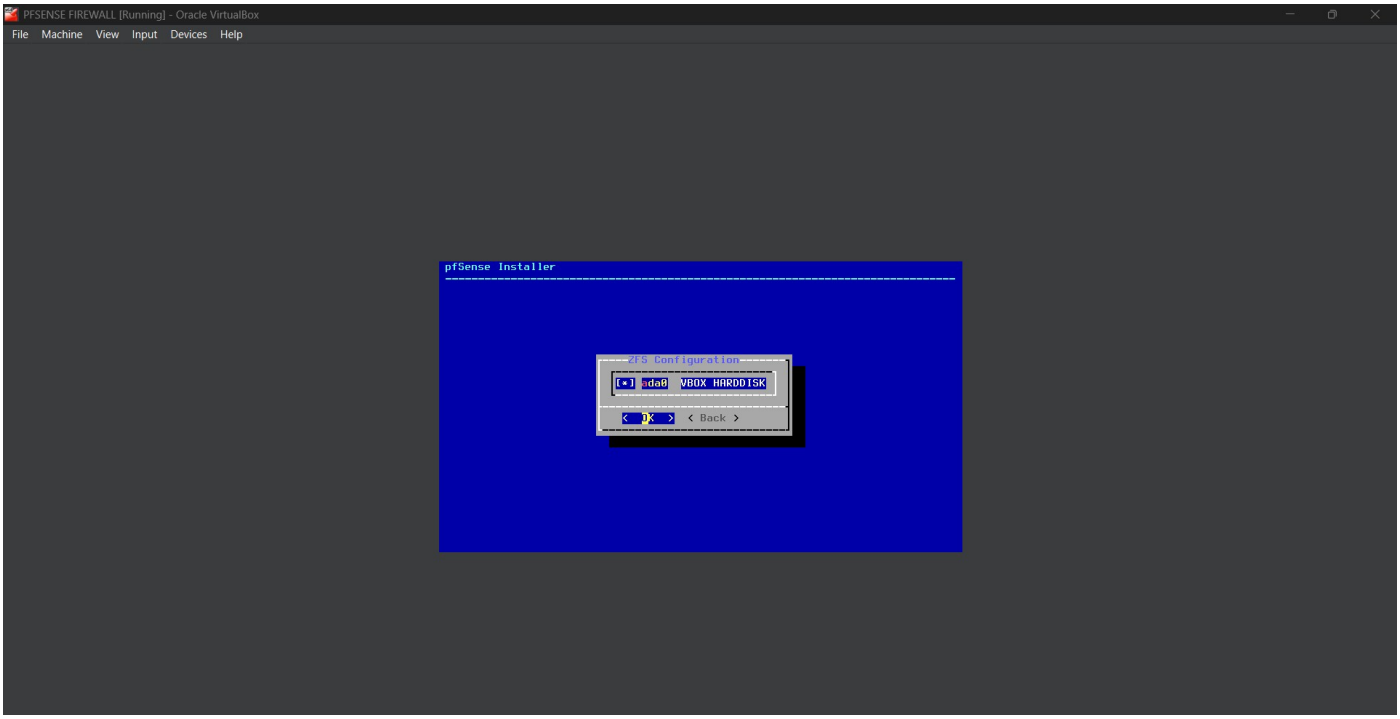


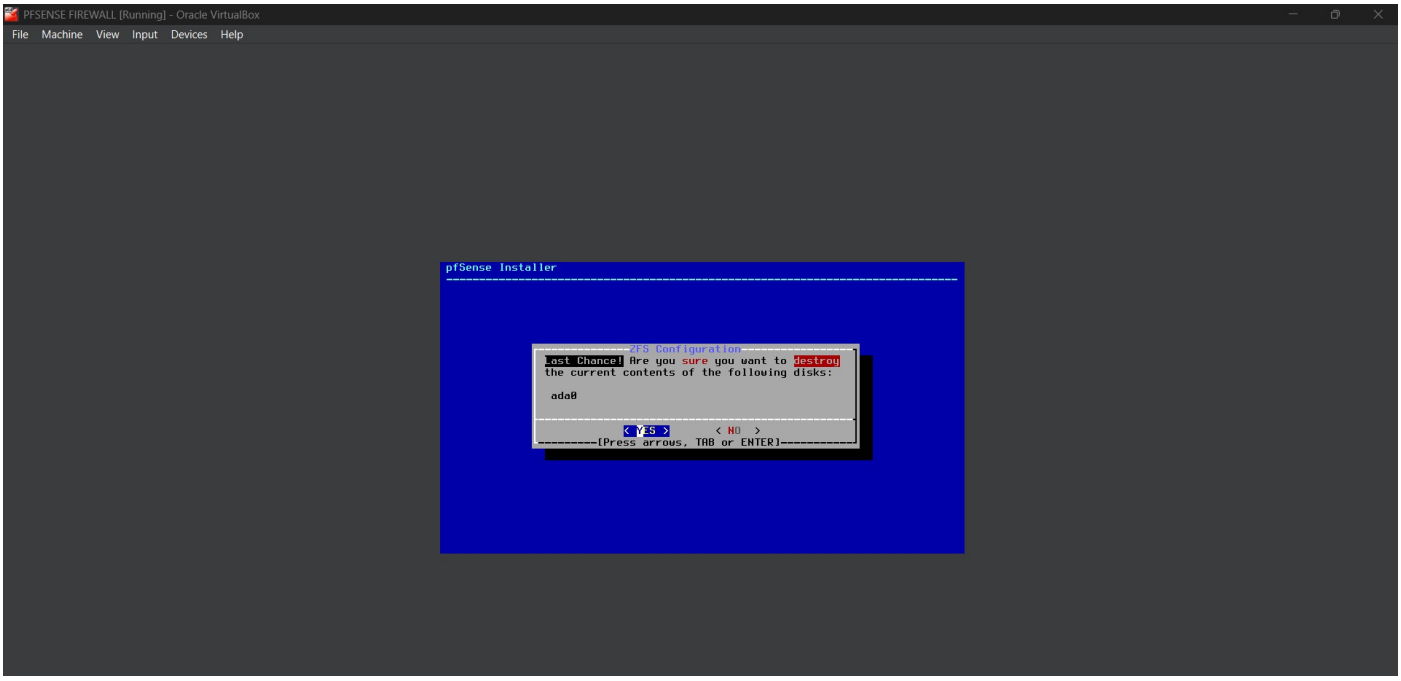
- Selected the Auto (ZFS) option for partitioning during installation. Selected Virtual device type as Stripe and proceeded with installation.



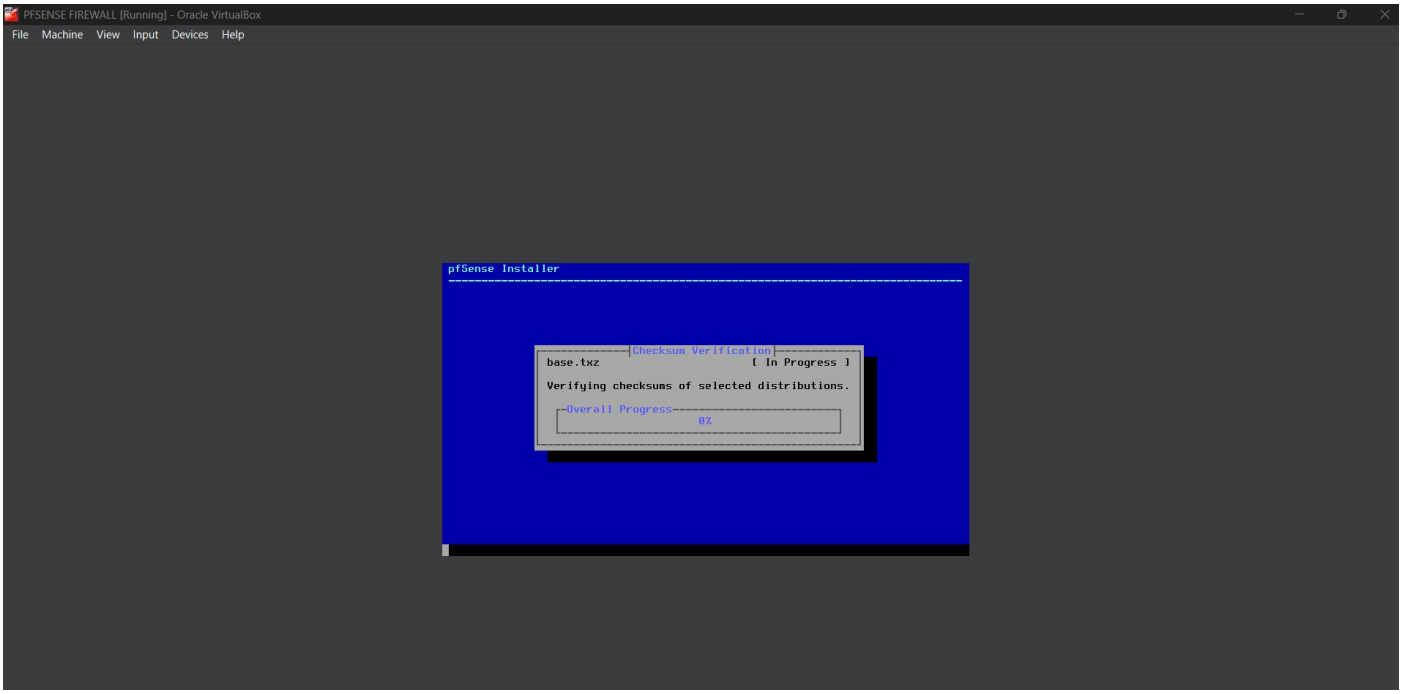

PFSENSE FIREWALL [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK >
<Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy

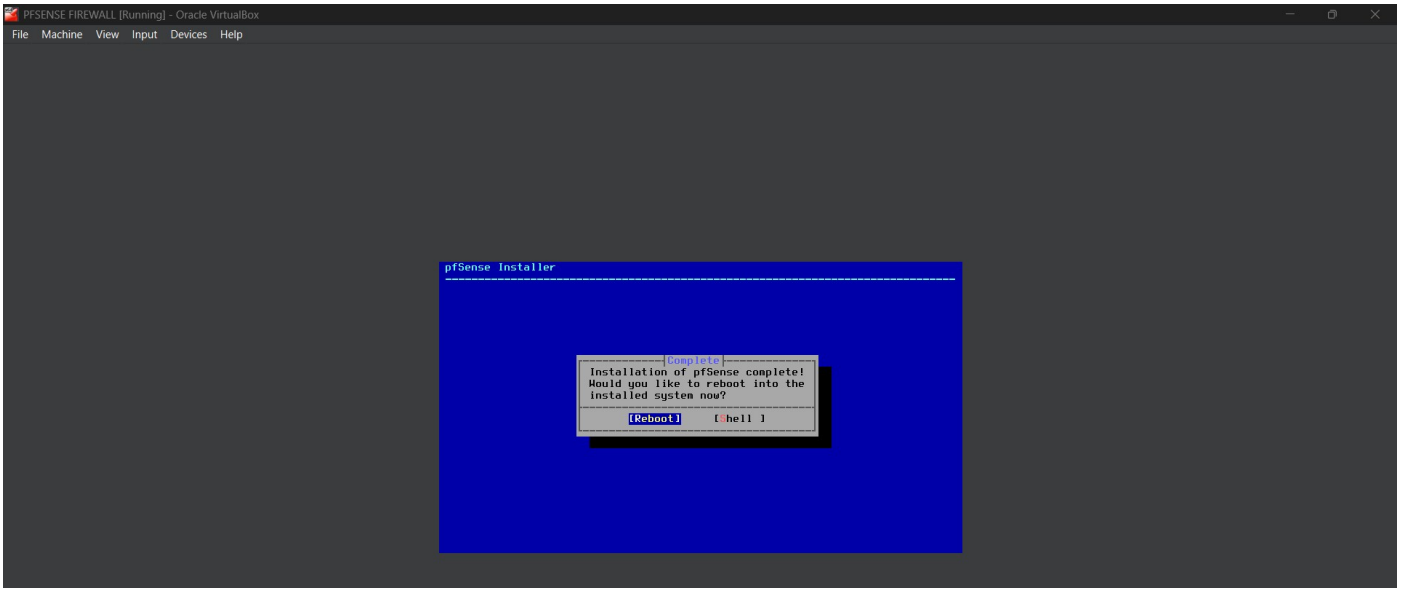

PFSENSE FIREWALL [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
~ Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select>
<Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options

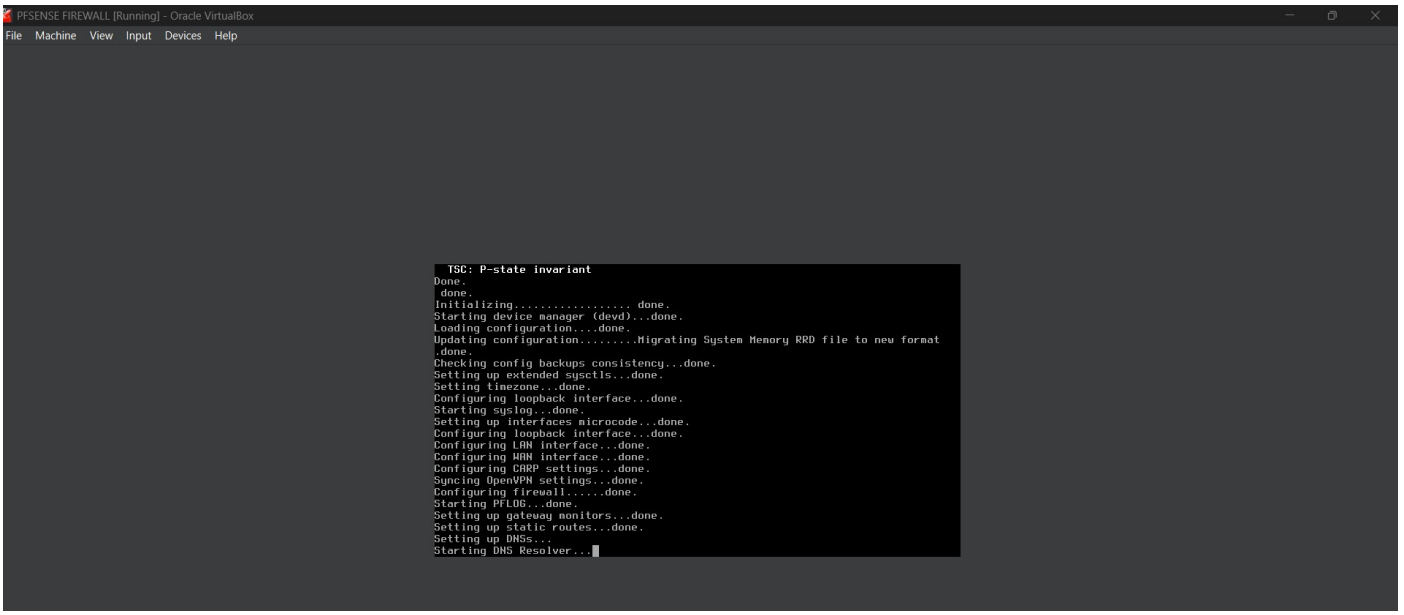




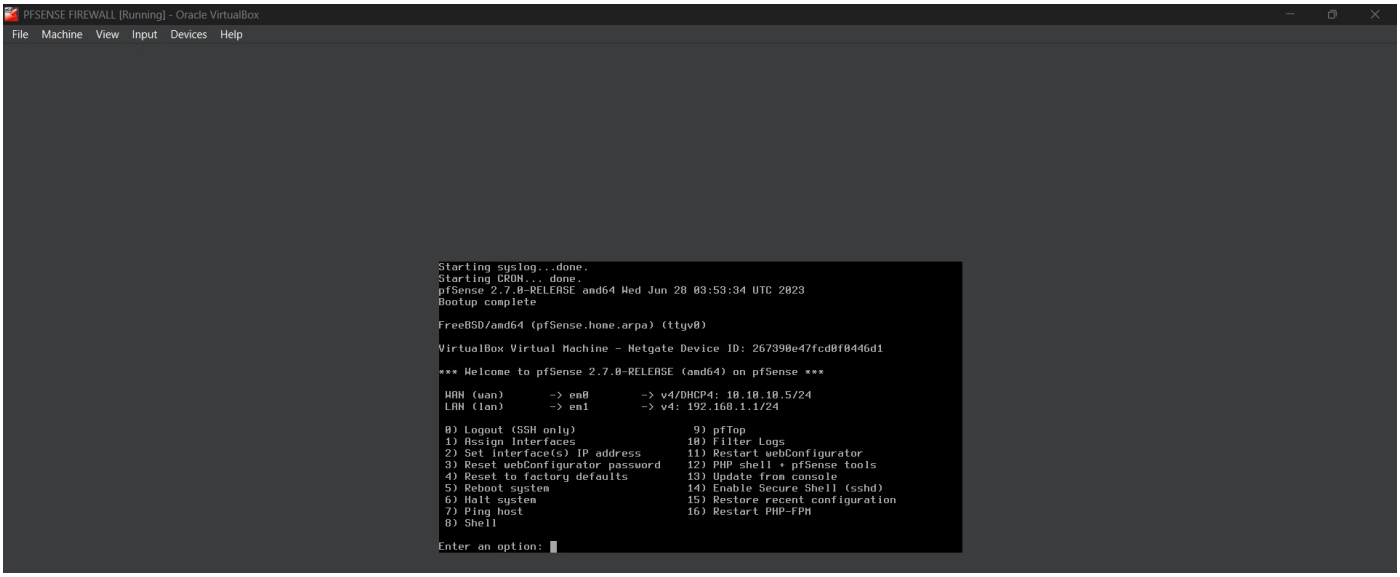
- Once installation was completed then, removed the Pfsense file and rebooted the system.

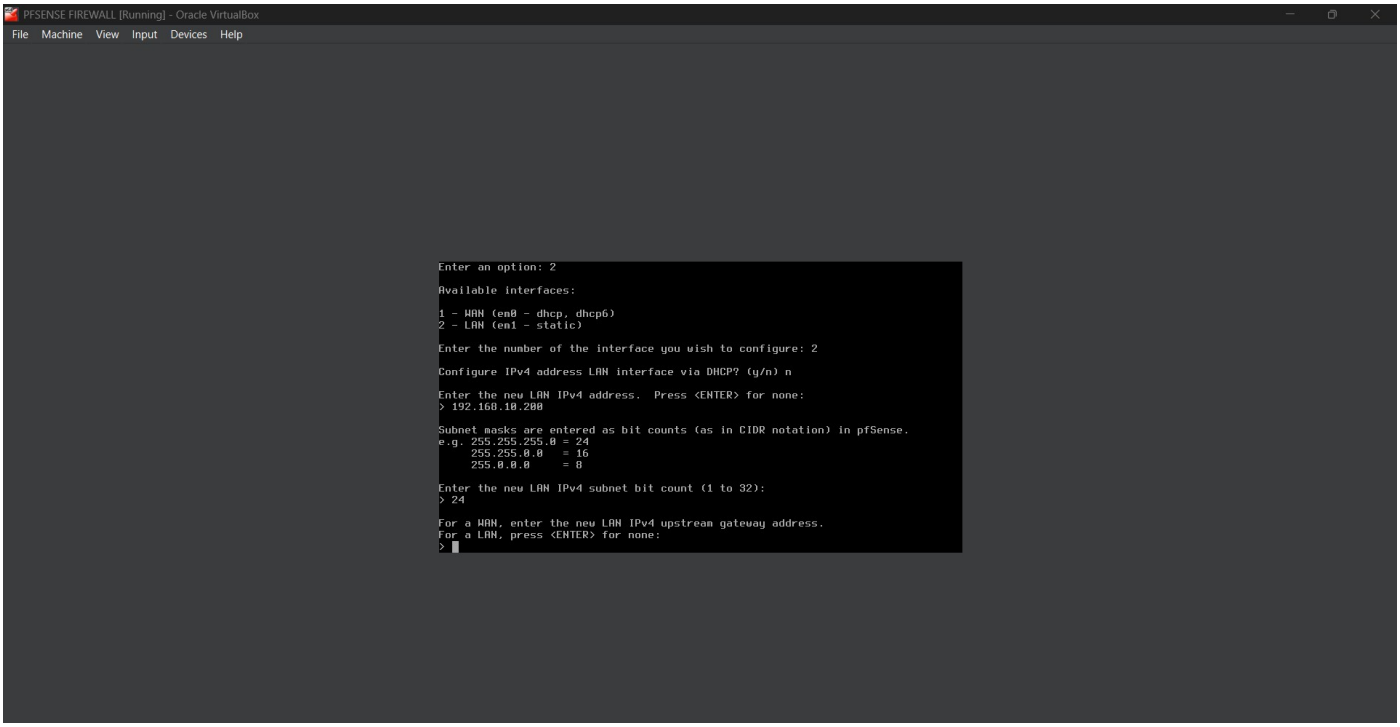

PFSENSE FIREWALL [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense Installer
Checksum Verification
base.txz [In Progress]
Verifying checksums of selected distributions.
Overall Progress
0%

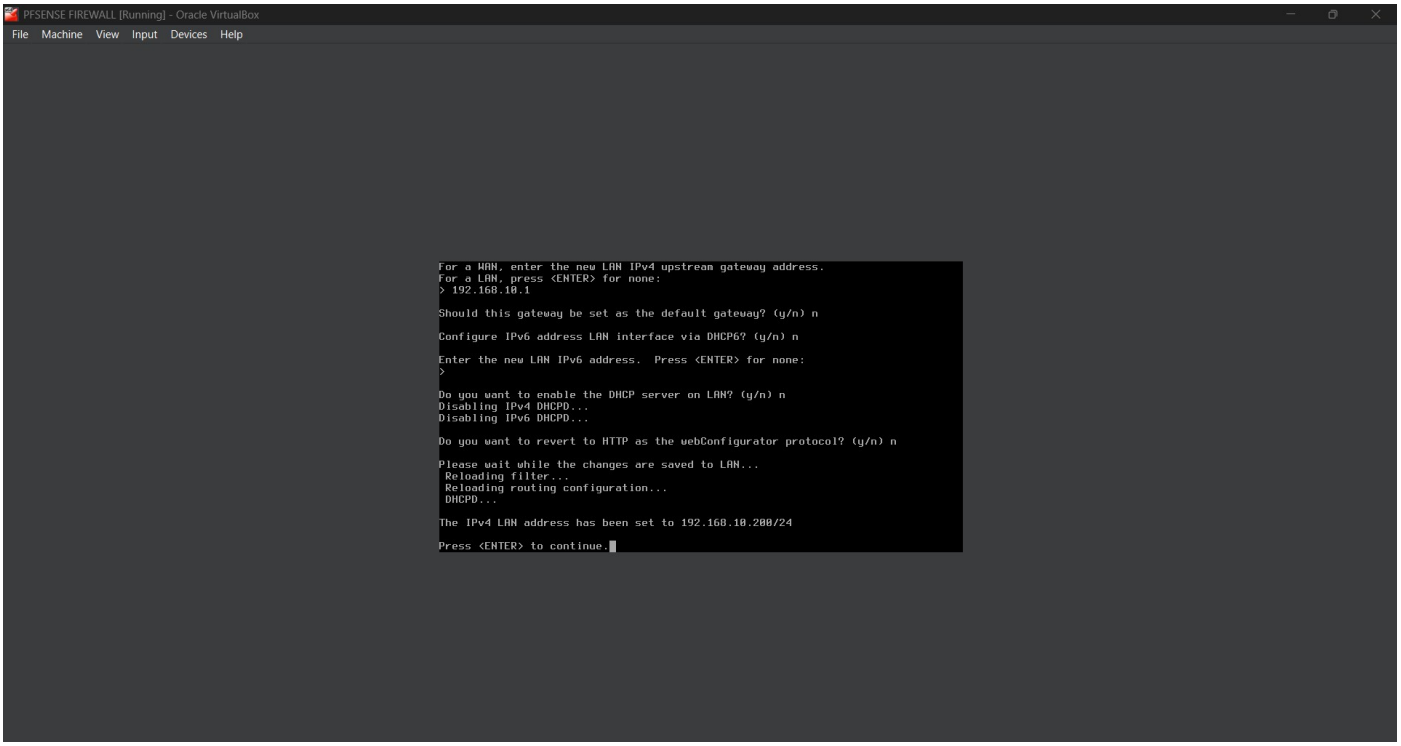

PFSENSE FIREWALL [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense Installer
Complete
Installation of pfSense complete!
Would you like to reboot into the
installed system now?
[Reboot] [Shell]


PFSENSE FIREWALL [Running] - Oracle VirtualBox
File Machine View Input Devices Help
TSC: P-state invariant
Done.
done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration....done.
Updating configuration.....Migrating System Memory RRD file to new format
.done.
Checking config backups consistency...done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting syslog...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Configuring LAN interface...done.
Configuring WAN interface...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...

- After reboot, set the LAN interface's IP address to 192.168.10.200 with a subnet mask of 24. Skipped specifying a gateway and chose whether to enable the DHCP server on the LAN interface as per lab requirements.

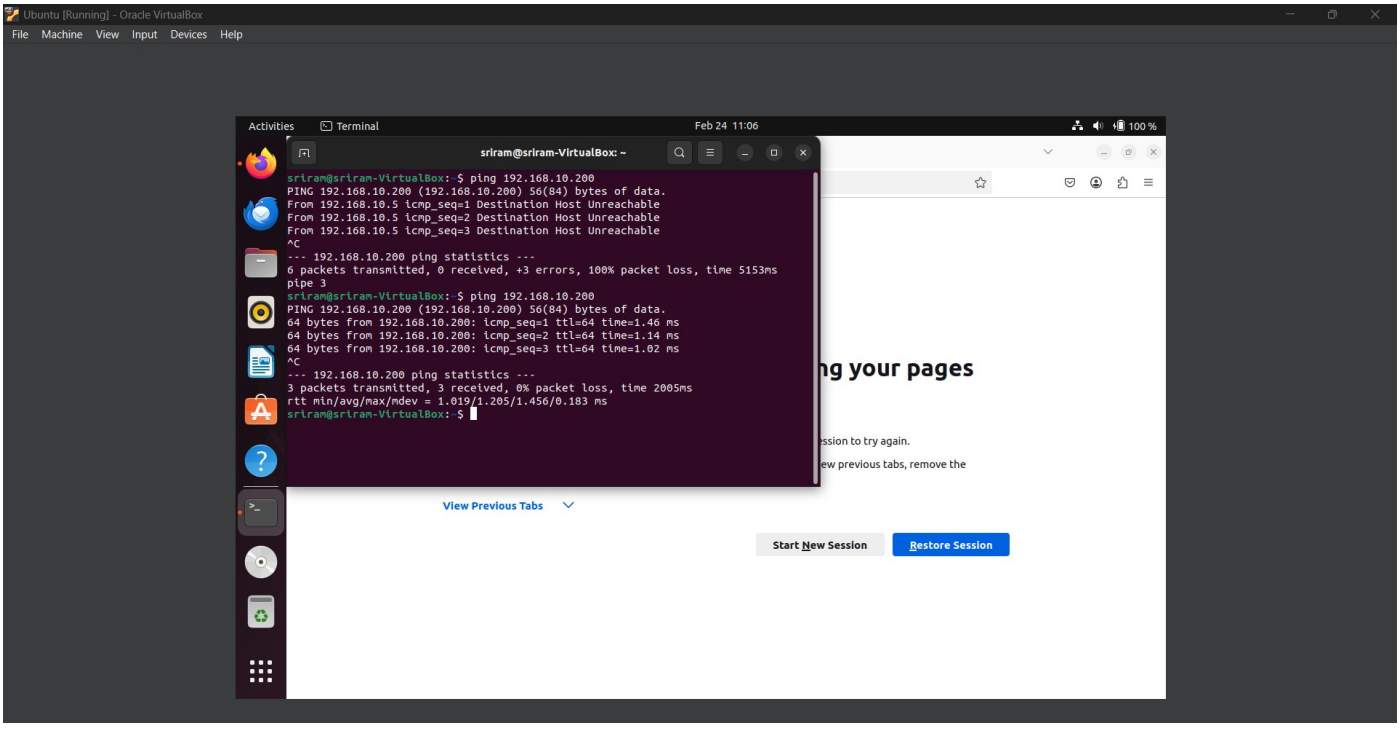


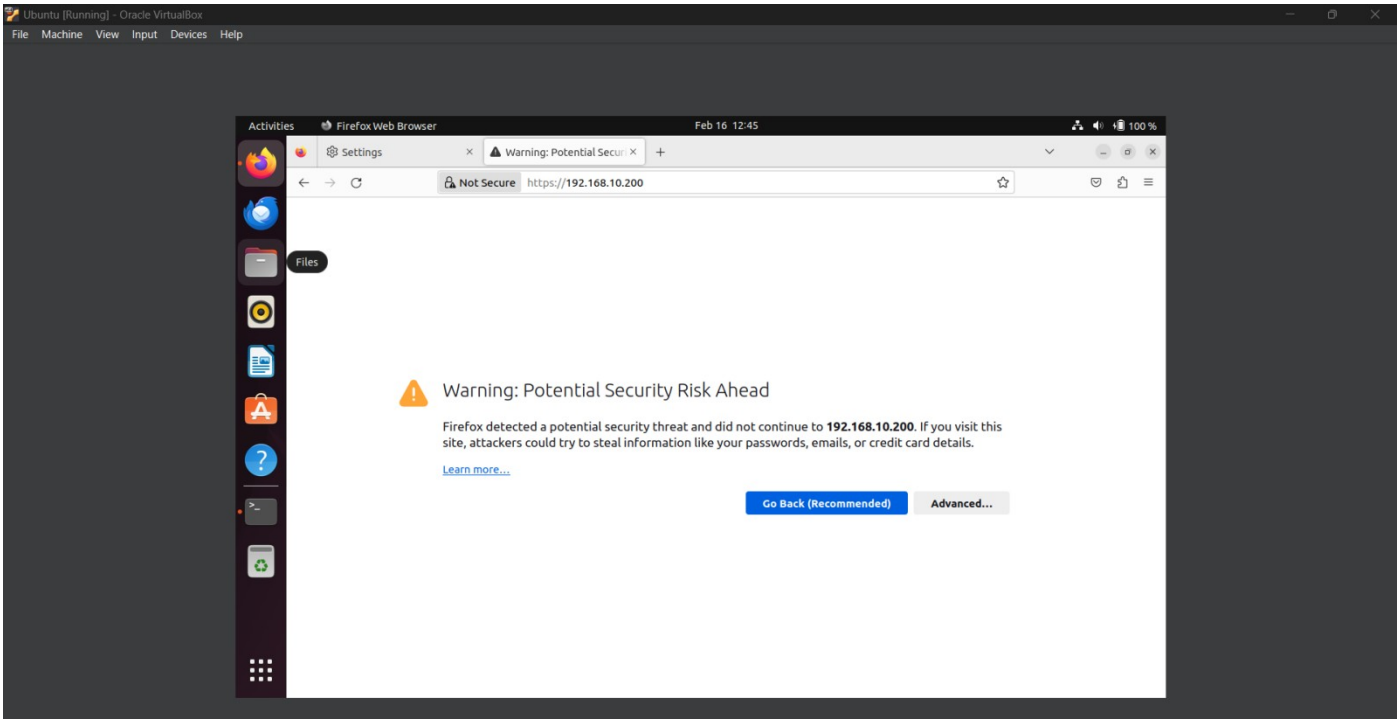


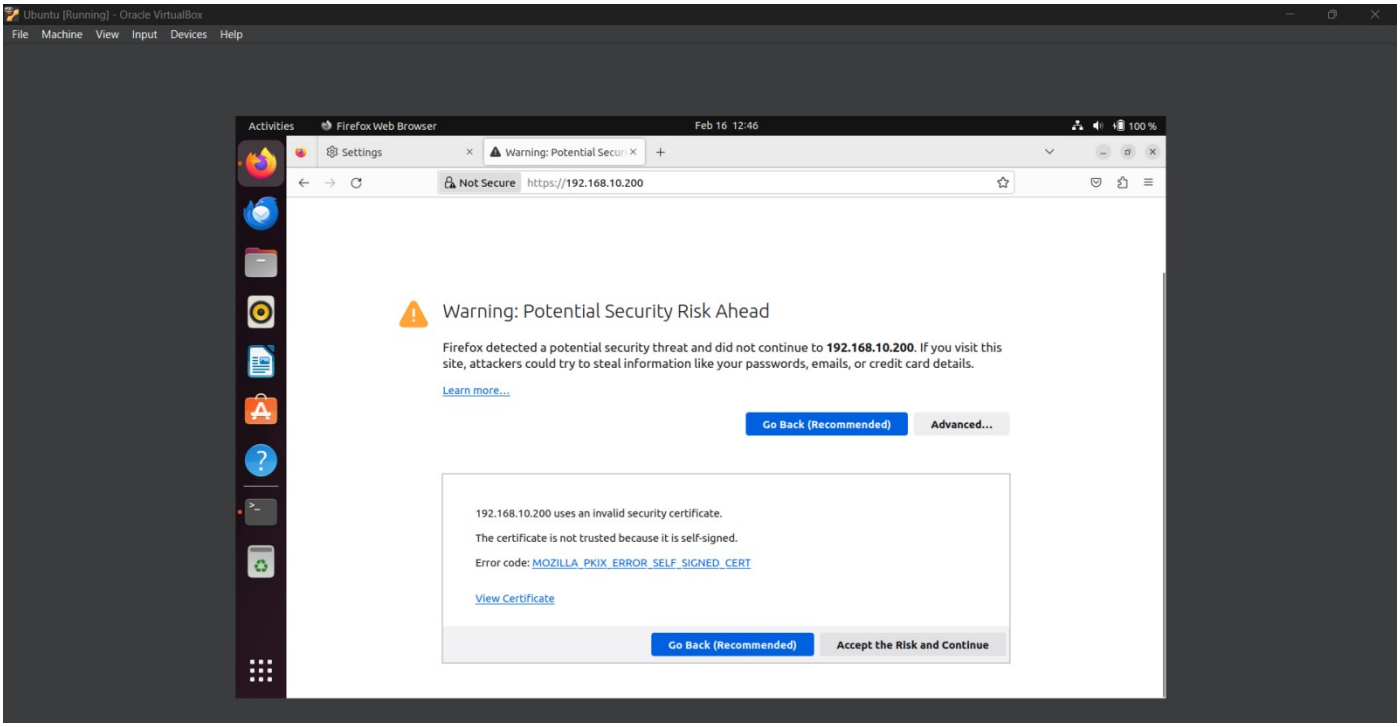


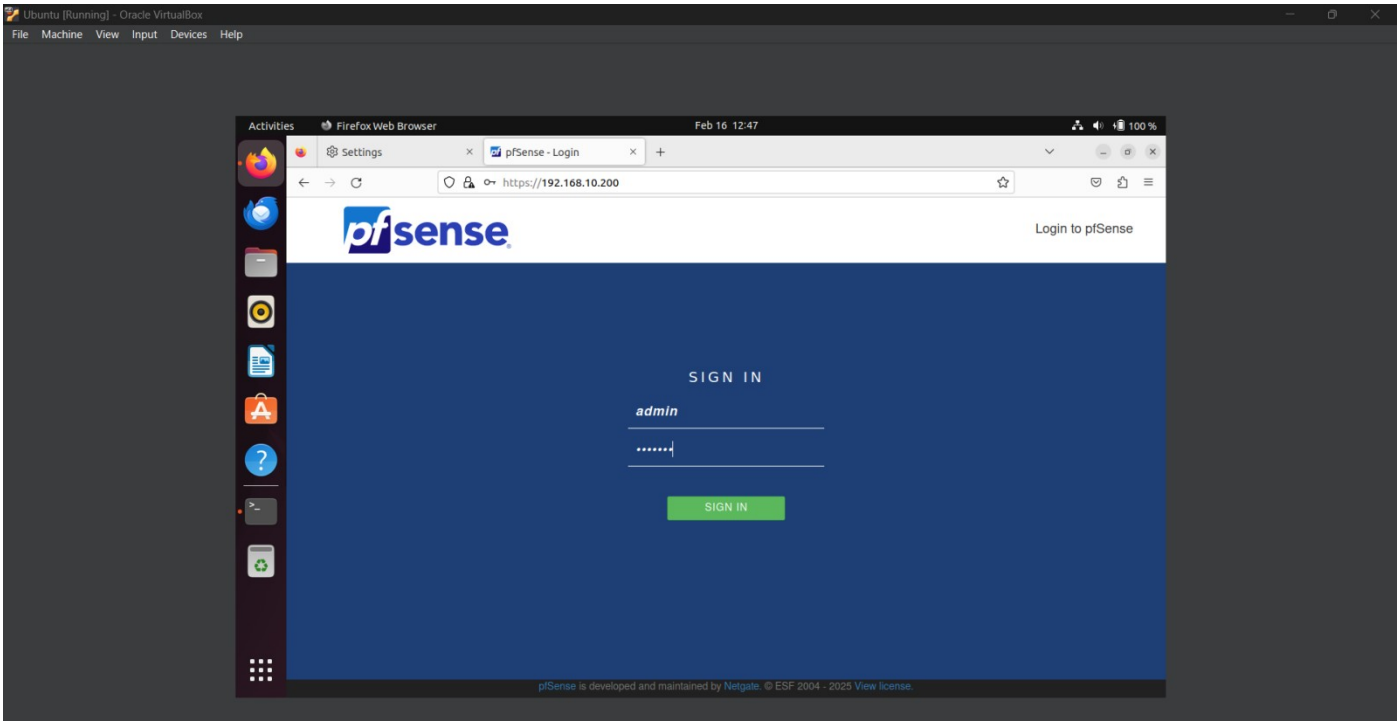
Objective 2: Configuring pfSense

- Accessed the pfSense WebConfigurator portal at https://192.168.10.200 in my Ubuntu Machine and logged in with default credentials (admin/pfsense).

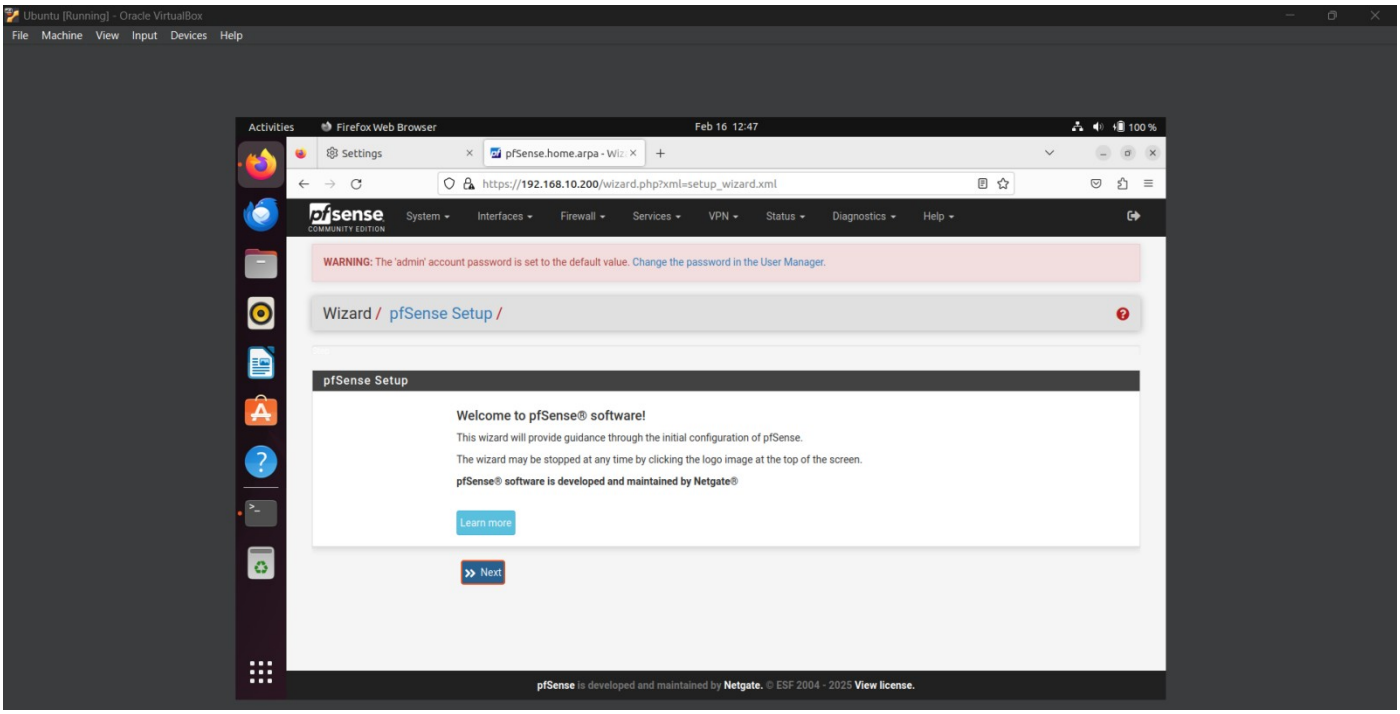


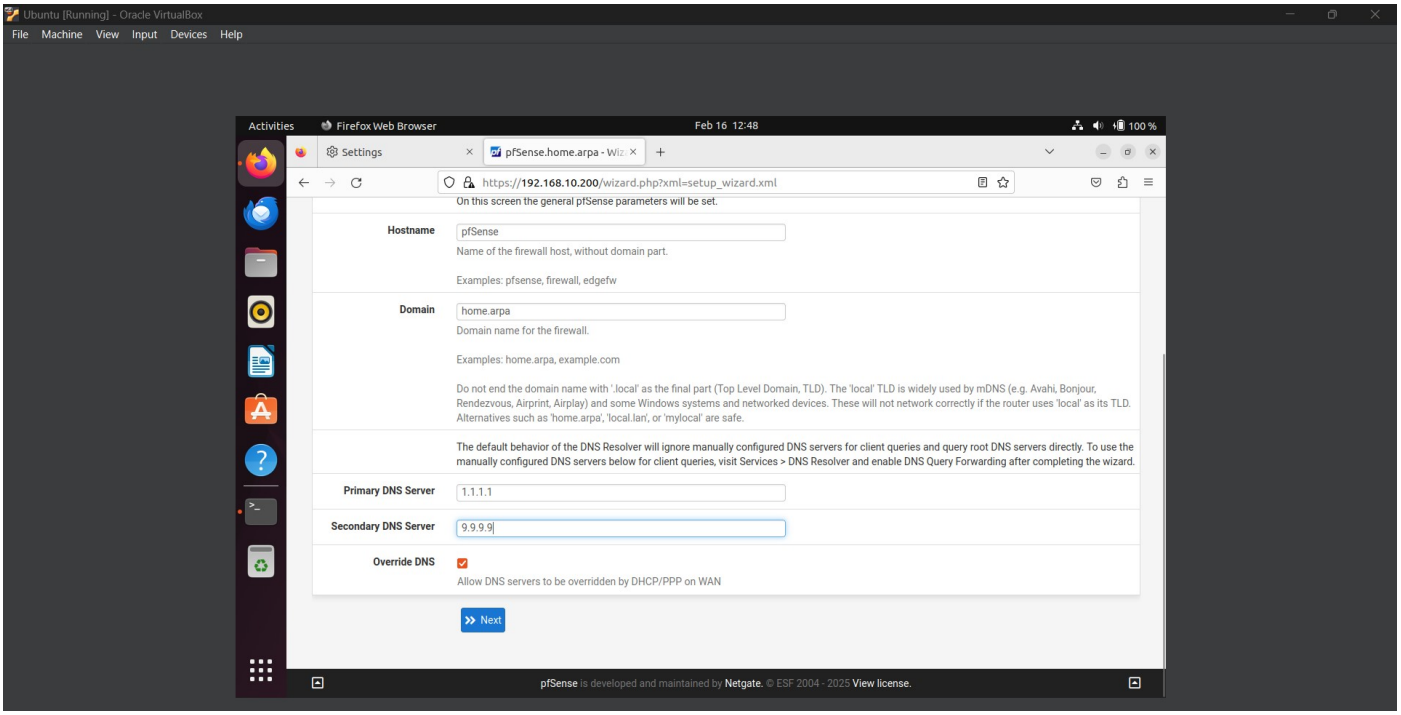

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:45
100 %
Settings
Warning: Potential Secur
Not Secure
https://192.168.10.200
Files
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 192.168.10.200. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...

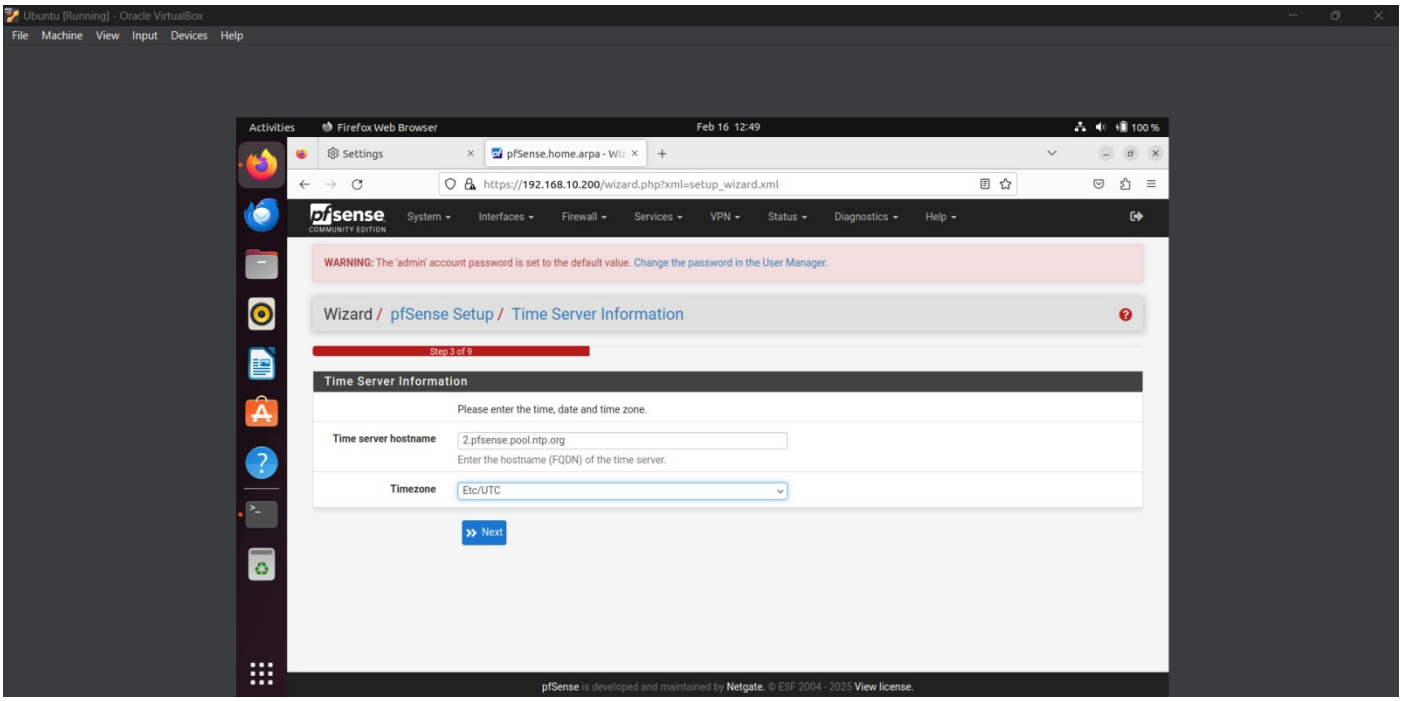

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:46
100 %
Settings
Warning: Potential Secur
Not Secure
https://192.168.10.200
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to 192.168.10.200. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
192.168.10.200 uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue

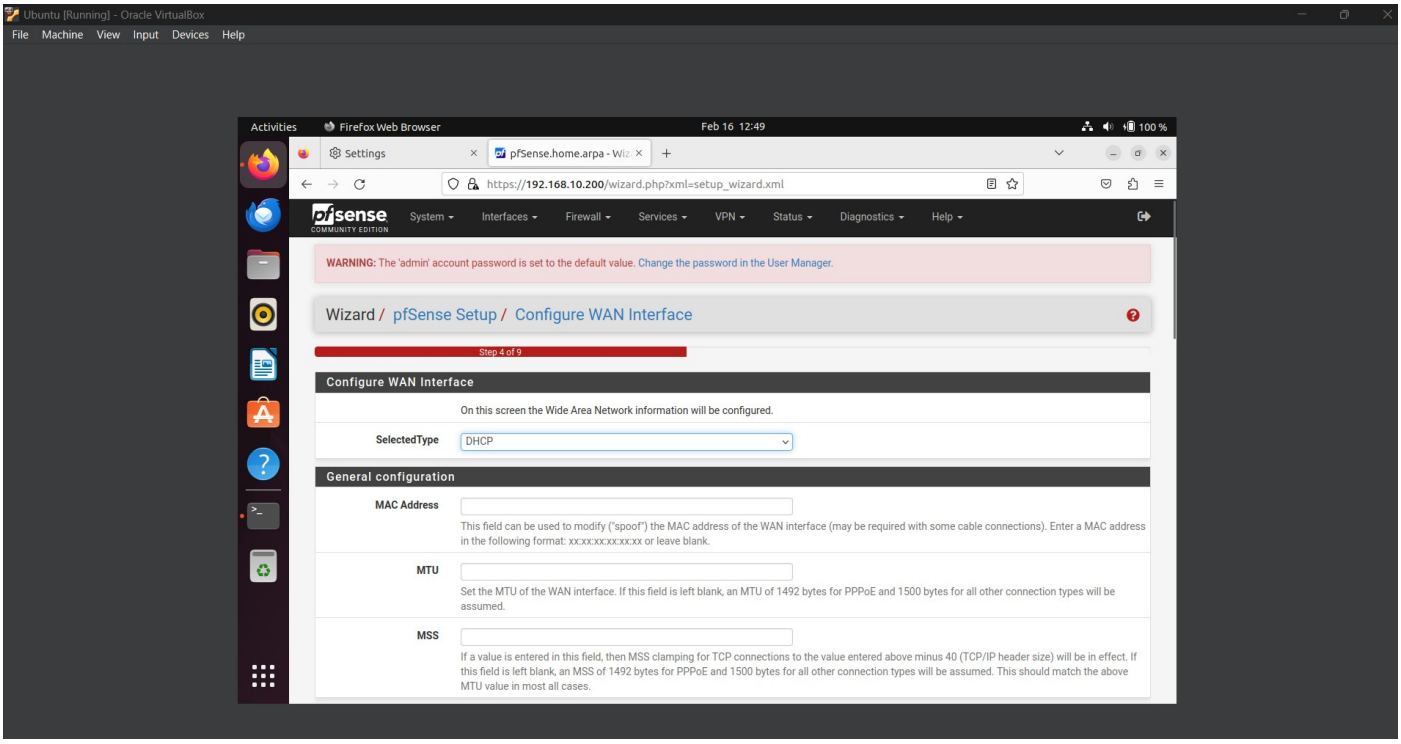


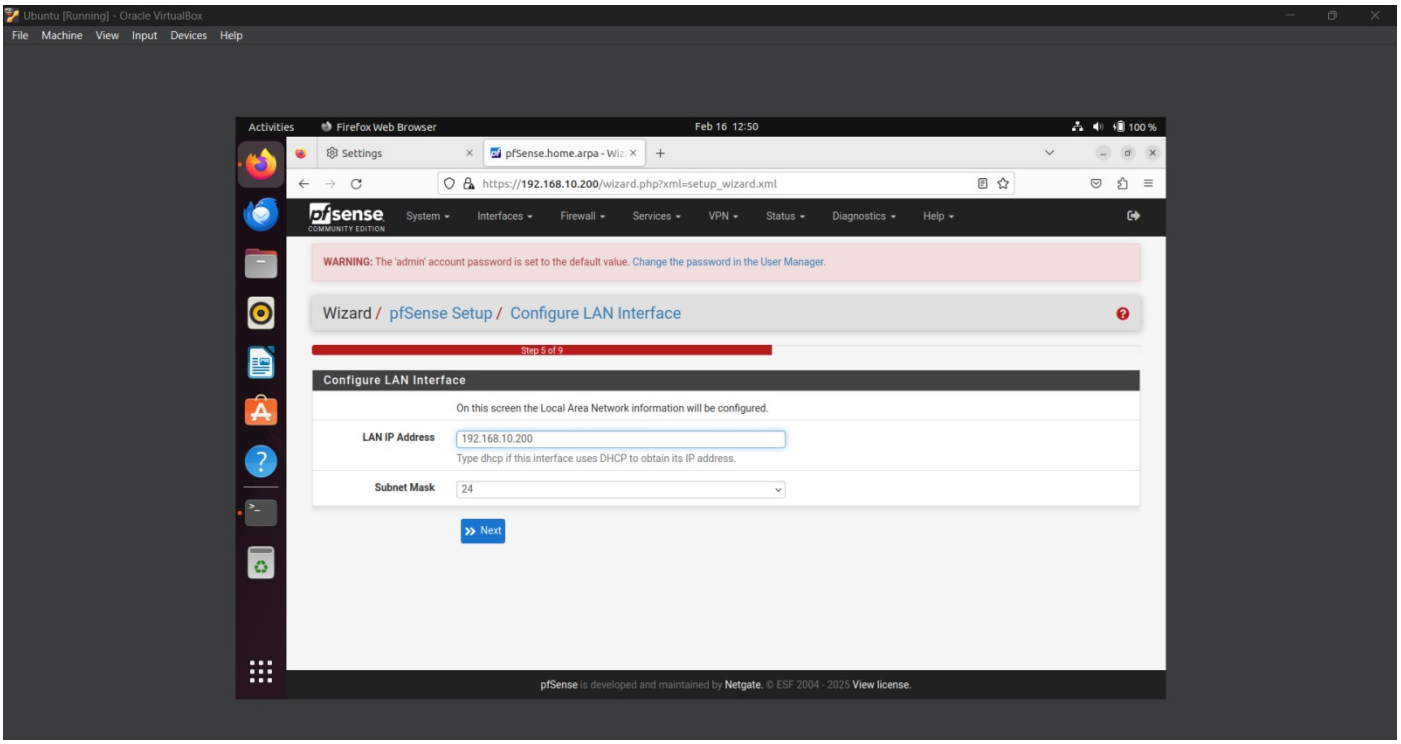
- Followed the setup wizard to specify DNS servers, set the time zone to UTC, configure WAN and LAN interfaces. Reloaded the configuration to apply changes after completing the initial setup.

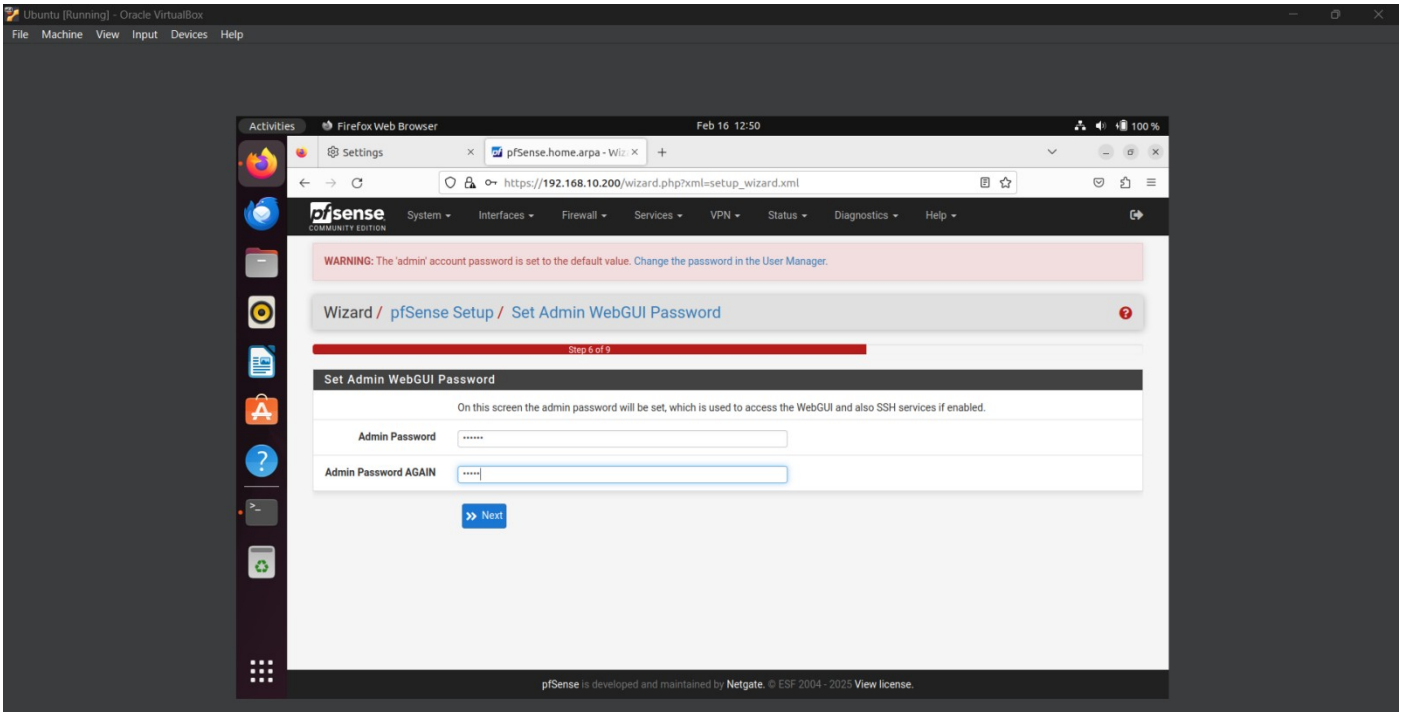


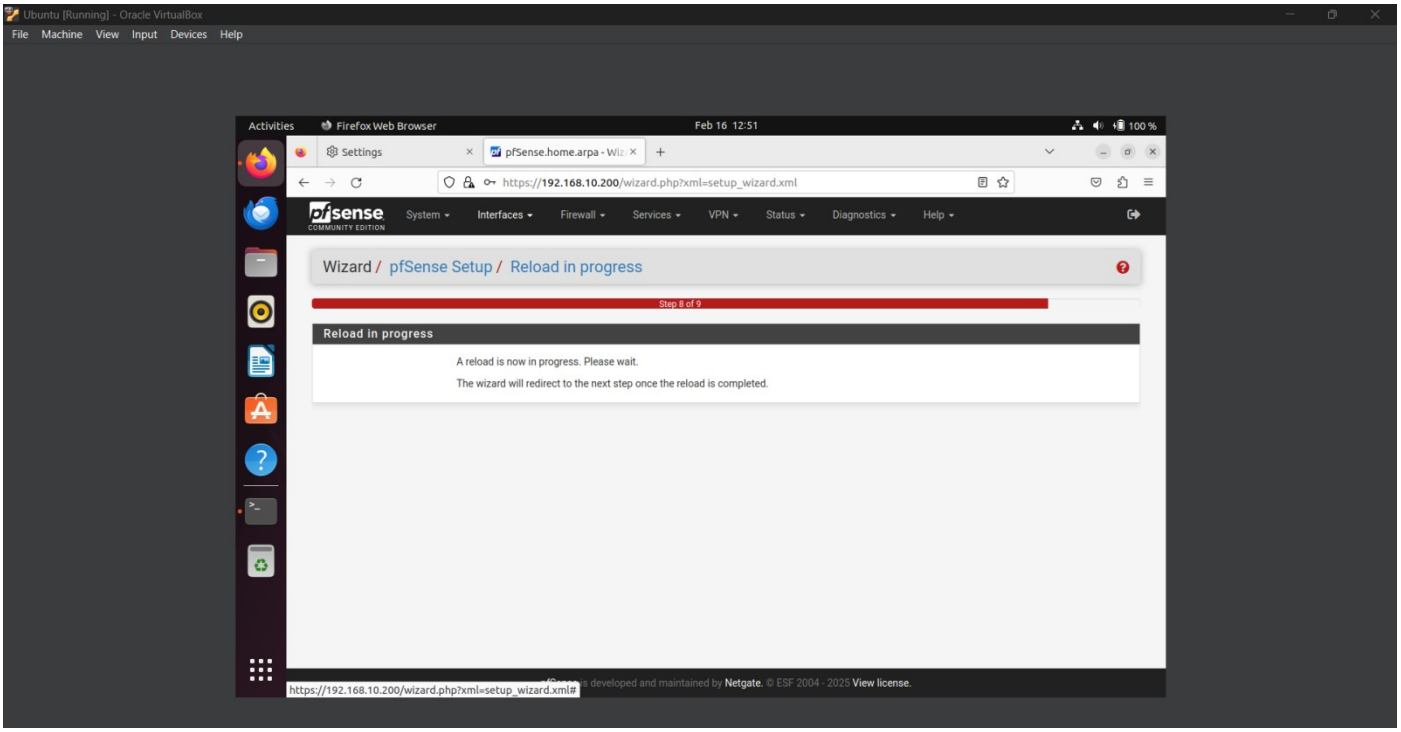

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:48
100 %
Settings
pfSense.home.arpa - Wiz
https://192.168.10.200/wizard.php?xml=setup_wizard.xml
On this screen the general pfSense parameters will be set.
Hostname
pfSense
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw
Domain
home.arpa
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
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
1.1.1.1
Secondary DNS Server
9.9.9.9
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

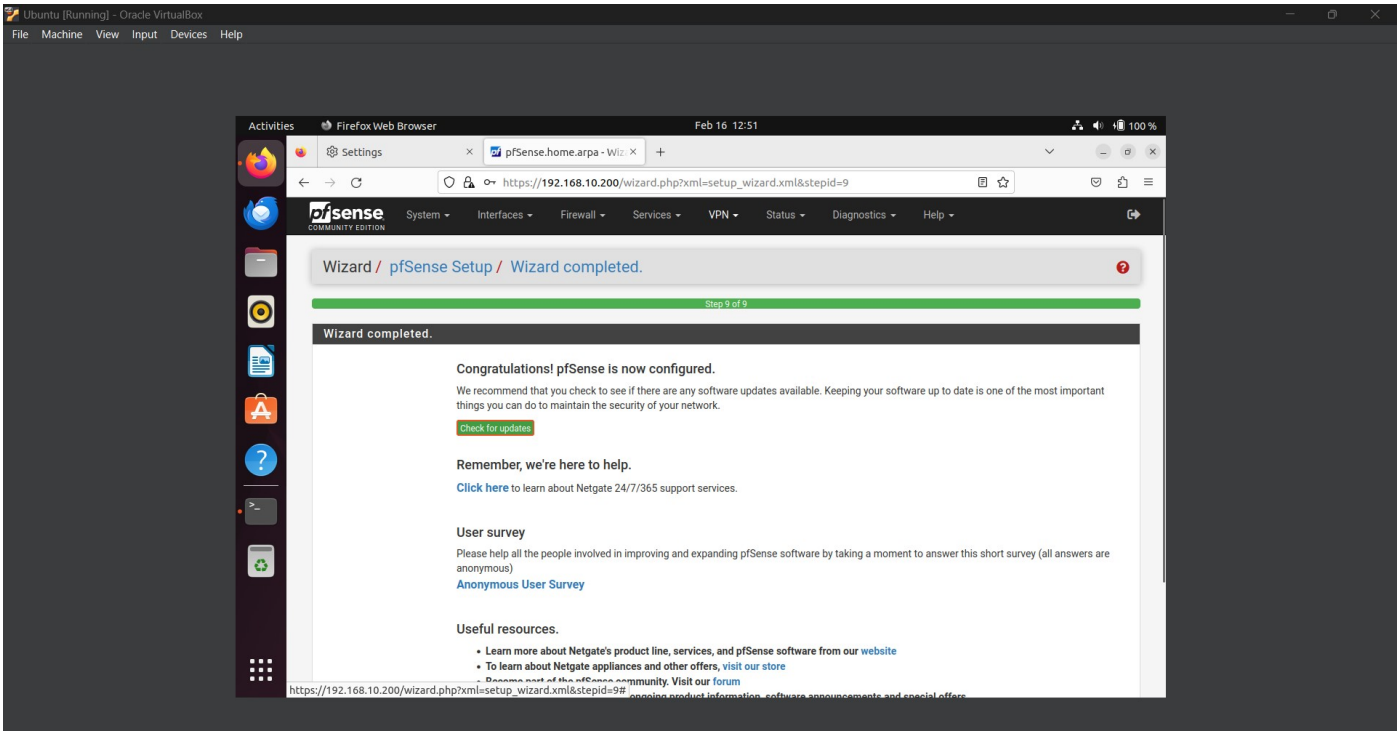

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:49
100 %
Settings
pfSense.home.arpa - Wiz
https://192.168.10.200/wizard.php?xml=setup_wizard.xml
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / Time Server Information
Step 3 of 9
Time Server Information
Please enter the time, date and time zone.
Time server hostname
2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.
Timezone
Etc/UTC
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.


Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:49
100 %
Settings
pfSense.home.arpa - Wiz
https://192.168.10.200/wizard.php?xml=setup_wizard.xml
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 / Configure WAN Interface
Step 4 of 9
Configure WAN Interface
On this screen the Wide Area Network information will be configured.
SelectedType
DHCP
General configuration
MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.


Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:50
100 %
Settings
pfSense.home.arpa - Wiz
https://192.168.10.200/wizard.php?xml=setup_wizard.xml
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 / Configure LAN Interface
Step 5 of 9
Configure LAN Interface
On this screen the Local Area Network information will be configured.
LAN IP Address
192.168.10.200
Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask
24
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

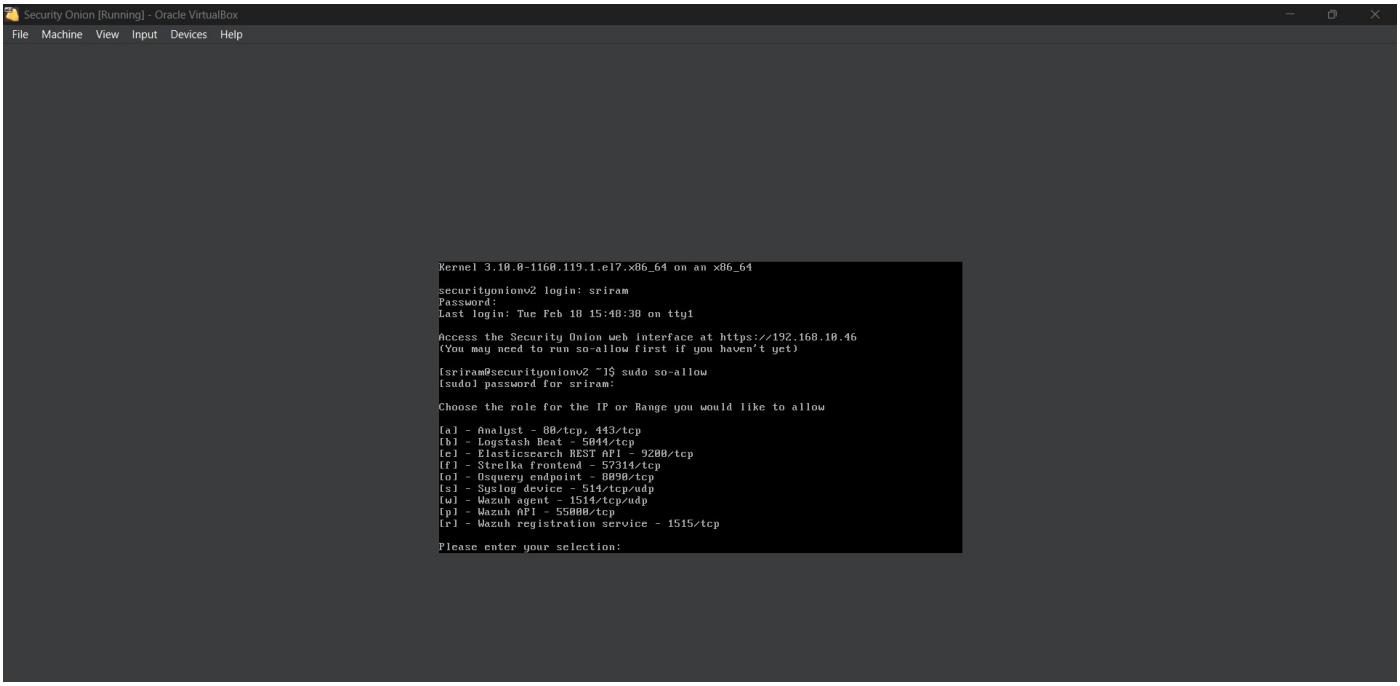

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:50
100 %
Settings
pfSense.home.arpa - Wiz
https://192.168.10.200/wizard.php?xml=setup_wizard.xml
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
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 - 2025 View license.

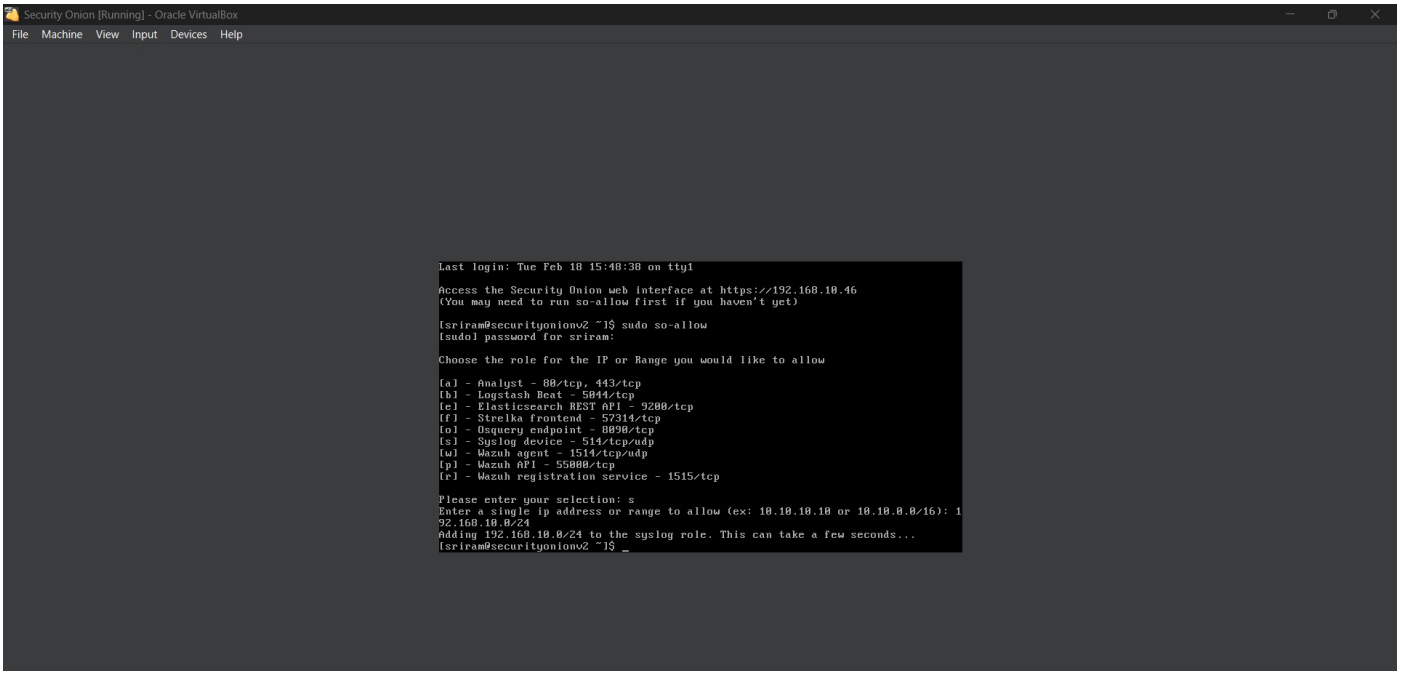

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Feb 16 12:51
100 %
Settings
pfSense.home.arpa - Wiz
https://192.168.10.200/wizard.php?xml=setup_wizard.xml
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Reload in progress
Step 8 of 9
Reload in progress
A reload is now in progress. Please wait.
The wizard will redirect to the next step once the reload is completed.
Netgate. © ESF 2004 - 2025 View license.
https://192.168.10.200/wizard.php?xml=setup_wizard.xml#



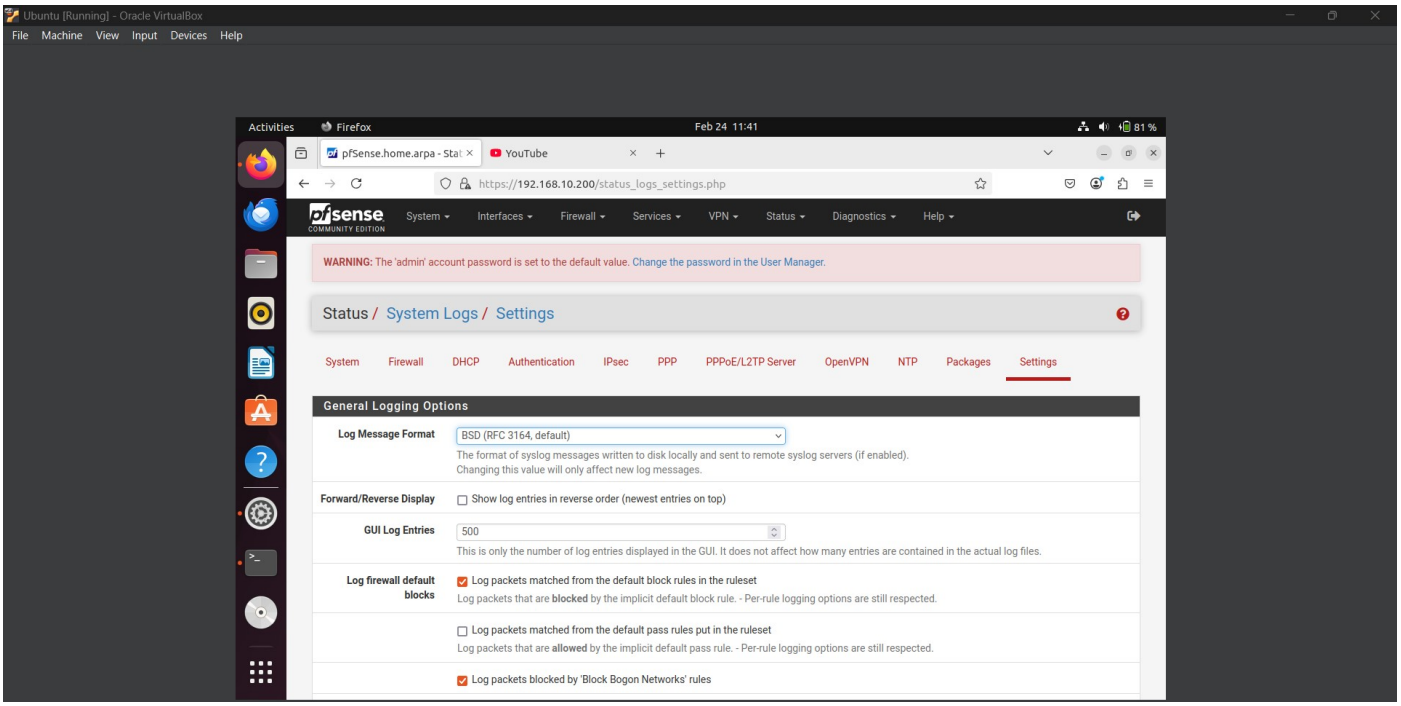
Objective 3: Configuring Log Forwarding to Syslog (Security Onion)

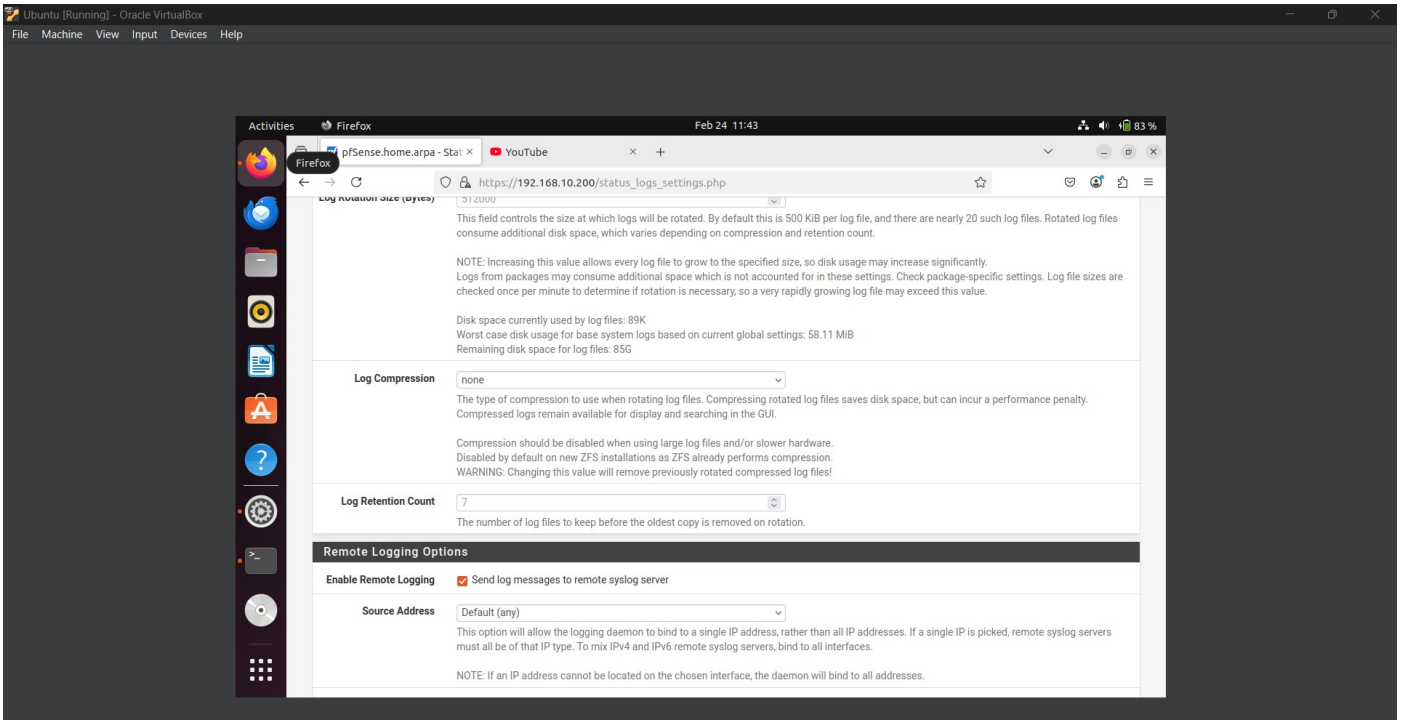
- Accessed the Security Onion VM via SSH and executed `sudo so-allow`, selecting the syslog service and specifying the pfSense LAN IP address (192.168.10.200) as an allowed source.



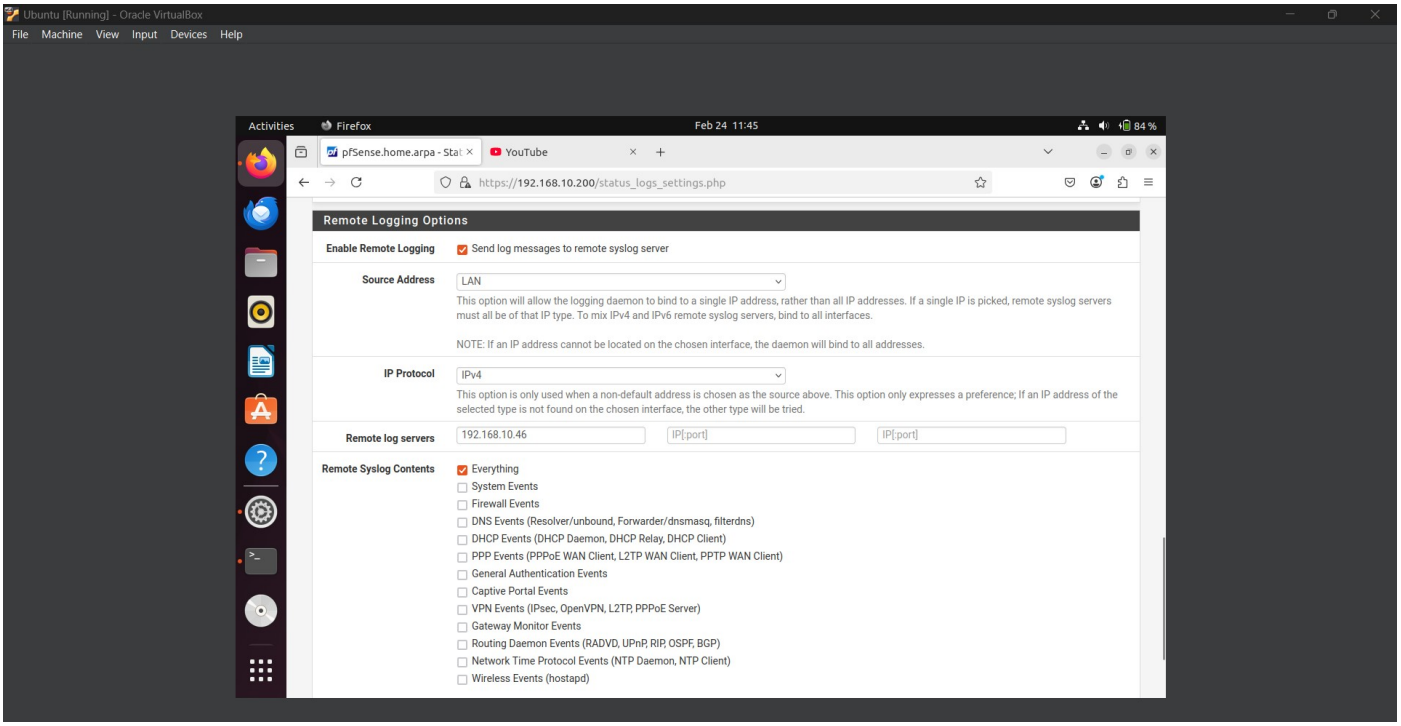


- In the pfSense WebConfigurator, navigated to Status > System Logs > Settings.

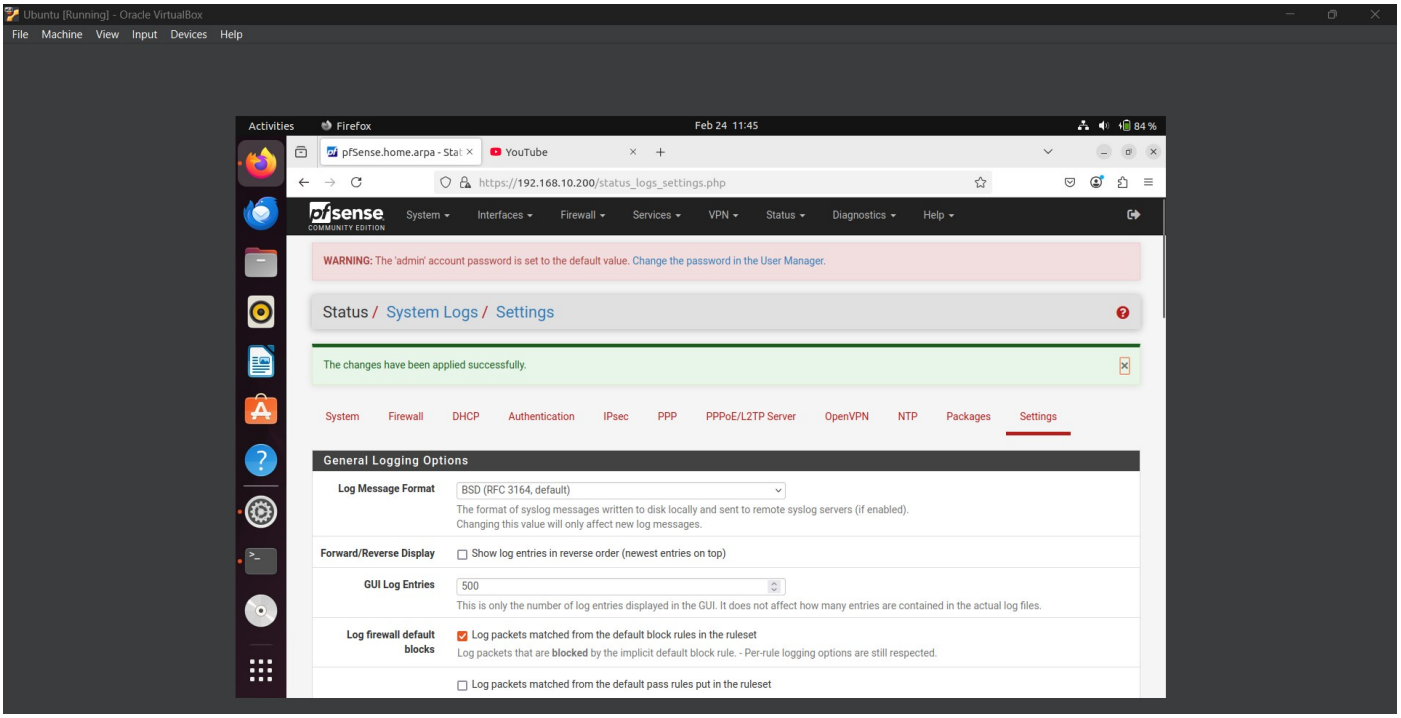




- Enabled the option to send log messages to a remote syslog server and entered the Security Onion syslog server's IP address (192.168.10.46).



- Saved the configuration to start forwarding logs to the Security Onion system.


Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox
Feb 24 11:45
84 %
pfSense.home.arpa - Stat
YouTube
https://192.168.10.200/status_logs_settings.php
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.
Status / System Logs / Settings
The changes have been applied successfully.
System
Firewall
DHCP
Authentication
IPsec
PPP
PPPoE/L2TP Server
OpenVPN
NTP
Packages
Settings
General Logging Options
Log Message Format
BSD (RFC 3164, default)
The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled).
Changing this value will only affect new log messages.
Forward/Reverse Display
Show log entries in reverse order (newest entries on top)
GUI Log Entries
500
This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.
Log firewall default blocks
Log packets matched from the default block rules in the ruleset
Log packets that are blocked by the implicit default block rule. - Per-rule logging options are still respected.
Log packets matched from the default pass rules put in the ruleset