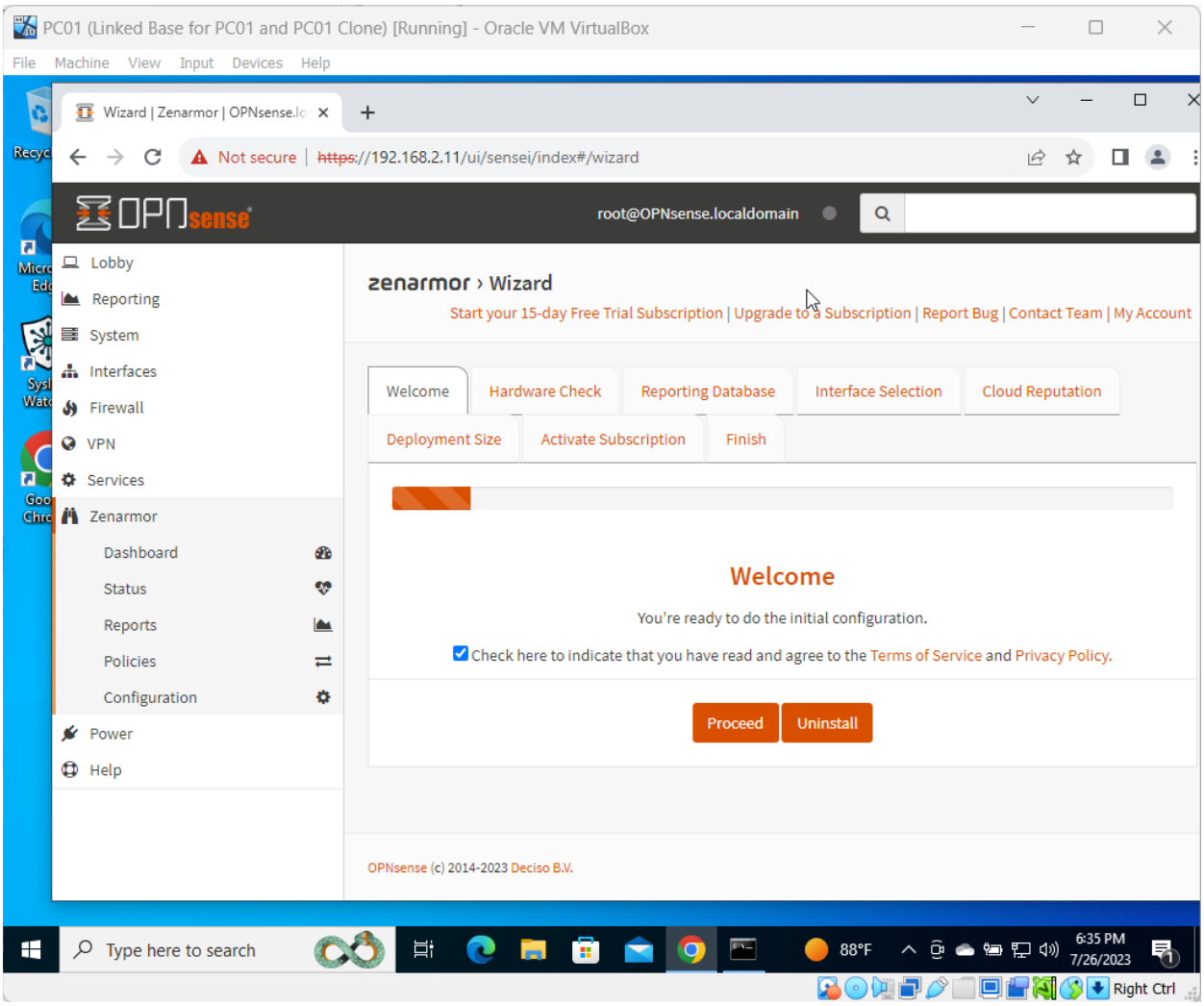
# Configuring Advanced Firewall Features via Sensei (Zenarmor)

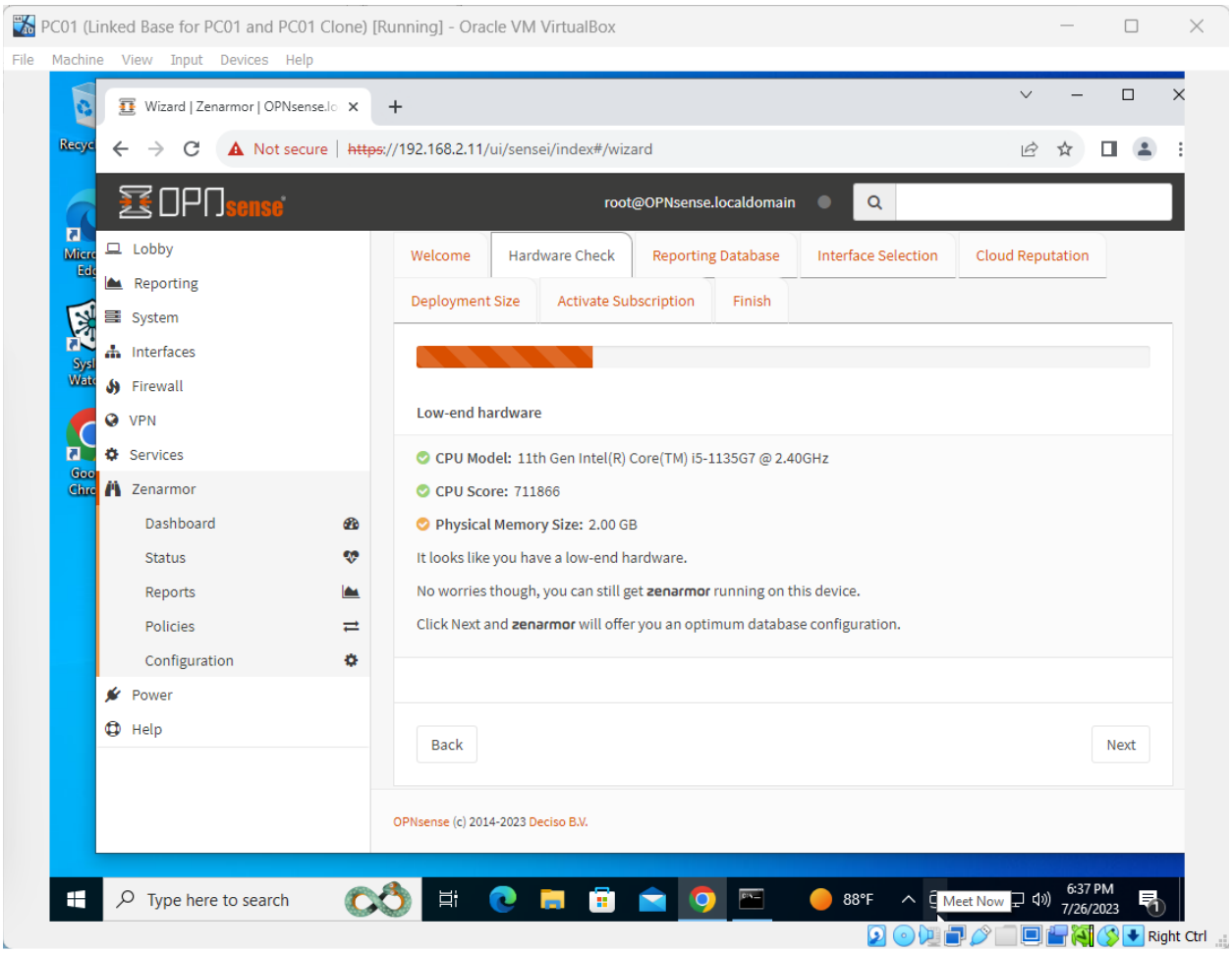
In this comprehensive lab, I delved into the installation, configuration, and overview of the Sensei module—a potent plugin enhancing OPNsense firewall capabilities. Sensei introduces next-generation features such as Application Control, Network Analytics, and TLS Inspection, expanding the firewall's functionalities beyond native capabilities.

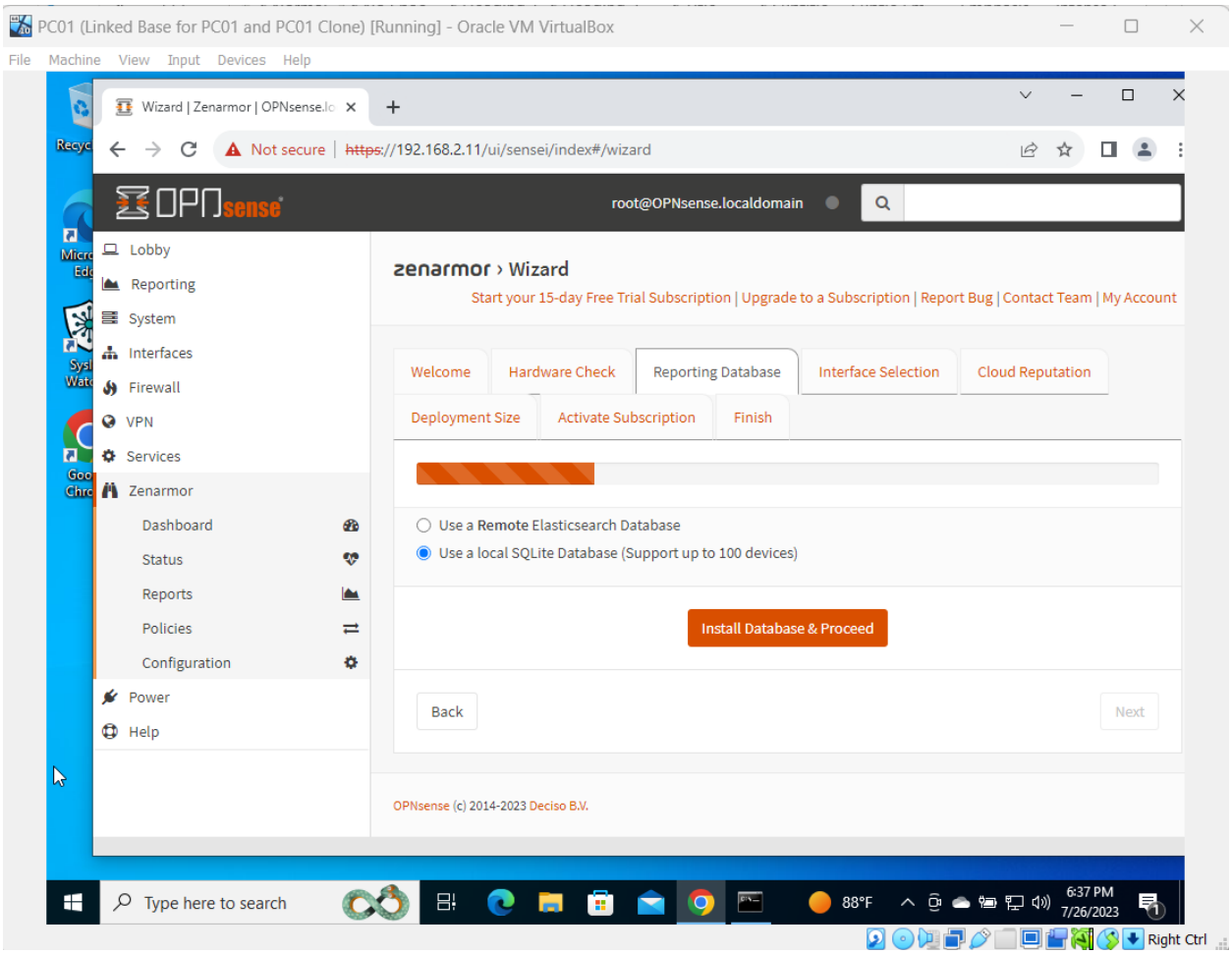
**Step 1 - Install Sensei:**

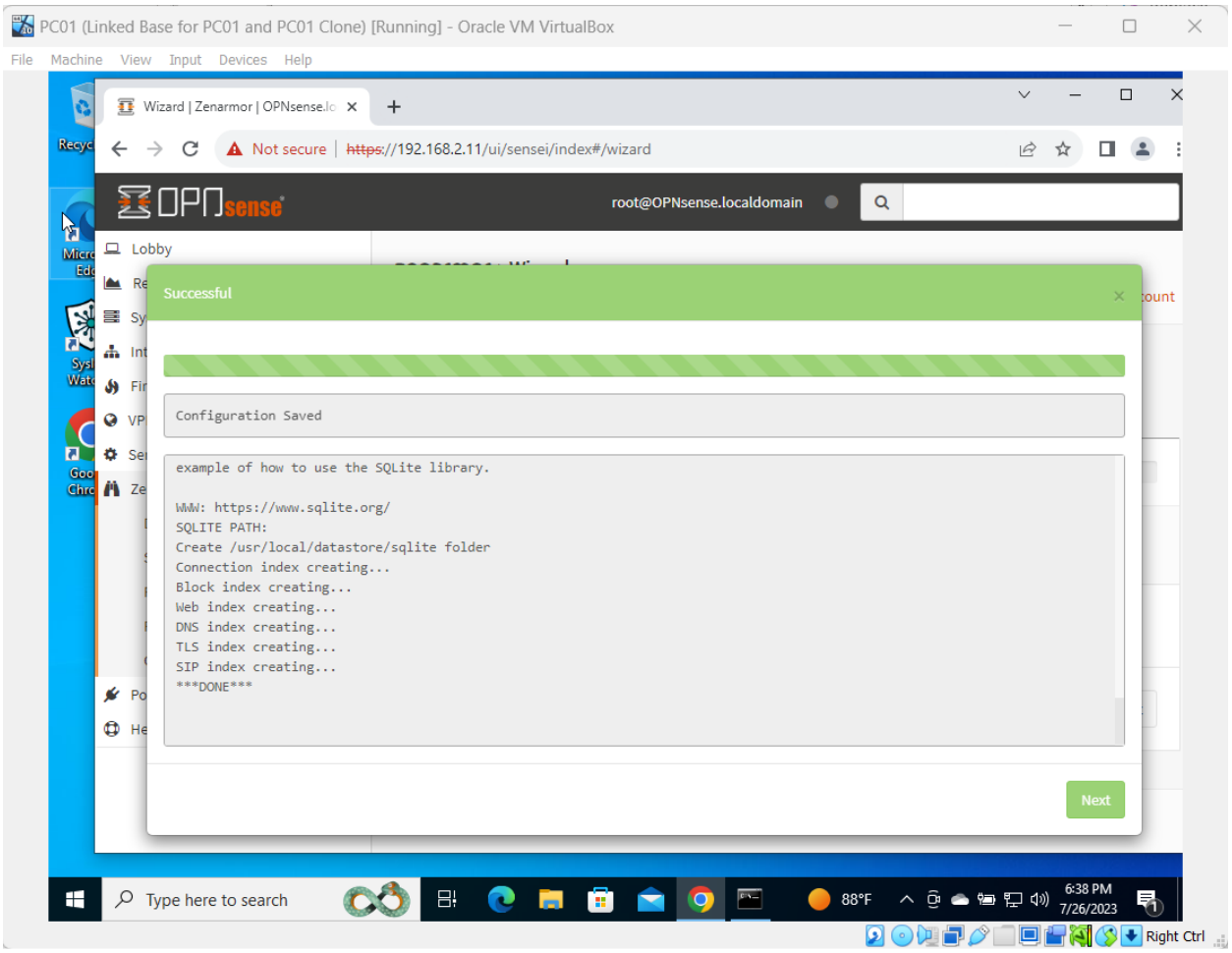
I initiated the Sensei installation by clicking on the dashboard, triggering the setup wizard. After accepting the Terms of Service and Privacy Policy, I checked the box and proceeded. Clicking "Next," I reached the "**Install Database & Proceed**" button, selected Deployment Mode #2, and added LAN and GuestNetwork to the Protected Interfaces list. I maintained default settings and completed the wizard, ensuring full help was enabled.

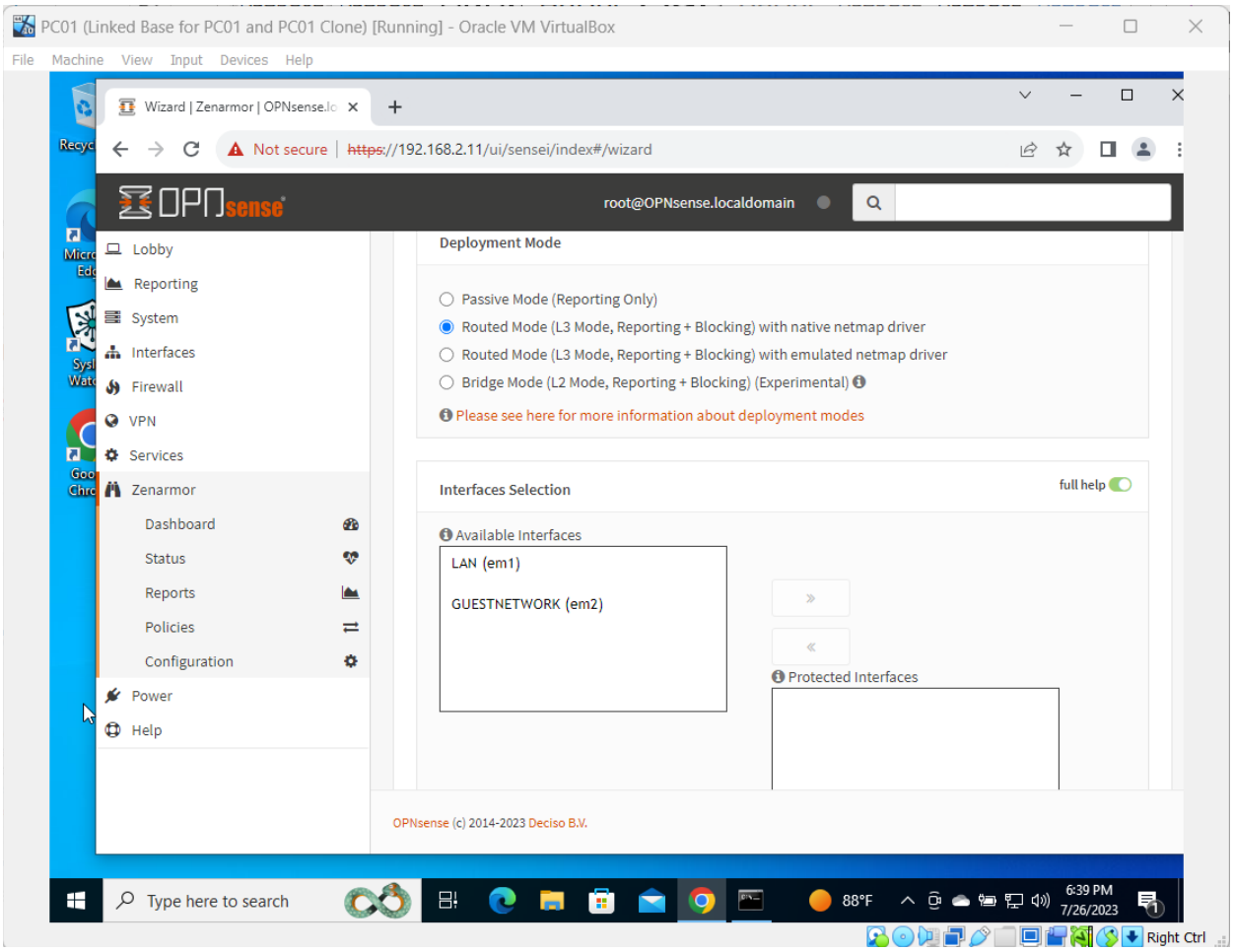
The following screenshots illustrates step 1 more:

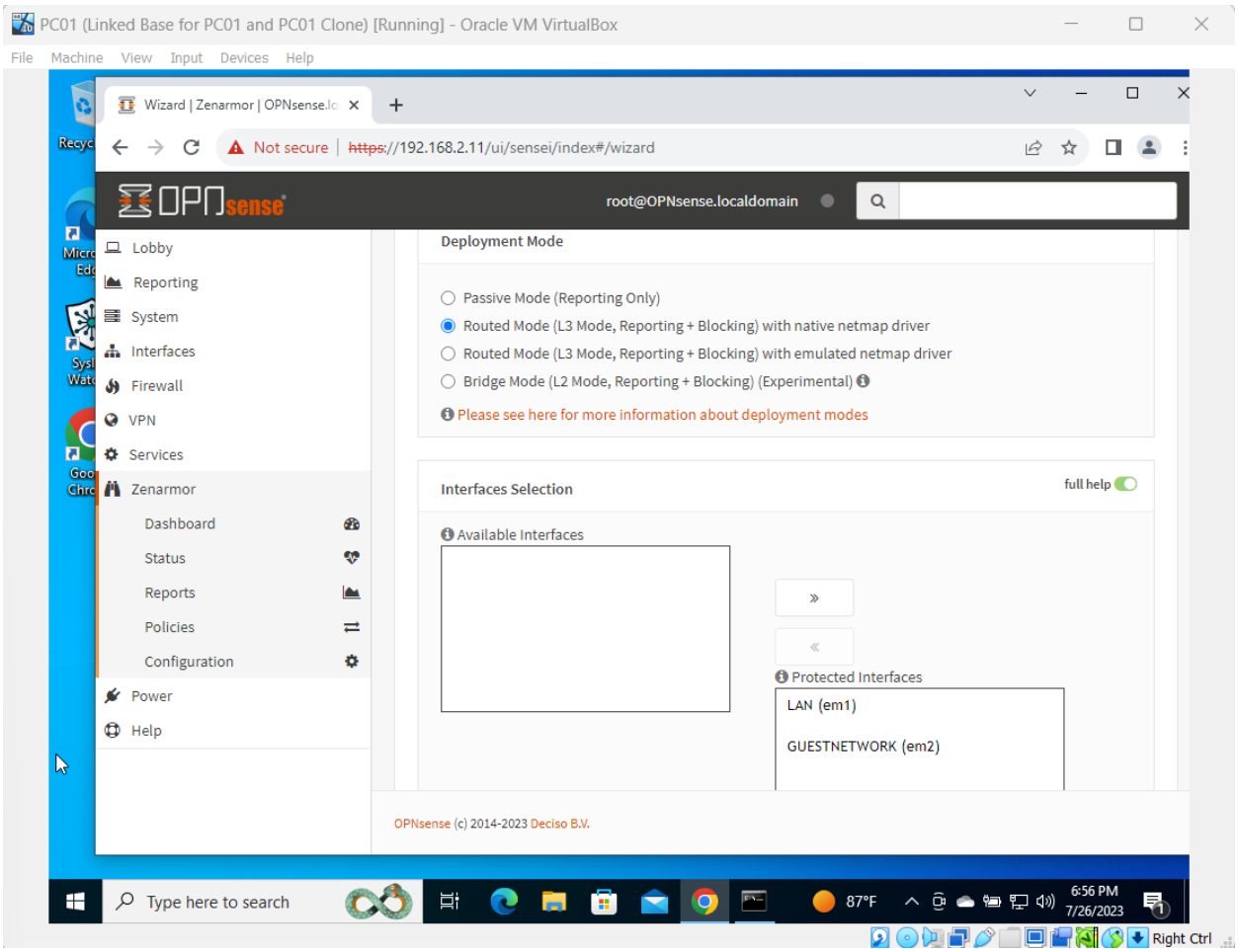

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure | https://192.168.2.11/ui/sensei/index#/wizard
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
zenarmor › Wizard
Start your 15-day Free Trial Subscription | Upgrade to a Subscription | Report Bug | Contact Team | My Account
Welcome
Hardware Check
Reporting Database
Interface Selection
Cloud Reputation
Deployment Size
Activate Subscription
Finish
Welcome
You're ready to do the initial configuration.
Check here to indicate that you have read and agree to the Terms of Service and Privacy Policy.
Proceed
Uninstall
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
88°F
6:35 PM
7/26/2023
Right Ctrl

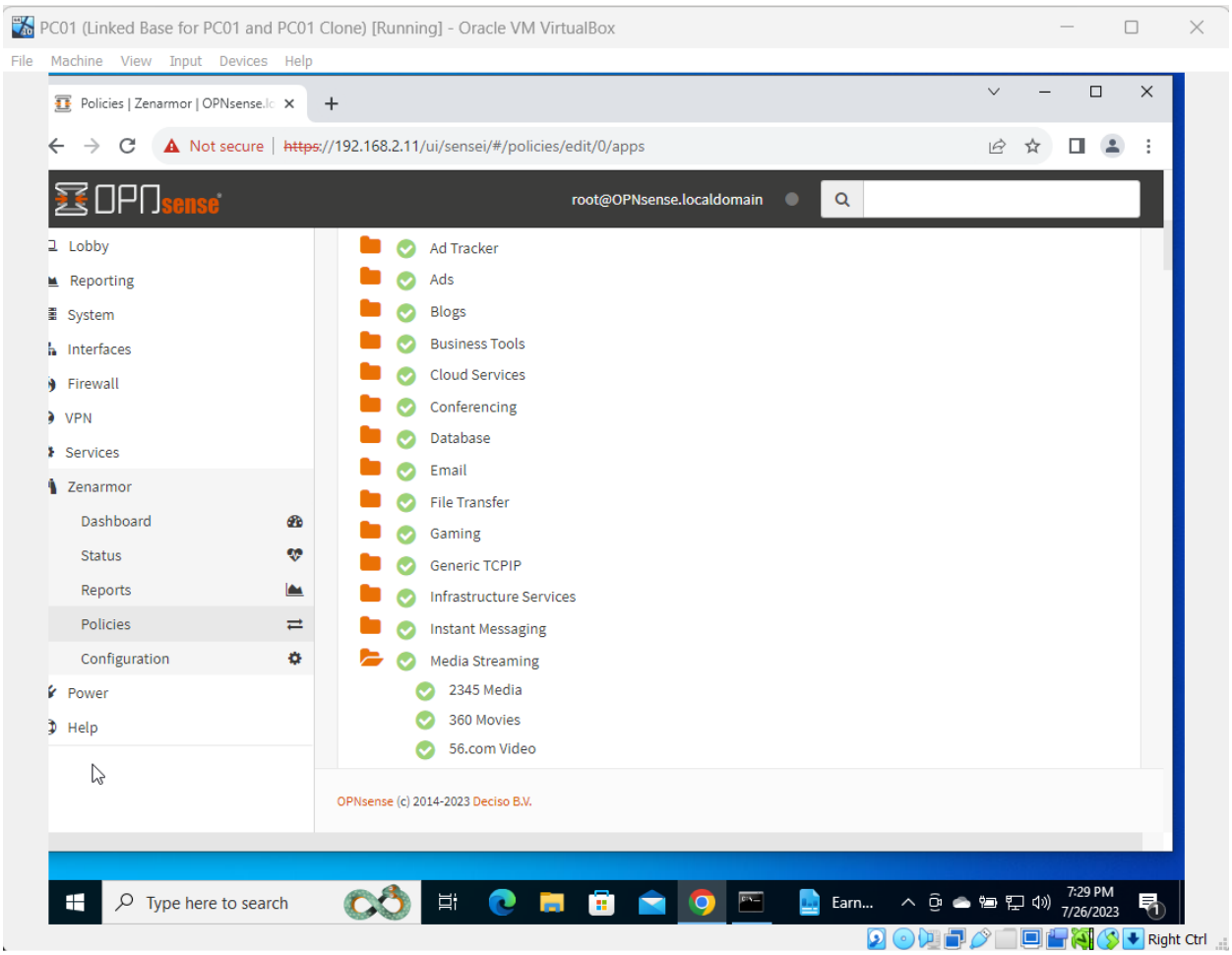

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure | https://192.168.2.11/ui/sensei/index#/wizard
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Welcome
Hardware Check
Reporting Database
Interface Selection
Cloud Reputation
Deployment Size
Activate Subscription
Finish
Low-end hardware
CPU Model: 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
CPU Score: 711866
Physical Memory Size: 2.00 GB
It looks like you have a low-end hardware.
No worries though, you can still get zenarmor running on this device.
Click Next and zenarmor will offer you an optimum database configuration.
Back
Next
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
88°F
Meet Now
6:37 PM
7/26/2023
Right Ctrl

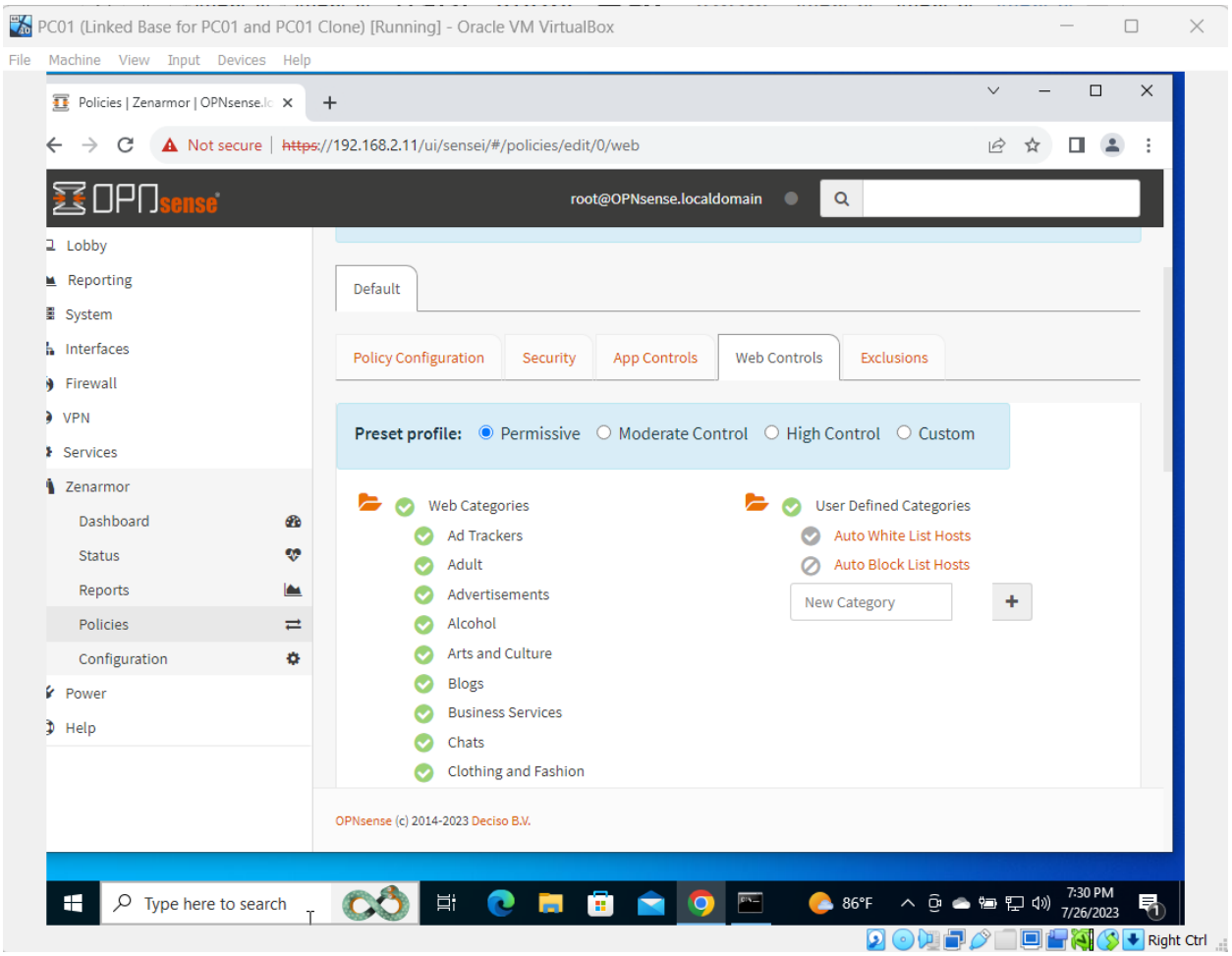

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure | https://192.168.2.11/ui/sensei/index#/wizard
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
zenarmor › Wizard
Start your 15-day Free Trial Subscription | Upgrade to a Subscription | Report Bug | Contact Team | My Account
Welcome
Hardware Check
Reporting Database
Interface Selection
Cloud Reputation
Deployment Size
Activate Subscription
Finish
Use a Remote Elasticsearch Database
Use a local SQLite Database (Support up to 100 devices)
Install Database & Proceed
Back
Next
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
88°F
6:37 PM
7/26/2023
Right Ctrl

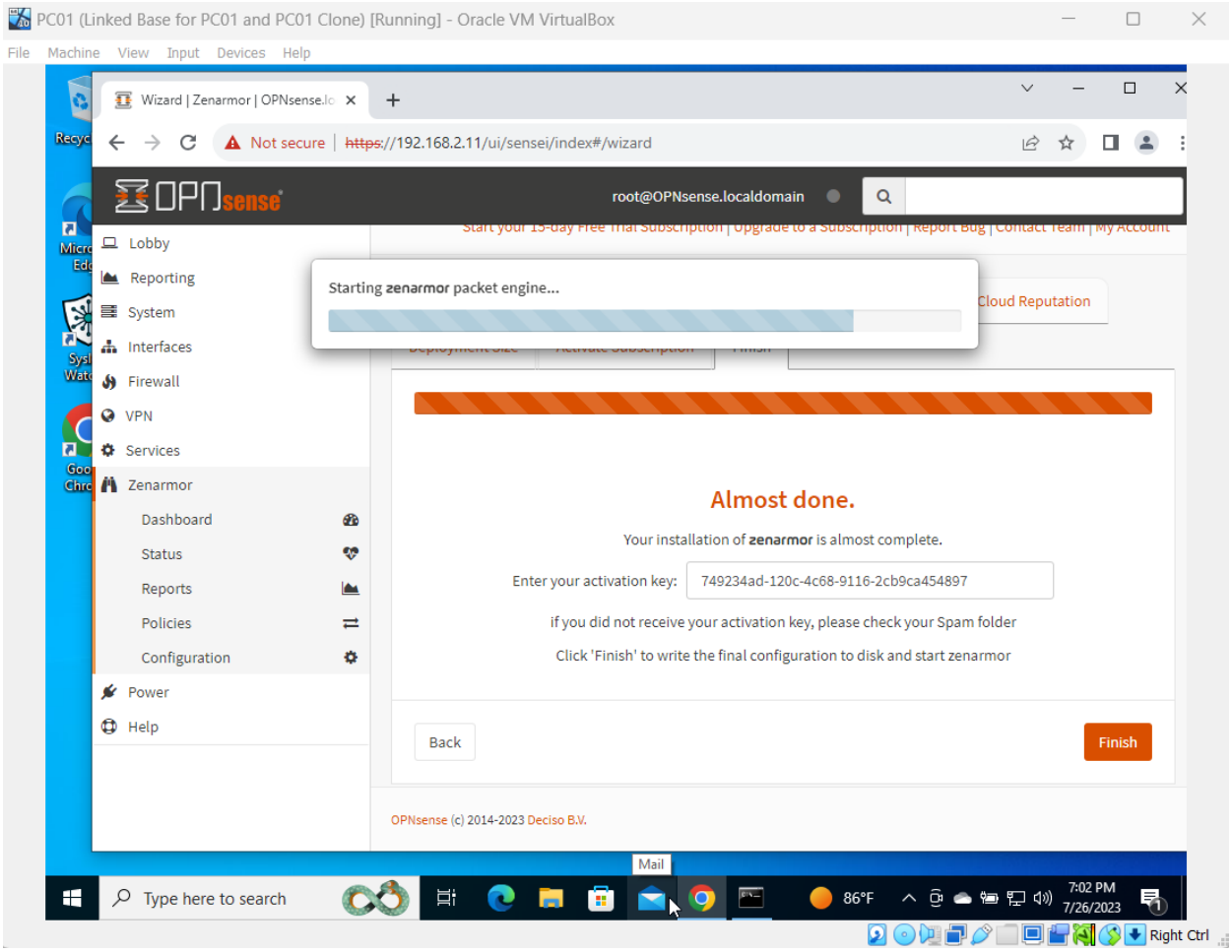

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure | https://192.168.2.11/ui/sensei/index#/wizard
root@OPNsense.localdomain
Lobby
Successful
Configuration Saved
example of how to use the SQLite library.
WWW: https://www.sqlite.org/
SQLITE PATH:
Create /usr/local/datastore/sqlite folder
Connection index creating...
Block index creating...
Web index creating...
DNS index creating...
TLS index creating...
SIP index creating...
***DONE***
Next
Type here to search
88°F
6:38 PM
7/26/2023
Right Ctrl

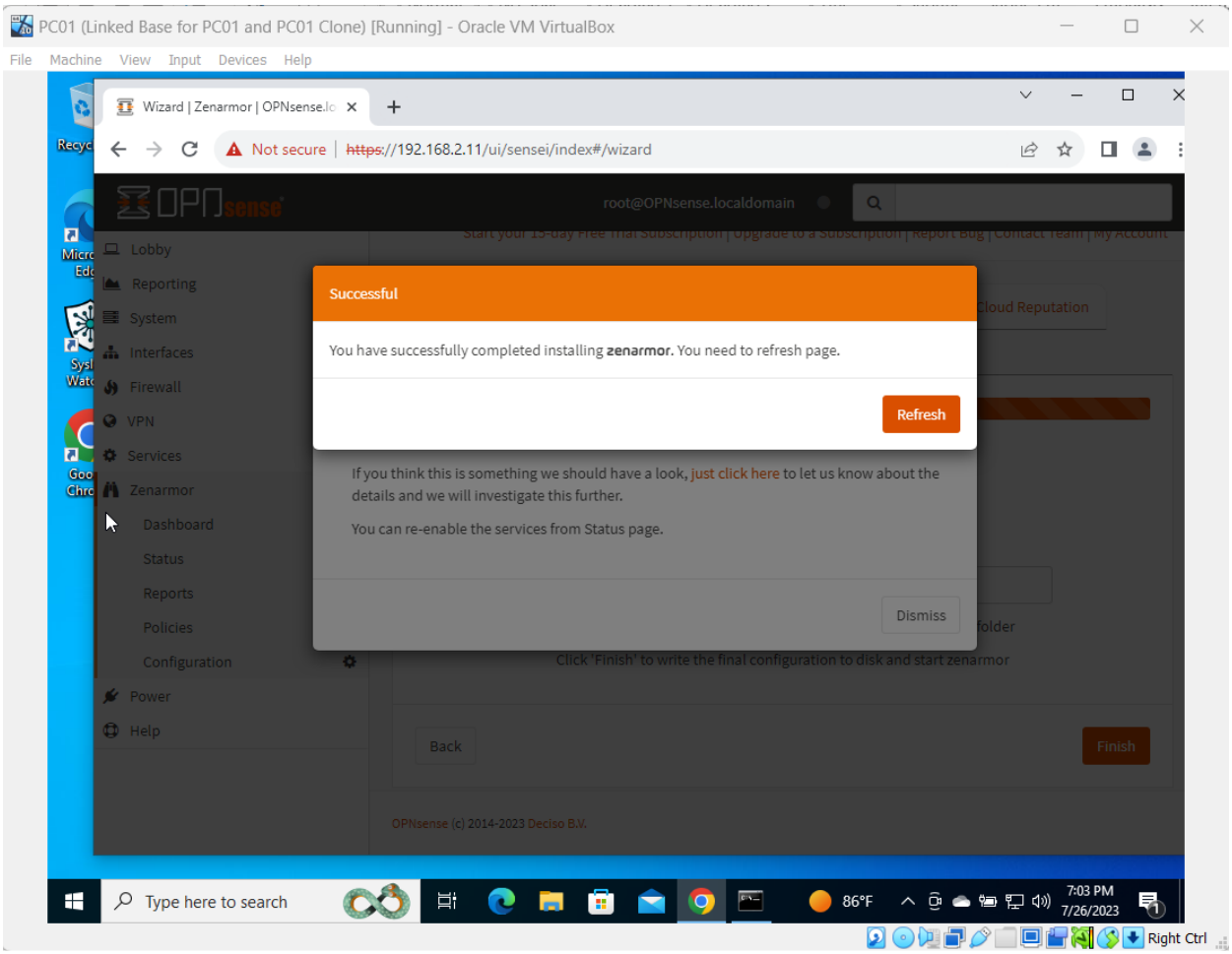

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure | https://192.168.2.11/ui/sensei/index#/wizard
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Deployment Mode
Passive Mode (Reporting Only)
Routed Mode (L3 Mode, Reporting + Blocking) with native netmap driver
Routed Mode (L3 Mode, Reporting + Blocking) with emulated netmap driver
Bridge Mode (L2 Mode, Reporting + Blocking) (Experimental)
Please see here for more information about deployment modes
Interfaces Selection
full help
Available Interfaces
LAN (em1)
GUESTNETWORK (em2)
Protected Interfaces
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
88°F
6:39 PM
7/26/2023
Right Ctrl


PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure | https://192.168.2.11/ui/sensei/index#/wizard
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Deployment Mode
Passive Mode (Reporting Only)
Routed Mode (L3 Mode, Reporting + Blocking) with native netmap driver
Routed Mode (L3 Mode, Reporting + Blocking) with emulated netmap driver
Bridge Mode (L2 Mode, Reporting + Blocking) (Experimental)
Please see here for more information about deployment modes
Interfaces Selection
full help
Available Interfaces
Protected Interfaces
LAN (em1)
GUESTNETWORK (em2)
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
87°F
6:56 PM
7/26/2023
Right Ctrl


PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Policies | Zenarmor | OPNsense.lc
Not secure | https://192.168.2.11/ui/sensei/#/policies/edit/0/apps
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Ad Tracker
Ads
Blogs
Business Tools
Cloud Services
Conferencing
Database
Email
File Transfer
Gaming
Generic TCPIP
Infrastructure Services
Instant Messaging
Media Streaming
2345 Media
360 Movies
56.com Video
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
Earn...
7:29 PM
7/26/2023
Right Ctrl


PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Policies | Zenarmor | OPNsense
Not secure https://192.168.2.11/ui/sensei/#/policies/edit/0/web
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Default
Policy Configuration
Security
App Controls
Web Controls
Exclusions
Preset profile: Permissive Moderate Control High Control Custom
Web Categories
Ad Trackers
Adult
Advertisements
Alcohol
Arts and Culture
Blogs
Business Services
Chats
Clothing and Fashion
User Defined Categories
Auto White List Hosts
Auto Block List Hosts
New Category
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
86°F
7:30 PM
7/26/2023
Right Ctrl

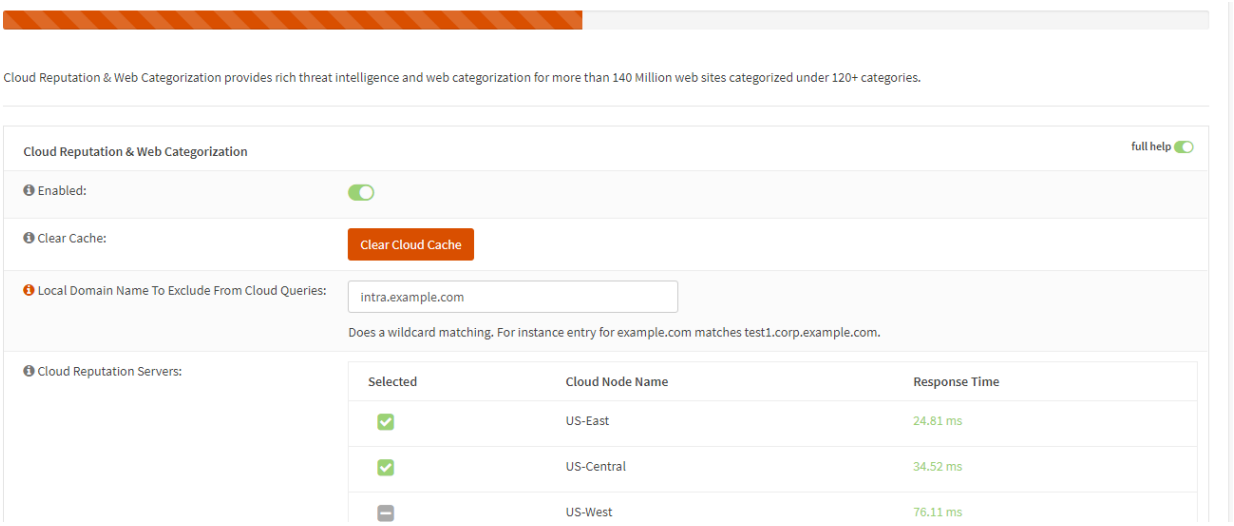

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure https://192.168.2.11/ui/sensei/index#/wizard
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Starting zenarmor packet engine...
Cloud Reputation
Almost done.
Your installation of zenarmor is almost complete.
Enter your activation key:
749234ad-120c-4c68-9116-2cb9ca454897
if you did not receive your activation key, please check your Spam folder
Click 'Finish' to write the final configuration to disk and start zenarmor
Back
Finish
OPNsense (c) 2014-2023 Deciso B.V.
Mail
Type here to search
86°F
7:02 PM
7/26/2023
Right Ctrl

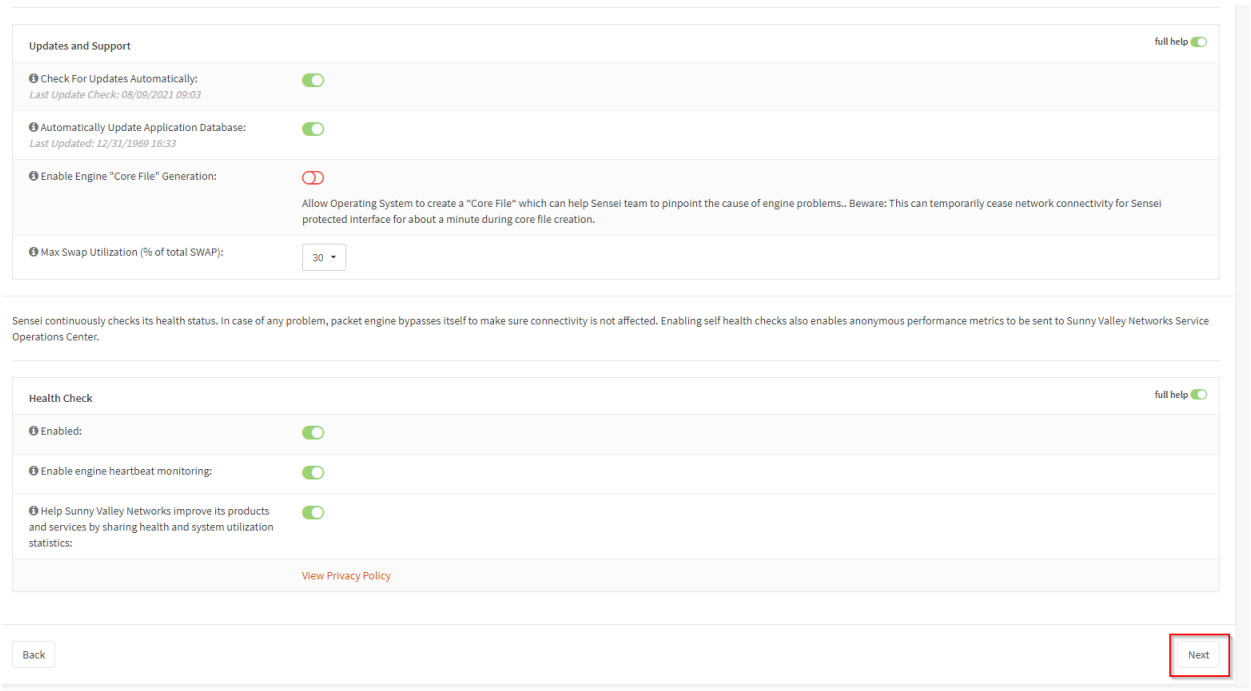


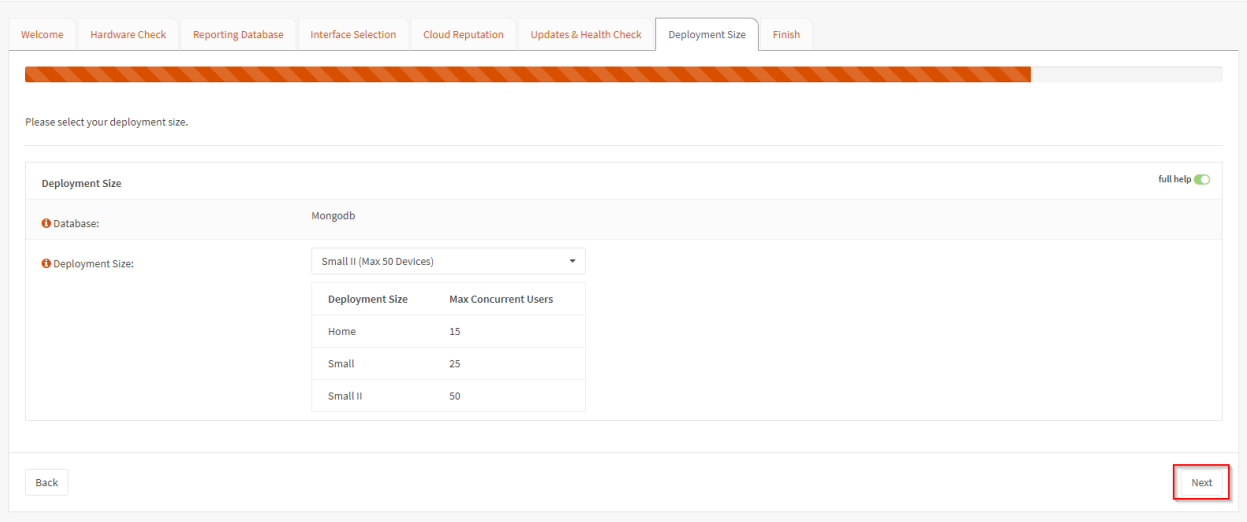

**Step 2 - Startup Configuration Wizard:**

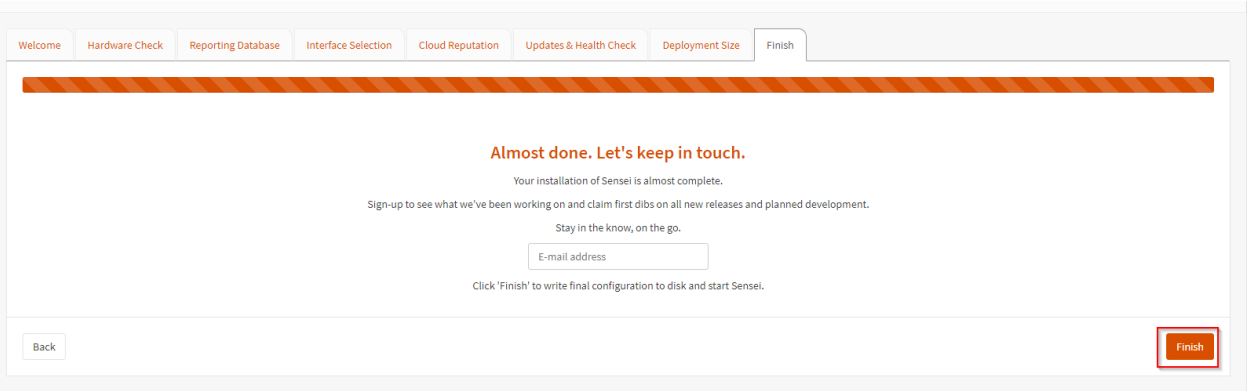
The startup configuration wizard led me through settings, deploying Sensei in Choice #2 deployment mode. I maintained default configurations, moving through the wizard, and completed the setup.

Here in the following figures, I left everything at default and clicked next for the proceeding step.


Cloud Reputation & Web Categorization provides rich threat intelligence and web categorization for more than 140 Million web sites categorized under 120+ categories.
Cloud Reputation & Web Categorization
full help
Enabled:
Clear Cache:
Clear Cloud Cache
Local Domain Name To Exclude From Cloud Queries:
intra.example.com
Does a wildcard matching. For instance entry for example.com matches test1.corp.example.com.
Cloud Reputation Servers:
Selected
Cloud Node Name
Response Time
US-East
24.81 ms
US-Central
34.52 ms
US-West
76.11 ms

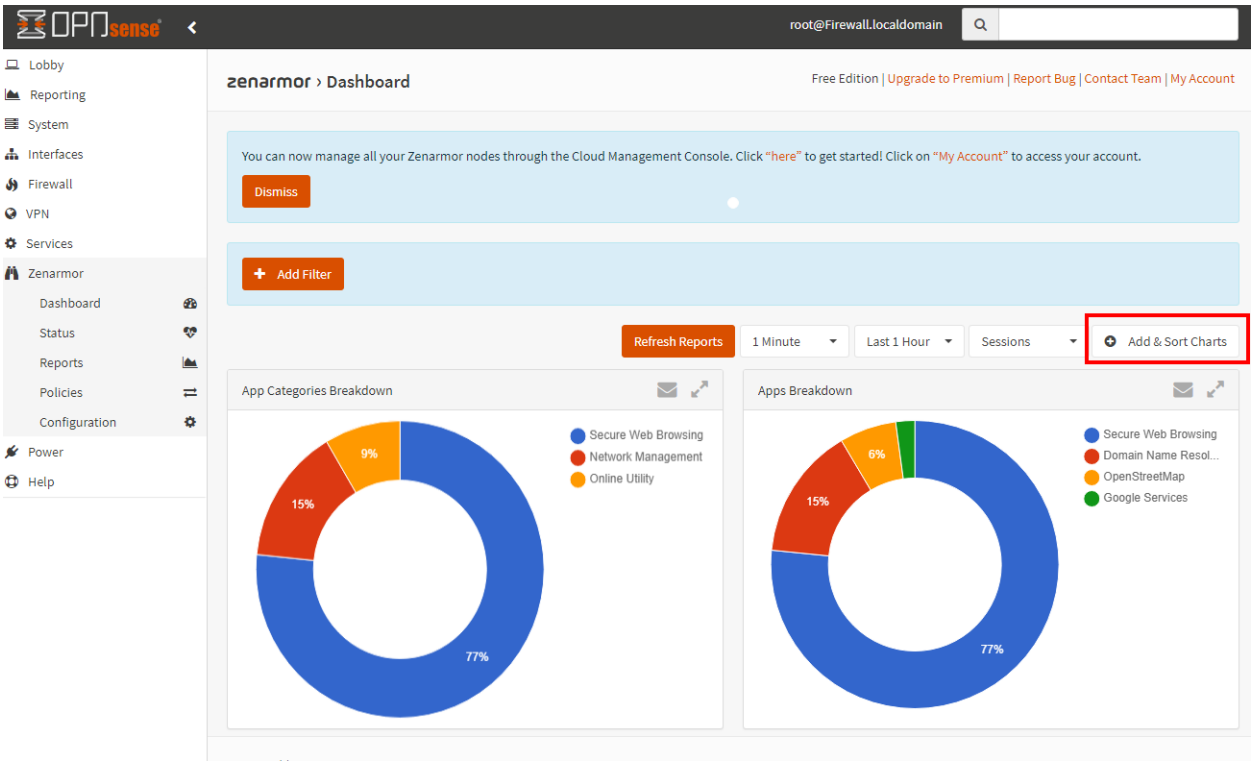

Updates and Support
full help
Check For Updates Automatically:
Last Update Check: 08/09/2021 09:03
Automatically Update Application Database:
Last Updated: 12/31/1969 16:33
Enable Engine "Core File" Generation:
Allow Operating System to create a "Core File" which can help Sensei team to pinpoint the cause of engine problems.. Beware: This can temporarily cease network connectivity for Sensei protected interface for about a minute during core file creation.
Max Swap Utilization (% of total SWAP):
30
Sensei continuously checks its health status. In case of any problem, packet engine bypasses itself to make sure connectivity is not affected. Enabling self health checks also enables anonymous performance metrics to be sent to Sunny Valley Networks Service Operations Center.
Health Check
full help
Enabled:
Enable engine heartbeat monitoring:
Help Sunny Valley Networks improve its products and services by sharing health and system utilization statistics:
View Privacy Policy
Back
Next

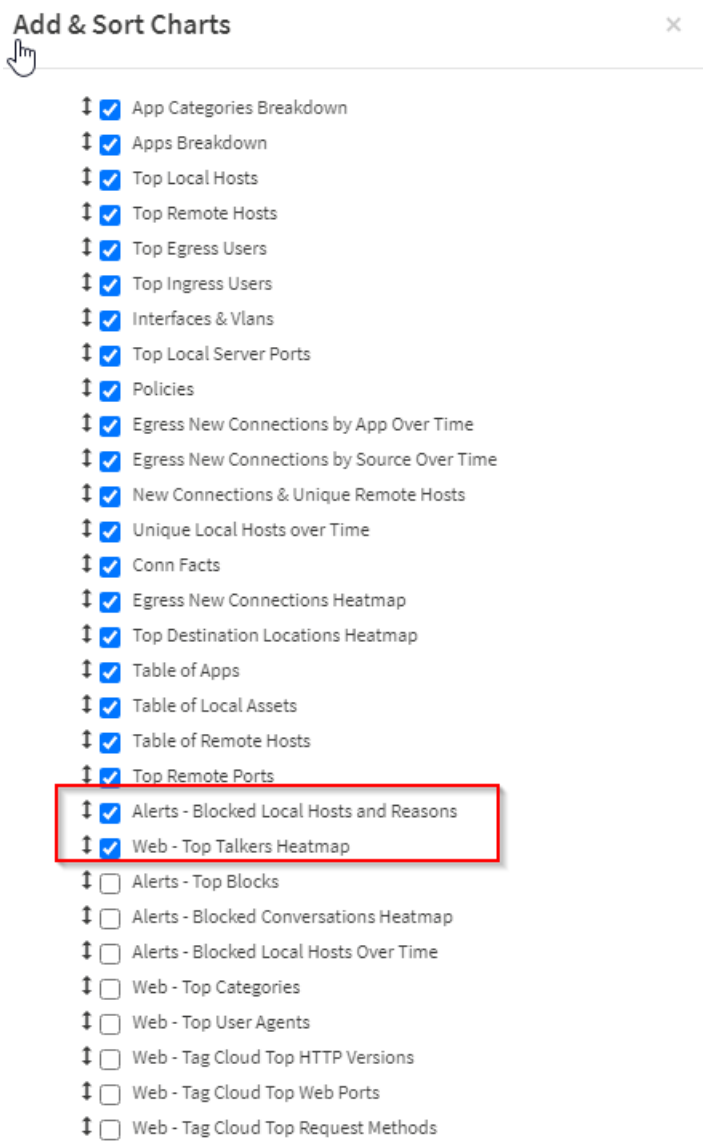



## Step 3 - Overview:

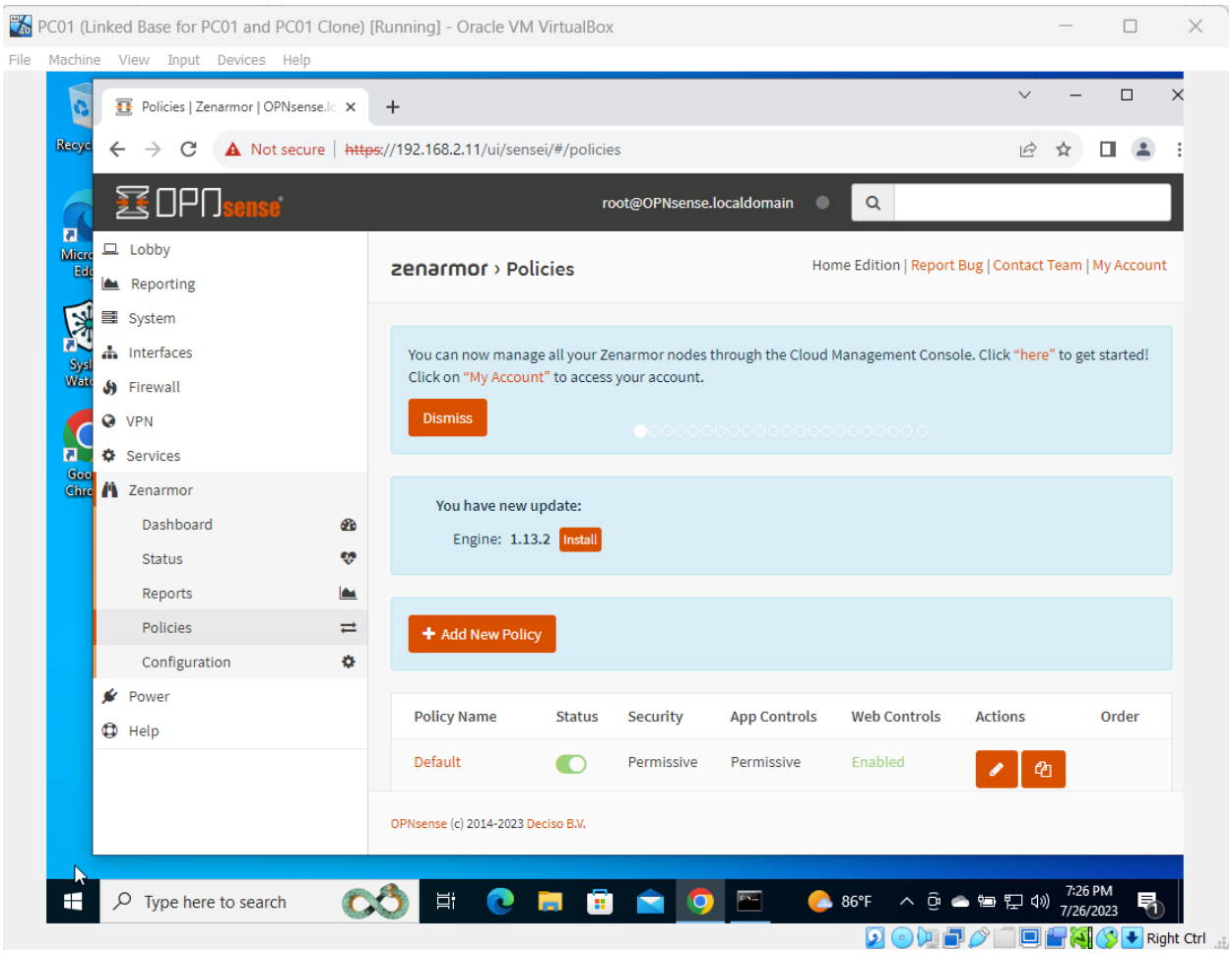
In the Zenamor dashboard, I added and sorted charts for better visualization. Navigating to the Policies tab, I accessed security options. Notably, I discovered that advanced features required a paid subscription. This is manifested in the following figures below.

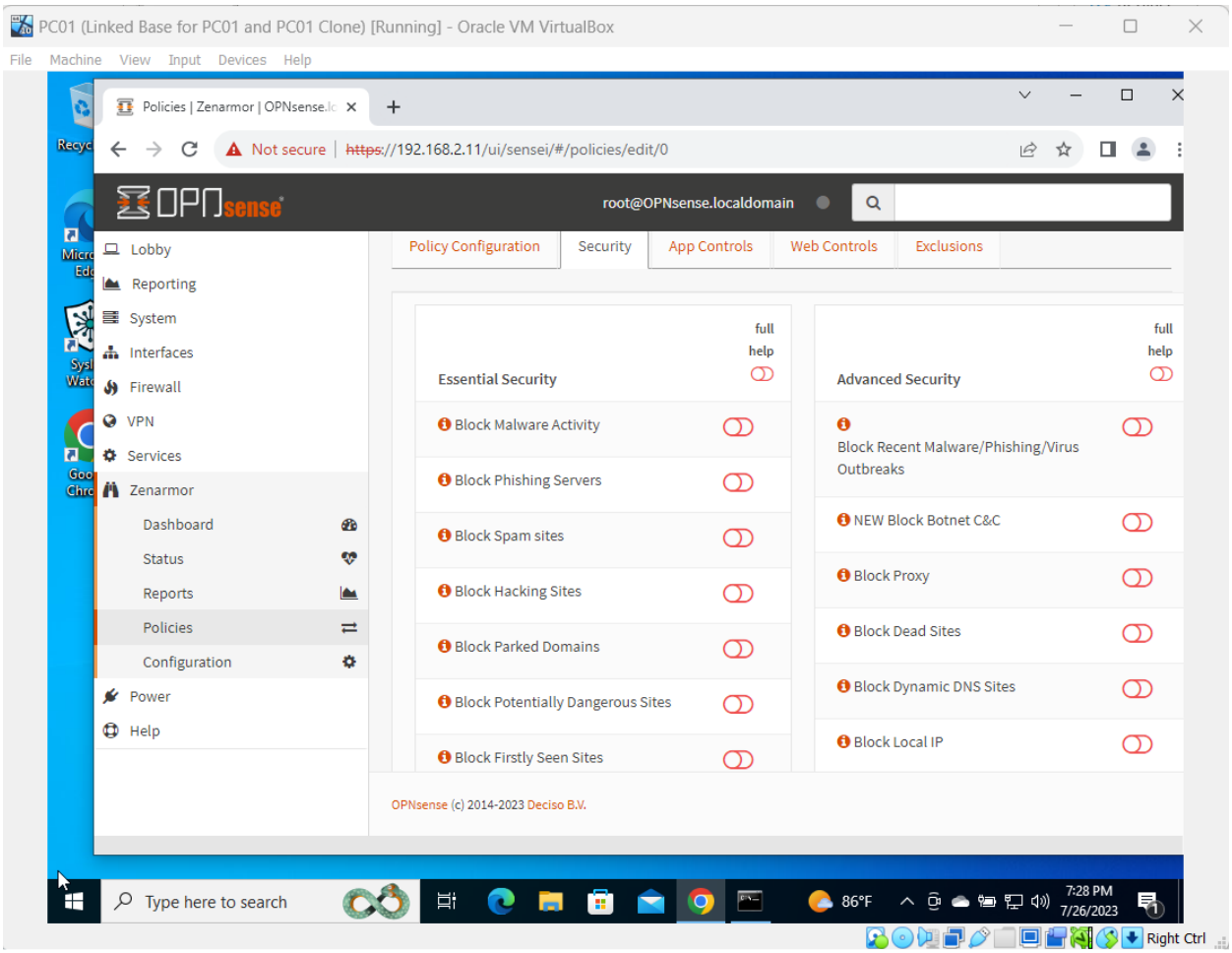

root@Firewall.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
zenarmor › Dashboard
Free Edition | Upgrade to Premium | Report Bug | Contact Team | My Account
You can now manage all your Zenarmor nodes through the Cloud Management Console. Click "here" to get started! Click on "My Account" to access your account.
Dismiss
Add Filter
Refresh Reports
1 Minute
Last 1 Hour
Sessions
Add & Sort Charts
App Categories Breakdown
Secure Web Browsing
Network Management
Online Utility
9%
15%
77%
Apps Breakdown
Secure Web Browsing
Domain Name Resol...
OpenStreetMap
Google Services
6%
15%
77%

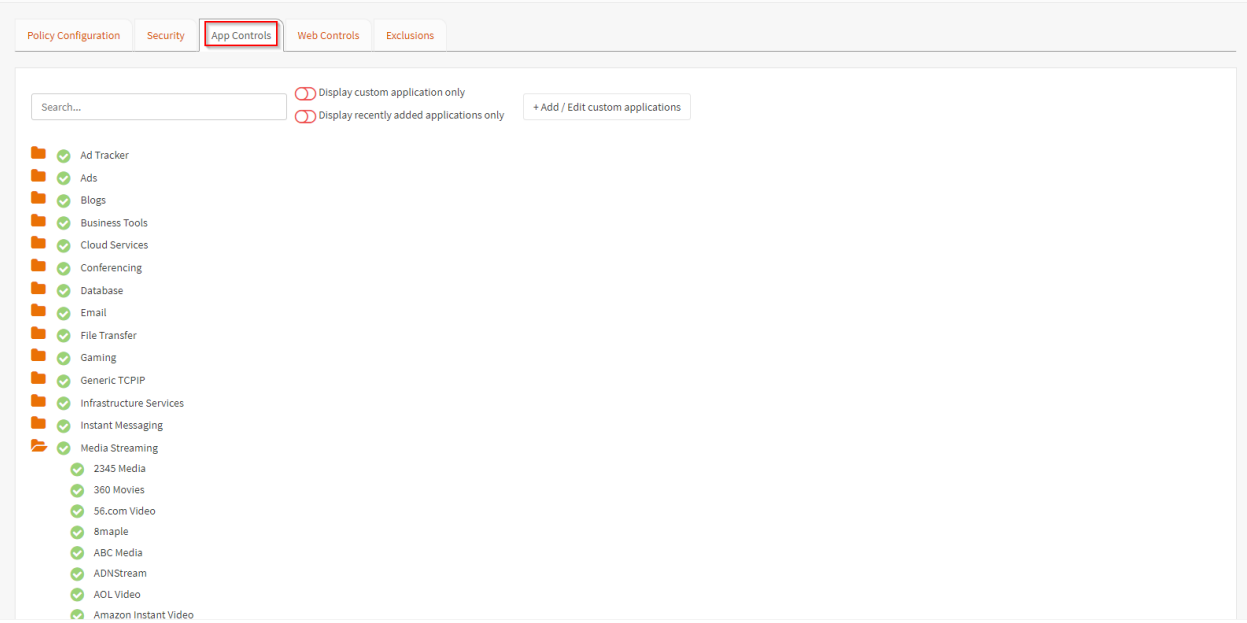


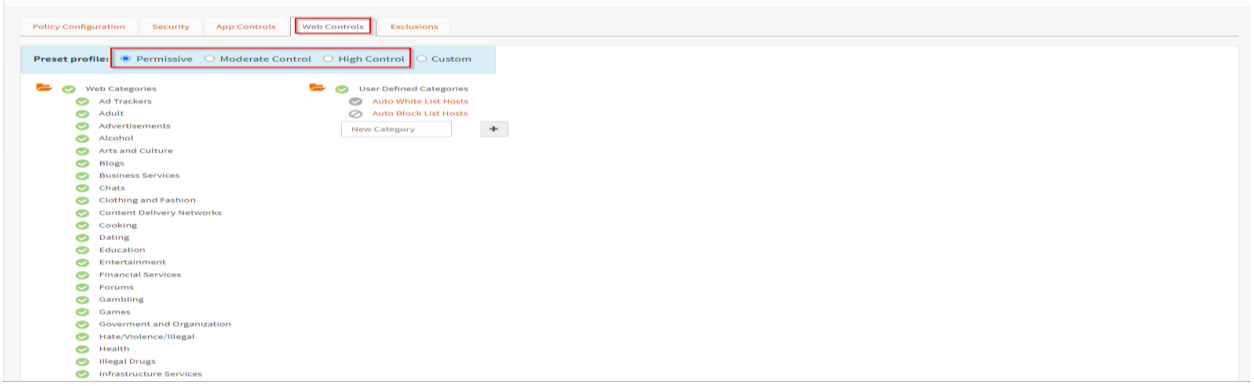

**Step 4 - Security Configuration:**

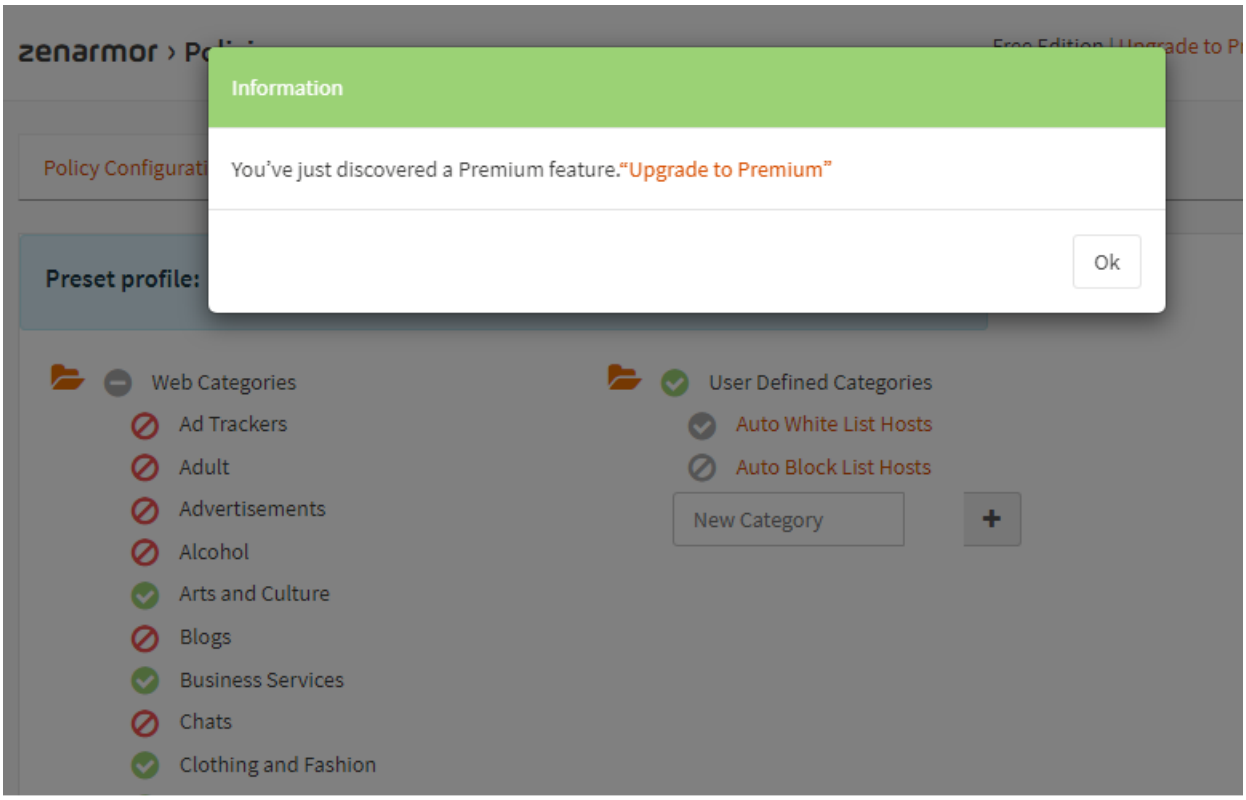
Within the Security tab, I explored various blocking options, noting that premium subscriptions were necessary for advanced security features. The App Controls section allowed me to manage application blocking. In Web Controls, I adjusted settings using a user-friendly GUI. These are manifested in the following figures below.


PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Policies | Zenarmor | OPNsense
Not secure | https://192.168.2.11/ui/sensei/#/policies
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
zenarmor › Policies
Home Edition | Report Bug | Contact Team | My Account
You can now manage all your Zenarmor nodes through the Cloud Management Console. Click "here" to get started!
Click on "My Account" to access your account.
Dismiss
You have new update:
Engine: 1.13.2 Install
+ Add New Policy
Policy Name
Status
Security
App Controls
Web Controls
Actions
Order
Default
Permissive
Permissive
Enabled
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
86°F
7:26 PM
7/26/2023
Right Ctrl


PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Policies | Zenarmor | OPNsense
Not secure | https://192.168.2.11/ui/sensei/#/policies/edit/0
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Policy Configuration
Security
App Controls
Web Controls
Exclusions
full help
Essential Security
Block Malware Activity
Block Phishing Servers
Block Spam sites
Block Hacking Sites
Block Parked Domains
Block Potentially Dangerous Sites
Block Firstly Seen Sites
full help
Advanced Security
Block Recent Malware/Phishing/Virus Outbreaks
NEW Block Botnet C&C
Block Proxy
Block Dead Sites
Block Dynamic DNS Sites
Block Local IP
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
86°F
7:28 PM
7/26/2023
Right Ctrl


Policy Configuration
Security
App Controls
Web Controls
Exclusions
Search...
Display custom application only
Display recently added applications only
+ Add / Edit custom applications
Ad Tracker
Ads
Blogs
Business Tools
Cloud Services
Conferencing
Database
Email
File Transfer
Gaming
Generic TCPIP
Infrastructure Services
Instant Messaging
Media Streaming
2345 Media
360 Movies
56.com Video
8maple
ABC Media
ADNStream
AOL Video
Amazon Instant Video


Policy Configuration
Security
App Controls
Web Controls
Exclusions
Preset profile:
Permissive
Moderate Control
High Control
Custom
Web Categories
Ad Trackers
Adult
Advertisements
Alcohol
Arts and Culture
Blogs
Business Services
Chats
Clothing and Fashion
Content Delivery Networks
Cooking
Dating
Education
Entertainment
Financial Services
Forums
Gambling
Games
Goverment and Organization
Hate/Violence/Illegal
Health
Illegal Drugs
Infrastructure Services
User Defined Categories
Auto White List Hosts
Auto Block List Hosts
New Category




**Conclusion Remark:**

This project, centered around the installation and configuration of the Sensei module within OPNsense, enriched my skills in implementing advanced firewall features. Navigating the intricacies of Sensei's interface provided valuable insights into Application Control, Network Analytics, and TLS Inspection. The hands-on experience enhanced my capabilities in managing and optimizing firewall functionalities.