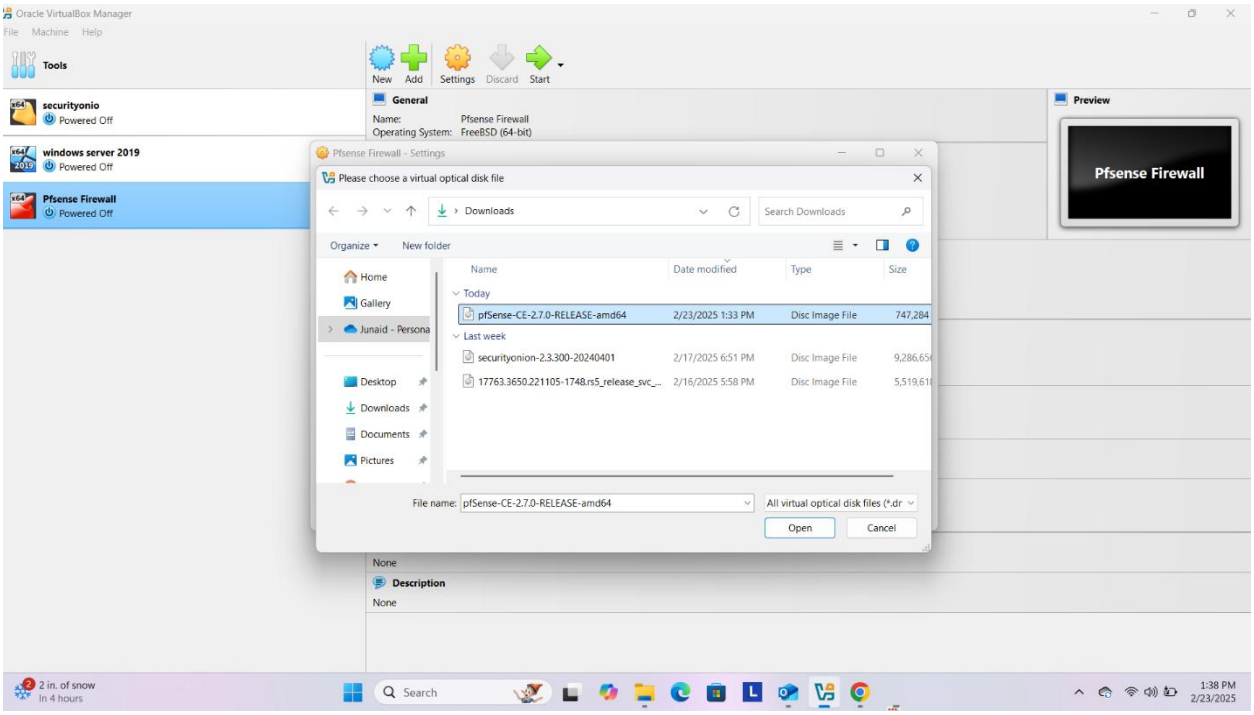
# Lab 2: Setting up and configuring a pfSense firewall

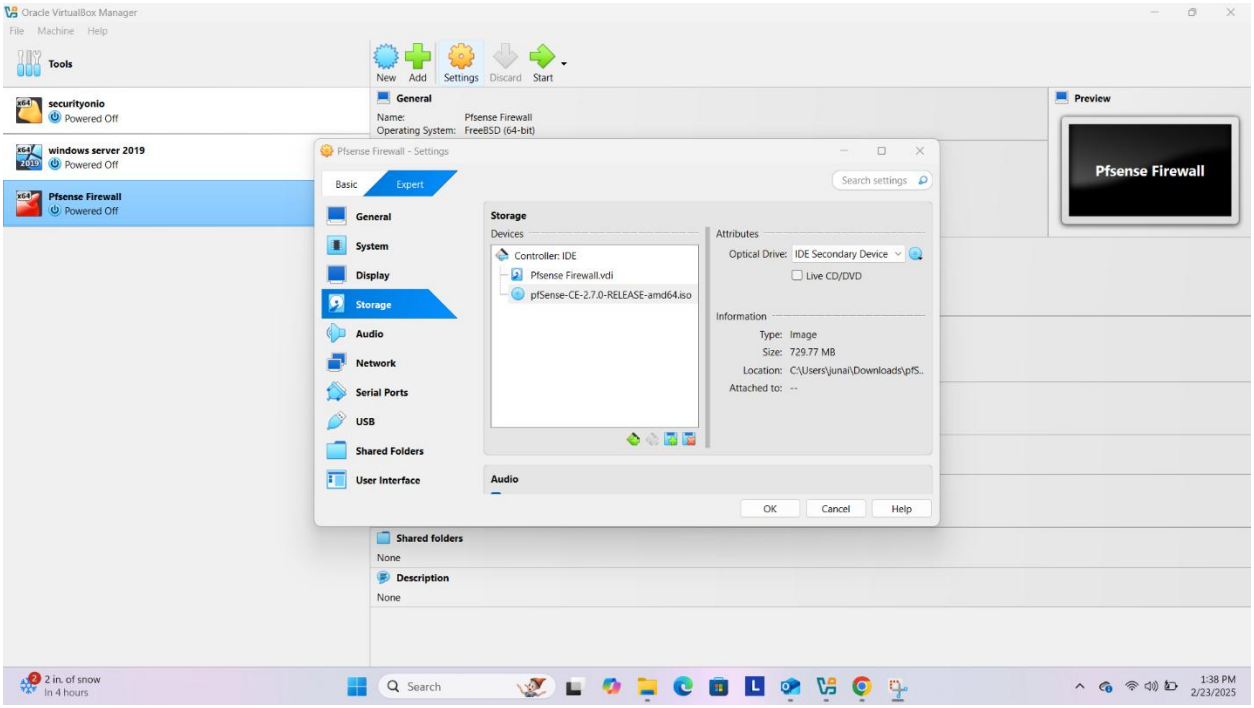
## ❖ Objective 1: Deploying the pfSense VM

To begin, I downloaded the latest **pfSense installation ISO** from the official website, selecting the **AMD64 architecture** and **ISO Installer** media.

Next, I created a **new Virtual Machine (VM)** in **VMware Workstation**, attaching the downloaded ISO file for installation. During the VM setup, I ensured the following configurations:

- Set the **operating system type** to **FreeBSD 10 and earlier (64-bit)** since VMware did not detect it automatically.
- Allocated the necessary **CPU, RAM, and disk storage**.
- Configured **two network interfaces** for the firewall setup.




Oracle VirtualBox Manager
File Machine Help
Tools
securityonio
Powered Off
windows server 2019
Powered Off
Pfsense Firewall
Powered Off
New Add Settings Discard Start
General
Name: Pfsense Firewall
Operating System: FreeBSD (64-bit)
Preview
Pfsense Firewall
Pfsense Firewall - Settings
Basic Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Storage
Devices
Controller: IDE
Pfsense Firewall.vdi
pfSense-CE-2.7.0-RELEASE-amd64.iso
Attributes
Optical Drive: IDE Secondary Device
Live CD/DVD
Information
Type: Image
Size: 729.77 MB
Location: C:\Users\junai\Downloads\pfS..
Attached to: --
Audio
OK Cancel Help
Shared folders
None
Description
None
2 in. of snow
in 4 hours
Search
1:38 PM
2/23/2025

Pfsense Firewall [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense Installer

Copyright and distribution notice

Copyright and Trademark Notices.

Copyright(c) 2004-2016. Electric Sheep Fencing, LLC ("ESF").
All Rights Reserved.

Copyright(c) 2014-2023. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.

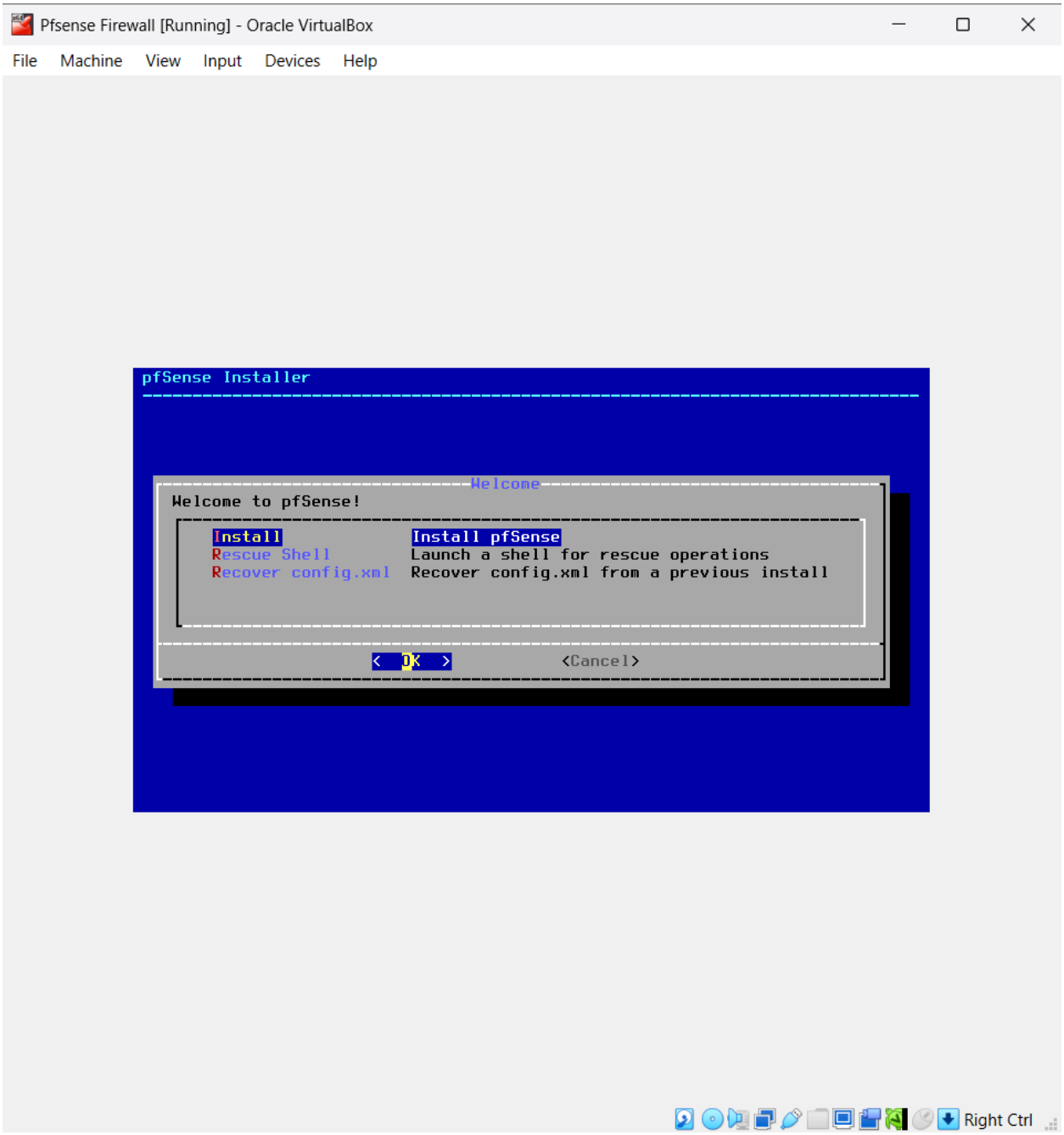
All logos, text, and content of ESF and/or Netgate, including underlying
HTML code, designs, and graphics used and/or depicted herein are
protected under United States and international copyright and trademark
laws and treaties, and may not be used or reproduced without the prior
express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to
Netgate, and may not be used without the prior express written
permission of ESF and/or Netgate. All other trademarks shown herein are

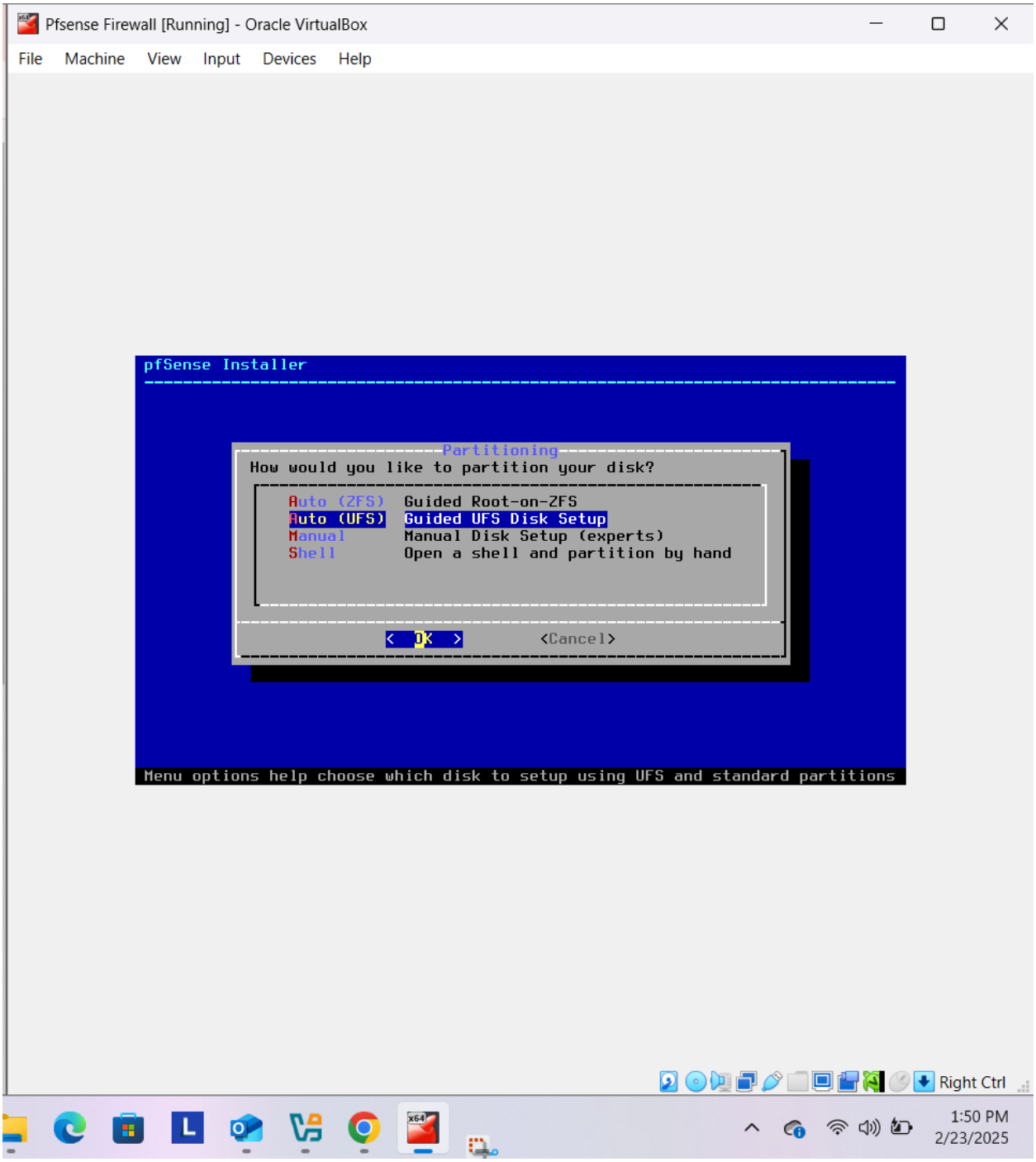
26%

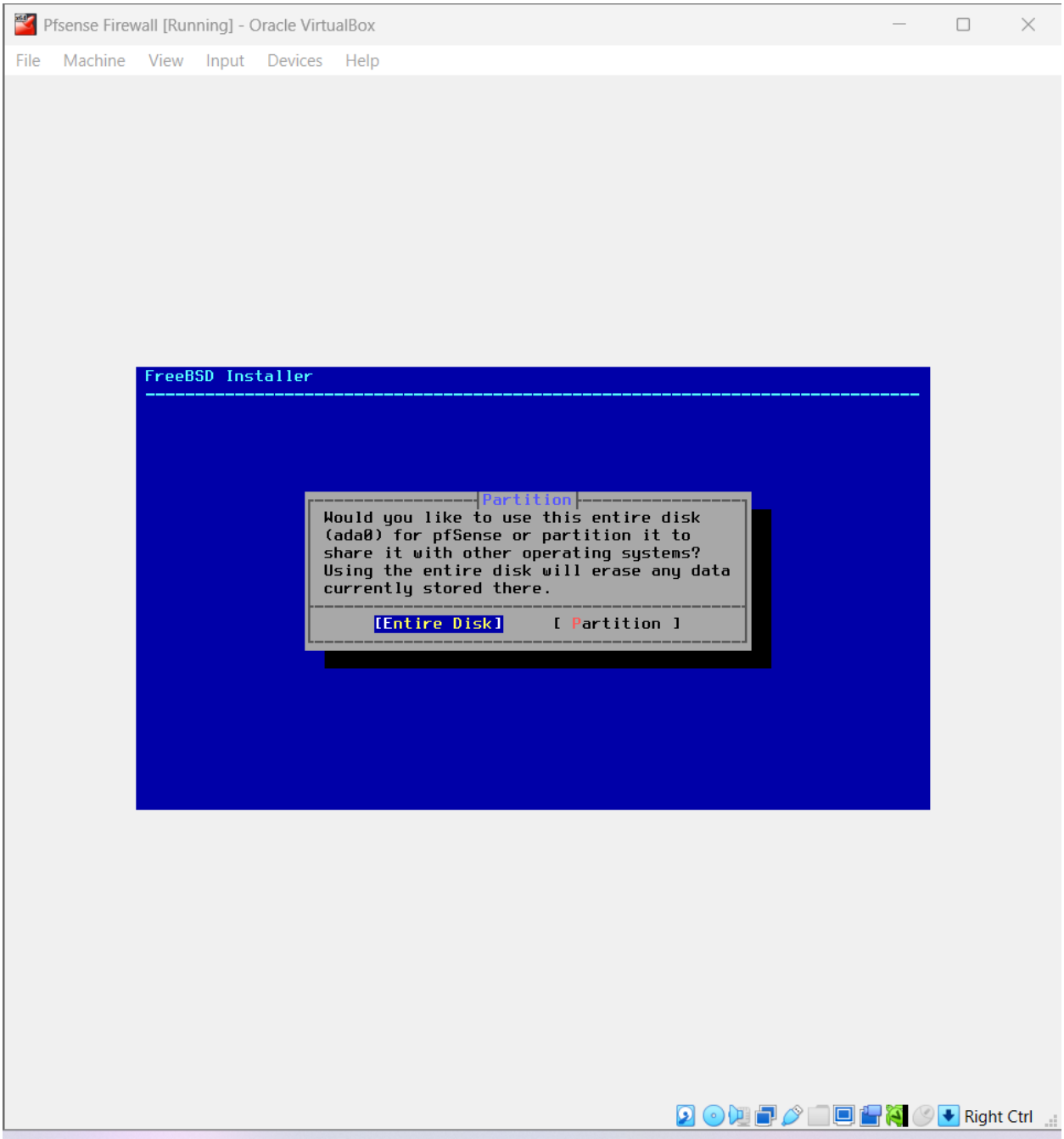
[Accept]

Right Ctrl


Pfsense Firewall [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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>
Right Ctrl

- After configuring the VM, I powered it on and initiated the **pfSense installation**. I accepted the **default keymap settings**, selected **Auto (UFS) partitioning**, and proceeded with the installation. Once the installation was complete, I rebooted the system.




Pfsense Firewall [Running] - Oracle VirtualBox
File Machine View Input Devices Help
FreeBSD Installer
Partition
Would you like to use this entire disk (ada0) for pfSense or partition it to share it with other operating systems? Using the entire disk will erase any data currently stored there.
[Entire Disk]
[ Partition ]
Right Ctrl

Pfsense Firewall [Running] - Oracle VirtualBox

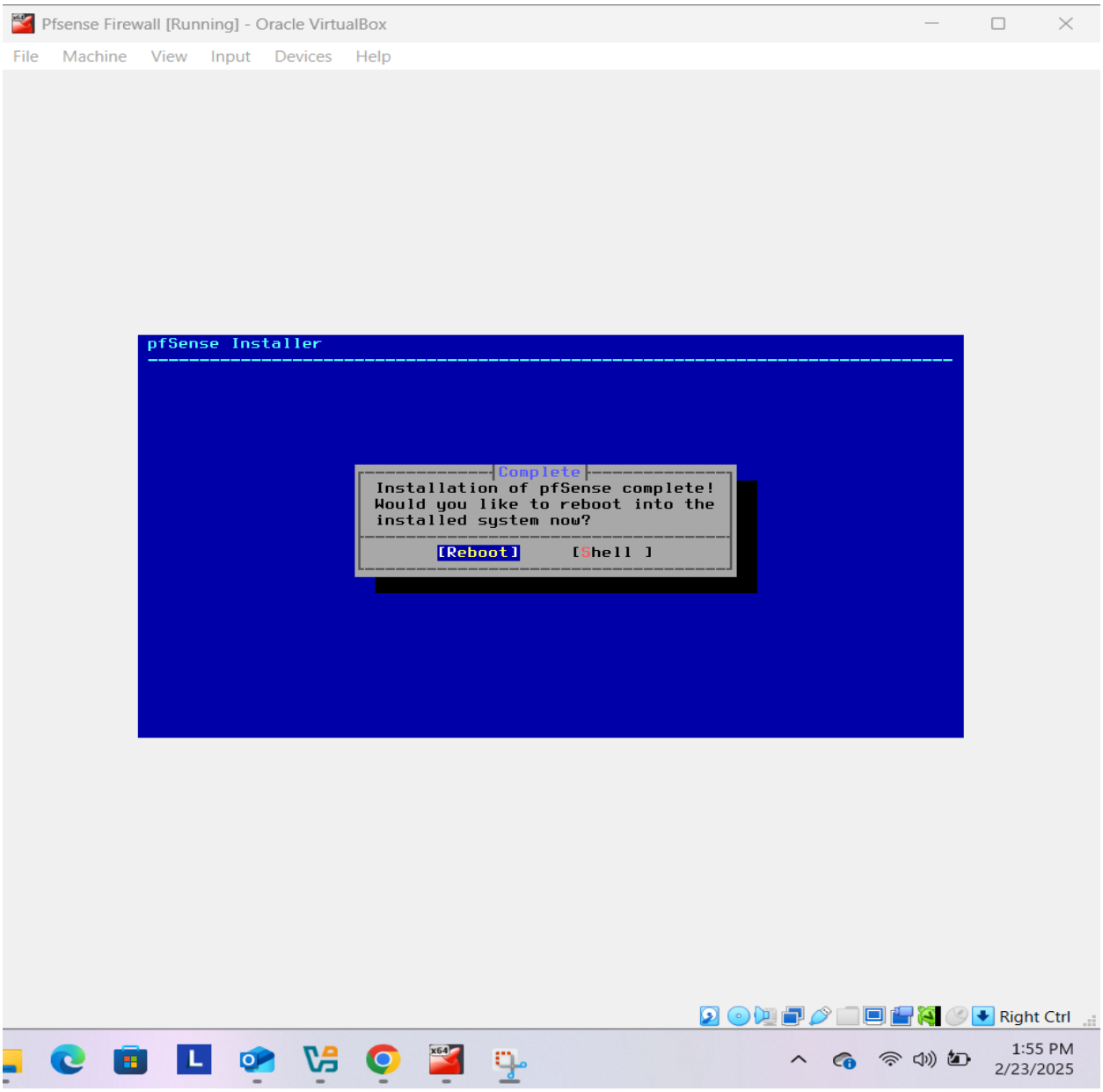
File Machine View Input Devices Help

```
FreeBSD Installer
-----------------------------------------------------------------------------
                          Partition Editor
 Please review the disk setup. When complete, press
 the Finish button.

                          Initializing
   Writing partition tables  [  Completed  ]
   Initializing ada0a        [ In Progress ]
   Initializing file systems. Please wait.
     Overall Progress
                    50%
 [
 [Create] [Delete] [Modify] [Revert] [ Auto ] [Finish]
```

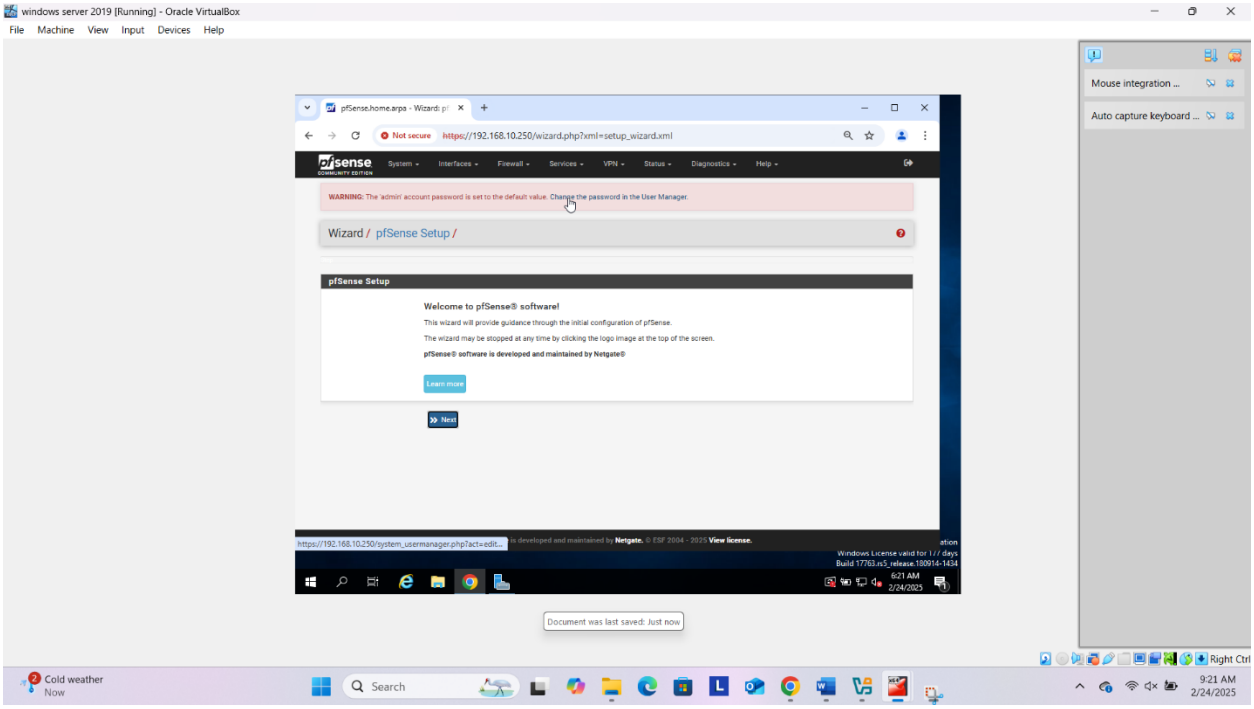
Right Ctrl

1:54 PM
2/23/2025




- Following the reboot, I accessed the pfSense console and selected **option 2** to configure the LAN interface. I assigned the IP address **192.168.10.125/24**, configured DHCP settings as required, and applied the changes. Finally, I restarted the system to ensure all settings were properly applied.

## ❖ Objective 2: Configuring pfSense




Once the system was up and running, I accessed the **WebConfigurator** by navigating to https://192.168.10.125 in a browser. I logged in using the default credentials (**admin / pfsense**).

- I then proceeded with the initial configuration steps:
- Set the **hostname** and defined the **primary and secondary DNS servers** (**1.1.1.1** and **9.9.9.9** respectively).
- Chose the **UTC time zone** to ensure accurate log synchronization.
- Configured the **WAN and LAN interfaces**.
- Changed the default **admin password** to enhance security.
- Saved the settings and reloaded the configuration to apply all changes.

windows server 2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense.home.arpa - Wizard: pf

Not secure https://192.168.10.250/wizard.php?xml=setup_wizard.xml

Step 2 of 9

## General Information

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.

Build 17763.rs5_release.1

6:27 AM

2/24/202

pfSense.home.arpa - Wizard: pf

Not secure https://192.168.10.250/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.

## Static IP Configuration

**IP Address** 192.168.10.250

windows server 2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense.home.arpa - Wizard: pf

Not secure https://192.168.10.250/wizard.php?xml=setup_wizard.xml

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.

**Static IP Configuration**

| | |
|---|---|
| **IP Address** | 192.168.10.250 |
| **Subnet Mask** | 24 |
| **Upstream Gateway** | |

**DHCP client configuration**

| | |
|---|---|
| **DHCP Hostname** | The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification). |

**PPPoE configuration**

| | |
|---|---|
| **PPPoE Username** | |
| **PPPoE Password** | |
| **Show PPPoE password** | Reveal password characters |
| **PPPoE Service name** | Hint: this field can usually be left empty |
| **PPPoE Dial on demand** | Enable Dial-On-Demand mode<br>This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected. |
| **PPPoE Idle timeout** | If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables |

windows server 2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense.home.arpa - Wizard: pf

Not secure https://192.168.10.250/wizard.php?xml=setup_wizard.xml

| | |
|---|---|
| **Show PPTP password** | Reveal password characters |
| **PPTP Local IP Address** | |
| **pptplocalsubnet** | 32 |
| **PPTP Remote IP Address** | |
| **PPTP Dial on demand** | Enable Dial-On-Demand mode<br>This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected. |
| **PPTP Idle timeout** | If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature. |

## RFC1918 Networks

| | |
|---|---|
| **Block RFC1918 Private Networks** | Block private networks from entering via WAN<br>When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too. |

## Block bogon networks

| | |
|---|---|
| **Block bogon networks** | Block non-Internet routed networks from entering via WAN<br>When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received. |

Next



Build 17763.rs5_release.1

6:34 AM

2/24/202

windows server 2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense.home.arpa - Wizard: pf

Not secure https://192.168.10.250/wizard.php?xml=setup_wizard.xml&stepid=6&next=Next

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.

Build 17763.rs5_release.1

6:38 AM
2/24/202

windows server 2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense.home.arpa - Wizard: pf

Not secure https://192.168.10.250/wizard.php?xml=setup_wizard.xml&stepid=6&next=Next

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 - 2025 View license.

Build 17763.rs5_release.1

6:39 AM
2/24/202

windows server 2019 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

pfSense.home.arpa - Wizard: pf

Not secure https://192.168.10.250/wizard.php?xml=setup_wizard.xml&stepid=6&next=Next

pfsense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Wizard / pfSense Setup / Reload in progress

Step 8 of 9

**Reload in progress**

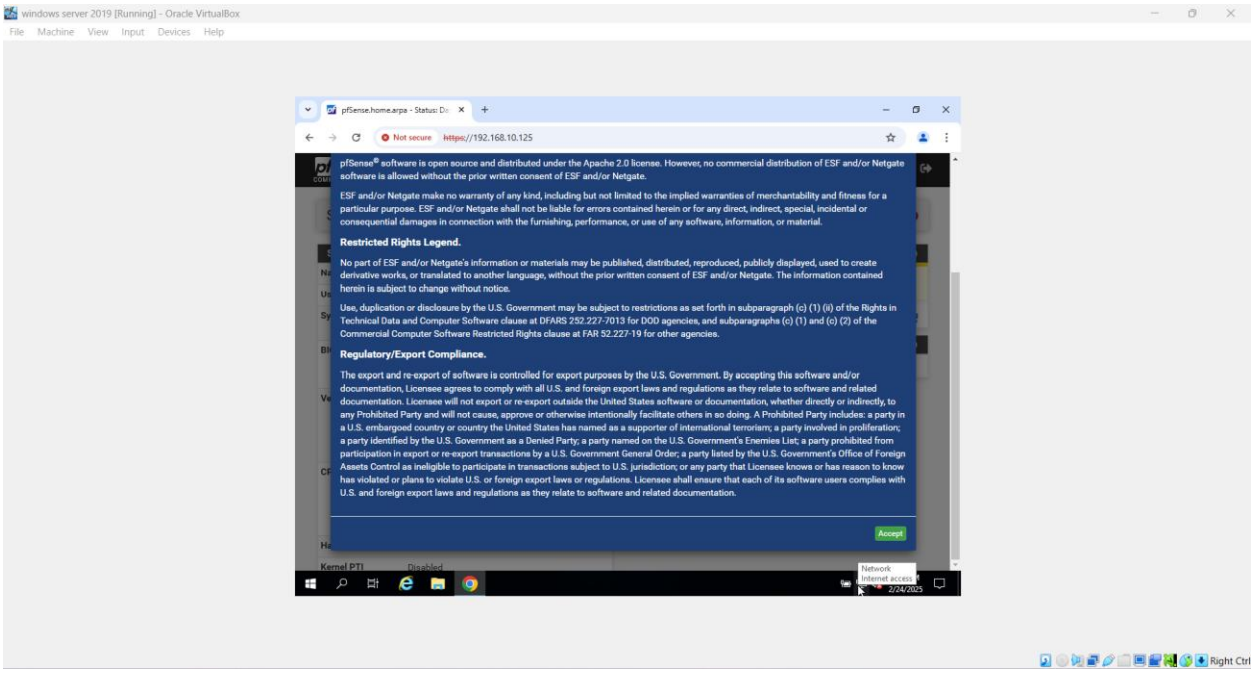
A reload is now in progress. Please wait.

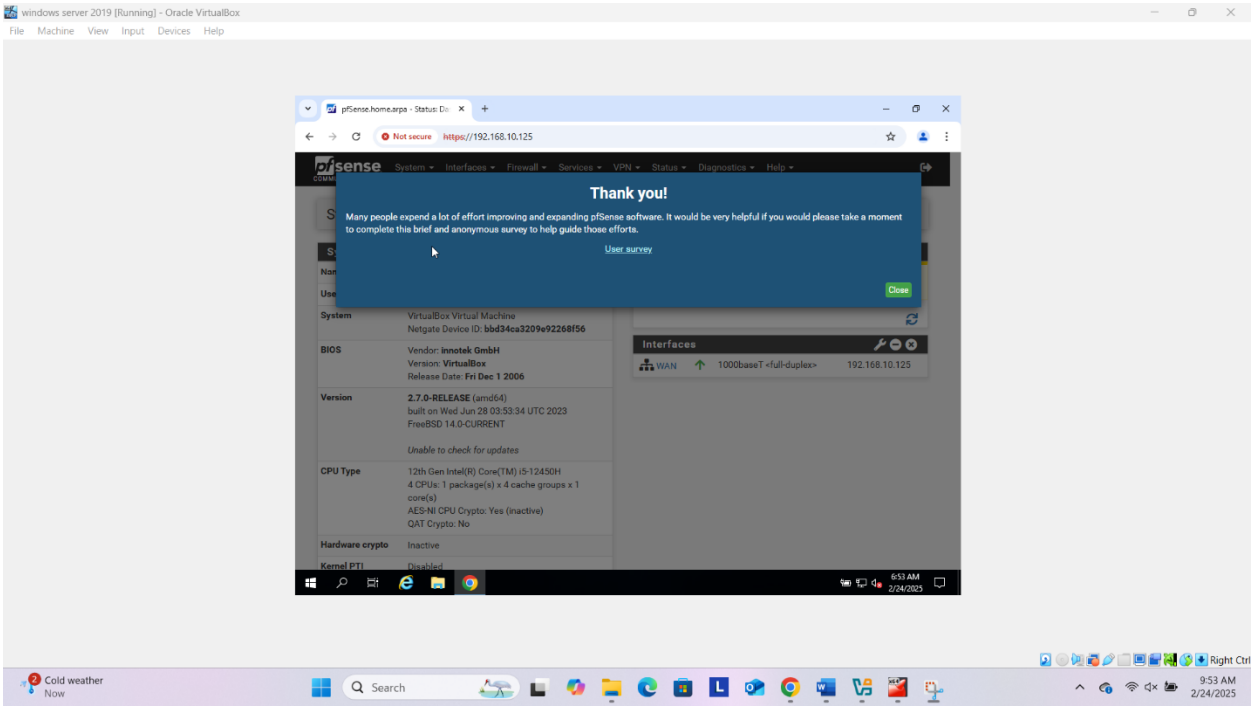
The wizard will redirect to the next step once the reload is completed.

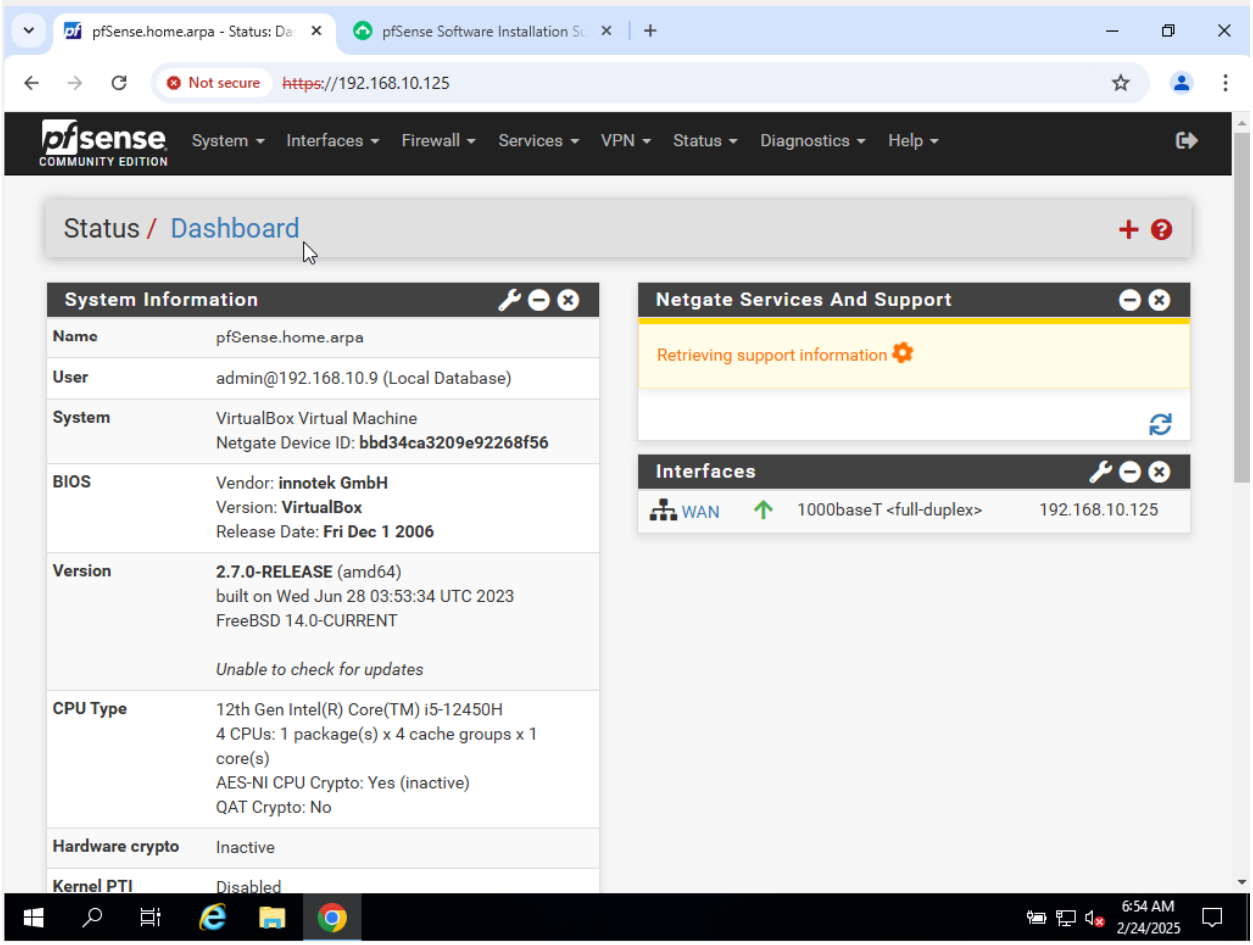
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

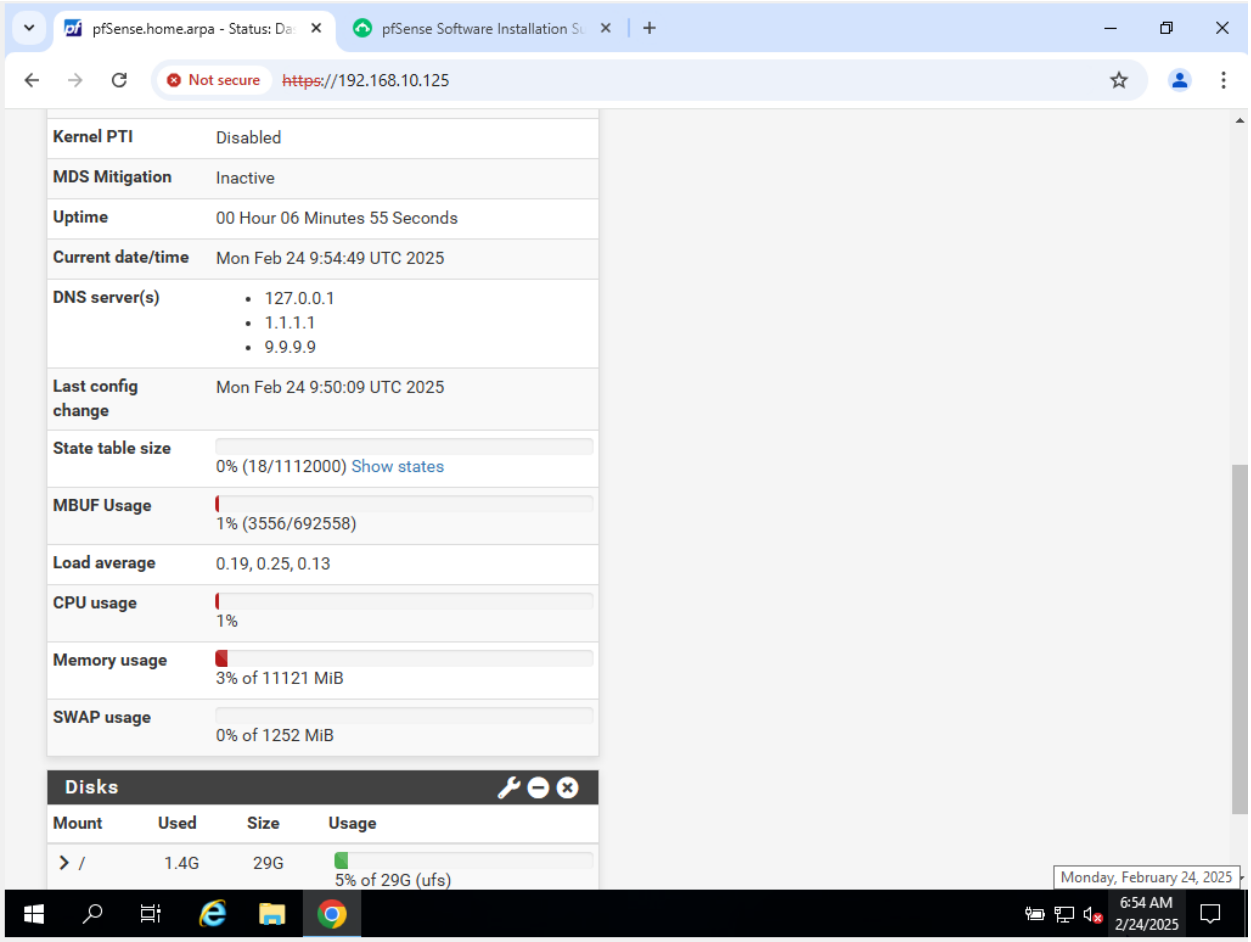
Build 17763.rs5_release.1

6:39 AM
2/24/202


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Status: Di
Not secure https://192.168.10.125
pfSense® software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate software is allowed without the prior written consent of ESF and/or Netgate.
ESF and/or Netgate make no warranty of any kind, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. ESF and/or Netgate shall not be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of any software, information, or material.
Restricted Rights Legend.
No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.
Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.
Regulatory/Export Compliance.
The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.
Accept
Kernel PTI Disabled
Network: Internet access
2/24/2025
Right Ctrl


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Status: Di
Not secure https://192.168.10.125
pfsense System Interfaces Firewall Services VPN Status Diagnostics Help
Thank you!
Many people expend a lot of effort improving and expanding pfSense software. It would be very helpful if you would please take a moment to complete this brief and anonymous survey to help guide those efforts.
User survey
Close
System VirtualBox Virtual Machine
Netgate Device ID: bbd34ca3209e92268f56
BIOS Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006
Version 2.7.0-RELEASE (amd64)
built on Wed Jun 28 03:53:34 UTC 2023
FreeBSD 14.0-CURRENT
Unable to check for updates
CPU Type 12th Gen Intel(R) Core(TM) i5-12450H
4 CPUs: 1 package(s) x 4 cache groups x 1 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto Inactive
Kernel PTI Disabled
Interfaces
WAN 1000baseT <full-duplex> 192.168.10.125
6:53 AM
2/24/2025
Right Ctrl
Cold weather
Now
Search
9:53 AM
2/24/2025

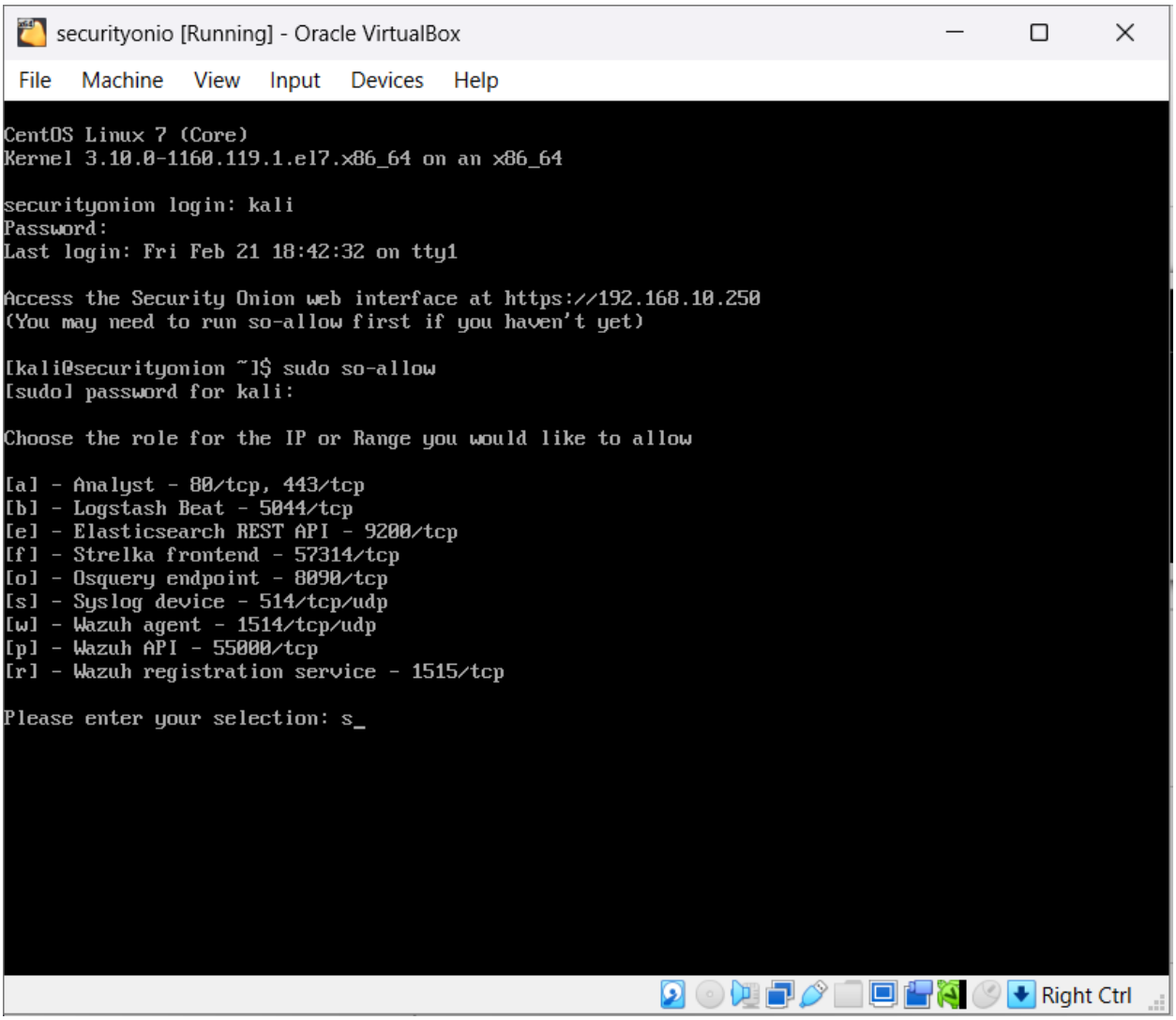

pfSense.home.arpa - Status: Da
pfSense Software Installation Su
Not secure
https://192.168.10.125
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name
pfSense.home.arpa
User
admin@192.168.10.9 (Local Database)
System
VirtualBox Virtual Machine
Netgate Device ID: bbd34ca3209e92268f56
BIOS
Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006
Version
2.7.0-RELEASE (amd64)
built on Wed Jun 28 03:53:34 UTC 2023
FreeBSD 14.0-CURRENT
Unable to check for updates
CPU Type
12th Gen Intel(R) Core(TM) i5-12450H
4 CPUs: 1 package(s) x 4 cache groups x 1 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto
Inactive
Kernel PTI
Disabled
Netgate Services And Support
Retrieving support information
Interfaces
WAN
1000baseT <full-duplex>
192.168.10.125
6:54 AM
2/24/2025

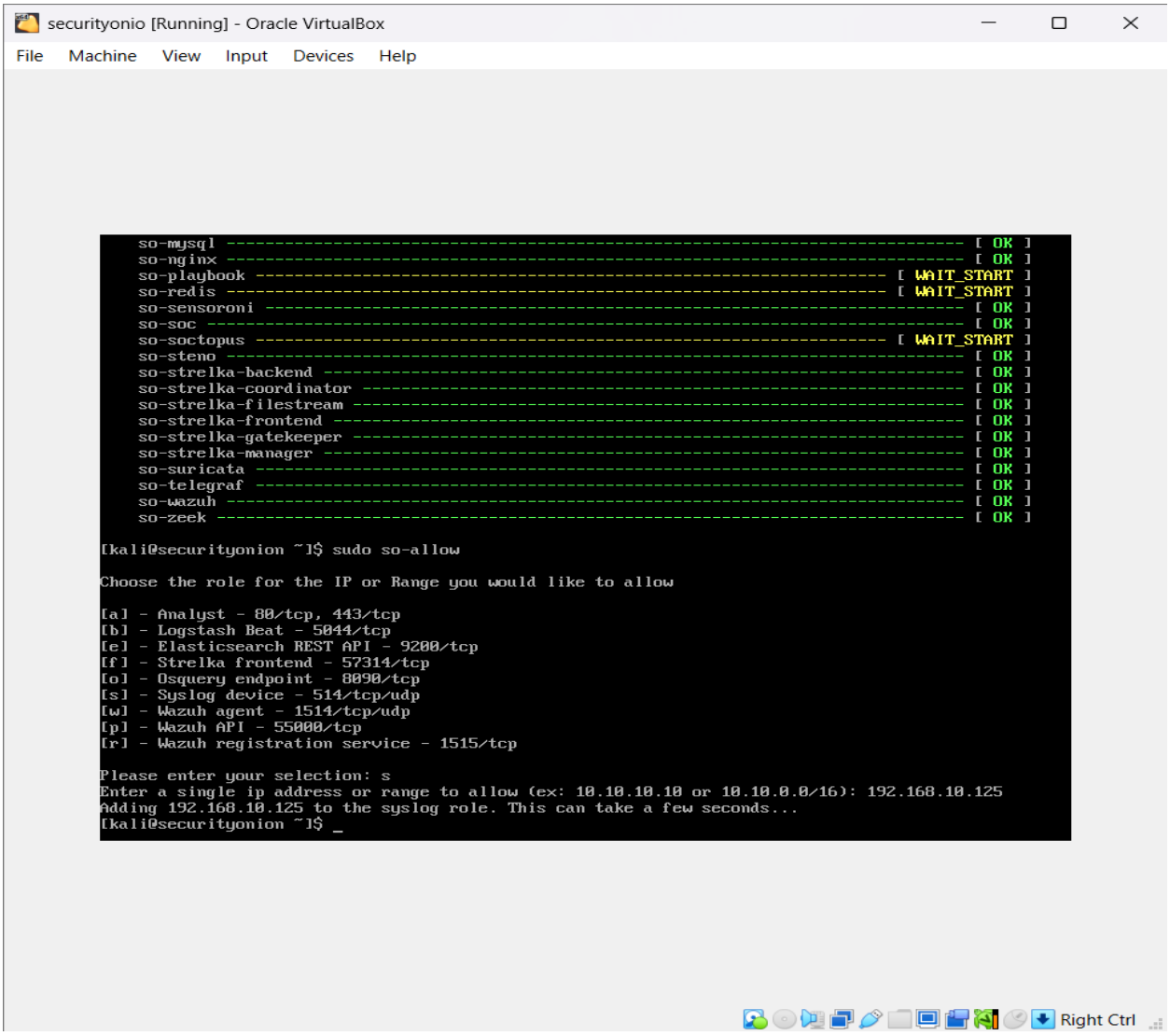

pfSense.home.arpa - Status: Da
pfSense Software Installation Su
Not secure
https://192.168.10.125
Kernel PTI
Disabled
MDS Mitigation
Inactive
Uptime
00 Hour 06 Minutes 55 Seconds
Current date/time
Mon Feb 24 9:54:49 UTC 2025
DNS server(s)
127.0.0.1
1.1.1.1
9.9.9.9
Last config change
Mon Feb 24 9:50:09 UTC 2025
State table size
0% (18/1112000) Show states
MBUF Usage
1% (3556/692558)
Load average
0.19, 0.25, 0.13
CPU usage
1%
Memory usage
3% of 11121 MiB
SWAP usage
0% of 1252 MiB
Disks
Mount
Used
Size
Usage
/
1.4G
29G
5% of 29G (ufs)
Monday, February 24, 2025
6:54 AM
2/24/2025

## ❖ Objective 3: Configuring Log Forwarding to Security Onion

To forward pfSense logs to **Security Onion**, I first needed to allow syslog access. I connected to **Security Onion** using SSH with the following command:
- ssh adm-pac@192.168.10.125

Then, I ran the following command to allow syslog connections:
- sudo so-allow






I selected **Syslog Device – port 514/tcp/udp** and added **192.168.10.125** as an allowed source.

Next, I configured **pfSense** to send logs to Security Onion:

- Logged into **pfSense WebConfigurator**.
- Navigated to **Status → System Logs → Settings**.
- Enabled **Remote Syslog Logging**.
- Entered **192.168.10.125:514** as the syslog server.
- Saved the configuration to apply the changes.

pfSense.home.arpa - Status: Sys

Not secure https://192.168.10.125/status_logs_settings.php

## Remote Logging Options

**Enable Remote Logging**

- [x] Send log messages to remote syslog server

**Source Address**

Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

**IP Protocol**

IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

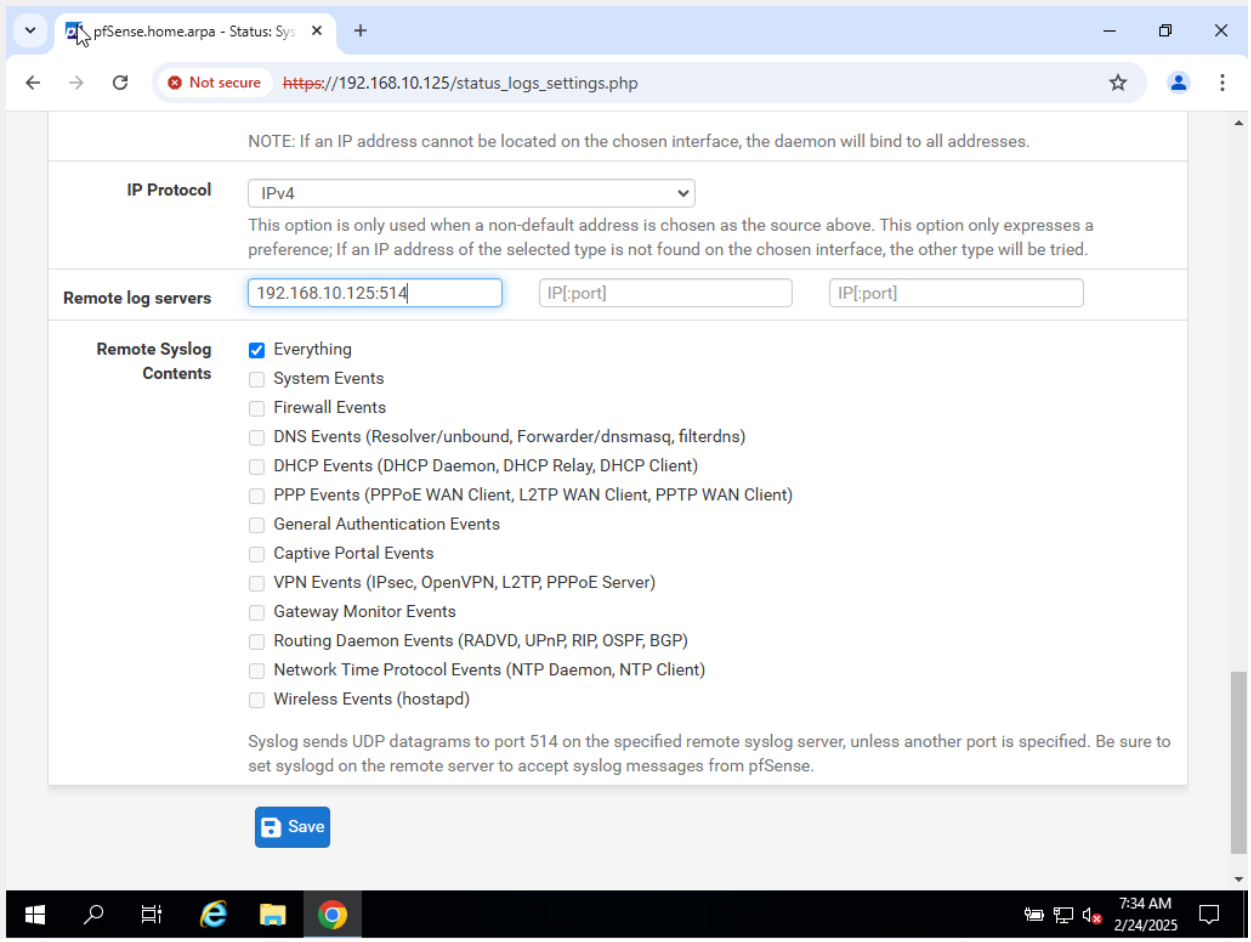
**Remote log servers**

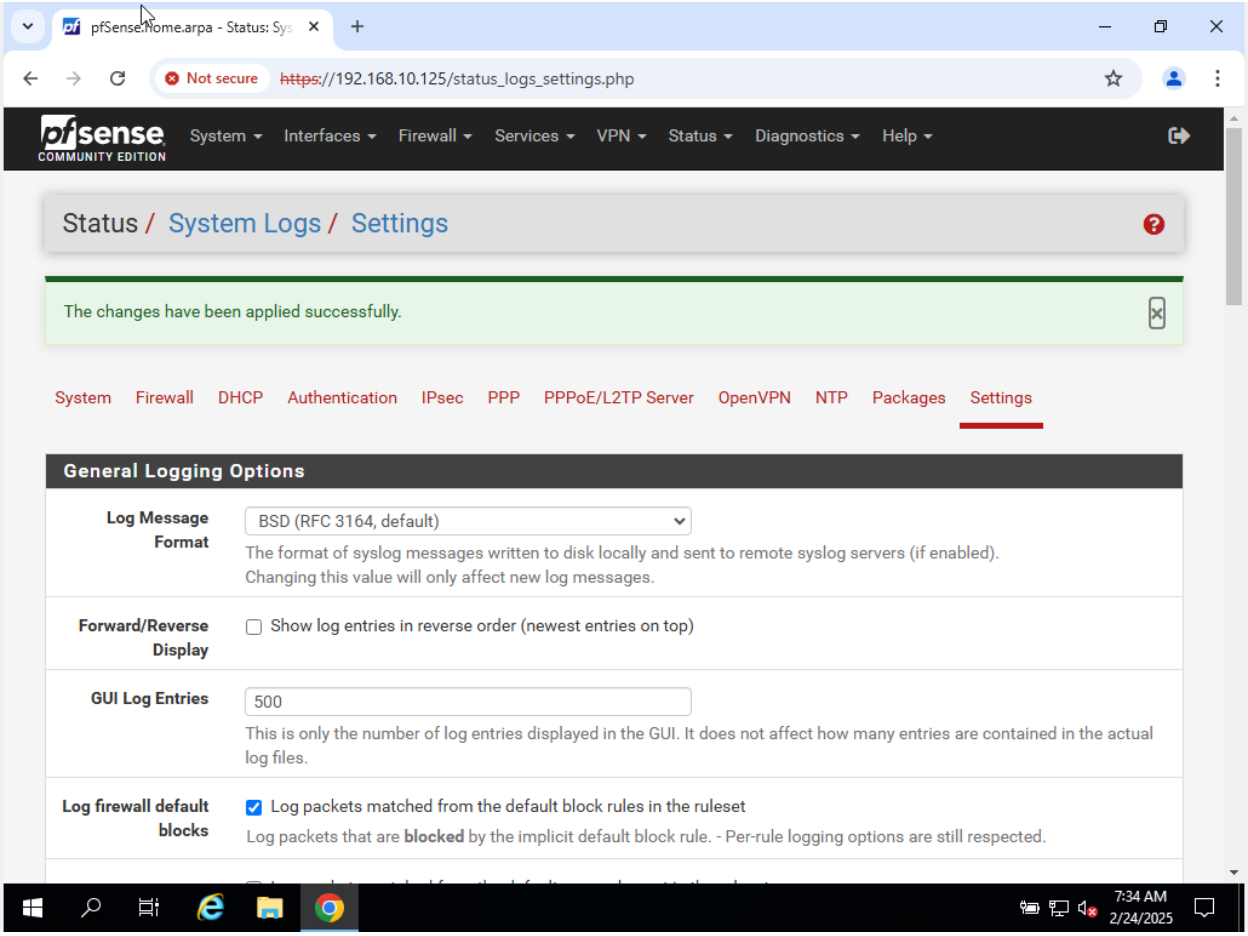
192.168.10.125:514 | IP[:port] | IP[:port]

**Remote Syslog Contents**

- [x] Everything
- [ ] System Events
- [ ] Firewall Events
- [ ] DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- [ ] DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- [ ] PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- [ ] General Authentication Events
- [ ] Captive Portal Events
- [ ] VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- [ ] Gateway Monitor Events
- [ ] Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)

7:33 AM
2/24/2025


pfSense.home.arpa - Status: Sys
Not secure
https://192.168.10.125/status_logs_settings.php
NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.
IP Protocol
IPv4
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.
Remote log servers
192.168.10.125:514
IP[:port]
IP[:port]
Remote Syslog Contents
Everything
System Events
Firewall Events
DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
General Authentication Events
Captive Portal Events
VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
Gateway Monitor Events
Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
Network Time Protocol Events (NTP Daemon, NTP Client)
Wireless Events (hostapd)
Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.
Save
7:34 AM
2/24/2025




- By following these steps, I successfully deployed and configured the **pfSense firewall**. I set up the network interfaces, secured the system, and enabled **log forwarding to Security Onion** for real-time monitoring and security analysis. With this configuration, I can now track network activity and analyze security events efficiently.