



Pfsense Firewall Intergration with wazuh

SAMEER HASSAN

Wazuh lab

Github-link: [GitHub - sameerhassancode/Wazuh-](https://github.com/sameerhassancode/Wazuh-)

Linkedin: <https://www.linkedin.com/in/sameer-hassan-15a428255/>

Overview

Wazuh is an open-source Security Information and Event Management (SIEM) tool that provides intrusion detection, log analysis, file integrity monitoring, and real-time threat detection across endpoints and servers.

Architecture Overview

- **Pfsense** acts as the network firewall, generating system, firewall, VPN, and DHCP logs.
- **Wazuh Manager** receives and analyzes logs.
- Logs are forwarded from pfSense via **Syslog (UDP/514)** to Wazuh directly or through a **Syslog server** (e.g., rsyslog).

Pfsense and Wazuh

Integrating pfSense with Wazuh allows for centralized security monitoring, real-time log analysis, and threat detection. This setup is foundational for building a robust SIEM environment in small to enterprise-grade networks.

Pfsense Installation manual:

[Pfsense-Firewall/Pfsense-Project Report-network security.docx at main · sameerhassancode/Pfsense-Firewall · GitHub](#)

Note: skip the internet setting

Need training on Wazuh ?

Contact number: +923355345678

Email: sameeerishassan@gmail.com

Linkedin: <https://pk.linkedin.com/in/sameer-hassan-15a428255>

Other SIEM

1. IBM Qradar
2. Splunk
3. Azure Sentinel

PfSense:

Log into pfSense web interface using **WAN ip : 192.168.0.117**

```
Enabling SSHD...
Reloading firewall rules. done.

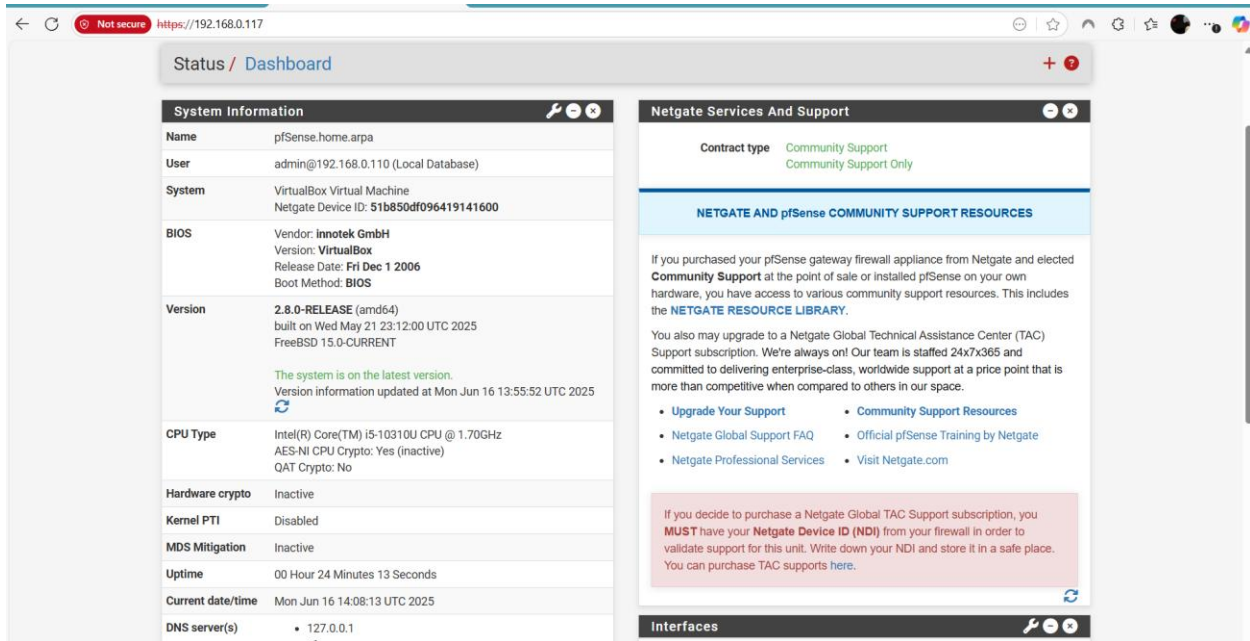
VirtualBox Virtual Machine - Netgate Device ID: 51b850df096419141600
*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 192.168.0.117/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address     11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                   14) Enable Secure Shell (sshd)
6) Halt system                     15) Restore recent configuration
7) Ping host                       16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Jun 16 14:07:33 ...
php-fpm[622191]: /index.php: Successful login for user 'admin' from: 192.168.0.11
0 (Local Database)
```

Pfsense Dashboard:



Enable the SSH login:

Select 14 to Enable SSH and press y to enable it

```
*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 192.168.0.117/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                   14) Enable Secure Shell (sshd)
6) Halt system                     15) Restore recent configuration
7) Ping host                       16) Restart PHP-FPM
8) Shell

Enter an option: 14

SSHD is currently disabled. Would you like to enable? [y/n]? S
```

Now access the pfsense using SSH:

Command:

Ssh [admin@192.168.0.117](https://192.168.0.117)

Password: pfsense

```
C:\WINDOWS\system32\cmd. x + v
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Users\786>ssh admin@192.168.0.117
The authenticity of host '192.168.0.117 (192.168.0.117)' can't be established.
ED25519 key fingerprint is SHA256:rVvTsb/07d637Je6yTLrEduvtY9vH9IuFWxIJ+UK5iE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.0.117' (ED25519) to the list of known hosts.
(admin@192.168.0.117) Password for admin@pfSense.home.arpa:
VirtualBox Virtual Machine - Netgate Device ID: 51b850df096419141600

*** Welcome to pfSense 2.8.0-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 192.168.0.117/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and 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: |
```

Now Press 8 to get the Shell

```
8) Shell
Enter an option: |
```

After Shell access change directory to

`Cd /usr/local/etc/pkg/repos`

And you will see the file `pfsense.conf`

```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: pwd
/usr/local/etc/pkg/repos
[2.8.0-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: ls
FreeBSD.conf pfSense.conf
[2.8.0-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: |
```

Open the file using
`nano pfsense.conf`

If nano not found install using usin

pkg install nano

```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: yum install nano
yum: Command not found.
[2.8.0-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: pkg install nano
Updating pfSense-core repository catalogue...
Fetching meta.conf: 0%
Fetching data.pkg: 0%
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
|
```

After opening the pfsense.conf file look for “FreeBsd” option



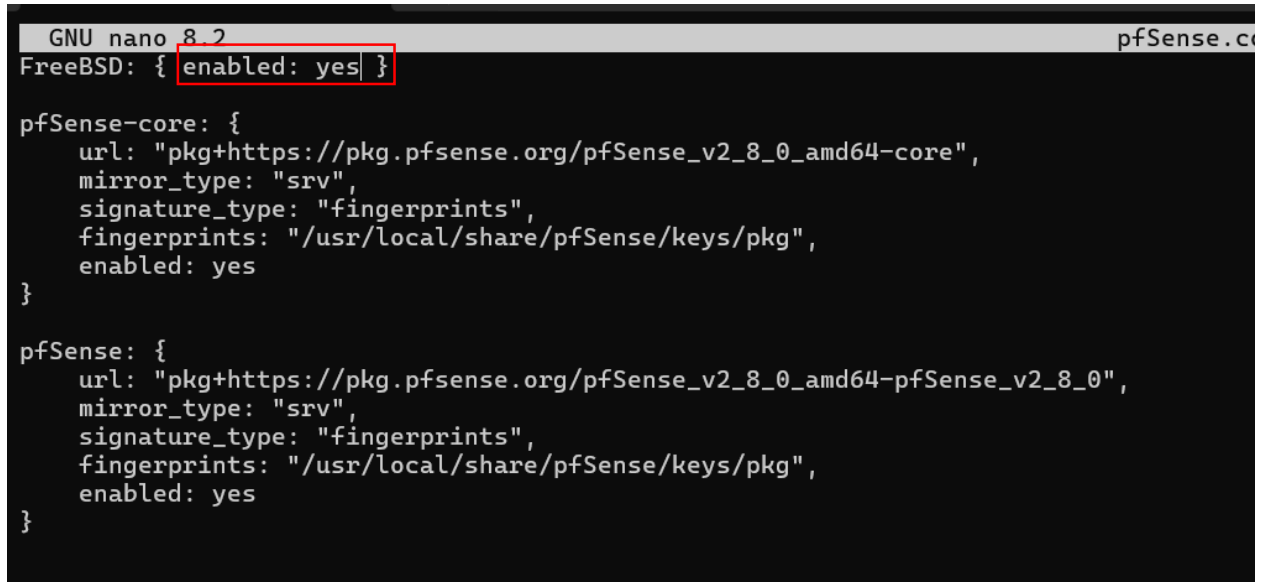
A screenshot of a terminal window showing the pfSense.conf file being edited with nano. The file is titled 'pfSense.conf'. The line 'FreeBSD: { enabled: no }' is highlighted with a red box. Below it, the 'pfSense-core' and 'pfSense' sections are visible, both with 'enabled: yes'.

```
GNU nano 0.2 pfSense.conf
FreeBSD: { enabled: no }

pfSense-core: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_8_0_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_8_0_amd64-pfSense_v2_8_0",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}
```

Now change No to Yes



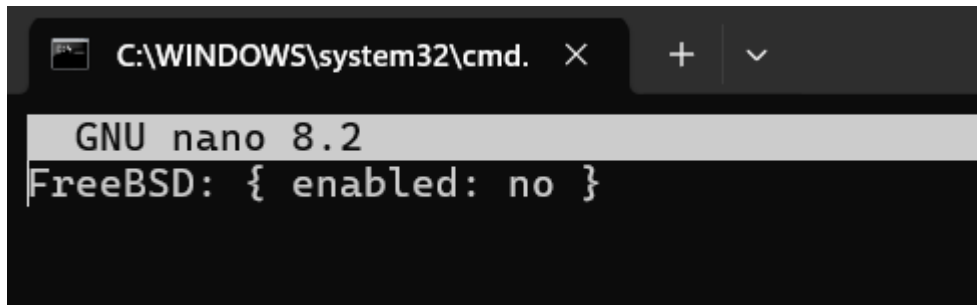
A screenshot of the same terminal window showing the pfSense.conf file. The line 'FreeBSD: { enabled: yes }' is now highlighted with a red box, indicating the change from 'no' to 'yes'. The rest of the file content remains the same.

```
GNU nano 8.2 pfSense.c
FreeBSD: { enabled: yes }

pfSense-core: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_8_0_amd64-core",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}

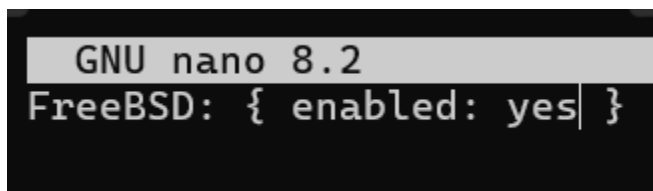
pfSense: {
  url: "pkg+https://pkg.pfsense.org/pfSense_v2_8_0_amd64-pfSense_v2_8_0",
  mirror_type: "srv",
  signature_type: "fingerprints",
  fingerprints: "/usr/local/share/pfSense/keys/pkg",
  enabled: yes
}
```

Save the file and open **FreeBsd.conf**



```
C:\WINDOWS\system32\cmd. X + v
GNU nano 8.2
FreeBSD: { enabled: no }
```

Now enable it. Change it from no to **yes**

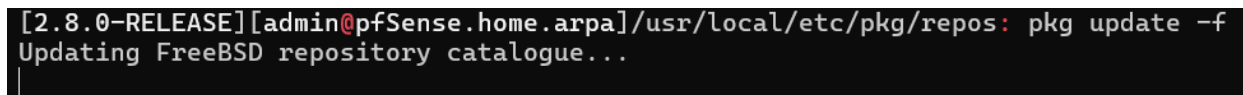


```
GNU nano 8.2
FreeBSD: { enabled: yes }
```

Now after changing both file update the directories

Command:

Pkg update -f

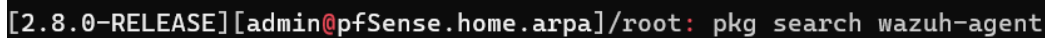


```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/usr/local/etc/pkg/repos: pkg update -f
Updating FreeBSD repository catalogue...
```

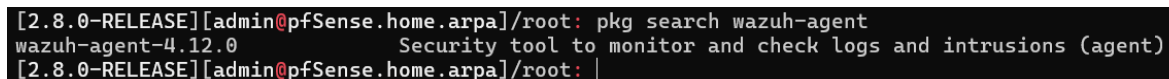
When update it complete search for Wazuh-agent

Command:

Pkg search Wazuh-agent



```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: pkg search wazuh-agent
```



```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: pkg search wazuh-agent
wazuh-agent-4.12.0      Security tool to monitor and check logs and intrusions (agent)
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: |
```

Now install the agent using command

Pkg install Wazuh-agent --v

```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: pkg install wazuh-agent-4.12.0
Updating FreeBSD repository catalogue...
FreeBSD repository is up to date.
Updating pfSense-core repository catalogue...
|
```

After installing change the directory to Wazuh agent configuration file.

Cd /var/ossec/etc/ossec.conf

```
[2.8.0-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
```

Now open the ossec.conf file

```
GNU nano 8.2                                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>IP</address>
      <port>1514</port>
      <protocol>udp</protocol>
    </server>
    <config-profile>freebsd, freebsd15</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>

  <!-- Policy monitoring -->
```

Replace the ip with real Wazuh server ip. In my case ip is **192.168.0.114** and change the protocol from **UDP** to **TCP**

```
<server>
  <address>192.168.0.114</address>
  <port>1514</port>
  <protocol>tcp</protocol>
</server>
<config-profile>freebsd, freebsd15</config-profile>
<crypto_method>aes</crypto_method>
</client>
```


Now again redo the freebsd.conf and Pfsense.conf file from **Yes** to **No**

Go to same folder again

Cd /usr/local/etc/pkg/repos

```
GNU nano 8.2
FreeBSD: { enabled: no| }

pfSense-core: {
    url: "pkg+https://pkg.pfsense.org
```

```
GNU nano 8.2
FreeBSD: { enabled: no }
```

Now enable and start the Wazuh agent using command:

Sysrc Wazuh_agent_enable="yes"

Systc Wazuh_agent_start="yes"

```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: wazuh_agent_enable="YES"
wazuh_agent_enable=YES: Command not found.
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: sysrc wazuh_agent_enable="YES"
wazuh_agent_enable: YES -> YES
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: sysrc wazuh_agent_start="YES"
wazuh_agent_start: -> YES
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: |
```

Now start the Wazuh agent

Command Service Wazuh-agent start

```
wazuh_agent_start: -> YES
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: service wazuh-agent start
Starting Wazuh Agent: success
```

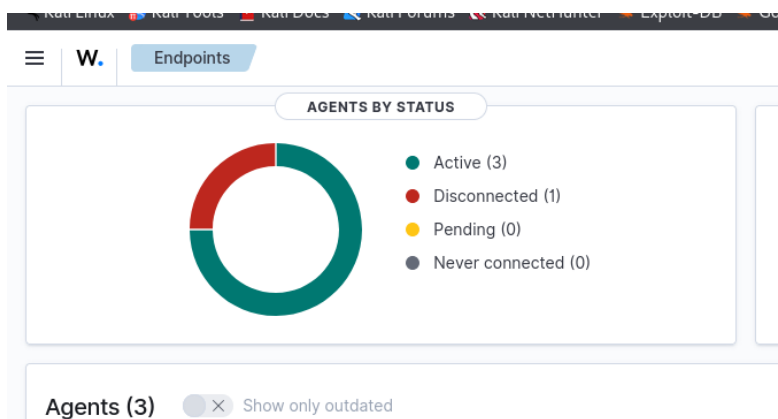
Check the status

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

Update the repository

```
[2.8.0-RELEASE][admin@pfSense.home.arpa]/root: pkg update -f
pkg: Setting ALTABI manually is no longer supported, set ABI and OSVERSION or ABI_FILE instead.
pkg: Setting ABI requires setting OSVERSION, guessing the OSVERSION as: 1500000
Updating pfSense-core repository catalogue...
Fetching meta.conf: 100% 179 B 0.2kB/s 00:01
Fetching data.pkg: 100% 2 KiB 1.6kB/s 00:01
Processing entries: 100%
pfSense-core repository update completed. 4 packages processed.
Updating pfSense repository catalogue...
Fetching meta.conf: 100% 179 B 0.2kB/s 00:01
Fetching data.pkg: 100% 191 KiB 195.2kB/s 00:01
Processing entries: 0%
Newer FreeBSD version for package xxd:
To ignore this error set IGNORE_OSVERSION=yes
- package: 1500029
- running userland: 1500000
Ignore the mismatch and continue? [y/N]: y
```

Now go to the Wazuh dashboard and refresh the page



Pfsense is configured with Wazuh and it's forwarding the logs properly

Agents (3) Show only outdated Deploy new agent Refresh Export formatted More WQL

status=active

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Win-001	192.168.0.109	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	active	
002	win-002	192.168.0.110	default	Microsoft Windows 11 Pro 10.0.26100.4351	node01	v4.12.0	active	
005	pfSense.home.arpa	192.168.0.117	default	BSD 15.0	node01	v4.12.0	active	

Rows per page: 10

W. Endpoints pfSense.home.arpa a

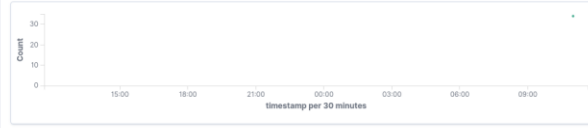
Threat Hunting File Integrity Monitoring Configuration Assessment MITRE ATT&CK Vulnerability Detection More...

pfSense.home.arpa (005) Inventory data Stats Configuration

ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
005	active	192.168.0.117	Wazuh v4.12.0	default	BSD 15.0	node01	Jun 16, 2025 @ 11:12:51.000	Jun 16, 2025 @ 11:39:12.000

Last 24 hours

Events count evolution



MITRE ATT&CK

Top Tactics

Defense Evasion	2
Initial Access	1
Lateral Movement	1
Persistence	1
Privilege Escalation	1

Compliance

PCI DSS

10.6.1	19
2.2.4	12
10.2.6	2
10.2.5	1

Vulnerability Detection

0 Critical

0 High

Top 5 Packages

Package	Count
---------	-------

You don't have SCA scans in this agent.

Check your agent settings to generate scans.

Nothing is playing

Forwarding Syslog:

Open Your Pfsense web dashboard

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help 2

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Status / Dashboard + ?

System Information

Name	pfSense.home.arpa
User	admin@192.168.0.110 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 51b850df096419141600
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006 Boot Method: BIOS
Version	2.8.0-RELEASE (amd64) built on Wed May 21 23:12:00 UTC 2025 FreeBSD 15.0-CURRENT The system is on the latest version. Version information updated at Mon Jun 16 13:55:52 UTC 2025
CPU Type	Intel(R) Core(TM) i5-10310U CPU @ 1.70GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

Netgate Services And Support

Contract type Community Support
Community Support Only

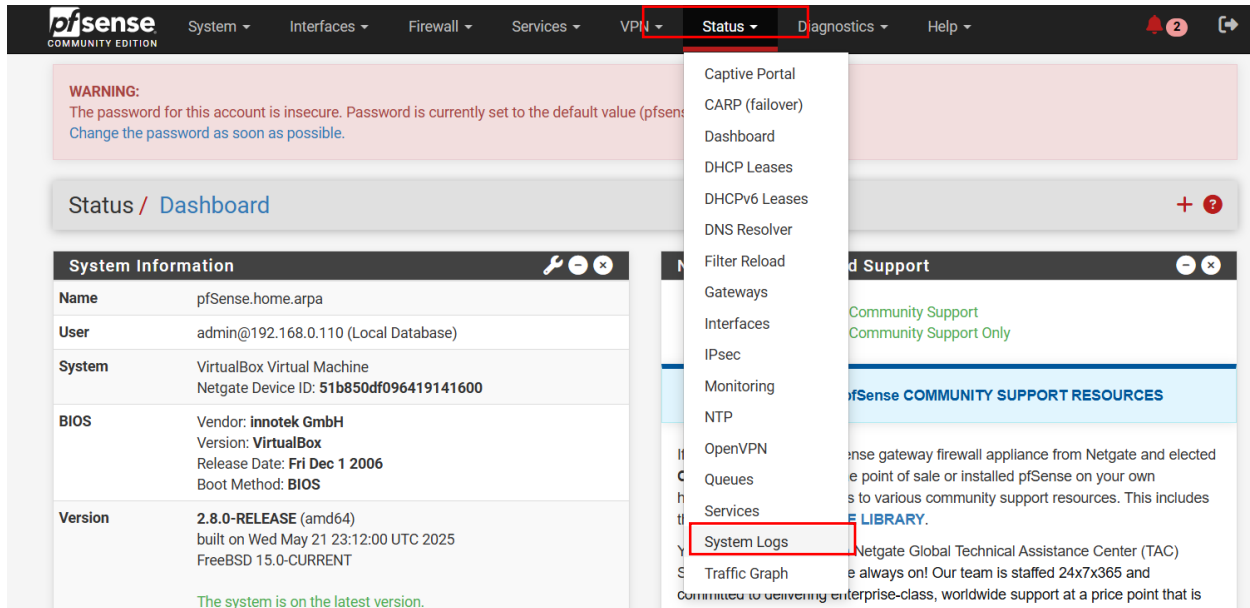
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

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**.

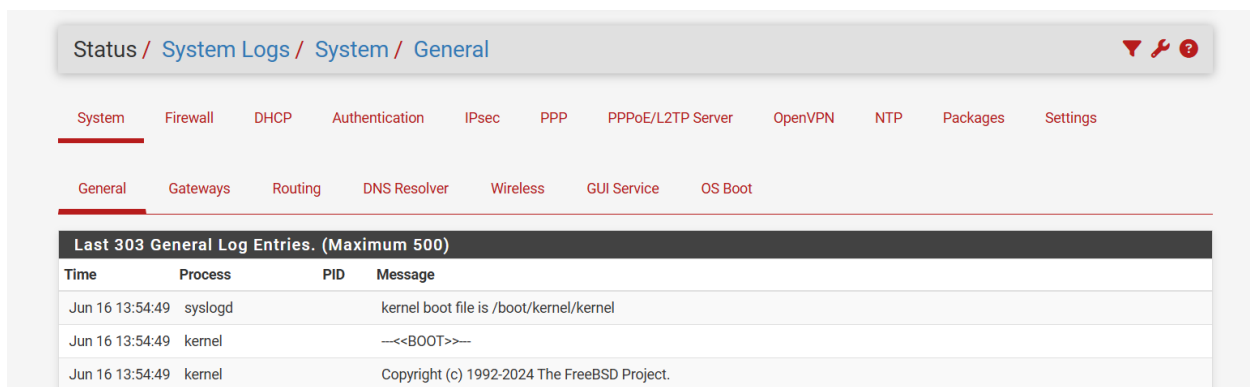
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

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

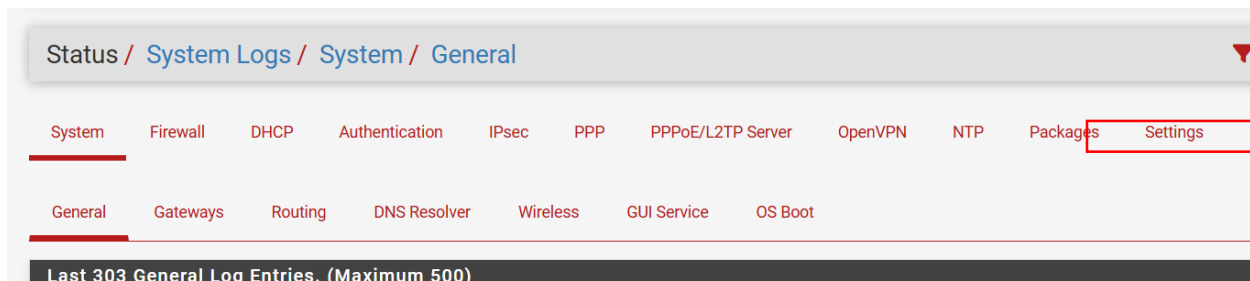
And Navigate to Status > System Logs > Settings



Click on System logs




Now go to setting and enable Remote logging



At the end of the page you will see the remote logging option

Remote Logging Options

Enable Remote Logging ☐ Send log messages to remote syslog server

 Save

Enable it and select the source ip **WAN**

Remote Logging Options

Enable Remote Logging ☒ Send log messages to remote syslog server

Source Address

WAN

Default (any) rather than all IP addresses. If a single IP is picked, remote syslog servers bind to all interfaces.

WAN demon will bind to all addresses.

Localhost

IP Protocol

IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the

Now add your Wazuh server ip and port

selected type is not found on the chosen interface, the other type will be used.

Remote log servers

192.168.0.101:1514

IP[:port]

IP[:port]

After that select the logs option you want to forward to the Wazuh server

Remote Syslog Contents

☐ Everything

☒ System Events

☒ Firewall Events

☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)

☒ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)

☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)

☒ General Authentication Events

☐ Captive Portal Events

☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)

☐ Gateway Monitor Events

☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)

☐ Network Time Protocol Events (NTP Daemon, NTP Client)


☒ Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Now save the file.

☒ **Wireless Events (hostapd)**

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, u
server to accept syslog messages from pfSense.

 Save

Summary:

Successfully integrated the Wazuh agent with pfSense by enabling and configuring it correctly using FreeBSD's service management system. After resolving startup warnings caused by incorrect variable names in `/etc/rc.conf`, you ensured the agent starts cleanly and securely at boot. Now, your pfSense logs and system events can be monitored centrally through Wazuh, improving visibility and security for your network infrastructure.

Need training on Wazuh ?

Contact number: +923355345678

Email: sameeerishassan@gmail.com

Linkedin: <https://pk.linkedin.com/in/sameer-hassan-15a428255>

Other SIEM

1. IBM Qradar
2. Splunk
3. Azure Sentinel