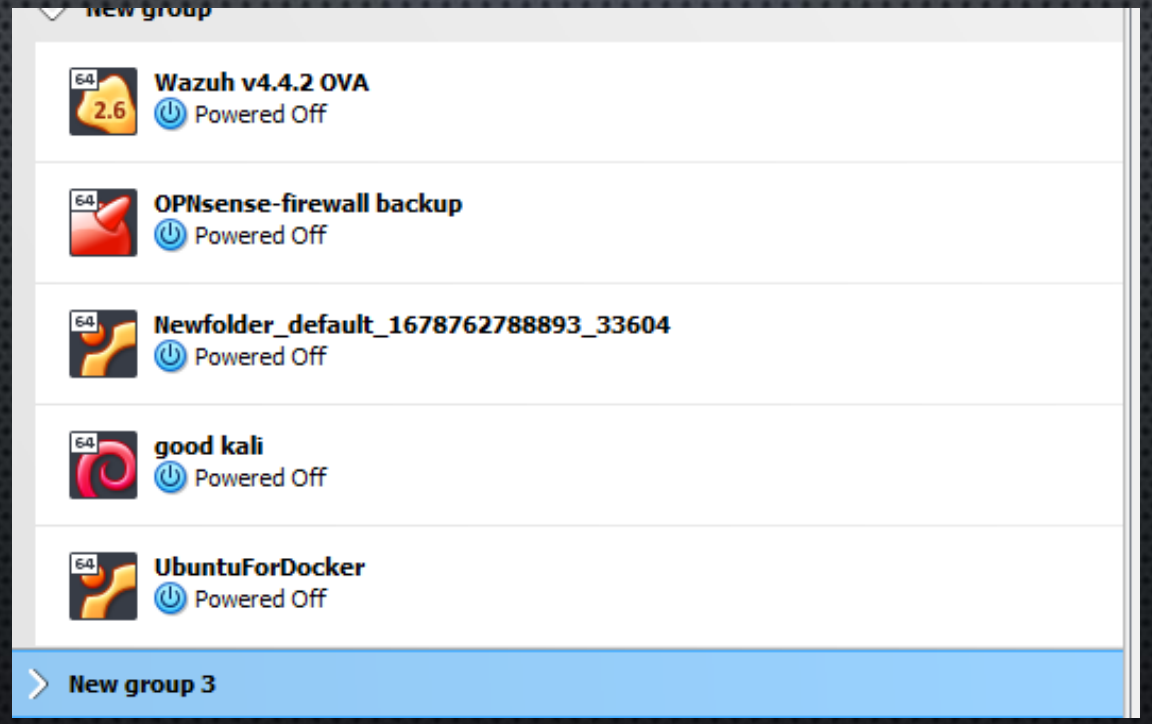
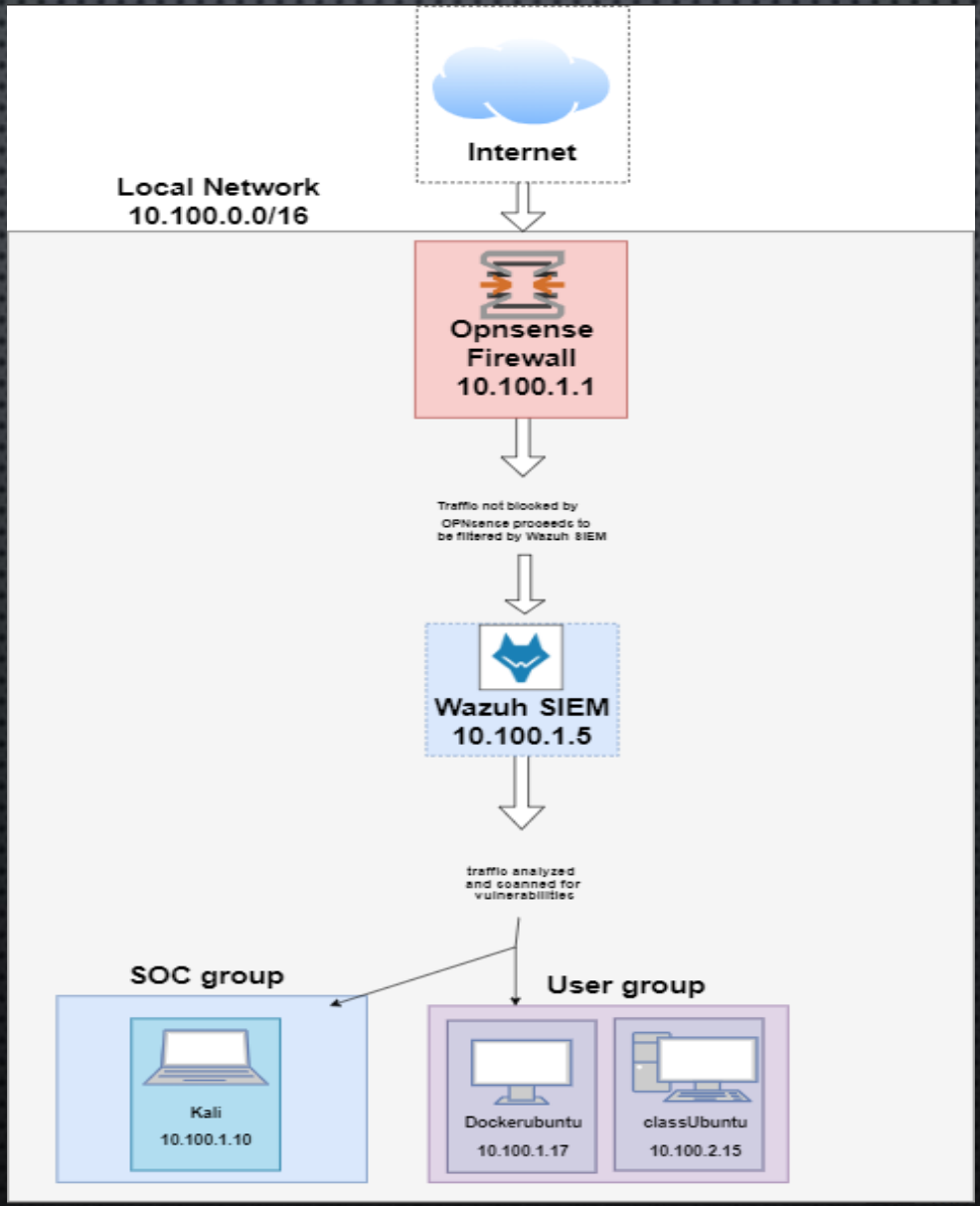
OPENSOURCE SOC ENVIRONMENT

Steven Owen

VIRTUAL MACHINES

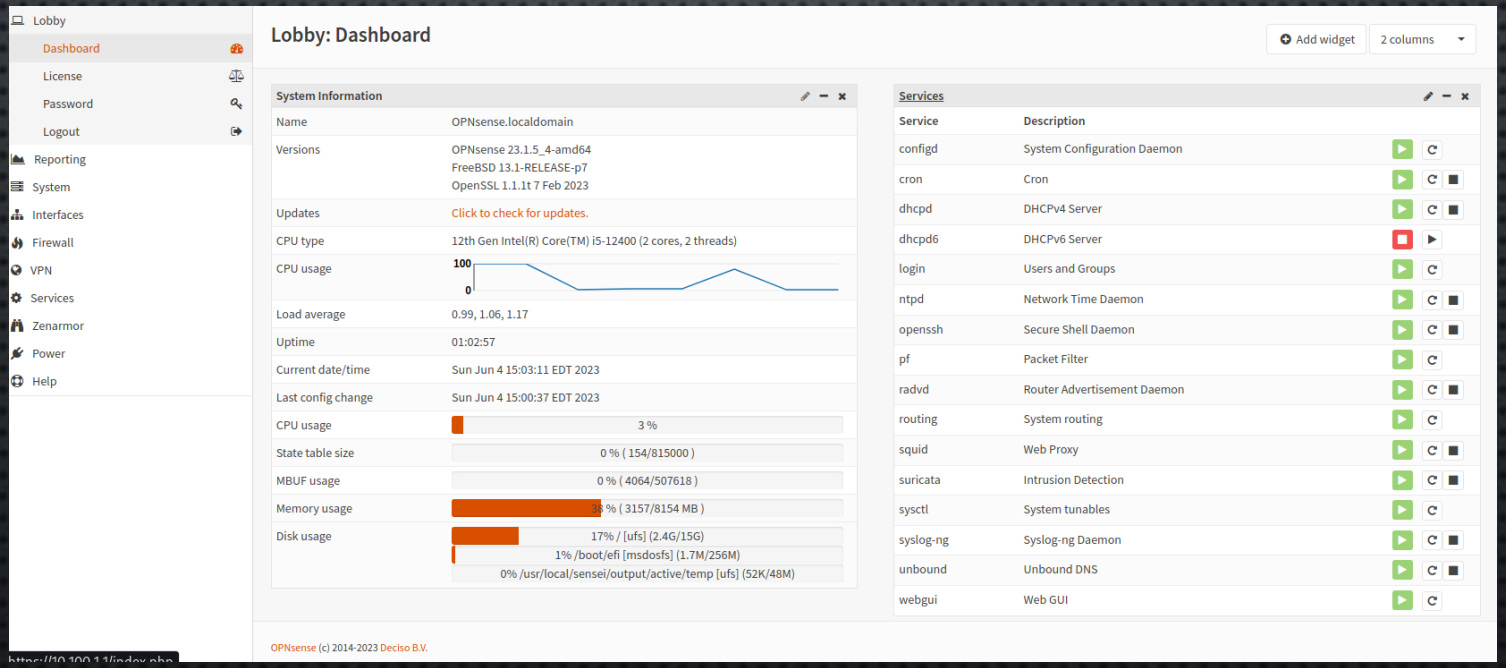


TOPOLOGY


Internet
Local Network
10.100.0.0/16
Opnsense
Firewall
10.100.1.1
Traffic not blocked by
OPNsense proceeds to
be filtered by Wazuh SIEM
Wazuh SIEM
10.100.1.5
traffic analyzed
and scanned for
vulnerabilities
SOC group
User group
Kali
10.100.1.10
Dockerubuntu
10.100.1.17
classUbuntu
10.100.2.15

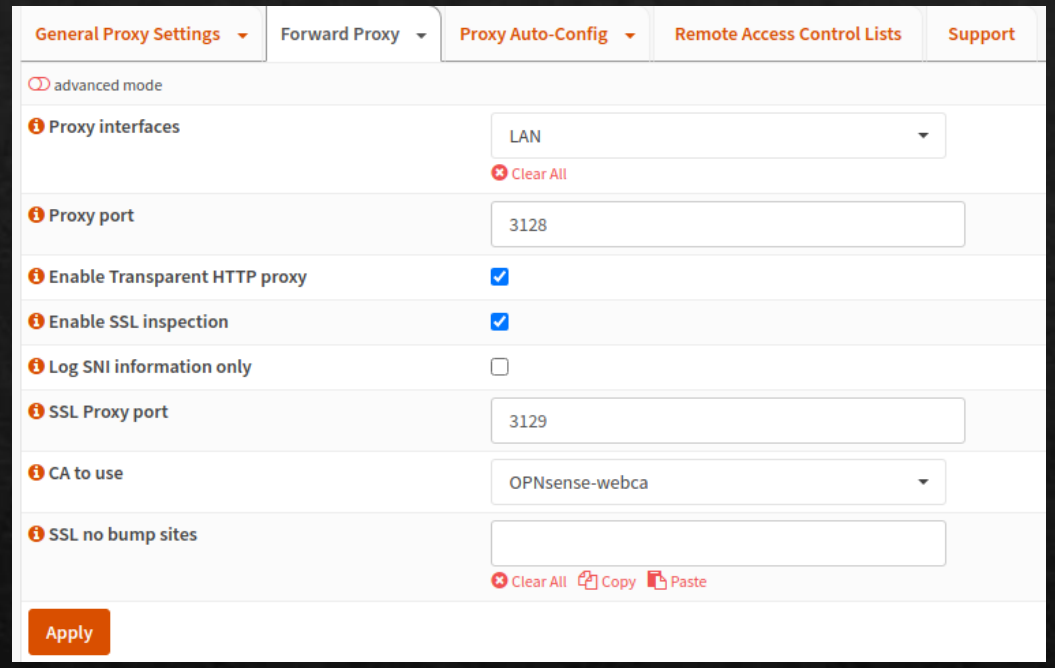
OPNSENSE

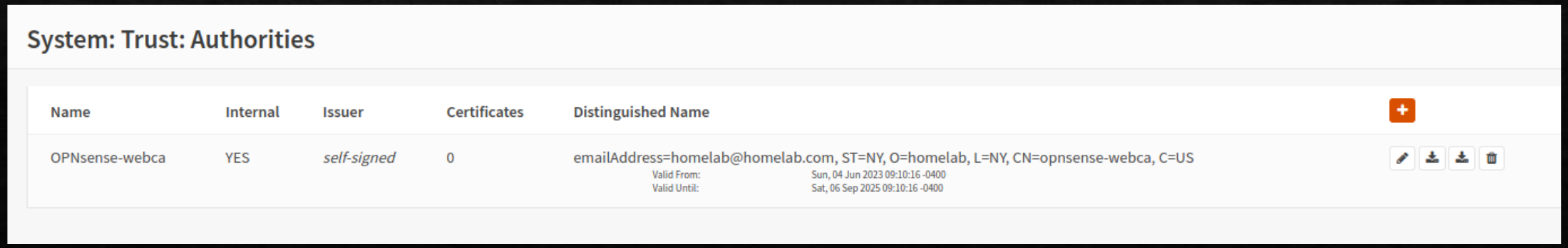
OPNSENSE DASHBOARD



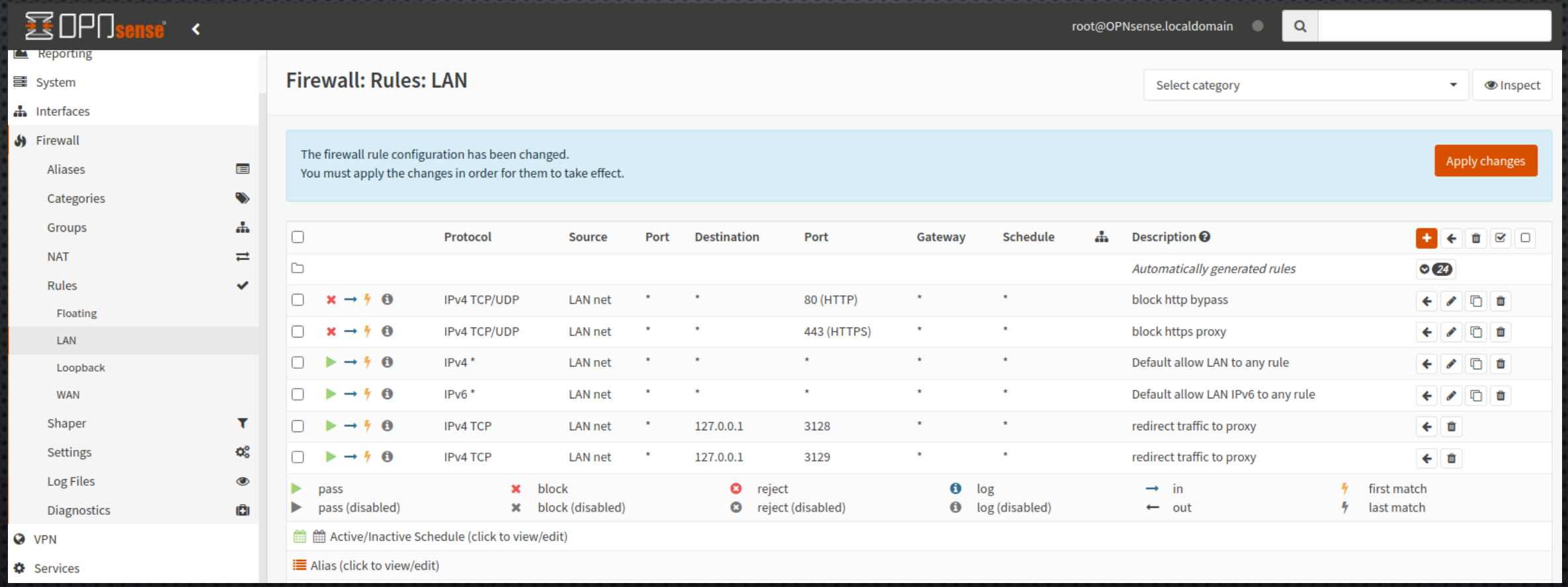
OPNSENSE WEB PROXY

Forward proxy--with a self-signed certificate--enables OPNsense to Intercept and filter traffic.





FIREWALL LAN RULES TO ALLOW PROXY INTERCEPT



ZENARMOR

Next-Gen Firewall

OPNSENSE ZENARMOR PLUGINS

OPNsense

root@OPNsense.localdomain

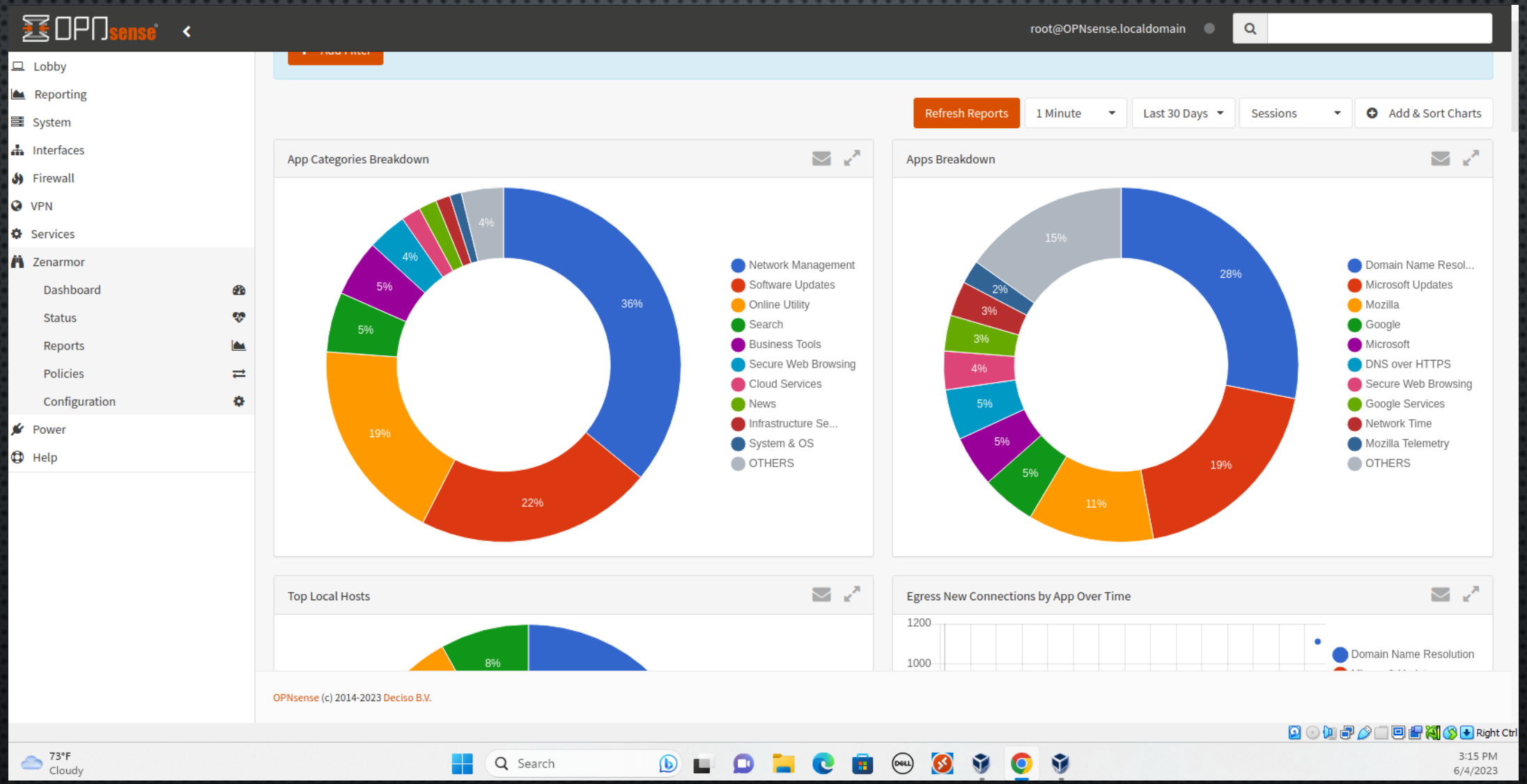
- Lobby
- Reporting
- System
  - Access
  - Configuration
  - Firmware
    - Status
    - Settings
    - Changelog
    - Updates
    - Plugins
    - Packages
  - Reporter
  - Log File
  - Gateways
  - High Availability
  - Routes
  - Settings
  - Trust
  - Wizard
  - Log Files
  - Diagnostics
- Interfaces

System: Firmware

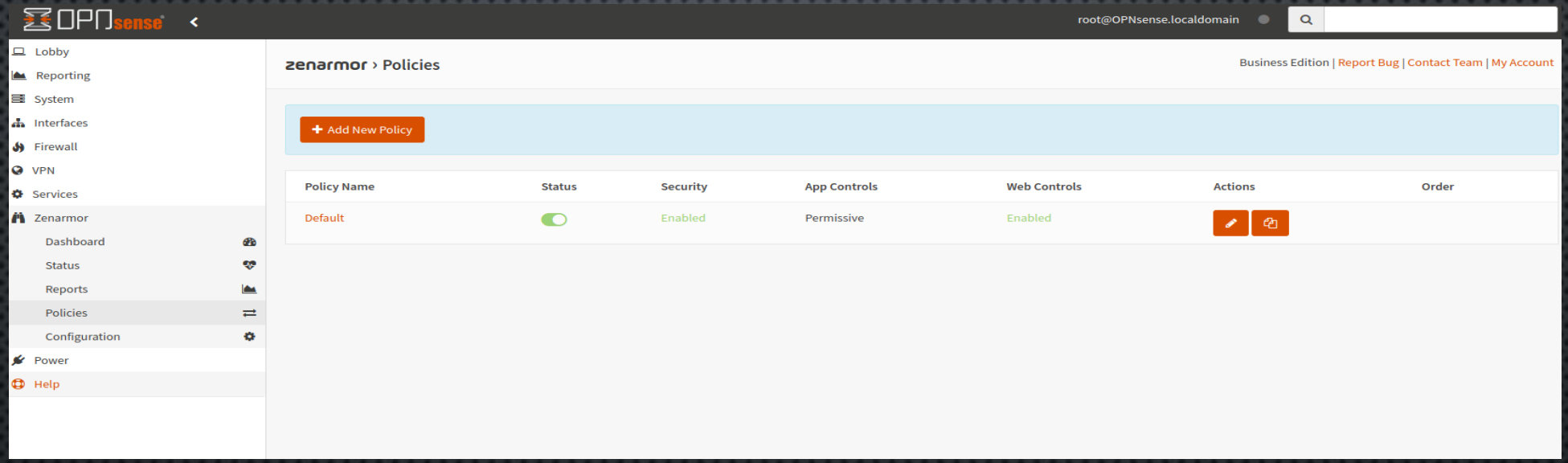
Status | Settings | Changelog | Updates | Plugins | Packages

Name	Version	Size	Repository	Comment
os-sensei (installed)	**1.13.1**	**205MiB**	**SunnyValley**	**Next Generation Firewall Extensions for OPNsense (ZENARMOR)**
os-sensei-updater (installed)	**1.13**	**4.79KiB**	**SunnyValley**	**OPNsense ZENARMOR Plugin Updater**
os-sunnyvalley (installed)	**1.2_3**	**643B**	**OPNsense**	**Vendor Repository for Zenarmor (a.k.a Sensei, Next Generation Firewall Extensions)**
os-virtualbox (installed)	**1.0_1**	**516B**	**OPNsense**	**VirtualBox guest additions**
os-acme-client	3.17	714KiB	OPNsense	ACME Client
os-apcupsd	1.1	56.6KiB	OPNsense	APCUPSD - APC UPS daemon
os-api-backup	1.1	3.80KiB	OPNsense	Provide the functionality to download the config.xml
os-bind	1.26_5	145KiB	OPNsense	BIND domain name service
os-c-icap	1.7_3	50.1KiB	OPNsense	c-icap connects the web proxy with a virus scanner
os-cache	1.0_1	520B	OPNsense	Webserver cache
os-chrony	1.5_1	20.4KiB	OPNsense	Chrony time synchronisation
os-clamav	1.8	47.7KiB	OPNsense	Antivirus engine for detecting malicious threats
os-collectd	1.4_1	36.8KiB	OPNsense	Collect system and application performance metrics periodically
os-crowdsec	1.0.5	63.2KiB	OPNsense	Lightweight and collaborative security engine
os-ddclient	1.13_2	97.6KiB	OPNsense	Dynamic DNS client
os-debug	1.5	434B	OPNsense	Debugging Tools

OPNSENSE ZENARMOR DASHBOARD



ZENARMOR POLICIES



ZENARMOR WEB CONTROLS

Policy Configuration | Security | App Controls | Web Controls | Exclusions

Enforce Safe Search | Preset profile: Permissive | Moderate Control | High Control | Custom

Search...

Web Categories
- Ad Trackers
- Adult
- Advertisements
- Alcohol and Tobacco
- Arts and Culture
- Blacklist
- Blogs
- Business Services
- Chats
- Clothing and Fashion
- Content Delivery Networks
- Cult and Occult
- Dating
- Education
- Entertainment
- Financial Services
- Forums

User Defined Categories
- Auto White List Hosts
- Auto Block List Hosts

New Category +

OPNsense | 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

Whitelists

example.com

Descript for exclusion site

Filter | Add | Clear

You can enter hostnames, domains and IP addresses. Domains match all subdomains. CIDR notation is acceptable for IP addresses.

host.sub.domain.com, domain.com, 172.16.1.1, 10.10.0.0/16).

Import list from file

Download Whitelist

Delete list

Id	Site	Desc	Global	Action

Send this re-categorization as a feedback to **zenarmor** Team to improve web categorization.

Blacklists

example.com

Descript for exclusion site

Filter | Add | Clear

You can enter hostnames, domains and IP addresses. Domains match all subdomains. CIDR notation is acceptable for IP addresses.

host.sub.domain.com, domain.com, 172.16.1.1, 10.10.0.0/16).

Import list from file

Download Blocklist

Delete list

Id	Site	Desc	Global	Action
1	Instagram.com			
2	facebook.com			

OPNsense (c) 2014-2023 Deciso B.V.

Save Changes

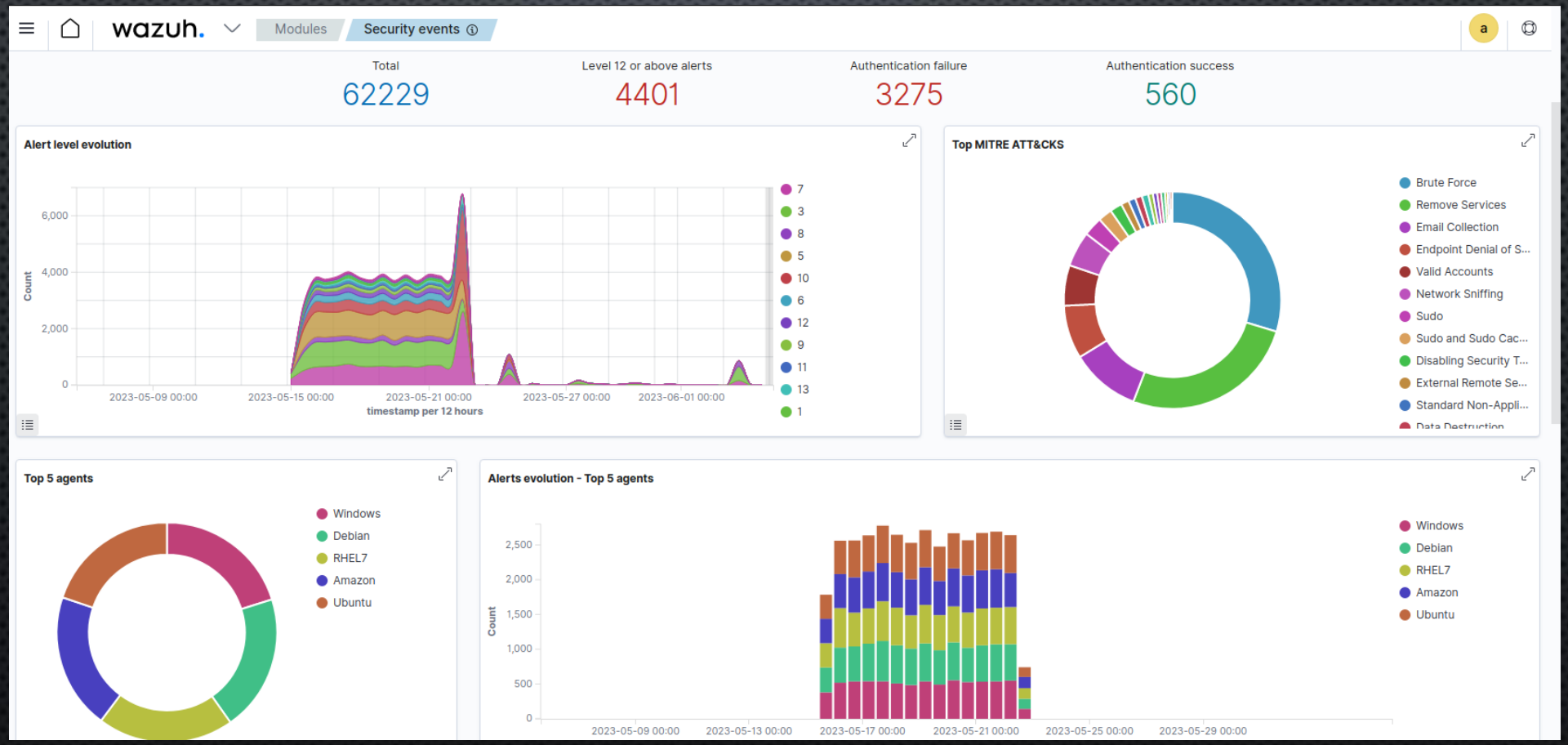
Policy Configuration | Security | App Controls | Web Controls | Exclusions

Essential Security (full help)
- Block Bad IP
- Block Non-existent Domain
- Block Malware Activity
- Block Phishing Servers
- Block Spam sites
- Block Hacking Sites
- Block Parked Domains
- Block Potentially Dangerous Sites
- Block Firstly Seen Sites
- Block Undecided Not Safe Sites
- Block Undecided Safe Sites

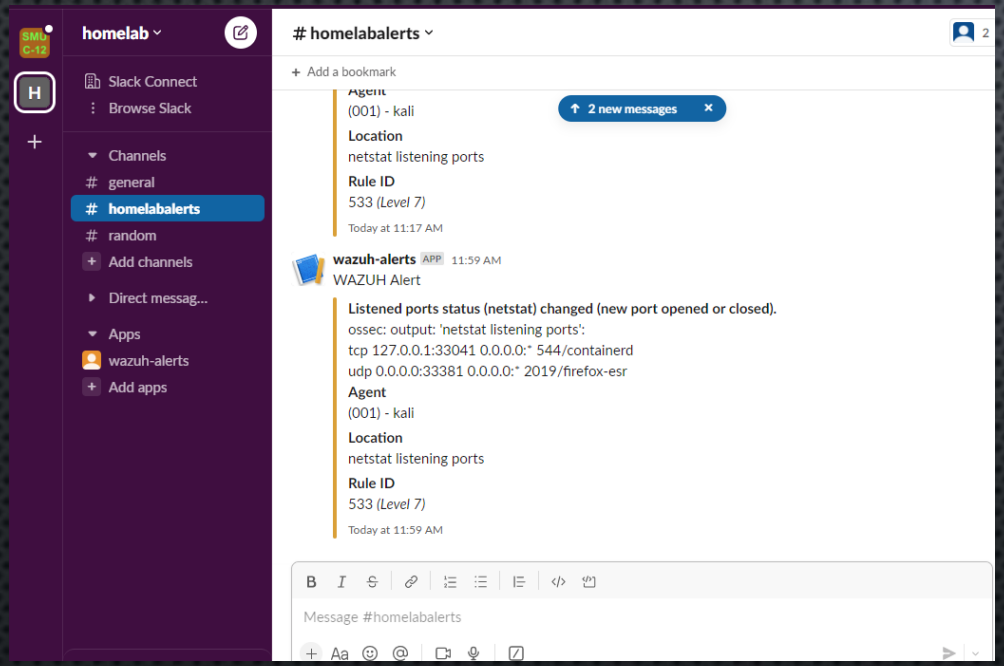
Advanced Security (full help)
- Block Recent Malware/Phishing/Virus Outbreaks
- NEW Block Botnet C&C
- Block Proxy
- Block Dead Sites
- Block Dynamic DNS Sites
- Block Local IP
- Block Newly Registered Sites
- Block Newly Recovered Sites
- Block Botnet DGA Domains (Coming soon)
- Block DNS Tunneling (Coming soon)

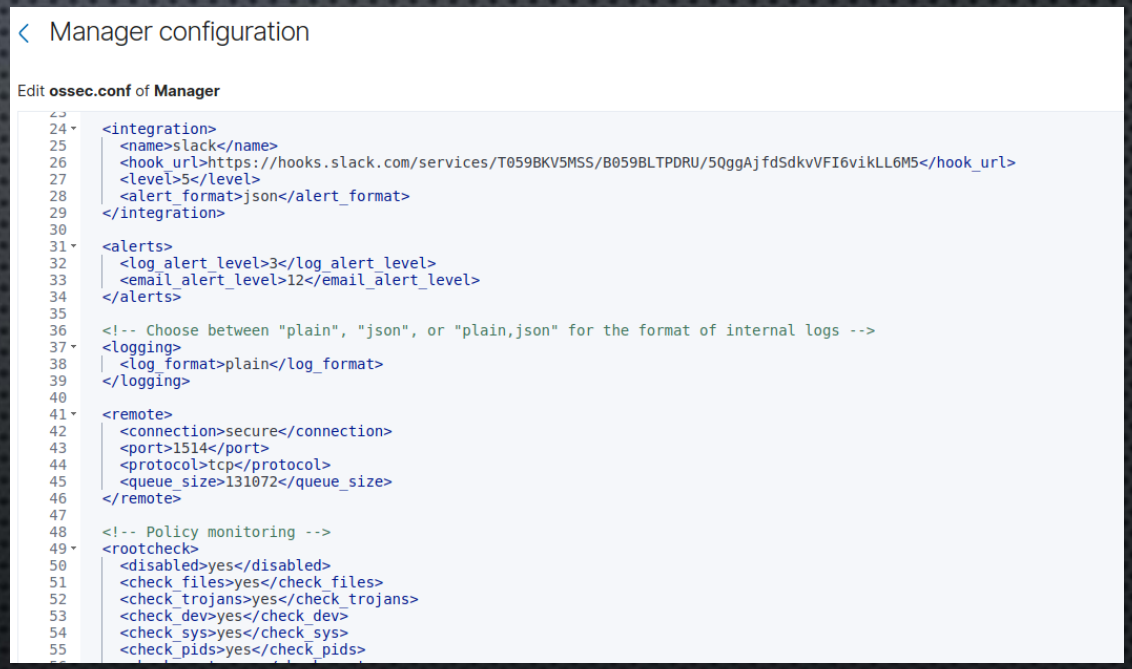

WAZUH

WAZUH DASHBOARD

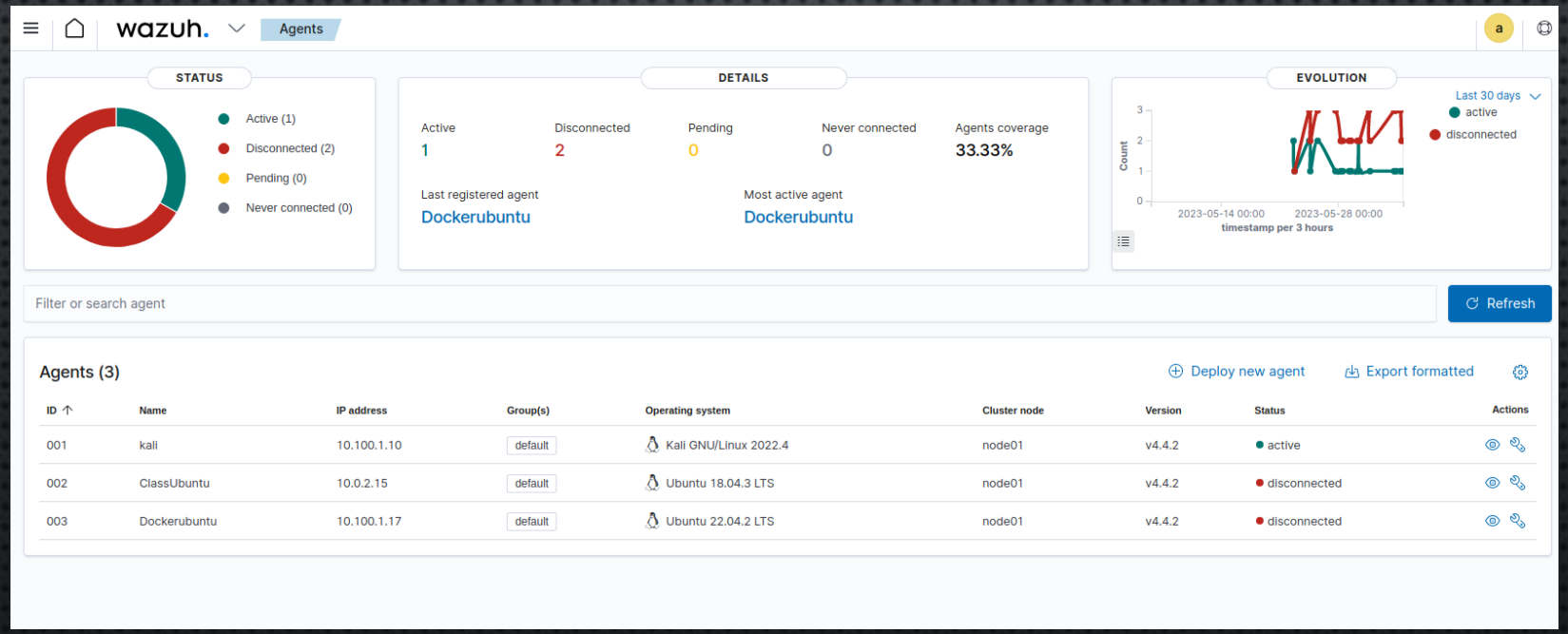


SLACK ALERTS AND CONFIGURATION





WAZUH CONNECTED AGENTS



"CLASSUBUNTU" AUDIT

CIS benchmark for Ubuntu Linux 18.04 LTS

Passed	Failed	Not applicable	Score	End scan
62	131	5	32%	May 22, 2023 @ 15:30:42.000

Checks (198)

Refresh Export formatted

wazuh. Modules ClassUbuntu Vulnerabilities

Inventory Events

ClassUbuntu (002)

SEVERITY

- Critical (293)
- High (2436)
- Medium (2224)
- Low (329)

DETAILS

Critical	High	Medium	Low
293	2436	2224	329

Last full scan: May 22, 2023 @ 15:41:36.000

Last partial scan: May 22, 2023 @ 17:09:26.000

SUMMARY

Name

- firefox (468)
- gir1.2-javascriptcoregtk-4.0 (124)
- gir1.2-webkit2-4.0 (124)
- libjavascriptcoregtk-4.0-18 (124)

Vulnerabilities (5282)

Export formatted

Filter or search

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time
accountsservice	0.6.45-1ubuntu1	amd64	Medium	CVE-2018-14036	4	6.5	May 22, 2023 @ 15:38:46.000
accountsservice	0.6.45-1ubuntu1	amd64	Low	CVE-2020-16126	2.1	3.3	May 22, 2023 @ 15:39:50.000
accountsservice	0.6.45-1ubuntu1	amd64	High	CVE-2021-3939	7.2	7.8	May 22, 2023 @ 15:40:42.000
apache2	2.4.29-1ubuntu4.25	amd64	Critical	CVE-2022-36760	0	9	May 22, 2023 @ 15:40:06.000
apache2	2.4.29-1ubuntu4.25	amd64	Medium	CVE-2022-37436	0	5.3	May 22, 2023 @ 15:40:18.000
apache2	2.4.29-1ubuntu4.25	amd64	Critical	CVE-2023-25690	0	9.8	May 22, 2023 @ 15:40:46.000
apache2-bin	2.4.29-1ubuntu4.25	amd64	Critical	CVE-2022-36760	0	9	May 22, 2023 @ 15:40:06.000

Right

WAZUH ACTIVE RESPONSE

```
<!--
<active-response>
  <command>firewall-drop</command>
  <location>kali</location>
  <rules_id>5720</rules_id>
  <timeout>1000</timeout>
</active-response>
-->
```

```
<active-response>
  <command>route-null</command>
  <location></location>
  <rules_id>5710</rules_id>
  <timeout>1000</timeout>
</active-response>
```

ID ↑	Description
5710	sshd: Attempt to login using a non-existent user

```
<command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>host-deny</name>
  <executable>host-deny</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>route-null</name>
  <executable>route-null</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>win_route-null</name>
  <executable>route-null.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>netsh</name>
  <executable>netsh.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

ACTIVE RESPONSE COMMANDS

Current White Listed Domains

127.0.0.1

localhost.localdomain

172.31.0.2

disable-account: Wazuh uses this active response on Linux/Unix endpoints to disable the account for the user in the dstuser field of a Wazuh alert

firewall-drop: uses iptables to block malicious IP adresses

host-deny:

When this command is triggered, Wazuh will add the IP address to the /etc/hosts.deny file, which will prevent the IP address from being able to connect to the system

The host-deny active response command can be used to help protect systems from a variety of threats, such as:

- SSH brute force attacks
- Port scans
- Denial-of-service attacks

route-null/win_route-null:

The Wazuh route-null active response command is used to route all traffic from a specific IP address to a nonexistent destination

Netsh: When this rule is triggered, Wazuh will execute the Netsh command to block the IP address. The block will be in effect for 1 hour

DEMONSTRATION

THANK YOU