



wazuh.

Wazuh – pfSense

FIREWALL INTEGRATION

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

Follow Me: [linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)

Integration of Wazuh with pfSense Firewall

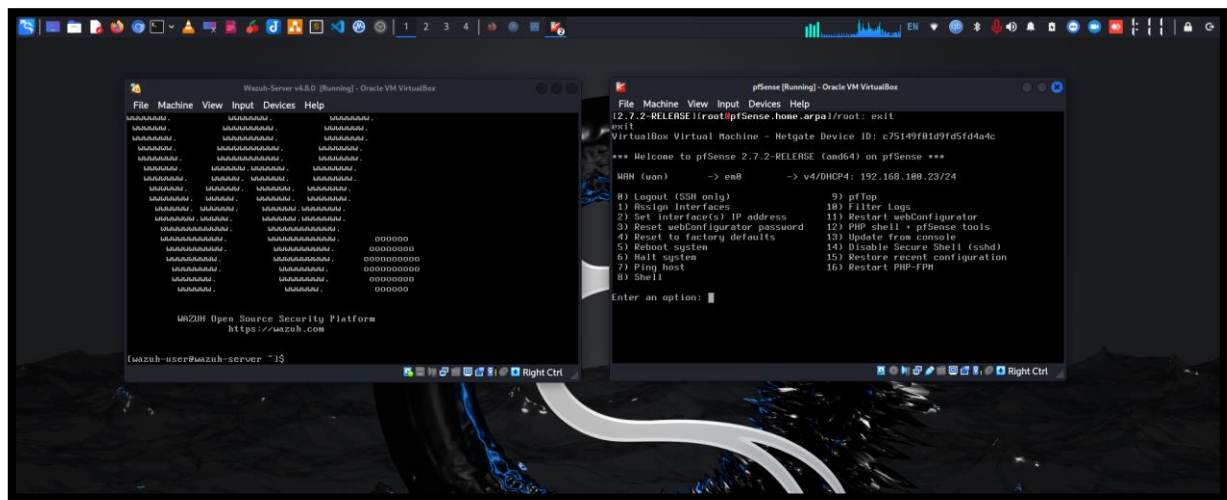
Introduction

Integrating Wazuh with pfSense Firewall enables a comprehensive security monitoring and management system. Wazuh, an open-source security monitoring platform, can collect, analyze, and correlate security events from pfSense, an open-source firewall/router computer software distribution. This integration helps to enhance the security posture by providing visibility into the network traffic and potential security threats.

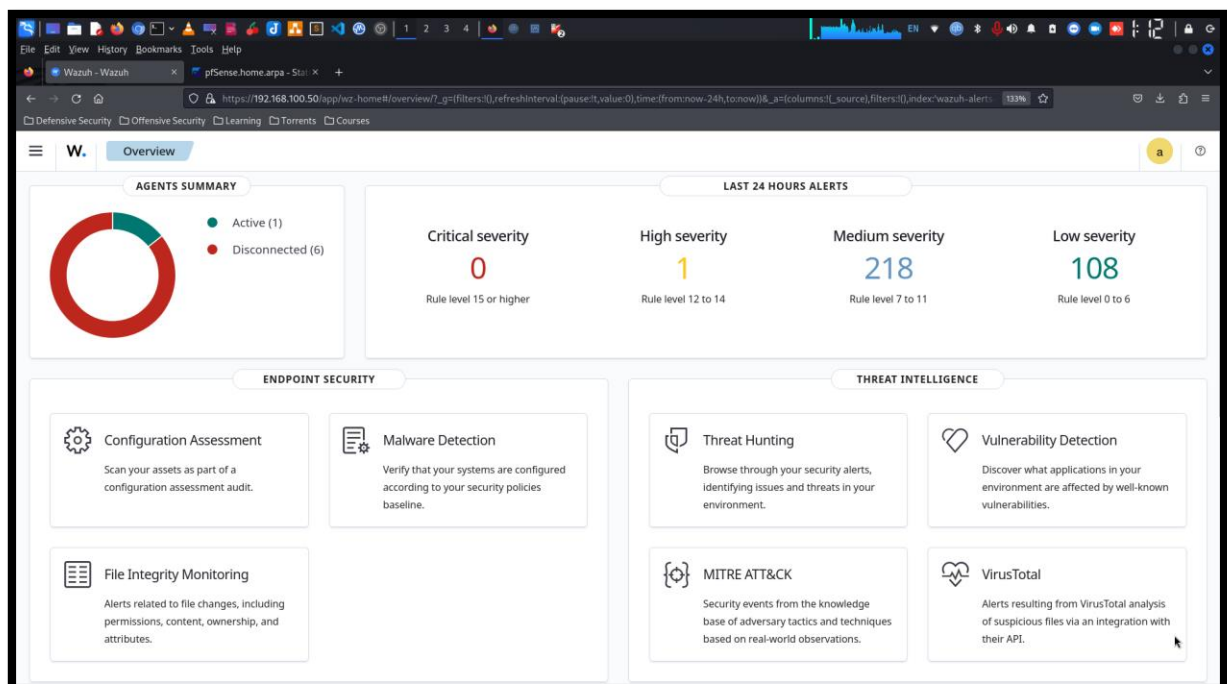
Prerequisites

- Wazuh Manager installed and configured.
- pfSense firewall installed and configured.
- Network connectivity between pfSense and Wazuh Manager.
- SSH access to both pfSense and Wazuh Manager.

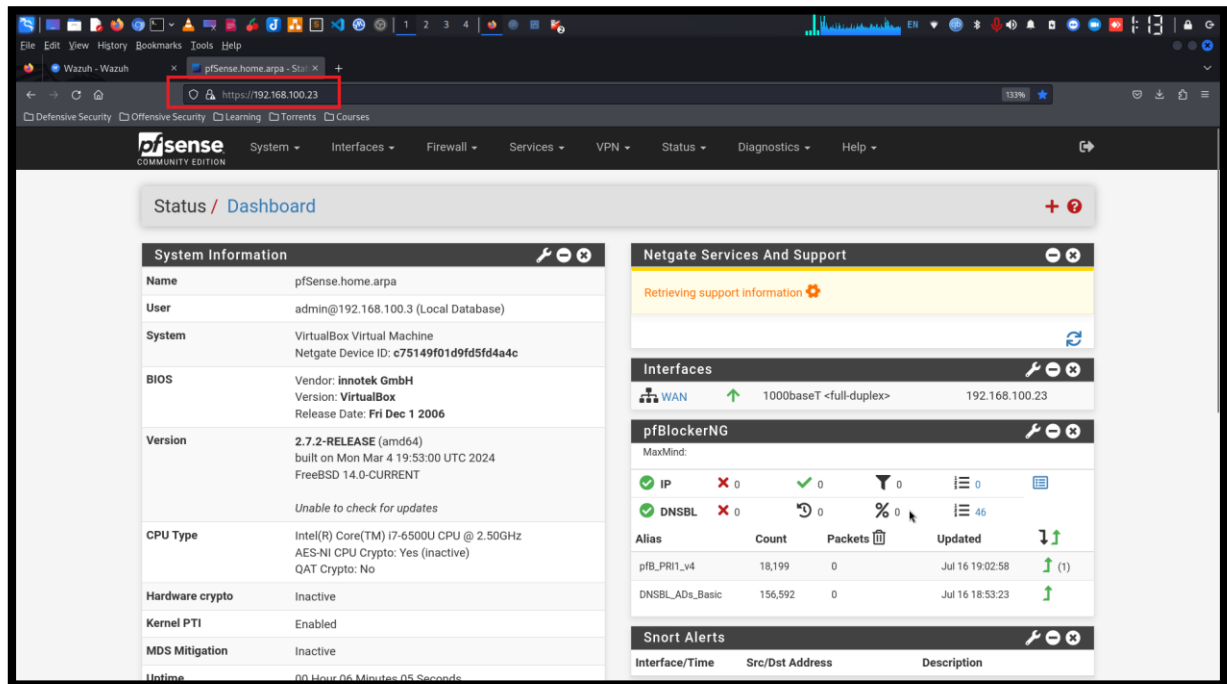
Here is my Wazuh server running along with pfSense machine on virtualbox.



Wazuh Dashboard

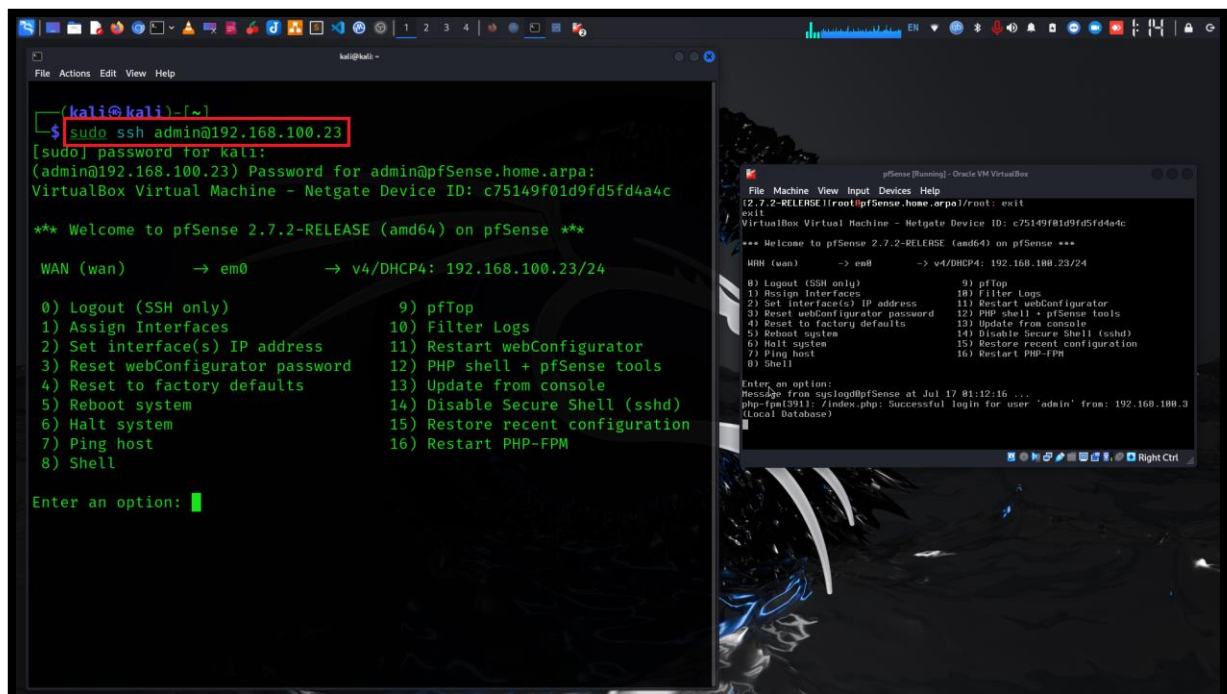


pfSense Dashboard



Step 01: Access pfSense via SSH

Command: `sudo ssh admin@192.168.100.23`



Wazuh – pfSense – Firewall Integration

Lab Created by: MUHAMMAD MOIZ UD DIN RAFAY

After accessing SSH we have to select option 8 “Shell”

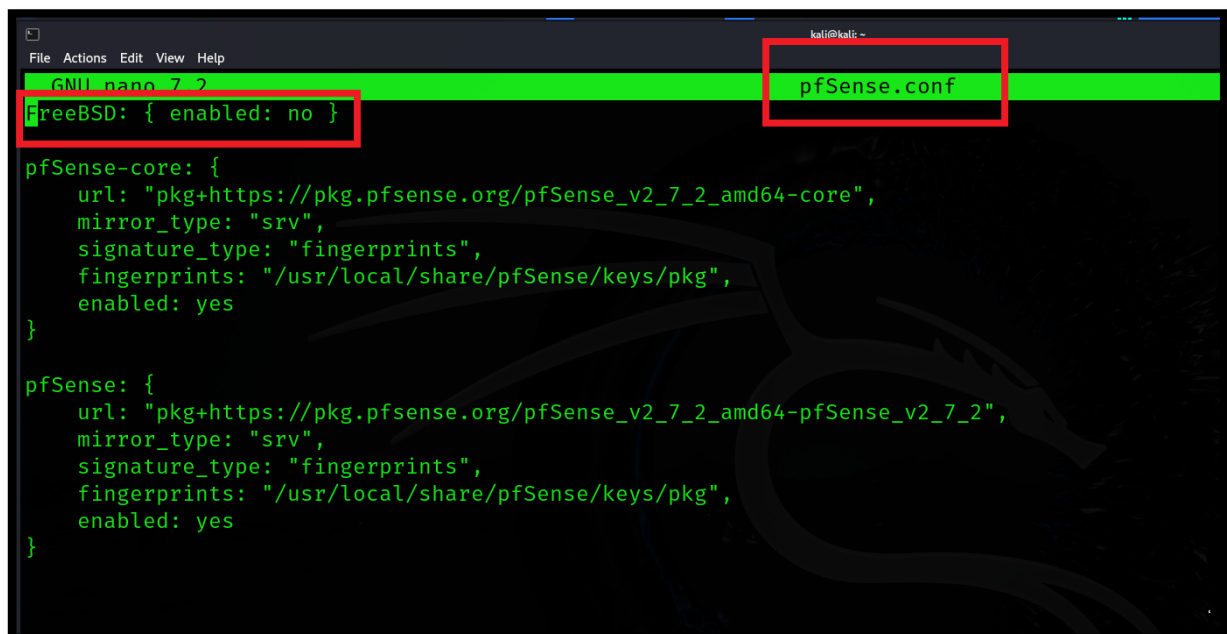
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo ssh admin@192.168.100.23  
[sudo] password for kali:  
(admin@192.168.100.23) Password for admin@pfSense.home.arpa:  
VirtualBox Virtual Machine - Netgate Device ID: c75149f01d9fd5fd4a4c  
  
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      → em0      → v4/DHCP4: 192.168.100.23/24  
  
0) Logout (SSH only)          9) pfTop  
1) Assign Interfaces          10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults    13) Update from console  
5) Reboot system              14) Disable Secure Shell (sshd)  
6) Halt system                15) Restore recent configuration  
7) Ping host                  16) Restart PHP-FPM  
8) Shell ←  
  
Enter an option: 8  
  
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: █
```

For installing Wazuh-agent on pfSense firewall we have to allow packages from FreeBSD. Go to directory “/usr/local/pkg/repos/” in this directory “FreeBSD.conf and pfSense.conf” file we have to made changes in these files.

```
kali@kali: ~  
File Actions Edit View Help  
  
[2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cd / ←  
[2.7.2-RELEASE][admin@pfSense.home.arpa]/: cd /usr/local/etc/pkg/repos ←  
[2.7.2-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: ls  
FreeBSD.conf pfSense.conf  
[2.7.2-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: █
```

Now first open “pfSense.conf” file in nano editor and enable FreeBSD options “no” to “yes” and save changes.

Note: by default nano editor is not available in pfSense you can install nano editor first.



```
File Actions Edit View Help
GNU nano 7.2 pfSense.conf
FreeBSD: { enabled: no }

pfSense-core: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}

pfSense: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-pfSense_v2_7_2",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}
```

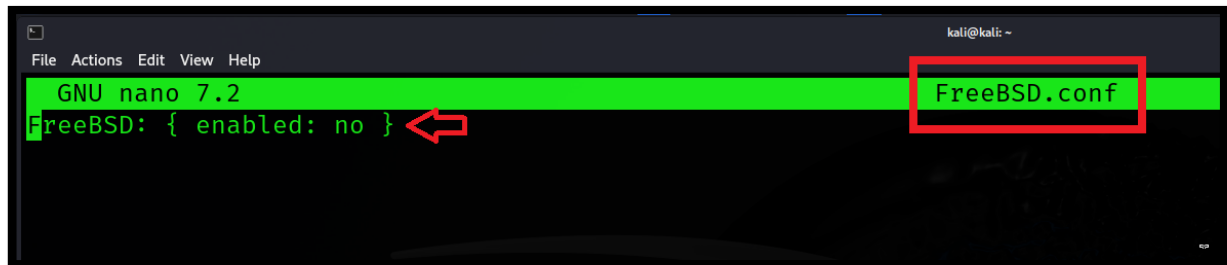


```
File Actions Edit View Help
GNU nano 7.2 pfSense.conf
FreeBSD: { enabled: yes }

pfSense-core: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}

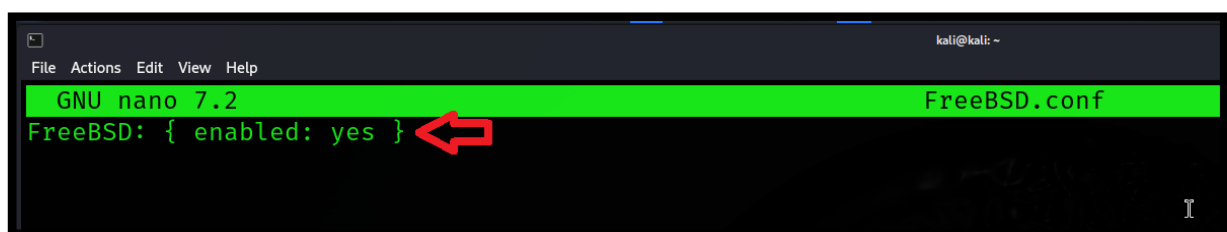
pfSense: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-pfSense_v2_7_2",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}
```

After edit “pfSense.conf” file we have to made changes in “FreeBSD.conf” file and set parameter “no” to “yes” and save changes.



```
File Actions Edit View Help
GNU nano 7.2
FreeBSD.conf
FreeBSD: { enabled: no }
```

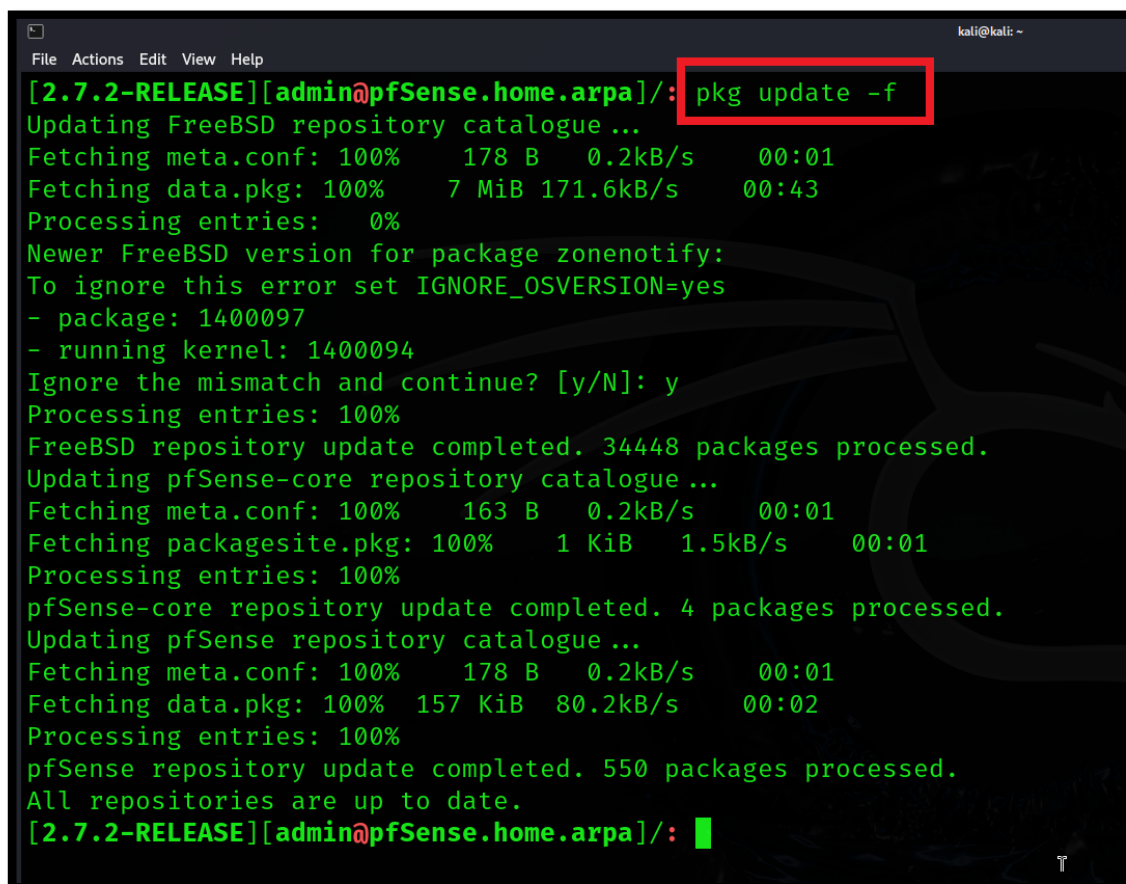
A screenshot of the nano text editor in a terminal window. The title bar shows 'kali@kali: ~'. The editor is editing a file named 'FreeBSD.conf', which is highlighted in green. The current line is 'FreeBSD: { enabled: no }'. A red arrow points to the word 'no', indicating it needs to be changed to 'yes'.



```
File Actions Edit View Help
GNU nano 7.2
FreeBSD.conf
FreeBSD: { enabled: yes }
```

A screenshot of the nano text editor in a terminal window. The title bar shows 'kali@kali: ~'. The editor is editing a file named 'FreeBSD.conf', which is highlighted in green. The current line is 'FreeBSD: { enabled: yes }'. A red arrow points to the word 'yes', indicating it has been successfully changed from 'no'.

After changes we have to update repository.
Command: `pkg update -f`

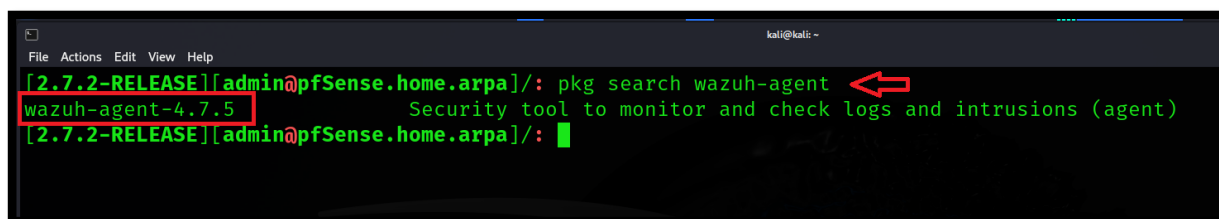


```
File Actions Edit View Help
[2.7.2-RELEASE][admin@pfSense.home.arpa]/: pkg update -f
Updating FreeBSD repository catalogue ...
Fetching meta.conf: 100% 178 B 0.2kB/s 00:01
Fetching data.pkg: 100% 7 MiB 171.6kB/s 00:43
Processing entries: 0%
Newer FreeBSD version for package zonenotify:
To ignore this error set IGNORE_OSVERSION=yes
- package: 1400097
- running kernel: 1400094
Ignore the mismatch and continue? [y/N]: y
Processing entries: 100%
FreeBSD repository update completed. 34448 packages processed.
Updating pfSense-core repository catalogue ...
Fetching meta.conf: 100% 163 B 0.2kB/s 00:01
Fetching packagesite.pkg: 100% 1 KiB 1.5kB/s 00:01
Processing entries: 100%
pfSense-core repository update completed. 4 packages processed.
Updating pfSense repository catalogue ...
Fetching meta.conf: 100% 178 B 0.2kB/s 00:01
Fetching data.pkg: 100% 157 KiB 80.2kB/s 00:02
Processing entries: 100%
pfSense repository update completed. 550 packages processed.
All repositories are up to date.
[2.7.2-RELEASE][admin@pfSense.home.arpa]/: █
```

A screenshot of a terminal window showing the output of the 'pkg update -f' command. The title bar shows 'kali@kali: ~'. The command 'pkg update -f' is highlighted with a red box. The output shows the process of updating the FreeBSD repository catalogue, followed by the pfSense-core and pfSense repository catalogues. It indicates that 34448 packages were processed for FreeBSD, 4 for pfSense-core, and 550 for pfSense. The final status is 'All repositories are up to date.'.

When update is complete, search for Wazuh-agent package.

Command: `pkg search Wazuh-agent`

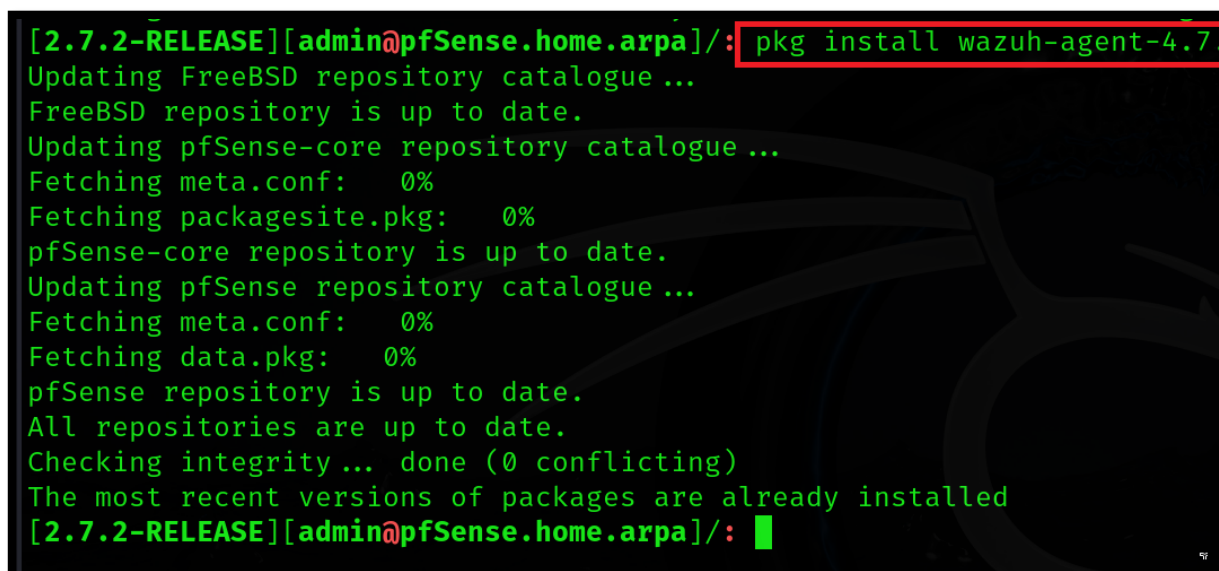


```
[2.7.2-RELEASE][admin@pfSense.home.arpa]: pkg search wazuh-agent
wazuh-agent-4.7.5      Security tool to monitor and check logs and intrusions (agent)
[2.7.2-RELEASE][admin@pfSense.home.arpa]: █
```

The available Wazuh-agent package is “Wazuh-agent-4.7.5”

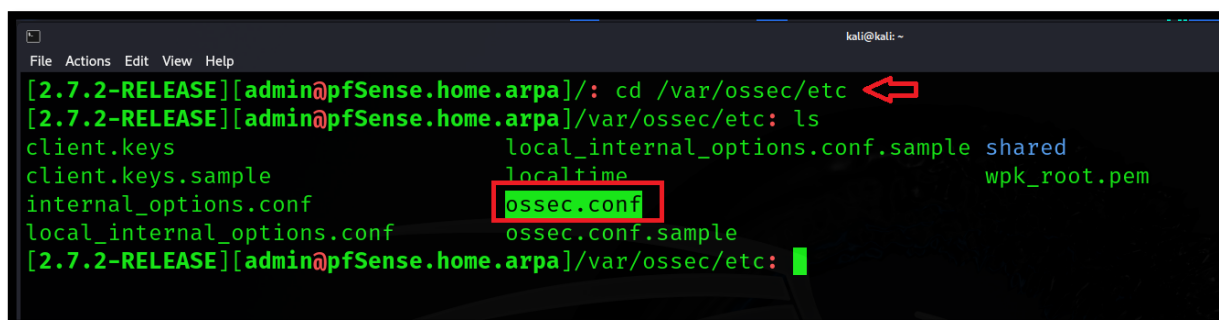
Now install this.

Command: `pkg install Wazuh-agent-4.7.5`



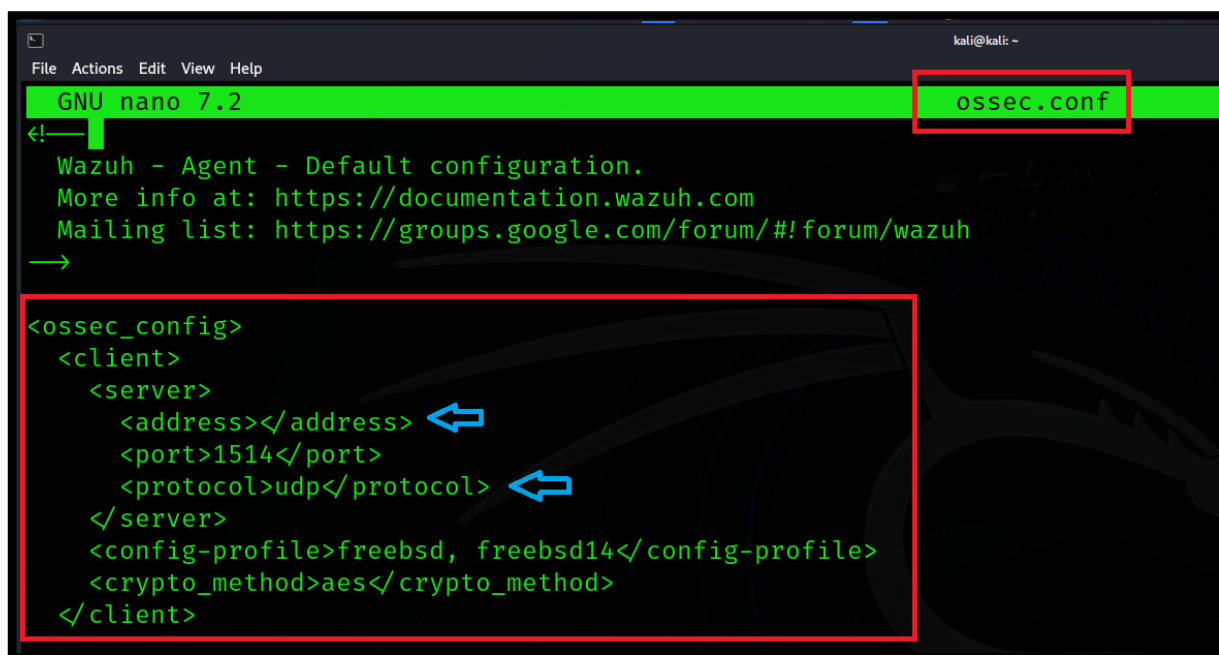
```
[2.7.2-RELEASE][admin@pfSense.home.arpa]: pkg install wazuh-agent-4.7.5
Updating FreeBSD repository catalogue ...
FreeBSD repository is up to date.
Updating pfSense-core repository catalogue ...
Fetching meta.conf: 0%
Fetching packagesite.pkg: 0%
pfSense-core repository is up to date.
Updating pfSense repository catalogue ...
Fetching meta.conf: 0%
Fetching data.pkg: 0%
pfSense repository is up to date.
All repositories are up to date.
Checking integrity... done (0 conflicting)
The most recent versions of packages are already installed
[2.7.2-RELEASE][admin@pfSense.home.arpa]: █
```

When installation is complete go to “/var/ossec/etc” director to configure Wazuh server IP address in agent “ossec.conf” file.



```
[2.7.2-RELEASE][admin@pfSense.home.arpa]: cd /var/ossec/etc
[2.7.2-RELEASE][admin@pfSense.home.arpa]/var/ossec/etc: ls
client.keys          local_internal_options.conf.sample  shared
client.keys.sample   localtime                            wpk_root.pem
internal_options.conf ossec.conf                           ossec.conf.sample
local_internal_options.conf
[2.7.2-RELEASE][admin@pfSense.home.arpa]/var/ossec/etc: █
```

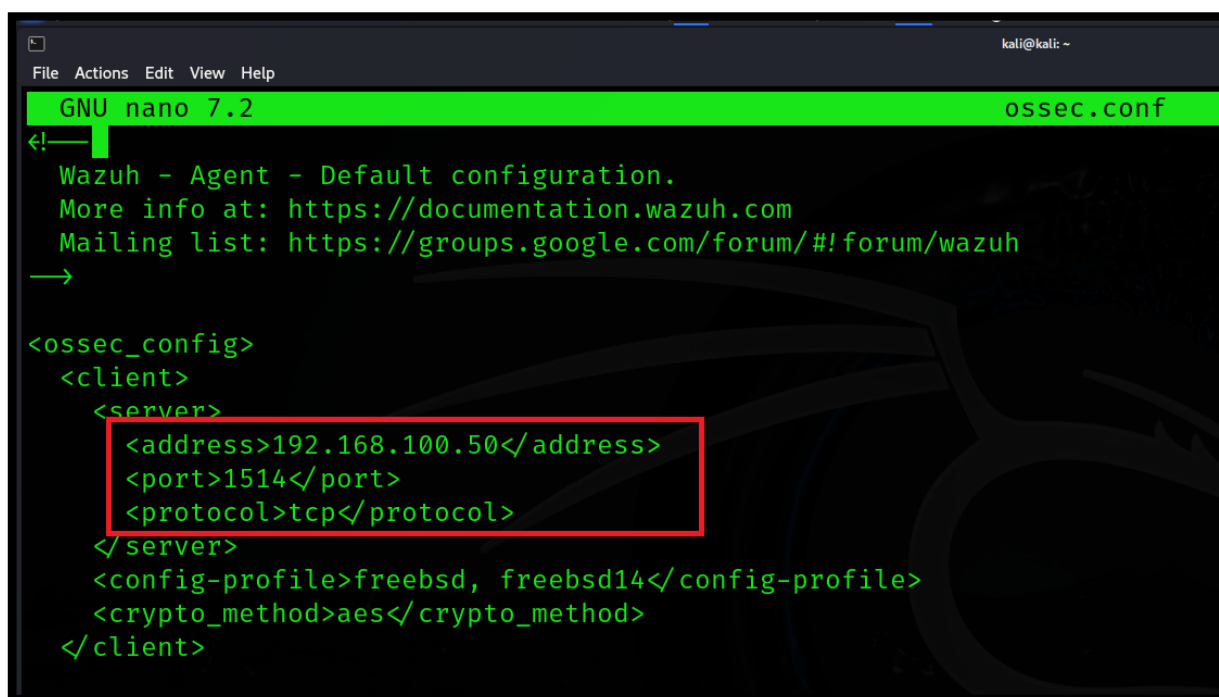

Here is “ossec.conf” file of Wazuh-agent in pfSense.



```
GNU nano 7.2 ossec.conf
Wazuh - Agent - Default configuration.
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh

<ossec_config>
  <client>
    <server>
      <address></address>
      <port>1514</port>
      <protocol>udp</protocol>
    </server>
    <config-profile>freebsd, freebsd14</config-profile>
    <crypto_method>aes</crypto_method>
  </client>
```

Set Wazuh-server IP address and protocol “tcp” and save changes.

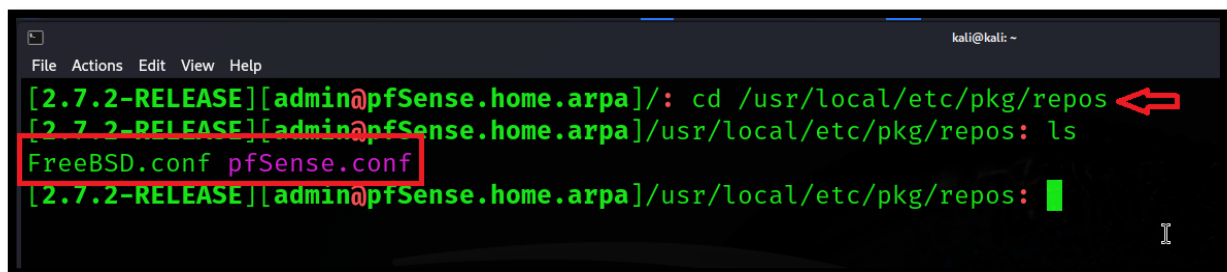


```
GNU nano 7.2 ossec.conf
Wazuh - Agent - Default configuration.
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh

<ossec_config>
  <client>
    <server>
      <address>192.168.100.50</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>freebsd, freebsd14</config-profile>
    <crypto_method>aes</crypto_method>
  </client>
```

Now Wazuh-agent is configured. In the next step we have to revert repository configuration.

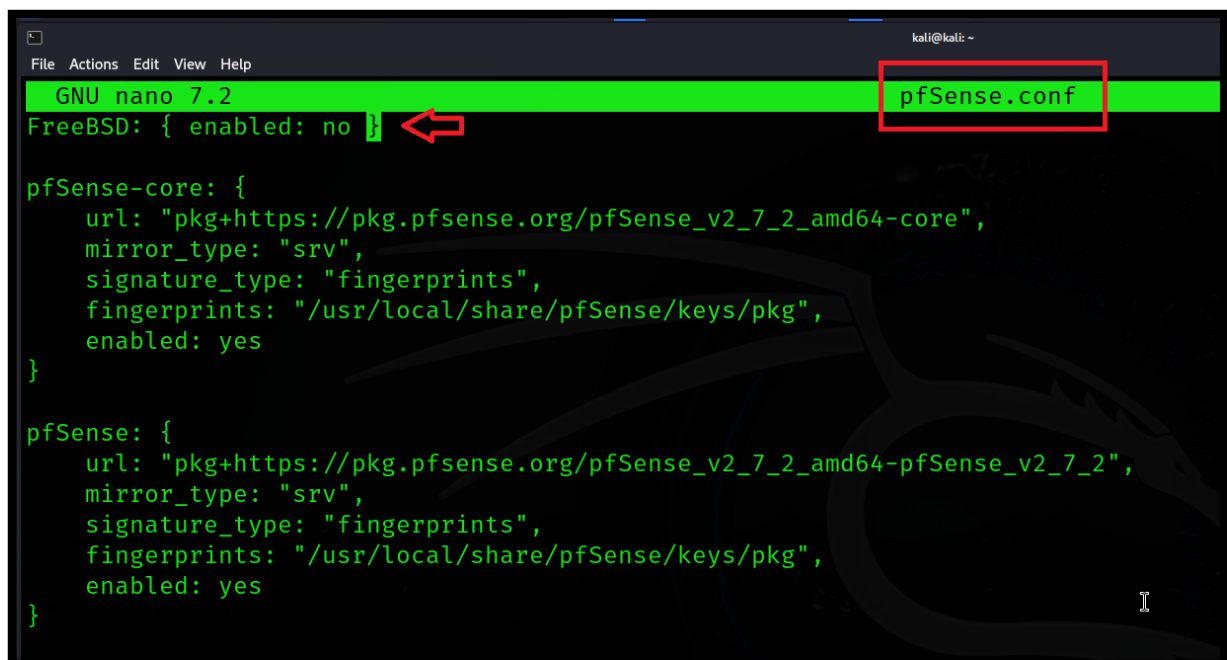
Step 02: Go again to “/usr/local/etc/pkg/repos” directory and revert configuration by following figures.



```
kali@kali: ~  
[2.7.2-RELEASE][admin@pfSense.home.arpa]: cd /usr/local/etc/pkg/repos  
[2.7.2-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: ls  
FreeBSD.conf  pfSense.conf  
[2.7.2-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: █
```

A terminal window showing the user navigating to the directory /usr/local/etc/pkg/repos and listing its contents. The files FreeBSD.conf and pfSense.conf are listed. A red box highlights the file names, and a red arrow points to the directory path in the first command.

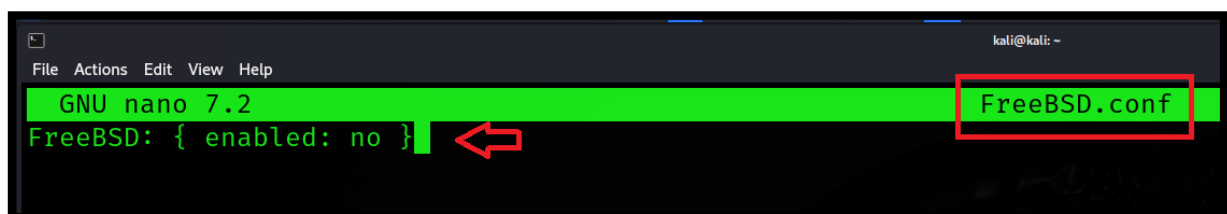
Open “pfSense.conf” file in nano editor and set FreeBSD parameter “yes” to “no”.



```
GNU nano 7.2 pfSense.conf  
FreeBSD: { enabled: no }  
  
pfSense-core: {  
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",  
  mirror_type: "srv",  
  signature_type: "fingerprints",  
  fingerprints: "/usr/local/share/pfSense/keys/pkg",  
  enabled: yes  
}  
  
pfSense: {  
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-pfSense_v2_7_2",  
  mirror_type: "srv",  
  signature_type: "fingerprints",  
  fingerprints: "/usr/local/share/pfSense/keys/pkg",  
  enabled: yes  
}
```

A terminal window showing the pfSense.conf file being edited in nano. The FreeBSD parameter is set to no. A red box highlights the filename pfSense.conf, and a red arrow points to the FreeBSD parameter line.

Set same parameter in “FreeBSD.conf” file and save changes.



```
GNU nano 7.2 FreeBSD.conf  
FreeBSD: { enabled: no }
```

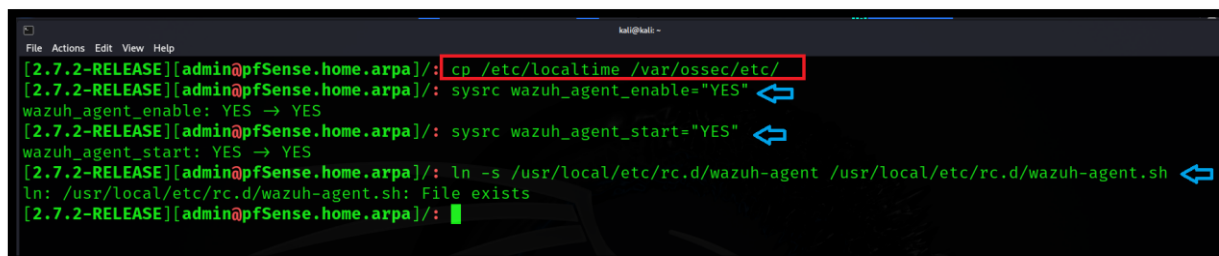
A terminal window showing the FreeBSD.conf file being edited in nano. The FreeBSD parameter is set to no. A red box highlights the filename FreeBSD.conf, and a red arrow points to the FreeBSD parameter line.

Now we have to enable Wazuh agent and configure start on boot.

Command: `sysrc wazuh_agent_enable="YES"`

Command: `sysrc wazuh_agent_start="YES"`

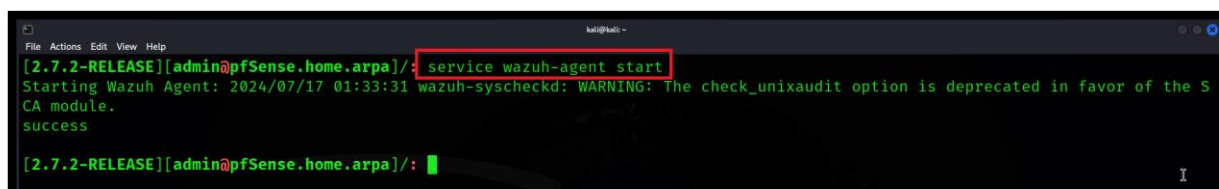
Command: `ln -s /usr/local/etc/rc.d/wazuh-agent /usr/local/etc/rc.d/wazuh-agent.sh`



```
[2.7.2-RELEASE][admin@pfSense.home.arpa]: cp /etc/localtime /var/ossec/etc/
[2.7.2-RELEASE][admin@pfSense.home.arpa]: sysrc wazuh_agent_enable="YES"
wazuh_agent_enable: YES → YES
[2.7.2-RELEASE][admin@pfSense.home.arpa]: sysrc wazuh_agent_start="YES"
wazuh_agent_start: YES → YES
[2.7.2-RELEASE][admin@pfSense.home.arpa]: ln -s /usr/local/etc/rc.d/wazuh-agent /usr/local/etc/rc.d/wazuh-agent.sh
ln: /usr/local/etc/rc.d/wazuh-agent.sh: File exists
[2.7.2-RELEASE][admin@pfSense.home.arpa]:
```

Now start Wazuh-agent service

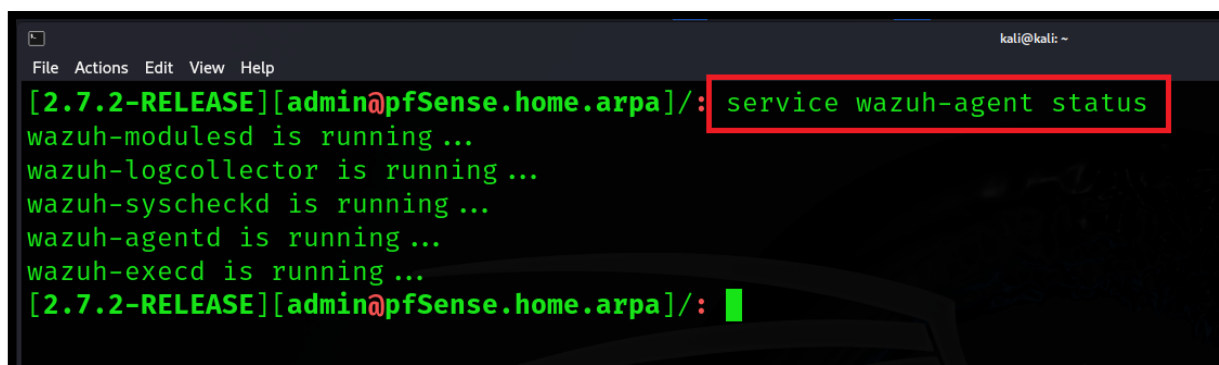
Command: `service wazuh-agent start`



```
[2.7.2-RELEASE][admin@pfSense.home.arpa]: service wazuh-agent start
Starting Wazuh Agent: 2024/07/17 01:33:31 wazuh-syscheckd: WARNING: The check_unixaudit option is deprecated in favor of the S
CA module.
Success
[2.7.2-RELEASE][admin@pfSense.home.arpa]:
```

Check the status of running Wazuh services.

Command: `service wazuh-agent status`

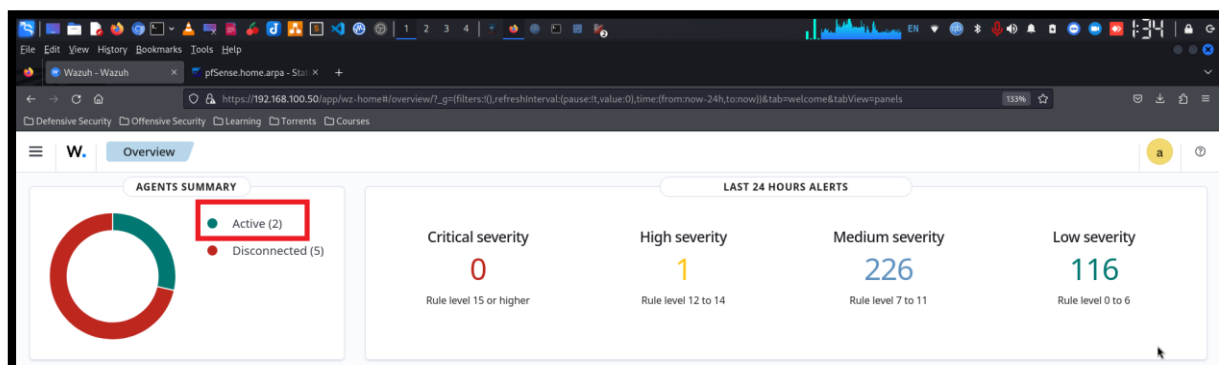


```
[2.7.2-RELEASE][admin@pfSense.home.arpa]: service wazuh-agent status
wazuh-modulesd is running...
wazuh-logcollector is running...
wazuh-syscheckd is running...
wazuh-agentd is running...
wazuh-execd is running...
[2.7.2-RELEASE][admin@pfSense.home.arpa]:
```

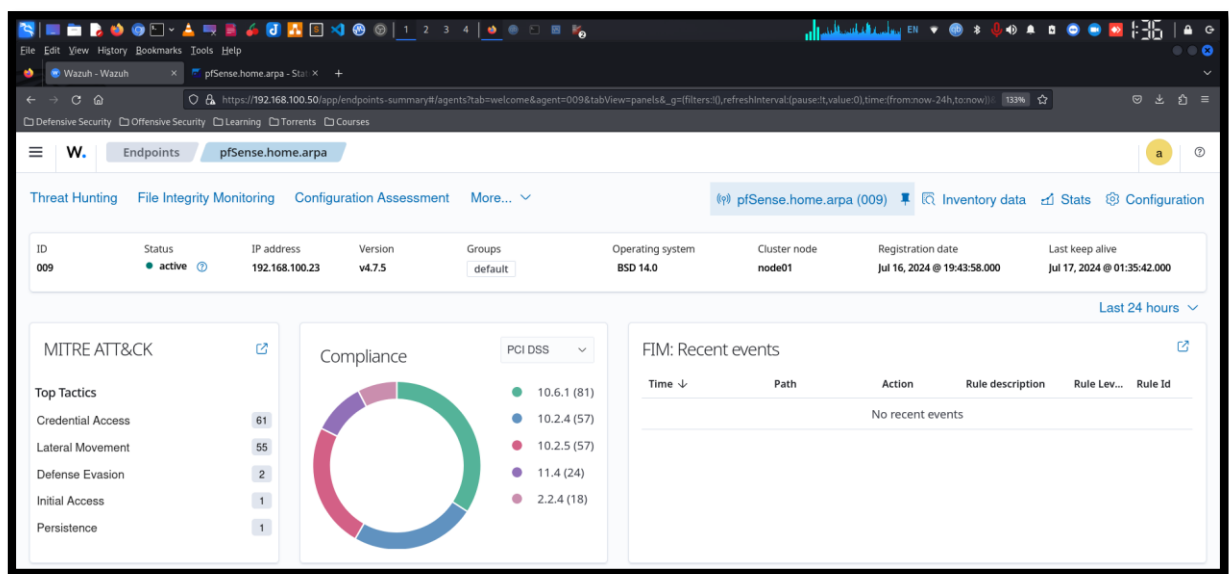
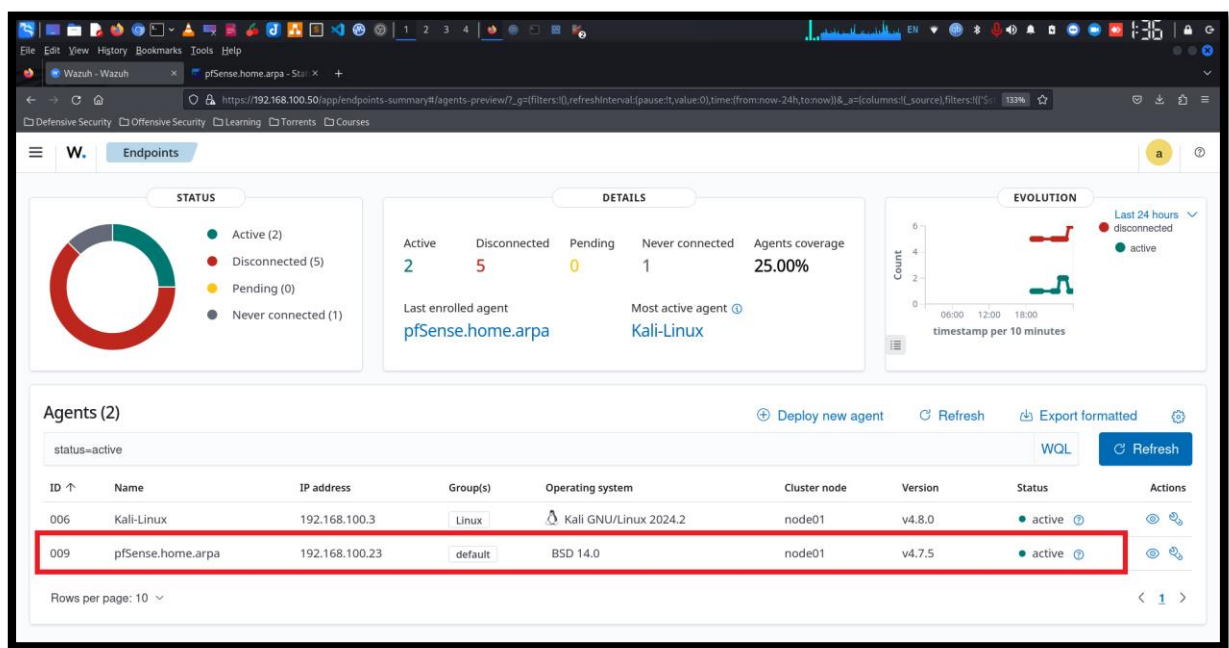
Update repository with “pkg update -f” command.

```
[2.7.2-RELEASE][admin@pfSense.home.arpa]: pkg update -f
Updating pfSense-core repository catalogue ...
Fetching meta.conf: 100% 163 B 0.2kB/s 00:01
Fetching packagesite.pkg: 100% 1 KiB 1.5kB/s 00:01
Processing entries: 100%
pfSense-core repository update completed. 4 packages processed.
Updating pfSense repository catalogue ...
Fetching meta.conf: 100% 178 B 0.2kB/s 00:01
Fetching data.pkg: 100% 157 KiB 53.5kB/s 00:03
Processing entries: 100%
pfSense repository update completed. 550 packages processed.
All repositories are up to date.
[2.7.2-RELEASE][admin@pfSense.home.arpa]:
```

Now go to Wazuh dashboard, here is 2 Active agents. Click on active agents.



pfSense.homearpa agent is connected with IP address 192.168.100.23 and active.



SUMMARY:

Integrating Wazuh with pfSense firewall allows for enhanced security monitoring by providing visibility into firewall events and potential threats. This integration helps in proactive threat detection and efficient incident response, ensuring a robust security posture for your network infrastructure.

Regards

MUHAMMAD MOIZ UD DIN RAFAY

Ethical Hacker | Cyber Security Analyst

Need Training on Wazuh..?

Contact: +92-3004962168

Email: muhammadmoizuddinrafay@gmail.com

LinkedIn: www.linkedin.com/in/moizuddinrafay