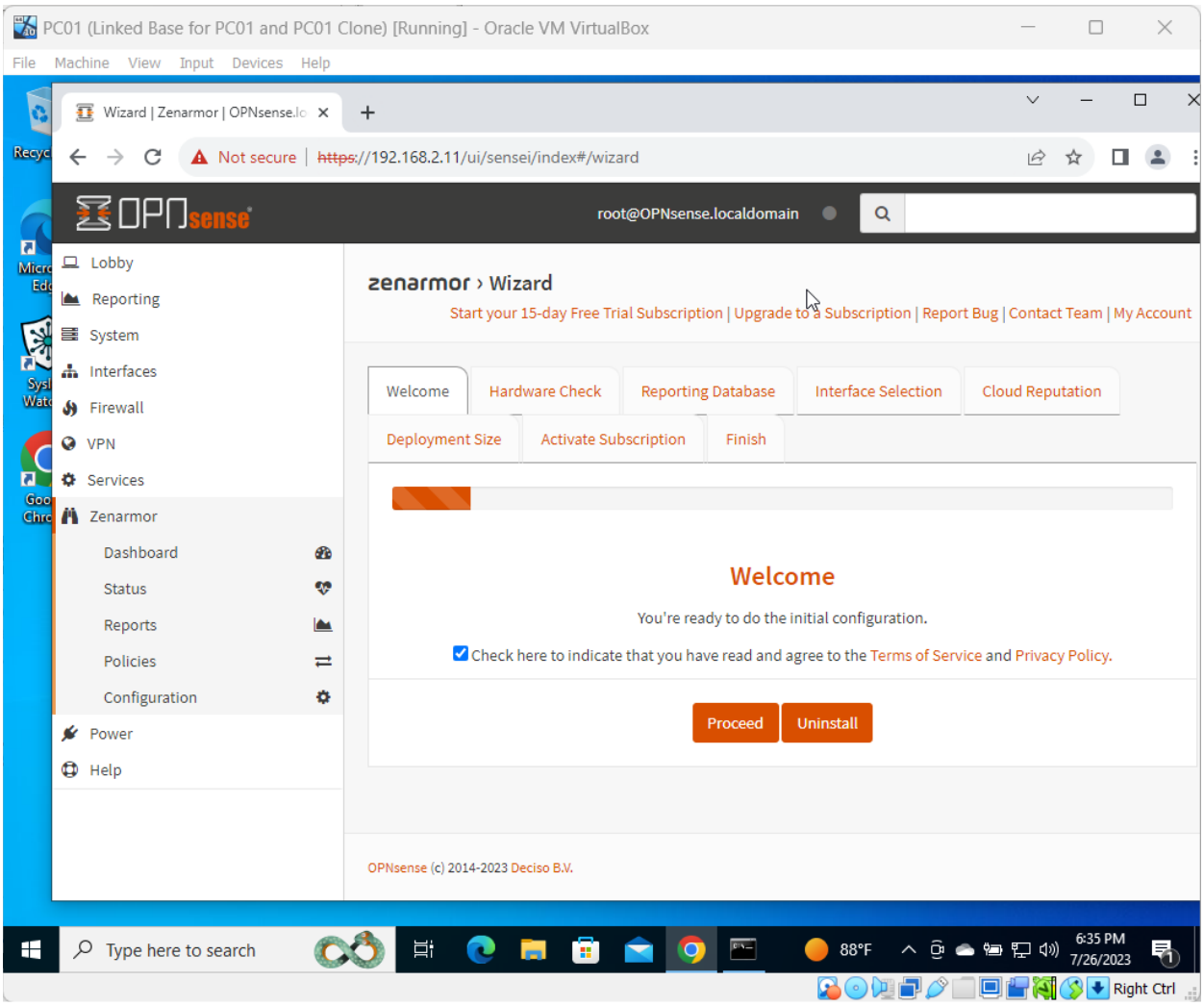
Configuring Advanced Network Security with OPNsense Sensei

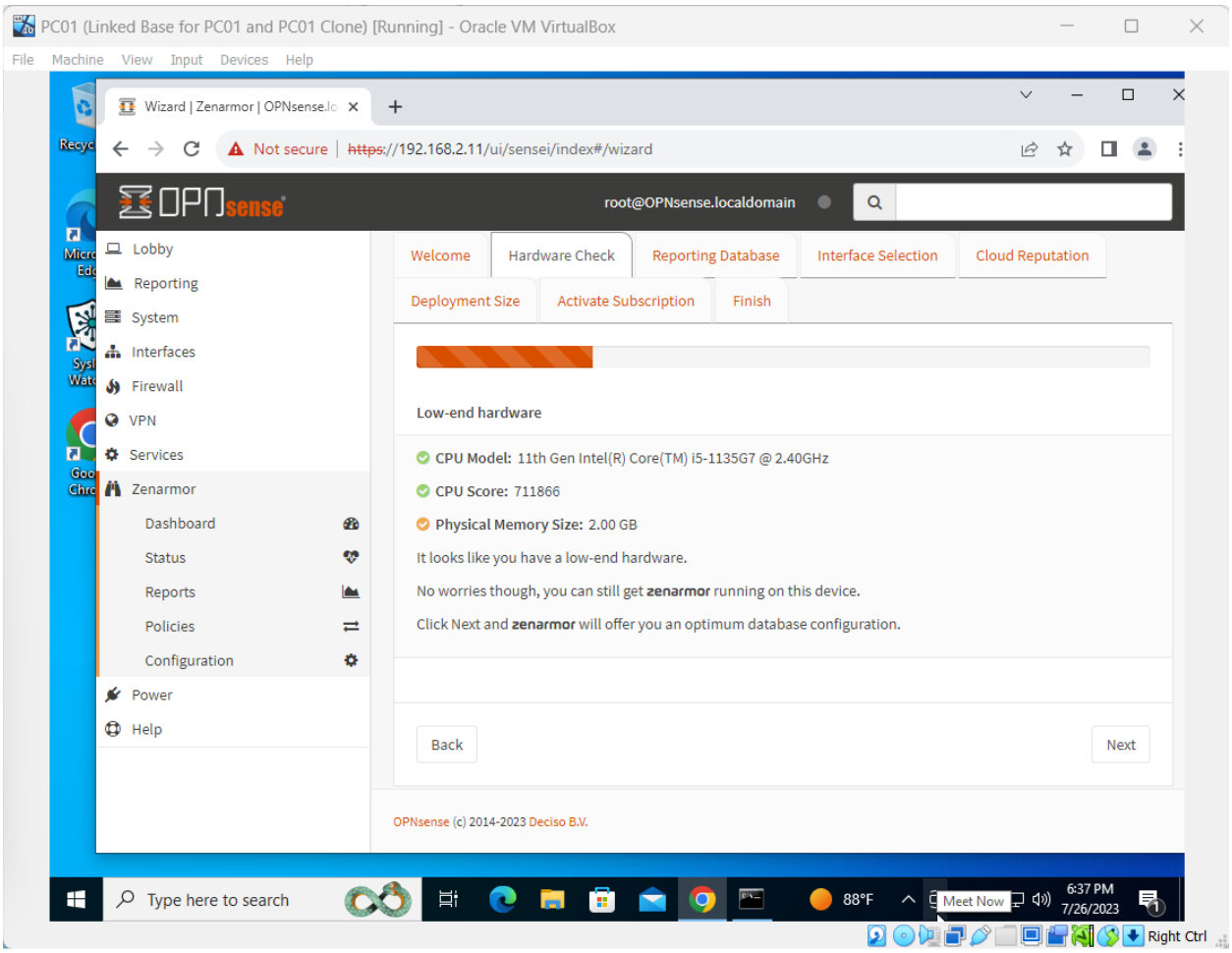
This project delves into the configuration and utilization of OPNsense Sensei, a powerful firewall module designed for advanced network security. The primary focus is on tailoring Sensei to monitor and control the Guest Network, encompassing tasks such as interface configuration, rule establishment, and security posture adjustments. The subsequent steps provide a detailed exploration of each facet, combining practical application with meticulous documentation through screenshots. This hands-on experience aims to enhance proficiency in leveraging advanced firewall features for targeted network management.

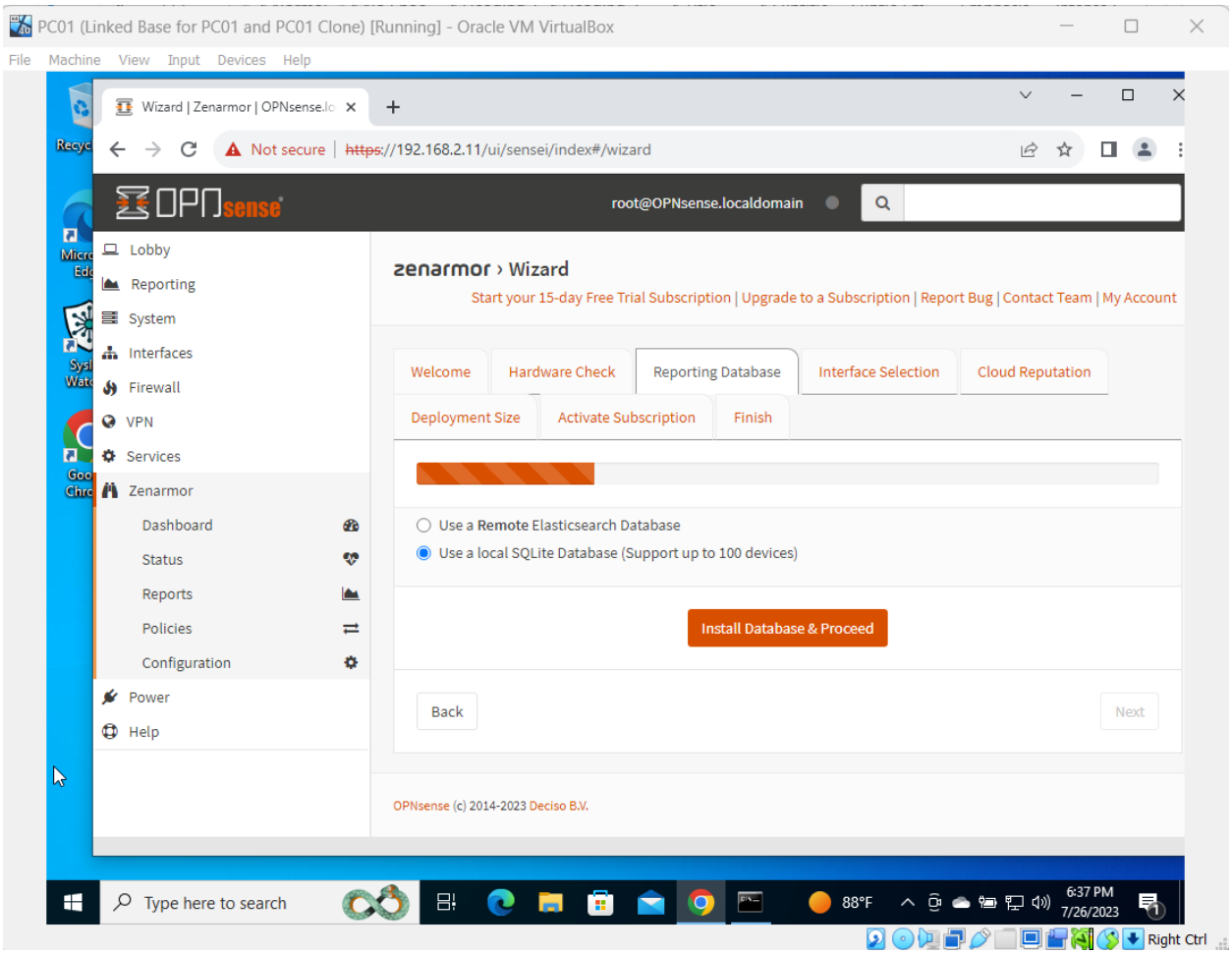
Task 1: Sensei Configuration for Guest Network Monitoring

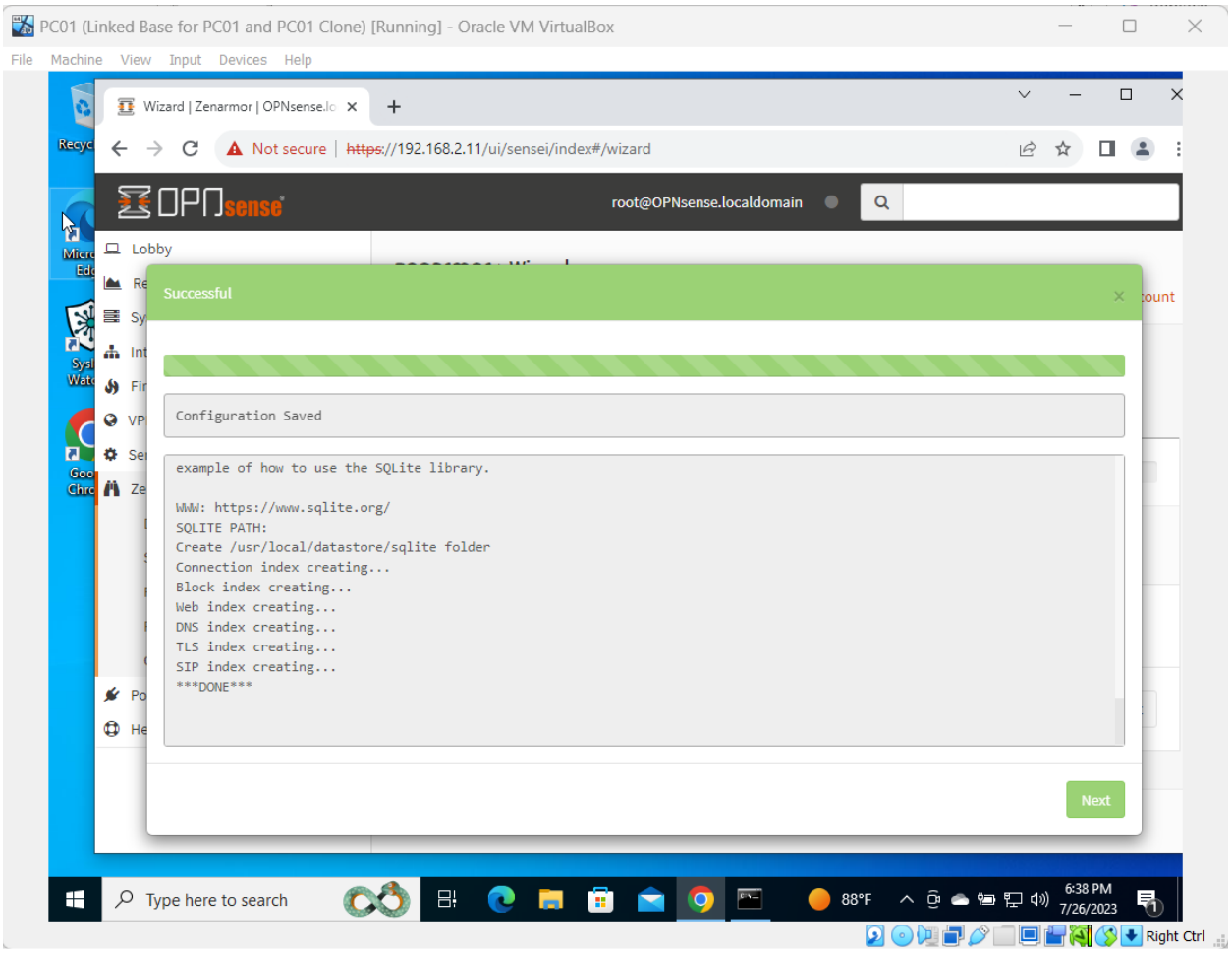
- **Navigation to Sensei Configuration:**
    - I initiated the configuration process by navigating to the Sensei module within the OPNsense firewall.
- **Guest Network Selection:**
    - The first task involved selecting the Guest Network as the exclusive network for monitoring by Sensei.
- **Implementation of Configuration Changes:**
    - After selecting the Guest Network, I implemented the necessary configuration changes to ensure Sensei focused on monitoring this specific network.

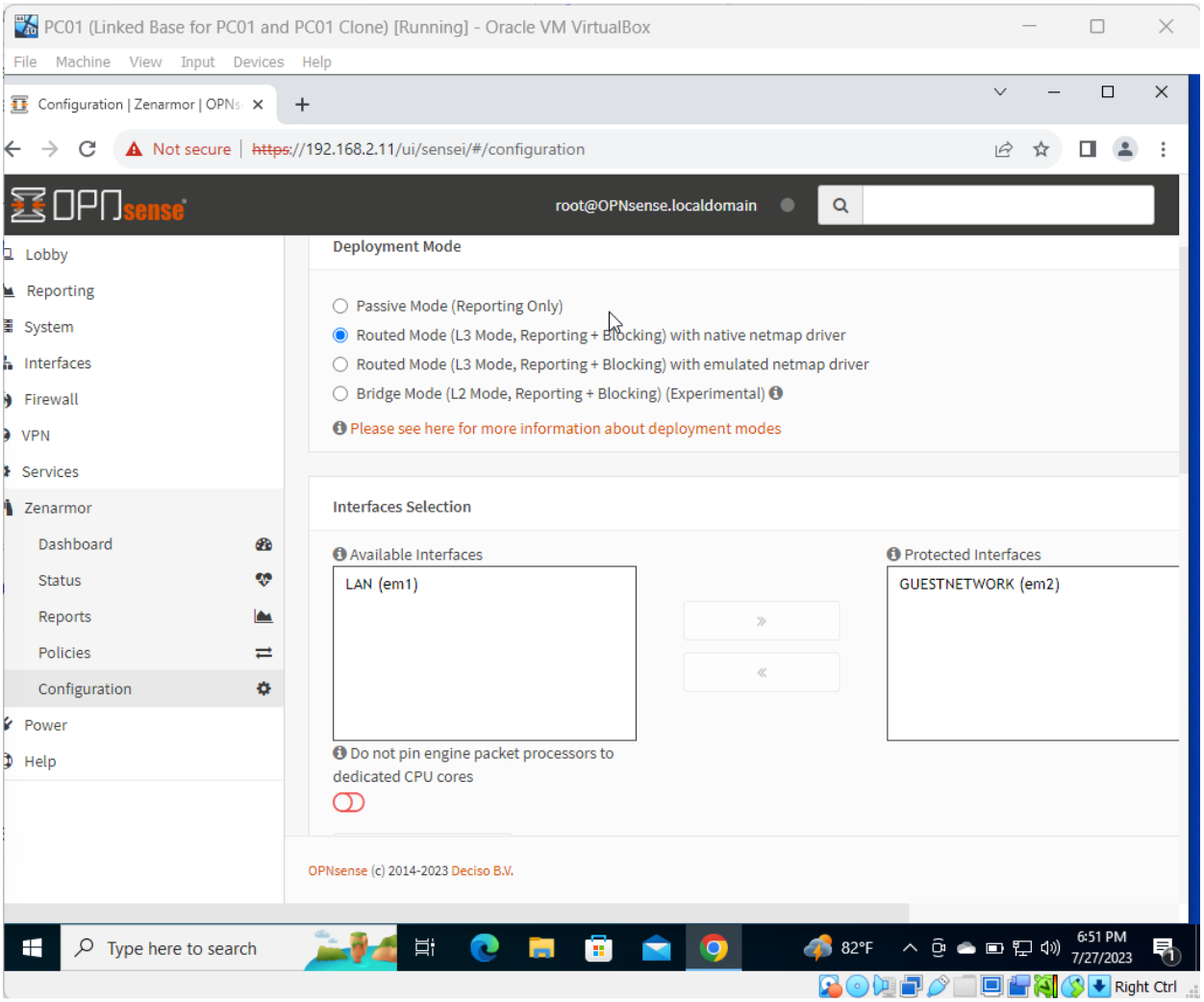
The following figures shows the initial configuration of Opnsense Sensei to monitor the Guest Network interface:


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

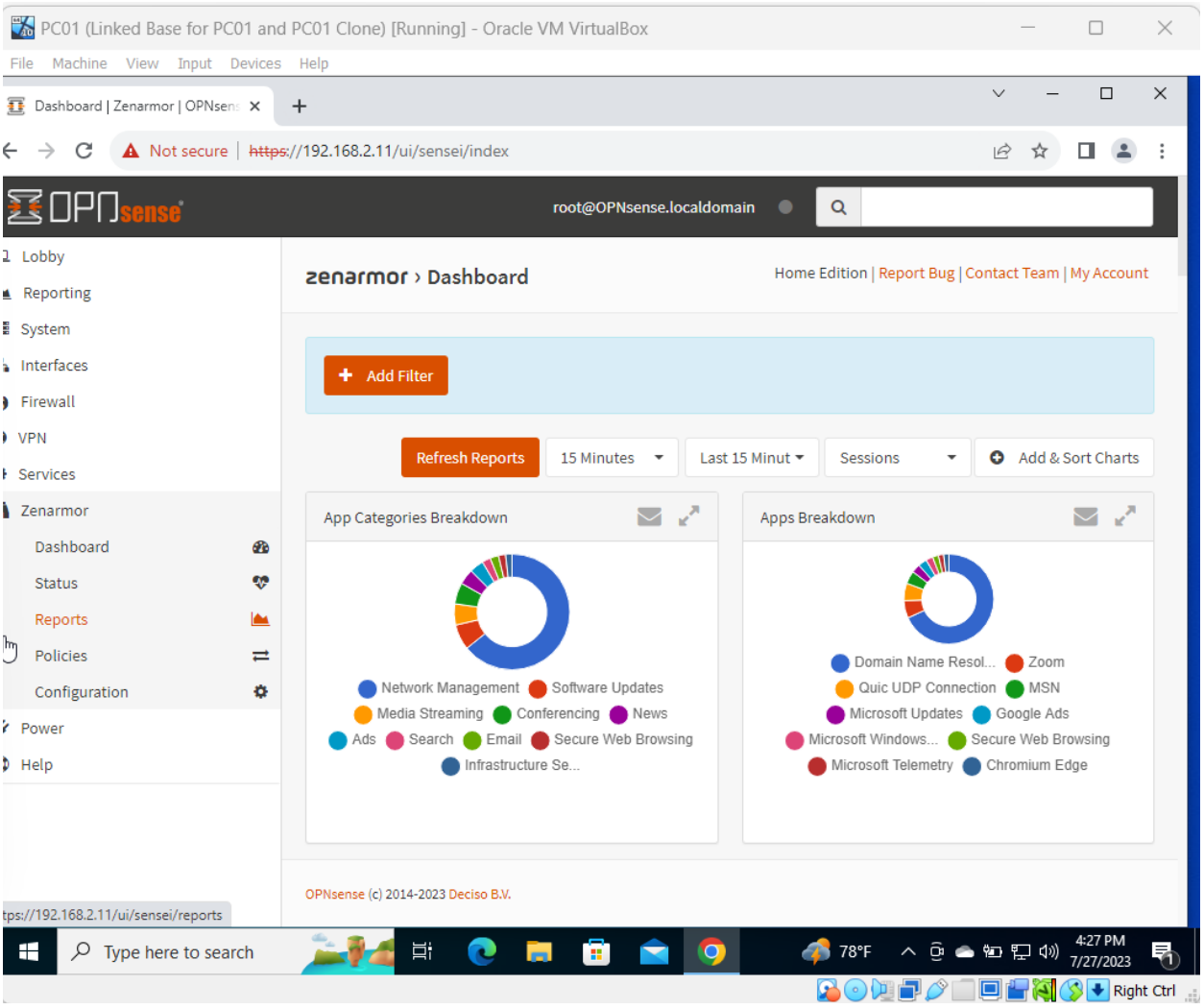

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wizard | Zenarmor | OPNsense.lo
Not secure | https://192.168.2.11/ui/sensei/index#/wizard
root@OPNsense.localdomain
Lobby
Successful
Configuration Saved
example of how to use the SQLite library.
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

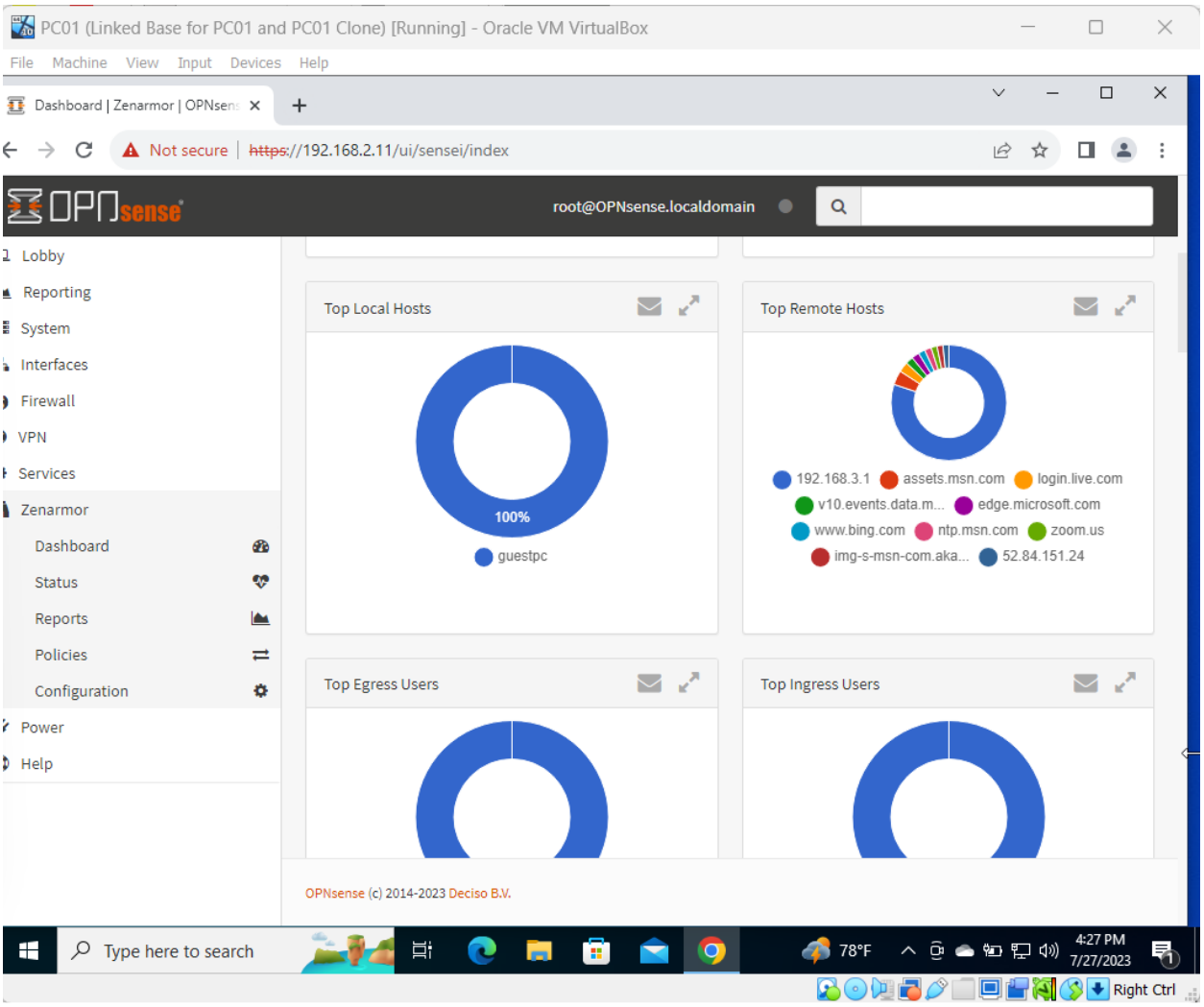


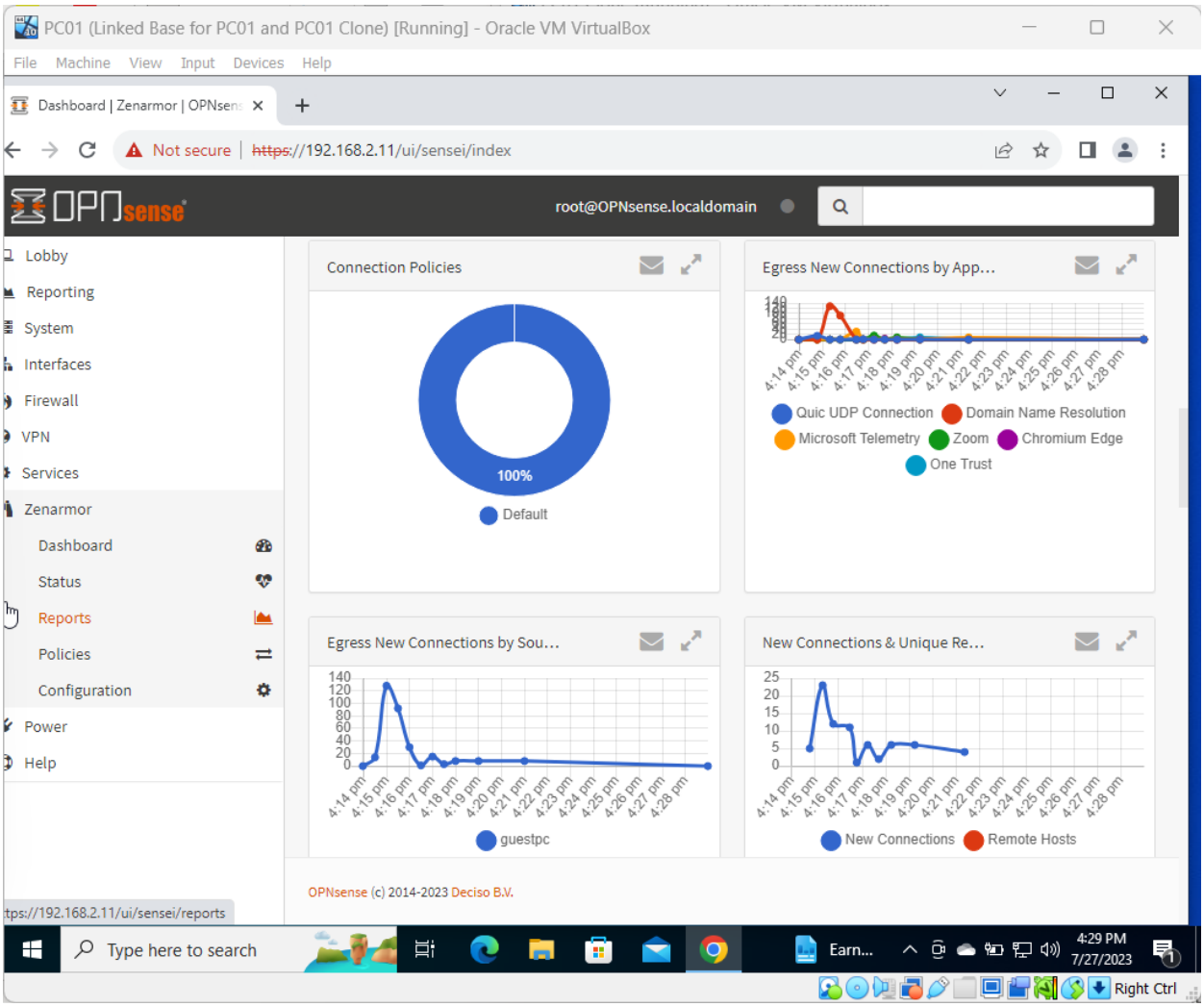
Task 2: Dashboard Verification

- **Access to Sensei Dashboard:**
  - I accessed the Sensei dashboard to review and verify the applied changes.
- **Confirmation of Guest Network Display:**
  - To ensure that only the Guest Network interface was being monitored, I inspected the dashboard, confirming the accuracy of the applied settings.

The following figures illustrates the Dashboards showing the GuestNetwork interface being monitored:

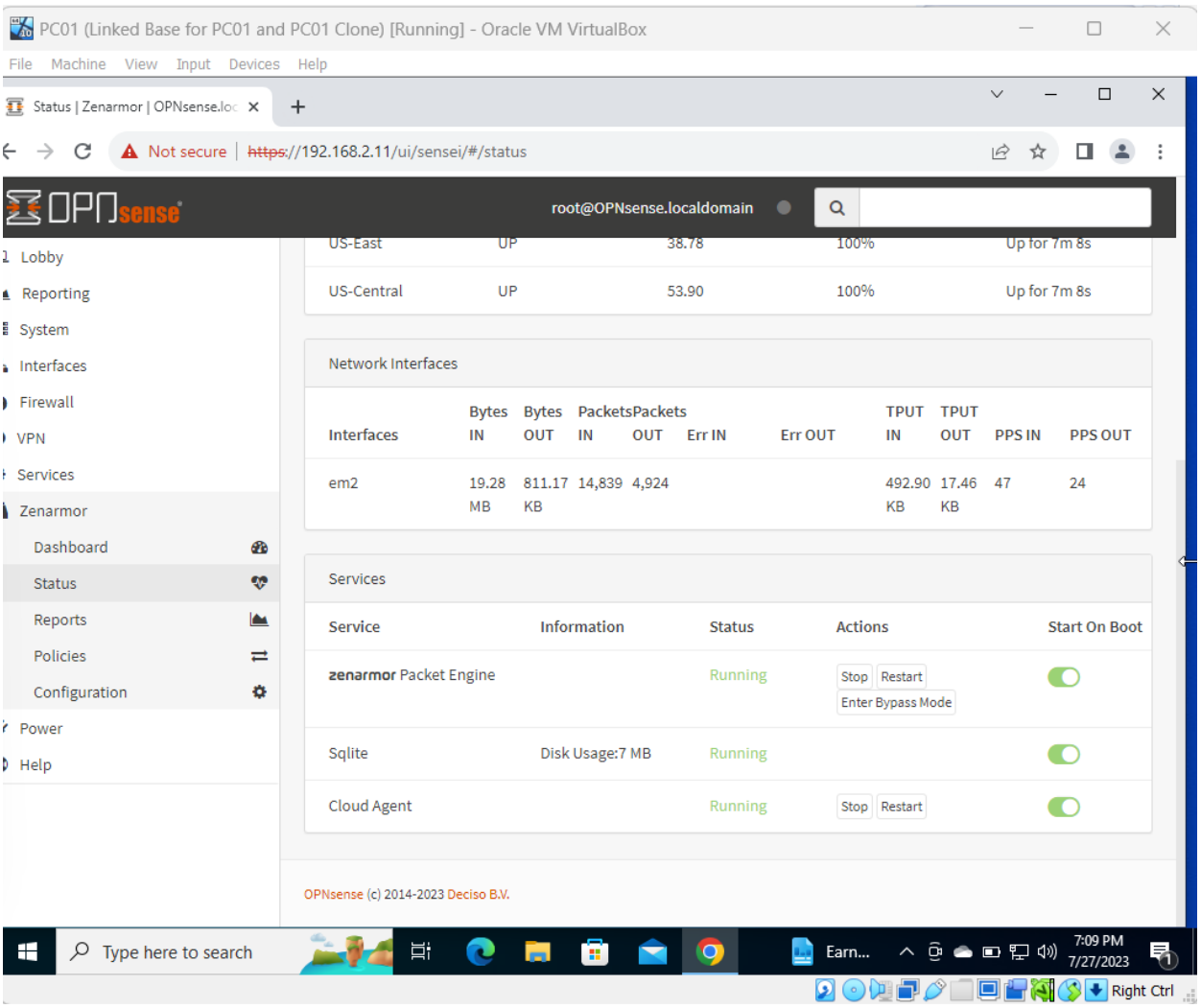

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dashboard | Zenarmor | OPNsens
Not secure | https://192.168.2.11/ui/sensei/index
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
zenarmor › Dashboard
Home Edition | Report Bug | Contact Team | My Account
Add Filter
Refresh Reports
15 Minutes
Last 15 Minut
Sessions
Add & Sort Charts
App Categories Breakdown
Network Management
Software Updates
Media Streaming
Conferencing
News
Ads
Search
Email
Secure Web Browsing
Infrastructure Se...
Apps Breakdown
Domain Name Resol...
Zoom
Quic UDP Connection
MSN
Microsoft Updates
Google Ads
Microsoft Windows...
Secure Web Browsing
Microsoft Telemetry
Chromium Edge
OPNsense (c) 2014-2023 Deciso B.V.
tps://192.168.2.11/ui/sensei/reports
Type here to search
78°F
4:27 PM
7/27/2023
Right Ctrl


PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dashboard | Zenarmor | OPNsens
Not secure | https://192.168.2.11/ui/sensei/index
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Top Local Hosts
100%
guestpc
Top Remote Hosts
192.168.3.1
assets.msn.com
login.live.com
v10.events.data.m...
edge.microsoft.com
www.bing.com
ntp.msn.com
zoom.us
img-s-msn-com.aka...
52.84.151.24
Top Egress Users
Top Ingress Users
OPNsense (c) 2014-2023 Deciso B.V.
Type here to search
78°F
4:27 PM
7/27/2023
Right Ctrl



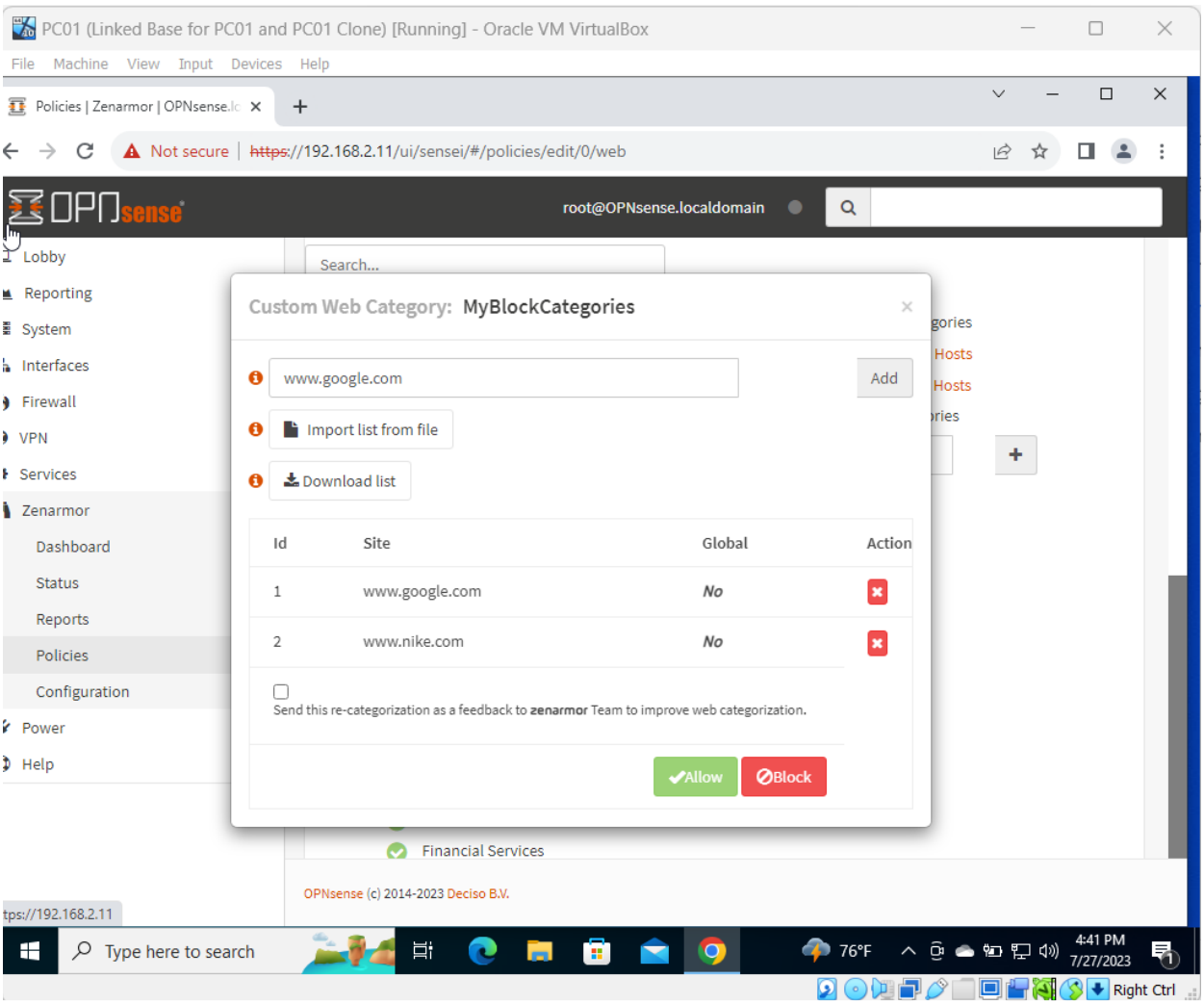
Task 3: Interface Monitoring Confirmation

- **Navigation to Interface Settings:**
  - I went into the interface settings within Sensei to validate the configuration and confirm the monitoring of the Guest Network.
- **Verification of Guest Network Display:**
  - Within the interface settings, I verified that the Guest Network interface was visibly monitored, ensuring Sensei was accurately configured. This is illustrated in the following screenshot taken from the project.

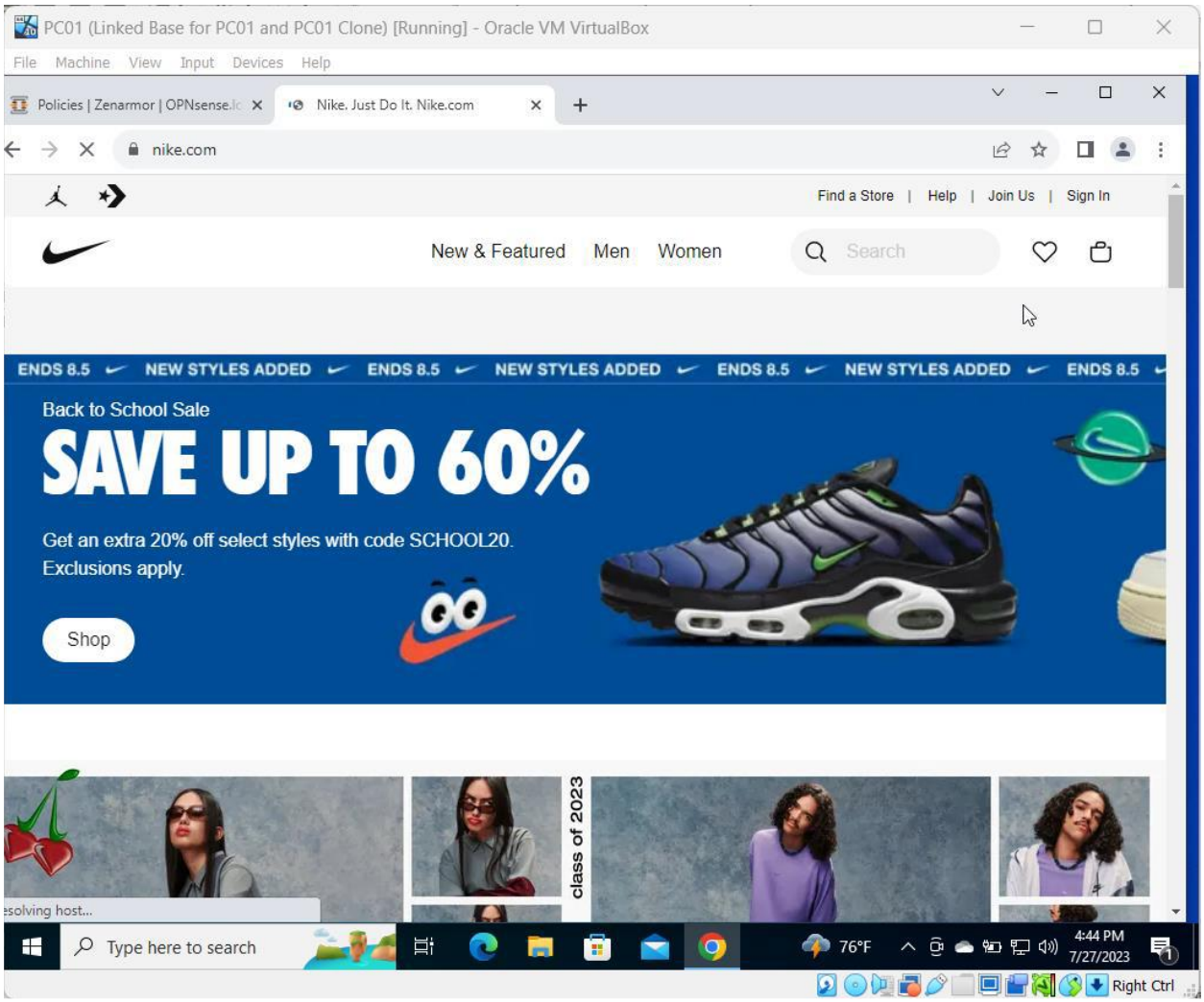


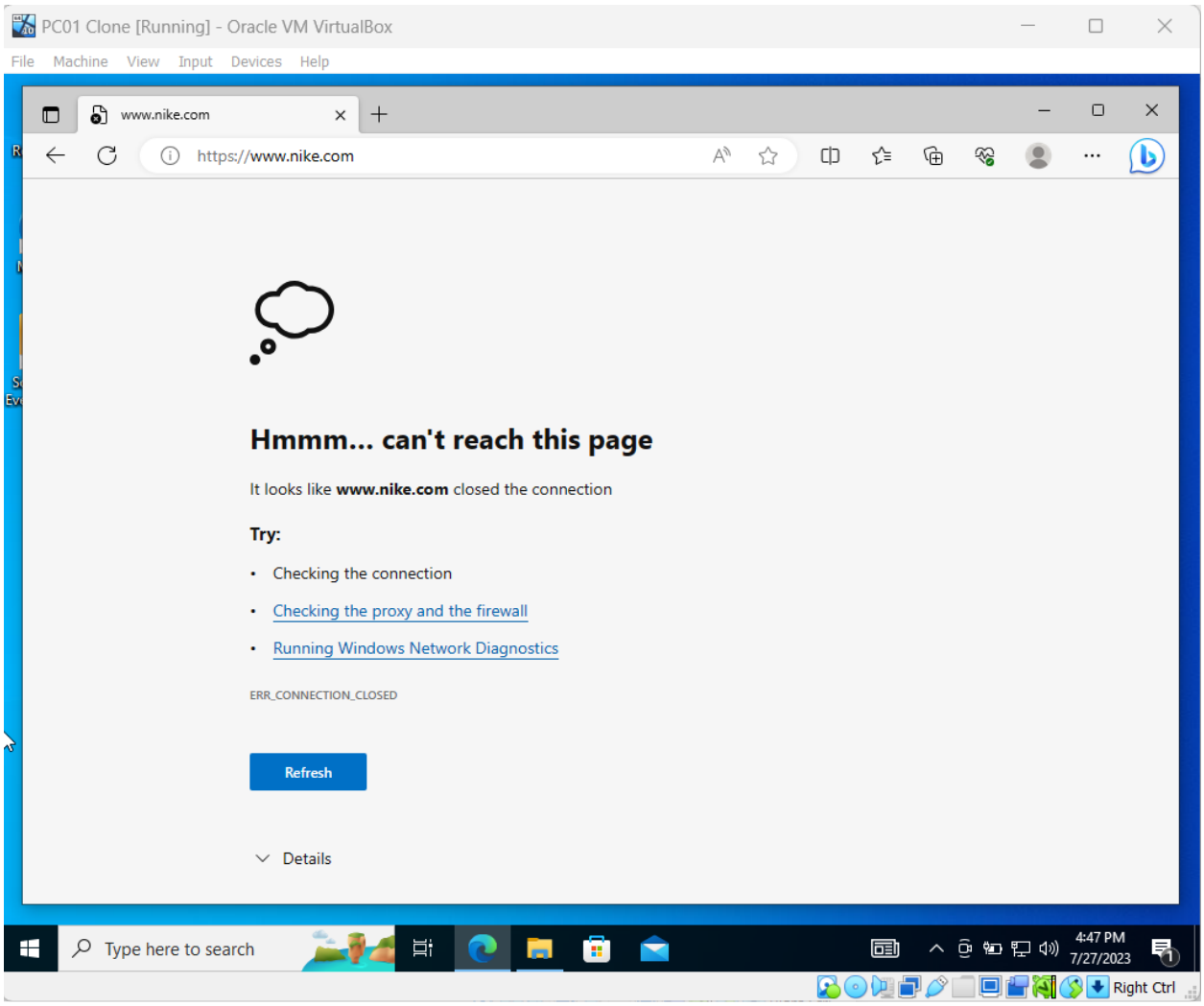
Task 4: Rule Configuration for Google and Nike Access

- **Creation of Rule in Sensei:**
  - I created a specific rule in Sensei allowing the Guest Network to access Google while preventing access to nike.com as illustrated in the following figure.

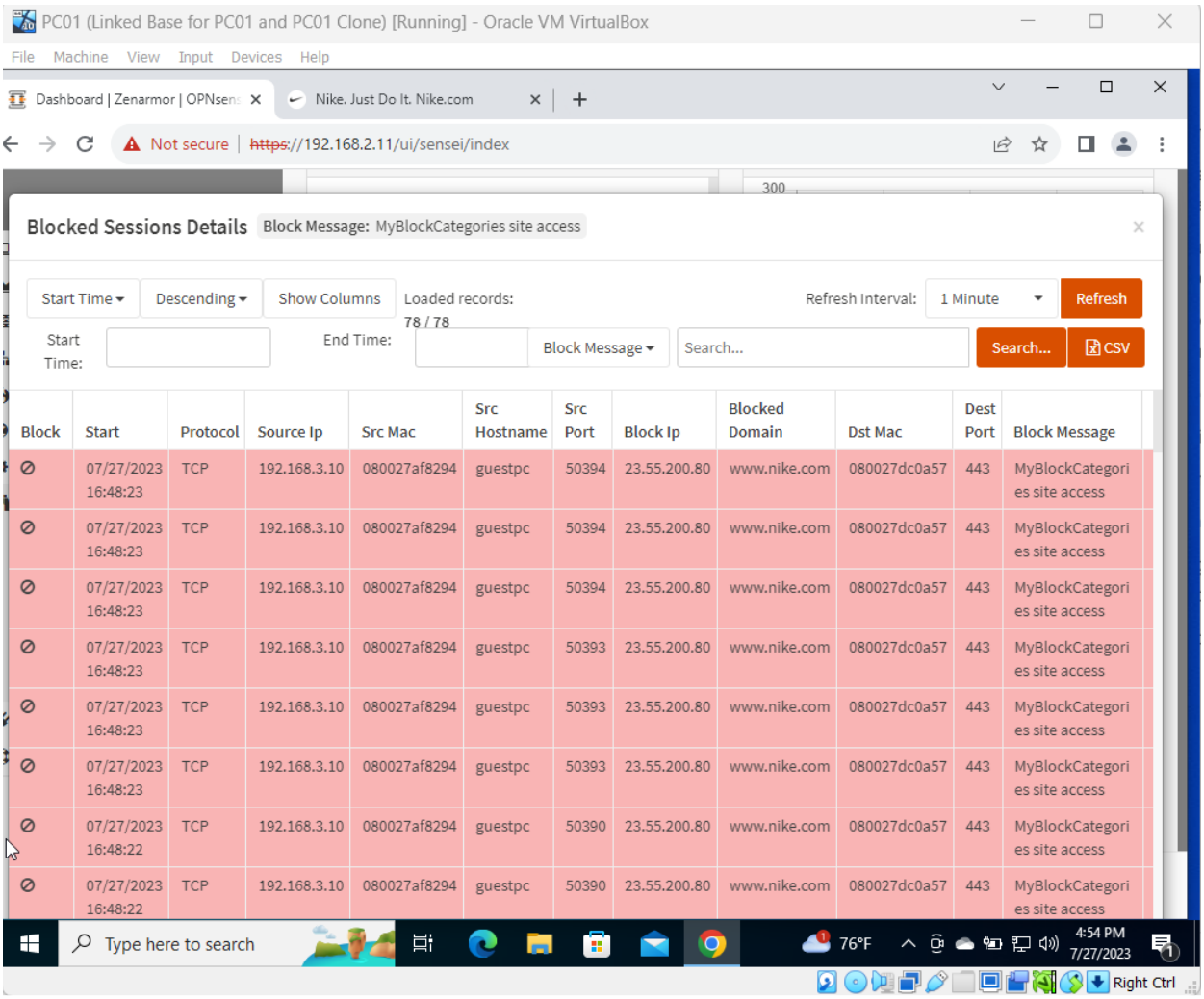


- **Access Verification:**
    - Screenshots were taken to demonstrate the effectiveness of the rule, including PC1 successfully accessing nike.com and PC2 being restricted from accessing nike.com.


PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Policies | Zenarmor | OPNsense.lc
Nike. Just Do It. Nike.com
nike.com
Find a Store | Help | Join Us | Sign In
New & Featured Men Women
Search
ENDS 8.5 NEW STYLES ADDED ENDS 8.5 NEW STYLES ADDED ENDS 8.5 NEW STYLES ADDED ENDS 8.5
Back to School Sale
SAVE UP TO 60%
Get an extra 20% off select styles with code SCHOOL20.
Exclusions apply.
Shop
class of 2023
Type here to search
76°F
4:44 PM
7/27/2023
Right Ctrl

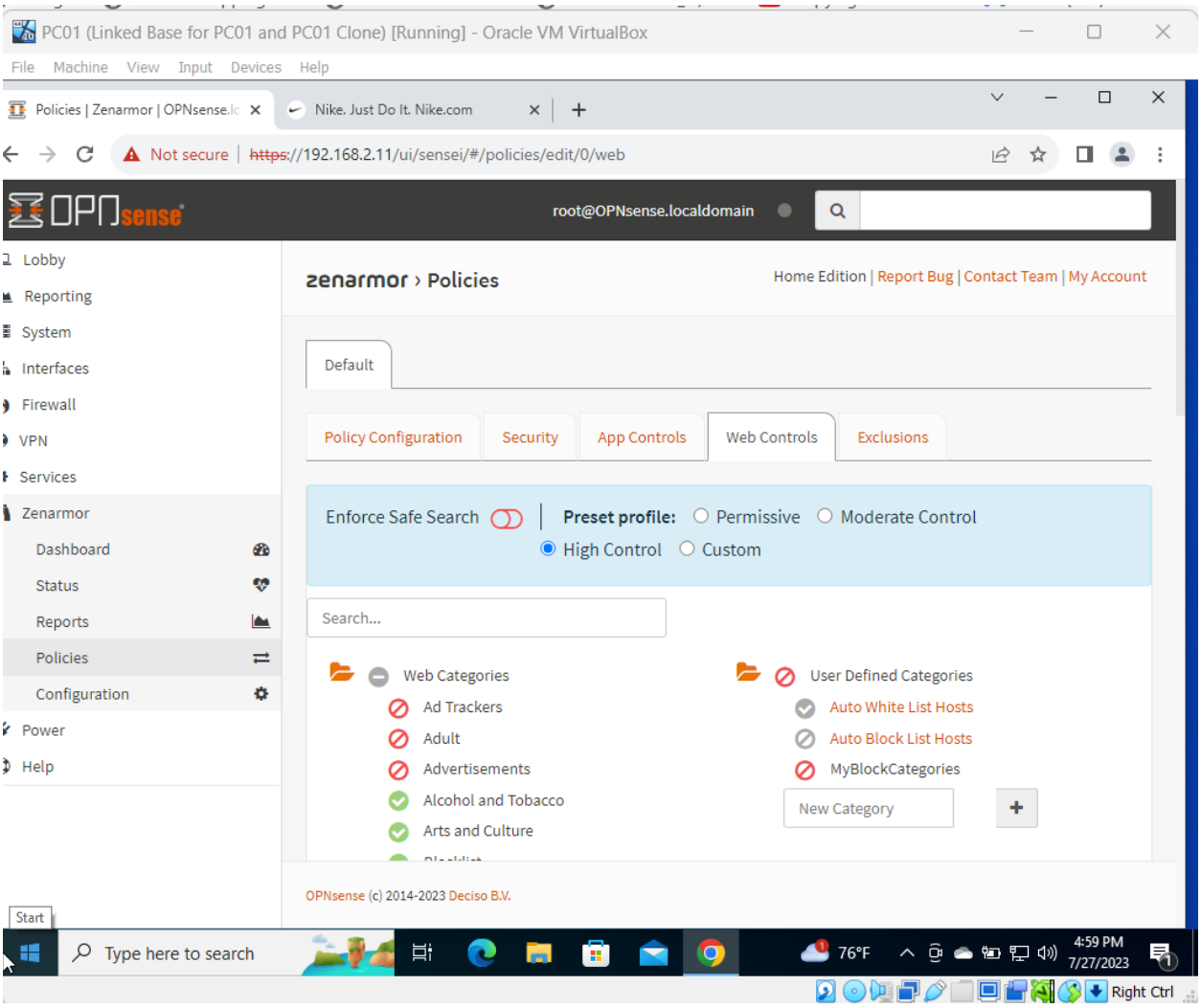


- **Logging Rule Activities:**
    - I captured screenshots of the log file and block report in Sensei to document the activities and outcomes of the configured rule.



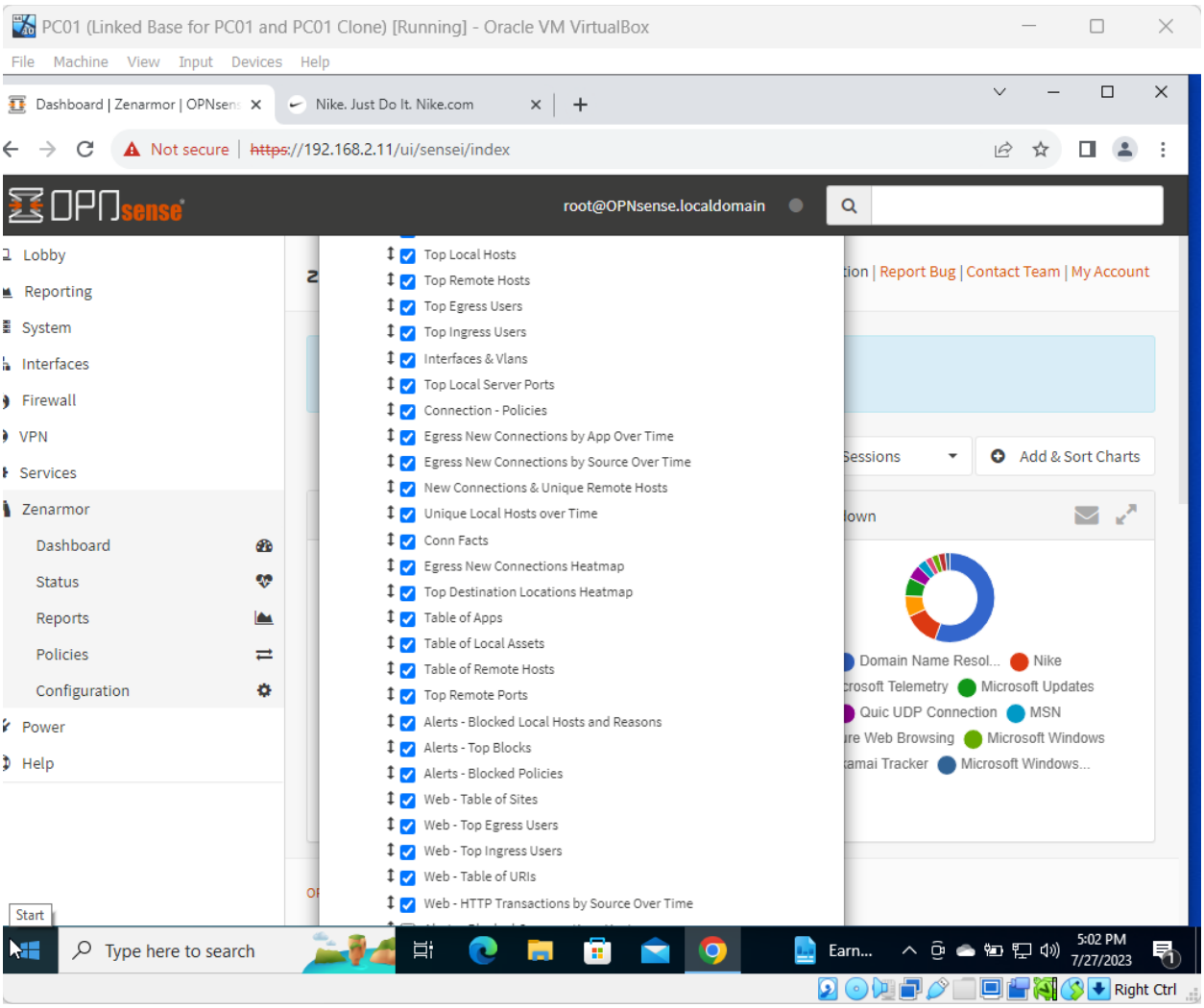
Task 5: Web Filter Security Posture Modification

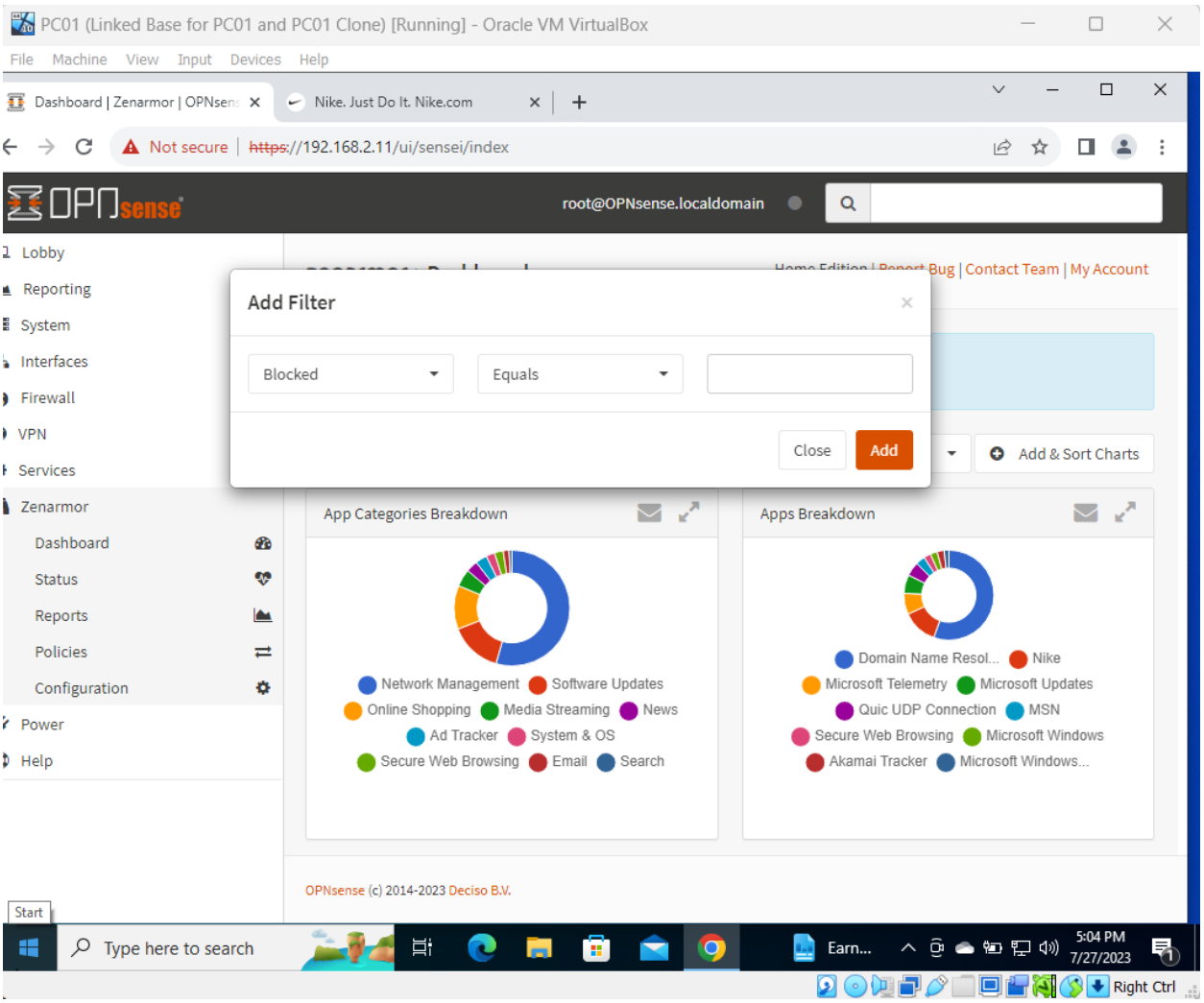
- **Modification of Web Filter Security Posture:**
  - I adjusted the security posture of the Web Filter within Sensei from Permissive to High Control.



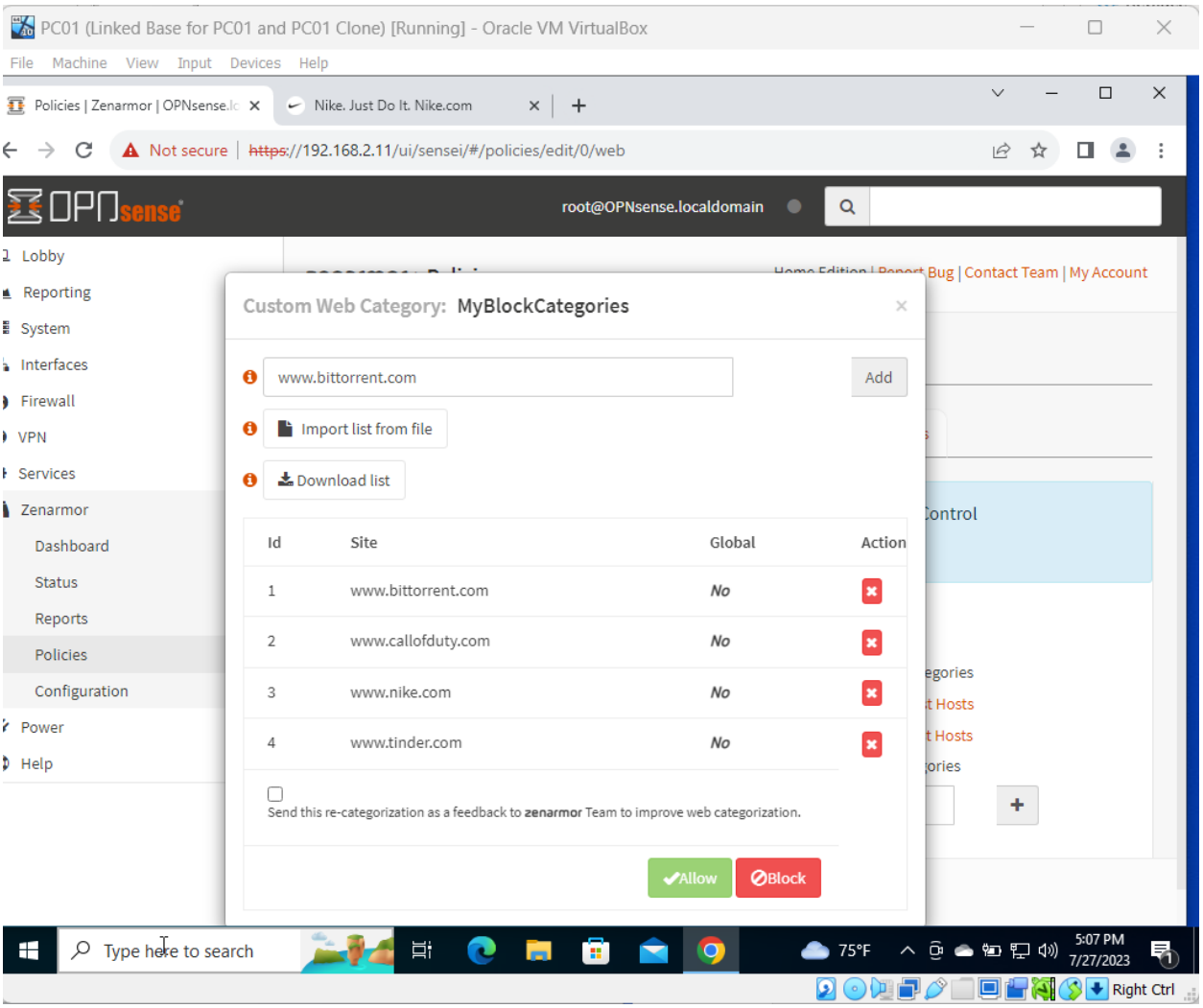
Task 6: Modify Dashboard to Include Blocked Host

- **Configuration of Dashboard:**
  - I edited the settings of the dashboard to incorporate information about blocked hosts, providing a comprehensive view.

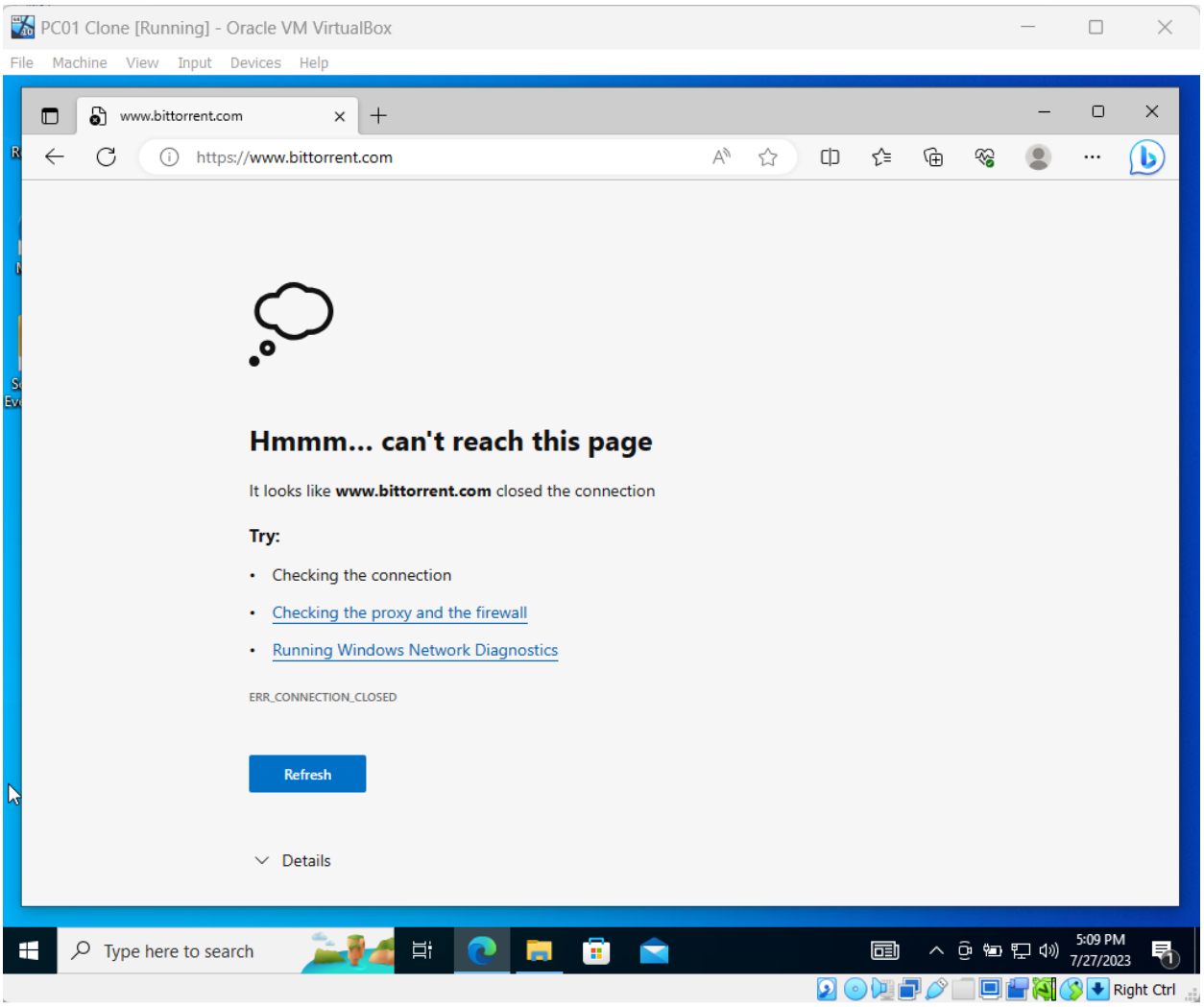

PC01 (Linked Base for PC01 and PC01 Clone) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Dashboard | Zenarmor | OPNsens
Nike. Just Do It. Nike.com
Not secure | https://192.168.2.11/ui/sensei/index
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
VPN
Services
Zenarmor
Dashboard
Status
Reports
Policies
Configuration
Power
Help
Top Local Hosts
Top Remote Hosts
Top Egress Users
Top Ingress Users
Interfaces & Vlans
Top Local Server Ports
Connection - Policies
Egress New Connections by App Over Time
Egress New Connections by Source Over Time
New Connections & Unique Remote Hosts
Unique Local Hosts over Time
Conn Facts
Egress New Connections Heatmap
Top Destination Locations Heatmap
Table of Apps
Table of Local Assets
Table of Remote Hosts
Top Remote Ports
Alerts - Blocked Local Hosts and Reasons
Alerts - Top Blocks
Alerts - Blocked Policies
Web - Table of Sites
Web - Top Egress Users
Web - Top Ingress Users
Web - Table of URIs
Web - HTTP Transactions by Source Over Time
tion | Report Bug | Contact Team | My Account
Sessions
Add & Sort Charts
Domain Name Resol...
Nike
Microsoft Telemetry
Microsoft Updates
Quic UDP Connection
MSN
Web Browsing
Microsoft Windows
Microsoft Windows...
Start
Type here to search
Earn...
5:02 PM
7/27/2023
Right Ctrl

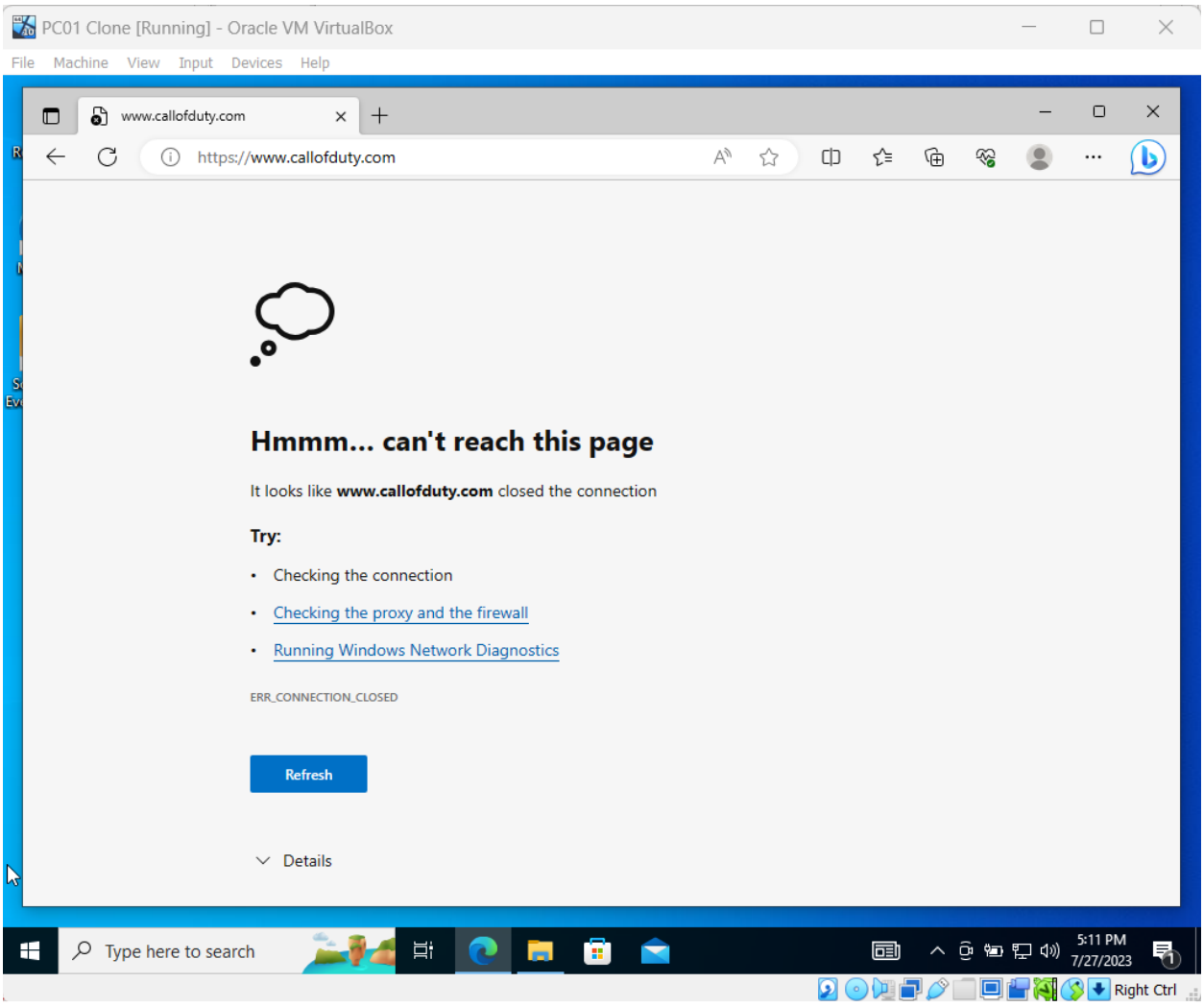


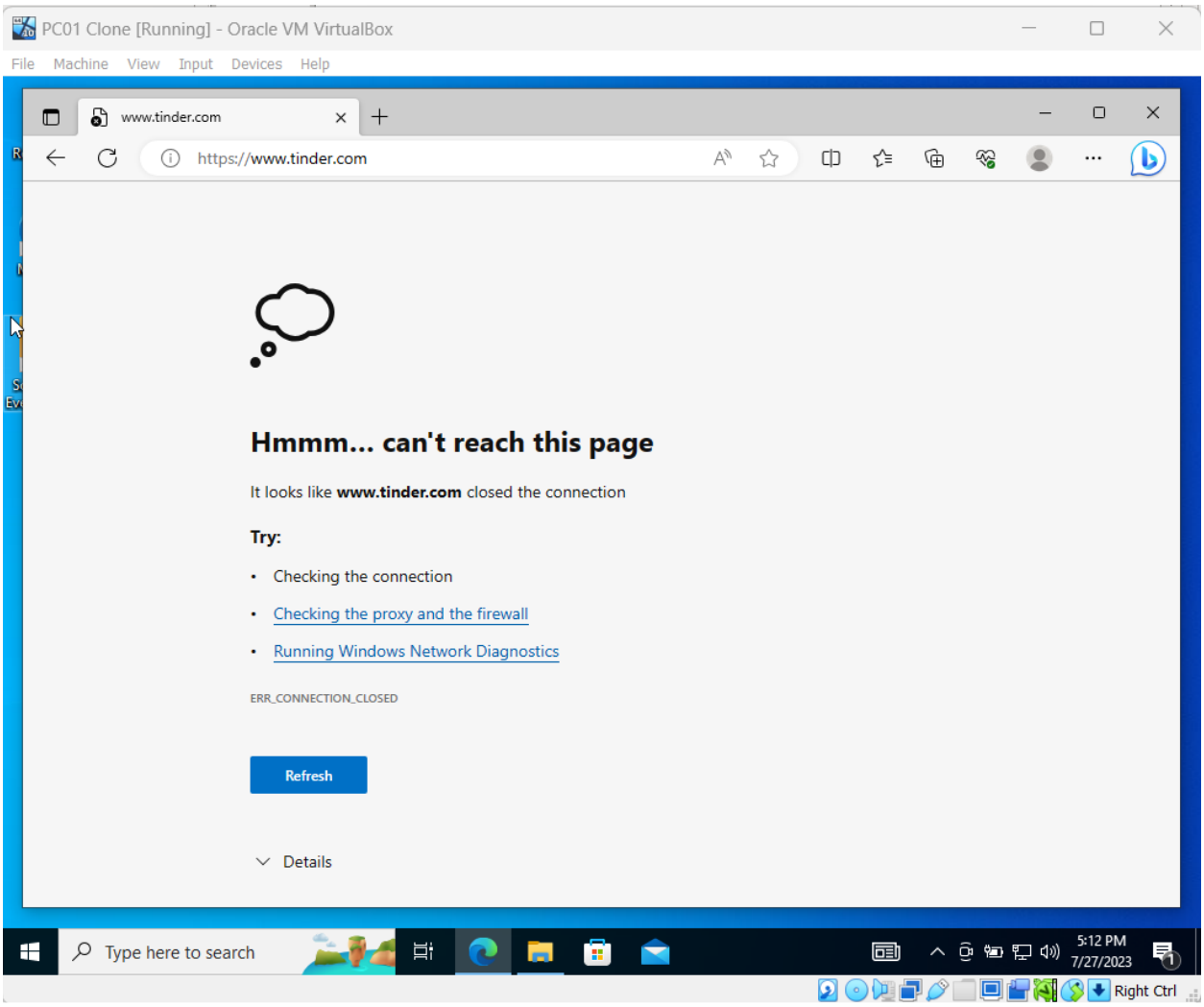
- **Rule Configuration for Blocking Sites:**
  - Screenshots were taken during the configuration of rules to block specific sites such as Tinder.com, Callofduty.com, and Bittorrent.com.



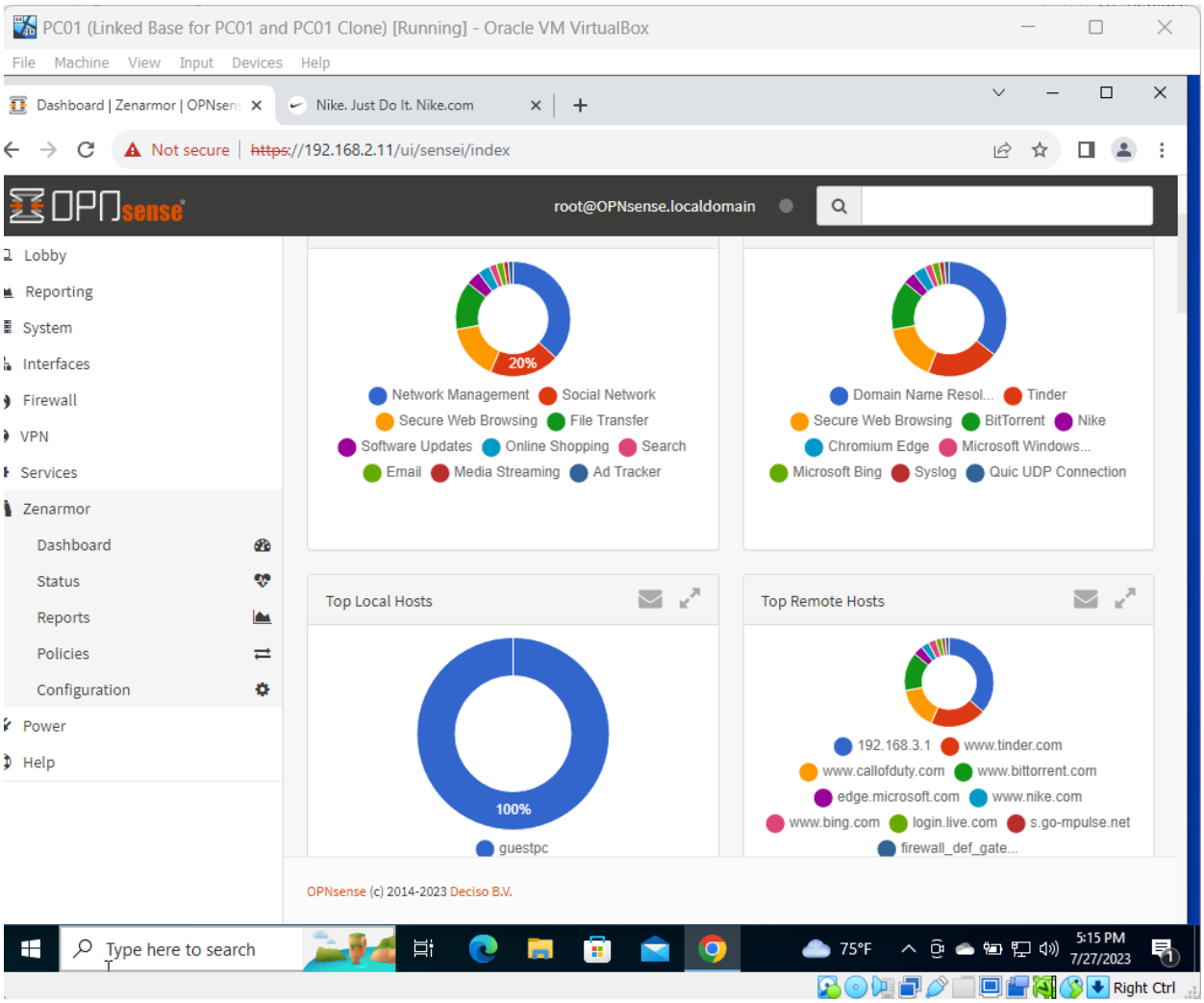
- **Verification of Blocked Sites:**
    - Screenshots were captured to showcase the successful blocking of each site as indicated by Sensei.


PC01 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
www.bittorrent.com
https://www.bittorrent.com
Hmmm... can't reach this page
It looks like www.bittorrent.com closed the connection
Try:
Checking the connection
Checking the proxy and the firewall
Running Windows Network Diagnostics
ERR_CONNECTION_CLOSED
Refresh
Details
Type here to search
5:09 PM
7/27/2023
Right Ctrl


PC01 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
www.callofduty.com
https://www.callofduty.com
Hmmm... can't reach this page
It looks like www.callofduty.com closed the connection
Try:
Checking the connection
Checking the proxy and the firewall
Running Windows Network Diagnostics
ERR_CONNECTION_CLOSED
Refresh
Details
Type here to search
5:11 PM
7/27/2023
Right Ctrl



- **Dashboard Configuration Verification:**
    - I ensured that the dashboard accurately reflected the status of blocked and allowed sites, validating the effectiveness of the configured rules.



Conclusion:

In this comprehensive lab, each step was meticulously performed and documented. The accompanying screenshots serve as visual evidence, providing clarity and transparency in the configuration of OPNsense Sensei for Guest Network monitoring and rule implementation. This hands-on experience has enriched my understanding of advanced firewall features.