

Wazuh – pfSense

FIREWALL INTEGRATION

Created By : Sayed Waqar Ali Bacha

Integration of Wazuh with pfSense Firewall

Introduction:

Integrating Wazuh with pfSense Firewall lets you keep a close eye on your network's security. Wazuh is a free tool that monitors security events, while pfSense is a free firewall that protects your network. By linking them together, Wazuh can track and analyze what's happening on your network, helping you spot any potential security threats. This integration boosts your overall security by giving you a clear view of your network traffic and any risks that might come up.

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.

```
192.168.71.130 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
Password for admin@pfSense.home.arpa:
End of keyboard-interactive prompts from server
VMware Virtual Machine - Netgate Device ID: 3dc4cc437cdf48534fd8

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.71.130/24

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: 0

root@server: /home/waqar
System load: 0.02734375    Processes: 128
Usage of /: 33.2% of 29.12GB    Users logged in: 1
Memory usage: 18%          IPv4 address for enp0s3: 192.168.100.127
Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

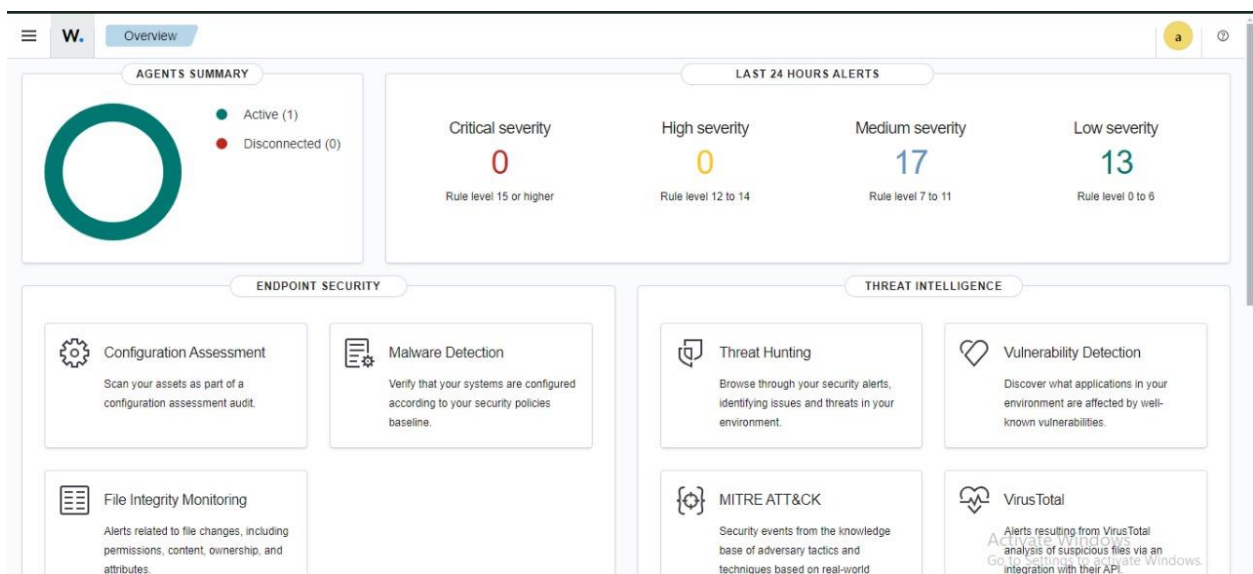
Expanded Security Maintenance for Applications is not enabled.

28 updates can be applied immediately.
27 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Aug 15 08:48:15 2024
waqar@server:~$ sudo -s
[sudo] password for waqar:
root@server:/home/waqar#
```

➤ Wazuh Dashboard



➤ PfSense Dashboard

Not secure https://192.168.71.130

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.71.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 3dc4cc437cdf48534fd8
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Thu Aug 15 9:15:38 UTC 2024
CPU Type	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

Activate Windows
Go to Settings to activate Windows

- **Step 01**: Access pfSense via SSH
- We can access PfSense Through Putty

```
192.168.71.130 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
Password for admin@pfSense.home.arpa:
End of keyboard-interactive prompts from server
VMware Virtual Machine - Netgate Device ID: 3dc4cc437cdf48534fd8

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.71.130/24

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: █
```

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

```
192.168.71.130 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
| Password for admin@pfSense.home.arpa:
| End of keyboard-interactive prompts from server
VMware Virtual Machine - Netgate Device ID: 3dc4cc437cdf48534fd8

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.71.130/24

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

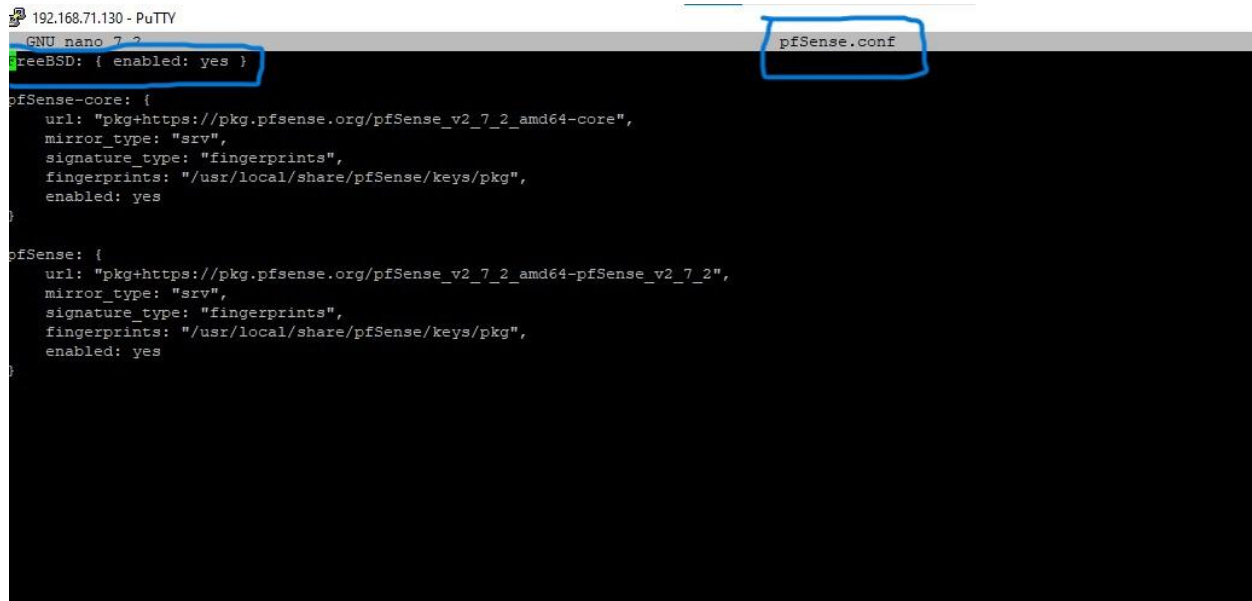
Enter an option: 8

[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.

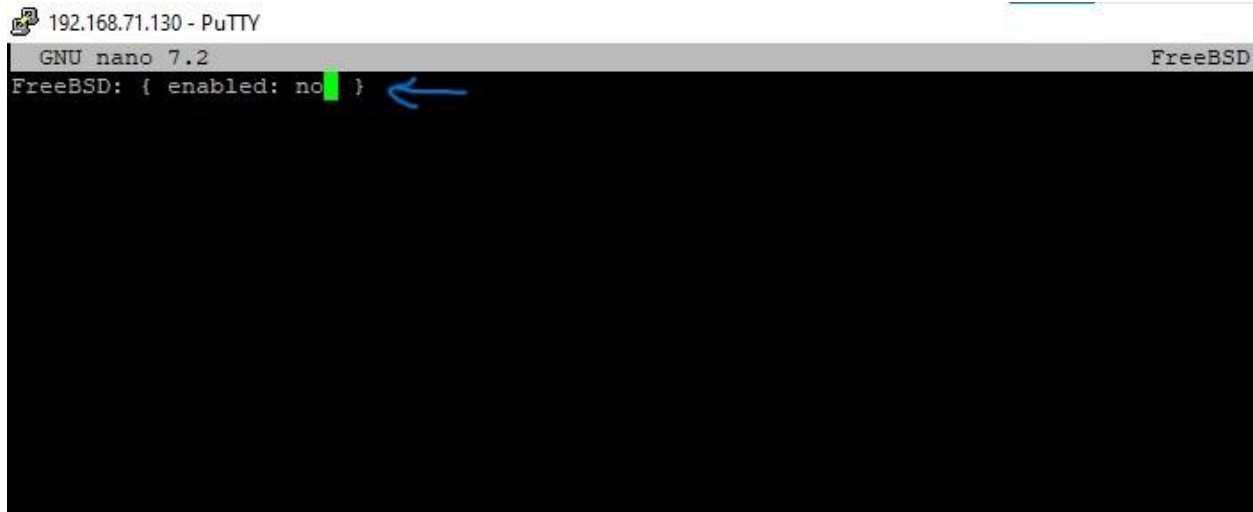
```
[2.7.2-RELEASE] [admin@pfSense.home.arpa]/root: cd /
[2.7.2-RELEASE] [admin@pfSense.home.arpa]/: cd /usr/local/etc/pkg/repos
[2.7.2-RELEASE] [admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: ls
FreeBSD.conf pfSense.conf
[2.7.2-RELEASE] [admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: █
```

- 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.

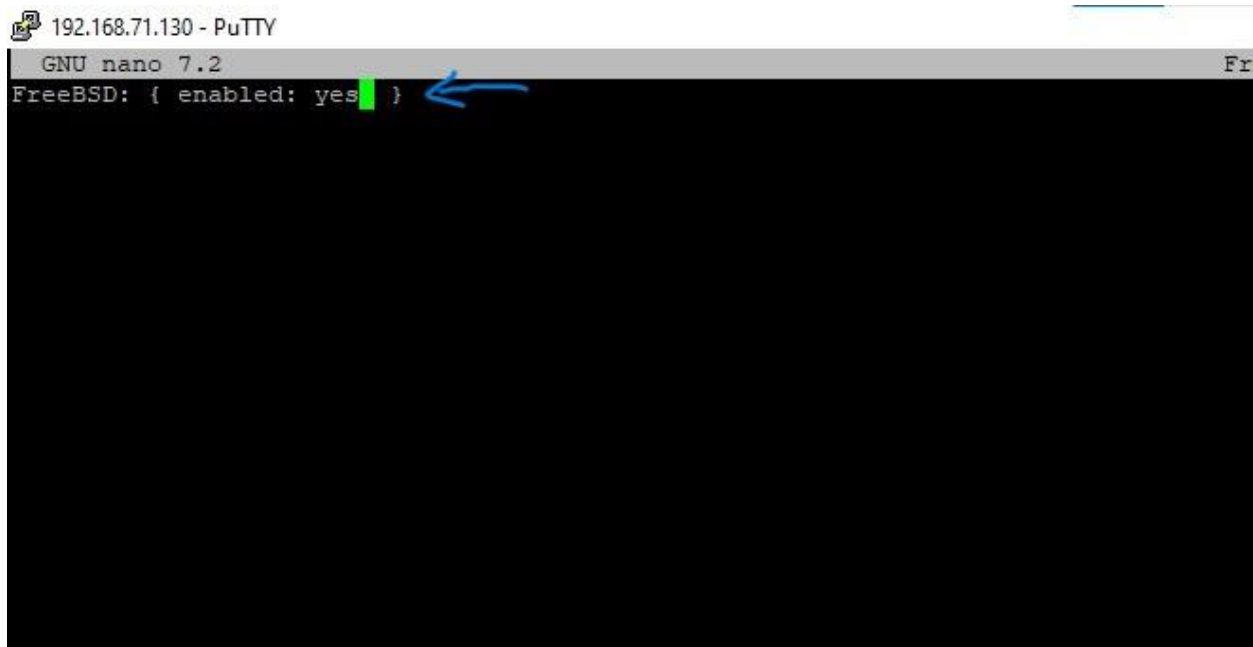


```
192.168.71.130 - PuTTY
GNU nano 2.2.6
freeBSD: { enabled: yes }
pfSense-core: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}
pfSense: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-pfSense_v2_7_2",
  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.



```
192.168.71.130 - PuTTY
GNU nano 7.2
FreeBSD: { enabled: no } ←
```



```
192.168.71.130 - PuTTY
GNU nano 7.2
FreeBSD: { enabled: yes } ←
```


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

```
[2.7.2-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: pkg update -f
Updating FreeBSD repository catalogue...
Fetching meta.conf: 100% 178 B 0.2kB/s 00:01
Fetching packagesite.pkg: 100% 7 MiB 13.0kB/s 09:33
Processing entries: 0%
Newer FreeBSD version for package zziplib:
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. 35262 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 packagesite.pkg: 100% 157 KiB 160.4kB/s 00:01
Processing entries: 100%
pfSense repository update completed. 550 packages processed.
All repositories are up to date.
[2.7.2-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos:
```

- When update is complete, search for Wazuh-agent package.
- Command: `pkg search Wazuh-agent`
- The available Wazuh-agent package is “Wazuh-agent-4.7.5”
- Now install this.
- Command: `pkg install Wazuh-agent-4.7.5`

```
192.168.71.130 - PuTTY
[2.7.2-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: 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]/usr/local/etc/pkg/repos:
```

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

Command : `cd /var/ossec/etc`

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

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

```
192.168.71.130 - PuTTY
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
-->

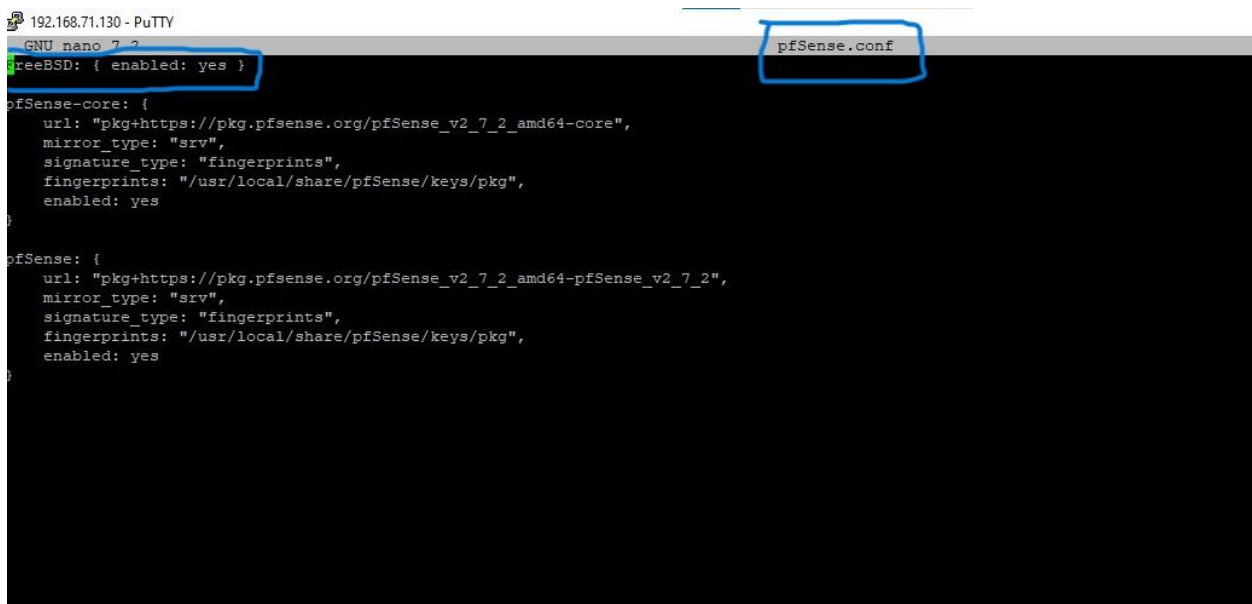
<ossec_config>
  <client>
    <server>
      <address>192.168.100.127</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>freebsd, freebsd14</config-profile>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>
```

- 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

```
[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: █
```

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

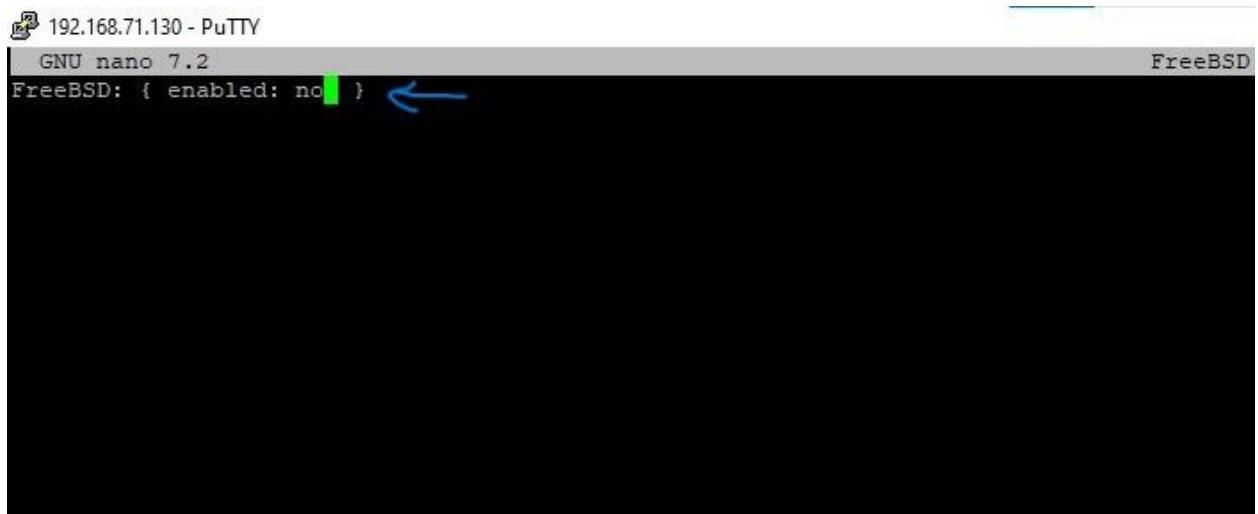


```
192.168.71.130 - PuTTY  
GNU nano 2.9.3  
FreeBSD: { enabled: yes }  
pfSense.conf  
pfSense-core: {  
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",  
  mirror_type: "srv",  
  signature_type: "fingerprints",  
  fingerprints: "/usr/local/share/pfSense/keys/pkg",  
  enabled: yes  
}  
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  
}
```

- Set same parameter in “FreeBSD.conf” file like we set it to yes
Now we will Set it “No” again.



```
192.168.71.130 - PuTTY
GNU nano 7.2
FreeBSD: { enabled: yes } ←
```



```
192.168.71.130 - PuTTY
GNU nano 7.2
FreeBSD: { enabled: no } ←
FreeBSD
```

- 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`

```
192.168.71.130 - PuTTY
[2.7.2-RELEASE][admin@pfSense.home.arp]: cp /etc/localtime /var/ossec/etc/
[2.7.2-RELEASE][admin@pfSense.home.arp]: sysrc wazuh_agent_enable="YES"
wazuh_agent_enable: -> YES
[2.7.2-RELEASE][admin@pfSense.home.arp]: sysrc wazuh_agent_start="YES"
wazuh_agent_start: -> YES
[2.7.2-RELEASE][admin@pfSense.home.arp]: 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: No such file or directory
[2.7.2-RELEASE][admin@pfSense.home.arp]: ln -s /usr/local/etc/rc.d/wazuh-agent /usr/local/etc/rc.d/wazuh-agent.sh
[2.7.2-RELEASE][admin@pfSense.home.arp]:
```

- Now start Wazuh-agent service
- Command: `service wazuh-agent start`

```
[2.7.2-RELEASE][admin@pfSense.home.arp]: service wazuh-agent start
Starting Wazuh Agent: 2024/08/15 11:39:45 wazuh-syscheckd: WARNING: The check_unixaudit option is deprecated in favor of the SCA module.
success
[2.7.2-RELEASE][admin@pfSense.home.arp]:
```

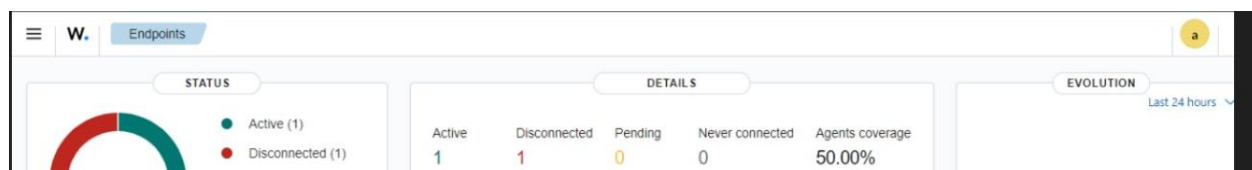
- Check the status of running Wazuh services.
- Command: `service wazuh-agent status`

```
192.168.71.130 - PuTTY
[2.7.2-RELEASE][admin@pfSense.home.arp]: 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.arp]:
```

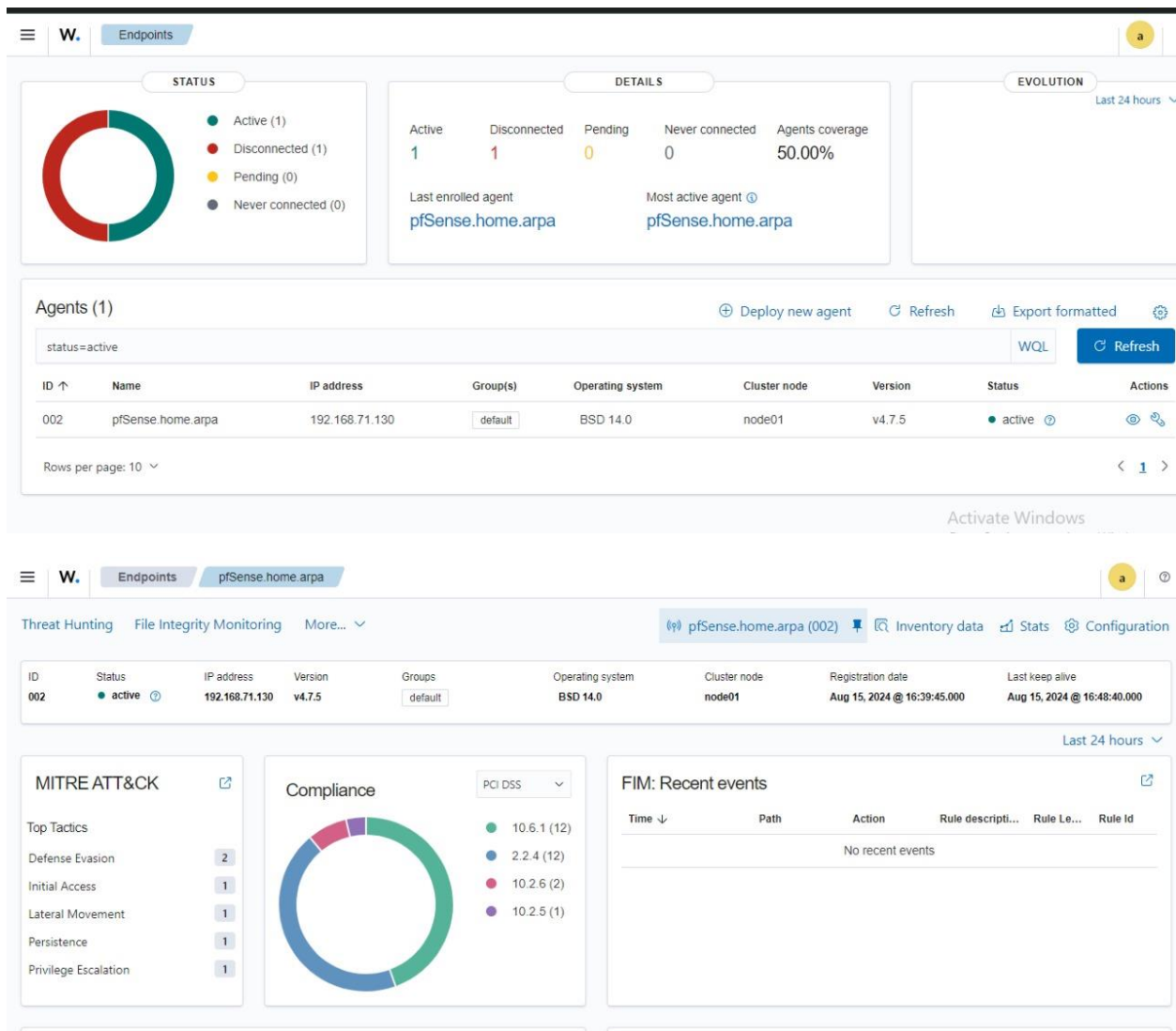
- Update repository with “pkg update -f” command.

```
[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 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]: / :
```

Now go to Wazuh dashboard, here is 1 Active agents. Click on active agent.



- PfSense.home arpa agent is connected with IP address 192.168.71.130 and active.



➤ SUMMARY:

Integrating Wazuh with pfSense enhances security by providing comprehensive visibility into firewall events and network traffic. This integration enables proactive threat detection and streamlined incident response, contributing to a stronger overall security posture for your network.

- **Regards:**
✓ **SAYED WAQAR ALI BACHA**
- **Follow Me On Linkedin:**
✓ **<https://www.linkedin.com/in/waqar-ali-8a5b6b228/>**
- **Contact Number:**
✓ **+92-3466052414**
- **Gmail:**
✓ **Wqrali713@gmail.com**