

TASK-2 : WAZUH x FIREWALL

Syed Muhammad Shah

TEAM ~ OMEGA

1) installing pfsense

Install firewall iso from official netgate website (<https://www.pfsense.org/download/>)

Setup & boot the VM in virtual box with following settings,

- RAM: 2 GB
- CPU: 1 core
- Disk: 20 GB

During installation , Add two network adapters:

- Adapter 1: Bridged for (WAN)
- Adapter 2: Internal Network for (LAN).

On first boot, pfSense will ask to assign interfaces:

- Assign WAN to Adapter 1, LAN to Adapter 2.

For Reference Video (<https://www.youtube.com/watch?v=Y-Dj8lHmXy8>)

2) Network Setup (Topology)

We want: All traffic from Kali → pfSense LAN → pfSense WAN → Router → Internet.

That way pfSense can filter traffic, log, and send logs to Wazuh.

- **pfsense VM:**
 - Adapter 1 = Bridged (WAN) → gets IP from router (DHCP keep as is).
 - Adapter 2 = Internal Network (LAN) → keep (192.168.0.1/24).

For 2 , we go to pfsense VM > option 2 > setup static LAN ip v4 to 192.168.0.1/24 (follow instructions)

- **Kali VM:**
 - Adapter 1 = Internal Network Adapter (same as pfsense LAN).
 - Remove Bridged (or disable).

For 1, after setup adapter in VBox > in kali linux

- sudo nano /etc/network/interfaces
- add this to file ,

```
auto eth0

iface eth0 inet static
    address 192.168.0.101
    netmask 255.255.255.0
    gateway 192.168.0.1
    dns-nameservers 8.8.8.8
```

Save.

- sudo systemctl restart networking

- **Wazuh VM:**

- Adapter 1 = Internal Network Adapter (same as pfSense LAN).
- If Wazuh needs Internet → you can add second adapter = Bridged/NAT (optional). But no need for me .

For 1 , in wazuh VM

- sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
- remove default and add this .

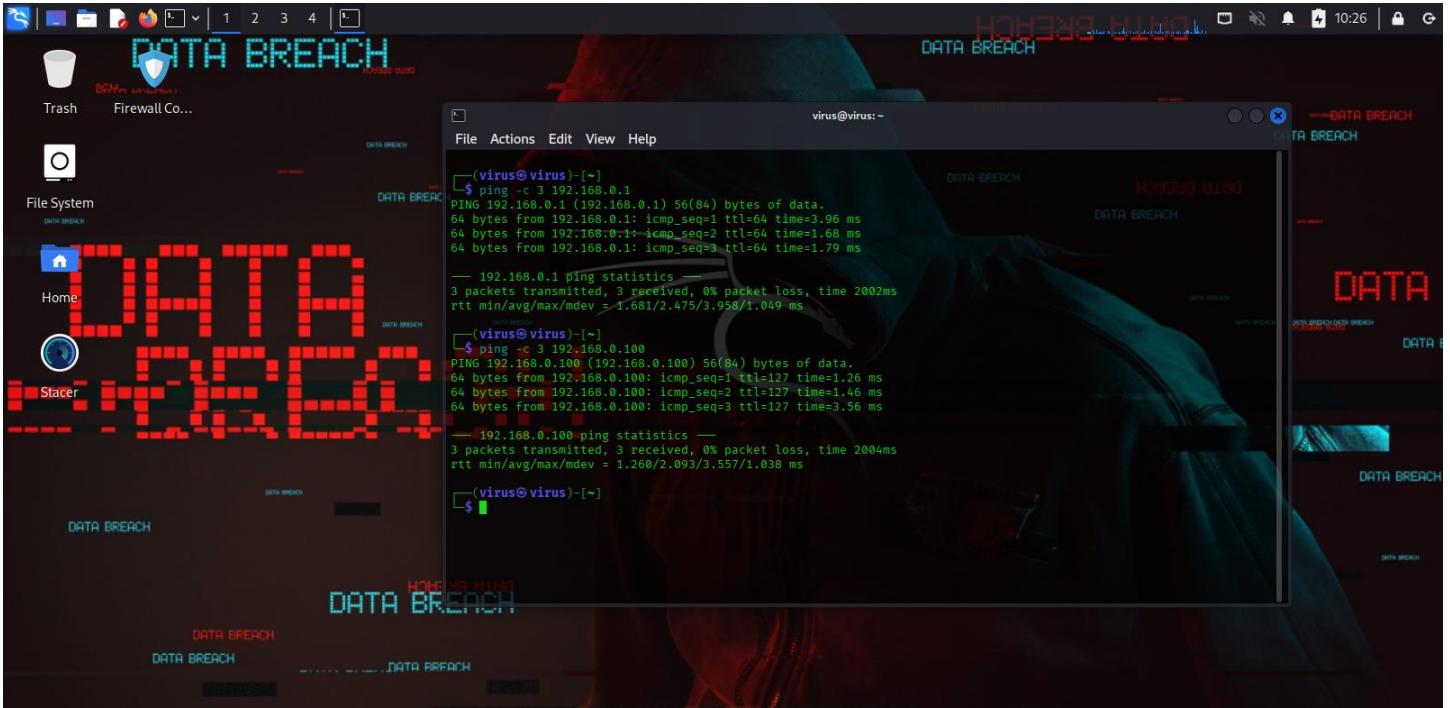
```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
TYPE=Ethernet
IPADDR=192.168.0.100
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
DNS1=8.8.8.8
DNS2=1.1.1.1
```

Save .

➤ sudo systemctl restart network

☞ This way, both Kali & Wazuh will be behind pfSense.

Verify Connections .



Checking Dashboards.

For pfSense first time access dashboard .

<http://192.168.0.1> (admin/pfsense) > then i change password

also switch to https,

Go to System → Advanced → Admin Access.

Under *Protocol*, choose HTTPS (default is HTTP on fresh installs).

Save & apply.

Now access properly (<https://192.168.0.1>)

For Wazuh is Already Same Setup in Task 1 .

<https://192.168.0.100>

Running Machines Check.

Terminal 1 (Wazuh host):

```
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qdisc qdisc none
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 brd :: scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qdisc qdisc none
        link/ether 00:00:27:2f:5f:37 brd ff:ff:ff:ff:ff:ff
        altname enp0s17
        inet 192.168.0.100/24 metric 1024 brd 192.168.0.255 scope global dynamic eth0
            valid_lft 4947sec preferred_lft 4947sec
            inet6 fe80::200:27ff:fe2f:5f37/64 scope link proto kernel ll
                valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

Terminal 2 (pfSense host):

```
[2.8.0-RELEASE]# grep 443 /var/log/syslog
[2.8.0-RELEASE]# ./index.php: Successful login for user 'admin' from: 192.168.0.101 (Local Database)
Message from syslogd@pfSense at Aug 18 15:09:59 ...
php-fpm[442]: ./index.php: Successful login for user 'admin' from: 192.168.0.101 (Local Database)
```

A) Blocking Countries-Geoip

installed pfBlockerNG-devel.

Please wait while the installation of **pfSense-pkg-pfBlockerNG-devel** completes.
This may take several minutes. Do not leave or refresh the page!

Installed Packages Available Packages Package Installer

Package Installation

```

lua54: 5.4.7 [pfSense]
nettle: 3.10.1 [pfSense]
pfSense-pkg-pfBlockerNG-devel: 3.2.8 [pfSense]
py311-maxminddb: 2.6.2 [pfSense]
py311-setuptools: 63.1.0.1 [pfSense]
py311-sqlite3: 3.11.11_8 [pfSense]
rsync: 3.4.0 [pfSense]
xxhash: 0.8.2_1 [pfSense]

```

Number of packages to be installed: 13

The process will require 27 MiB more space.
9 MiB to be downloaded.

[1/13] Fetching py311-sqlite3-3.11.11_8.pkg: ... done

Firewall / pfBlockerNG

General IP DNSBL Update Reports Feeds Logs Sync Wizard

General Settings

Links	Firewall Aliases	Firewall Rules	Firewall Logs
pfBlockerNG	<input checked="" type="checkbox"/> Enable	Note: Context help is available on various pages by clicking the 'blue infoblock' icons →	
Keep Settings	<input checked="" type="checkbox"/> Enable	Note: With 'Keep settings' enabled, pfBlockerNG will maintain run state on Installation/Upgrade. If 'Keep Settings' is not 'enabled' on pkg Install/De-Install, all settings will be Wiped!	
Note: To clear all downloaded lists, uncheck these two checkboxes and 'Save'. Re-check both boxes and run a 'Force Update Reload'			
CRON Settings	Every hour	00	0
	Default: Every hour	Default: :00	Default: 0
	Select the Cron hour interval.	Select the Cron update minute.	Select the Cron start hour.
Download Failure Threshold	No Limit	Default: 0 Select the 'Daily/Weekly' start hour.	

Update geoip database with maxmind license & added GeoIP blocking for Afghanistan & China.

You're using our free data. [Upgrade to GeoIP for more accurate data.](#)

MAXMIND Products Resources Company My Account Cart Search

Account summary

Account

- [Account summary](#)
- [Account information](#)
- [Manage license keys](#)
- [Manage account services](#)
- [Manage users](#)
- [Account activity](#)
- [Edit my info](#)
- [Sign-in security](#)

Billing

- [Payment method](#)
- [Payment history](#)
- [Purchase or manage databases](#)
- [Query usage report](#)

Resources

- [Learn how to Manage your Account](#)
- [MaxMind Knowledge Base](#)
- [Developer Portal](#)
- [minFraud Release Notes and GeoIP Release Notes](#)

Database Products and Subscriptions

Databases	Access Starts	Access Ends
GeoLite Country	2025-08-19	No end date
GeoLite City	2025-08-19	No end date
GeoLite ASN	2025-08-19	No end date

[Download Databases](#)
[View Your Download History](#)

pfSense.home.arpa - Firewall + https://192.168.0.1/pfblockerng/pfblockerng_Asia.php

Also consider protecting just the specific open WAN ports and it's just as important to protect the outbound LAN traffic.

GeoIP ISOs can also be configured in the pfBlockerNG IPv4/IPv6 Alias(es) Source Definitions (Format: GeoIP)

Use **CTRL+CLICK** to select/unselect the IPv4/6 Countries below as required.

AA ASIA UNDEFINED 6255147 (224) AA ASIA UNDEFINED 6255147.rep (0) Afghanistan [149361] AF (213) Afghanistan [149361] AF.rep (1) Armenia [174982] AM (327) Armenia [174982] AM.rep (90) Azerbaijan [587116] AZ (439) Azerbaijan [587116] AZ.rep (34) Bahrain [290291] BH (266) Bahrain [290291] BH.rep (3) Bangladesh [1210997] BD (2436) Bangladesh [1210997] BD.rep (90) Bhutan [1252634] BT (125) Bhutan [1252634] BT.rep (2) British Indian Ocean Territory [1282588] IO (38) British Indian Ocean Territory [1282588] IO.rep (0) Brunei [1820814] BN (127) Brunei [1820814] BN.rep (0) Cambodia [1831722] KH (496) Cambodia [1831722] KH.rep (10) China [1814991] CN (7697) China [1814991] CN.rep (685) Cocos (Keeling) Islands [1547376] CC (25) Cocos (Keeling) Islands [1547376] CC.rep (0) Georgia [614540] GE (439) Georgia [614540] GE.rep (109) Hong Kong [1819730] HK (10400) Hong Kong [1819730] HK.rep (2174) India [1269750] IN (12175)	AA ASIA UNDEFINED 6255147 (101) Afghanistan [1149361] AF (614) Armenia [174982] AM (501) Azerbaijan [587116] AZ (256) Bahrain [290291] BH (177) Bangladesh [1210997] BD (1861) Bhutan [1252634] BT (117) British Indian Ocean Territory [1282588] IO (72) Brunei [1820814] BN (83) Cambodia [1831722] KH (198) China [1814991] CN (1947) Cocos (Keeling) Islands [1547376] CC (48) Georgia [614540] GE (328) Hong Kong [1819730] HK (4102) India [1269750] IN (6745) Indonesia [1643084] ID (4449) Iran [130758] IR (671) Iraq [99237] IQ (1173) Israel [294640] IL (1099) Japan [1861060] JP (4549) Jordan [248816] JO (152) Kazakhstan [1522867] KZ (1401) Kuwait [285570] KW (495) Kyrgyzstan [1527747] KG (144) Laos [1655842] LA (108) Lebanon [272103] LB (221) Macao [1821275] MO (322) Malaysia [1733045] MY (1567) Maldives [1282028] MV (708)
---	---

pfSense created automatic firewall rules (pfB_Asia_v4) in Firewall → Rules → LAN/WAN.

tried to ping a China IP (123.125.115.110 = Baidu, Beijing), it got blocked.

The screenshot shows the pfBlockerNG interface on a pfSense system. The top navigation bar includes tabs for General, IP, DNSBL, Update, Reports, Feeds, Logs, and Sync. The Reports tab is selected, and within it, the Alerts sub-tab is active. Below these are tabs for Unified, Alerts, IP Block Stats, IP Permit Stats, IP Match Stats, and DNSBL Block Stats. The main content area displays two tables of log entries.

Block - Last 25 Alert Entries:

Date	IF	Rule	Proto	Source	Destination	GeolP	Feed
Aug 19 10:10:56 [7]	LAN	pfb_Asia_v4 (17700903)	ICMP	192.168.0.101 Unknown	i+ 123.125.115.110 Unknown	CN	CN_v4 123.112.0.0/12

Found 1 Alert Entries - Insufficient Alerts found.

DNSBL Block - Last 25 Alert Entries:

Date	IF	Source	Domain/Referer/URI/Agent	Feed/Group
Aug 19 09:49:11		192.168.0.101	device.maxmind.com [DNSBL] DNSBL-Full [PRI]HTTP/2.0	StevenBlack_ADs DNSBL_ADS_Basic
Aug 19 09:49:11		192.168.0.101	www.googleletsgmanager.com [DNSBL] DNSBL-Full [PRI]HTTP/2.0	StevenBlack_ADs DNSBL_ADS_Basic The Feed and Group that blocked the indicated Domain: Feed: StevenBlack_ADs Group: DNSBL_ADS_Basic
Aug 19 09:49:09		192.168.0.101	js.hs-scripts.com [DNSBL] DNSBL-Full [PRI]HTTP/2.0	StevenBlack_ADs DNSBL_ADS_Basic

→ This proves your GeolP block is working 🎉.

B) Blocking Facebook & Youtube Website

In pfSense GUI → Firewall → pfBlockerNG → DNSBL.

Scroll down > dnsbl ip > deny both > log enable

Then, dnsbl groups at top > add another list > enter domain > safe > update

The screenshot shows a Firefox browser window with the URL https://www.youtube.com. The page displays a warning message: "Did Not Connect: Potential Security Issue". The message states: "Firefox detected a potential security threat and did not continue to www.youtube.com because this website requires a secure connection." Below the message are links for "Learn more..." and "Advanced...". At the bottom of the browser window, there are "Go Back" and "Advanced..." buttons.

The screenshot shows the pfBlockerNG Firewall / Alerts interface. The top navigation bar includes links for General, IP, DNSBL, Update, Reports (which is currently selected), Feeds, Logs, and Sync. Below this is a secondary navigation bar with Unified, Alerts, IP Block Stats, IP Permit Stats, IP Match Stats, and DNSBL Block Stats. The main area is titled "Alert Settings" and "Alert Filter". A table titled "Unified - Last 200 Alert Entries" displays the following data:

Date	SRC	Rule Mode/Type	IF/TTL	Destination	Resolved/Feed	GeoIP
Aug 19 11:23:02	192.168.0.101 Unknown	pfB_Asia_v4 (1770009033) ICMP	LAN	i + 123.125.115.110 Q Unknown	CN_v4 123.112.0.0/12	CN
Aug 19 11:20:25	192.168.0.101	DNSBL DNSBL-Full -PRI HTTP/2.0-	+	www.facebook.com	blocked_web_custom DNSBL_blocked_web	
Aug 19 11:20:24	192.168.0.101	DNSBL DNSBL-Full -PRI HTTP/2.0-	+	www.facebook.com	blocked_web_custom DNSBL_blocked_web	
Aug 19 11:20:24	192.168.0.101	DNSBL	+	www.facebook.com	blocked_web_custom	

C) Admin GUI access logging & restriction

◊ Step 1 — Allow Kali to access GUI

1. Go to Firewall → Rules → LAN.
2. Add Rule (top of list):
 - Action: Pass
 - Protocol: TCP
 - Source: Single host → 192.168.0.101 (Kali IP)
 - Destination: This Firewall (self)
 - Destination port: HTTPS (443) (also add port 80 if HTTP is enabled)
 - Description: Allow GUI from Kali
3. Save → Apply.

◊ Step 2 — Block GUI for everyone else

1. Still in LAN rules, Add a second rule (below the one above):
 - Action: Block
 - Protocol: TCP
 - Source: any
 - Destination: This Firewall (self)
 - Destination port: 443 (and 80 if needed)

- Log packets: enabled
- Description: Block GUI from all except Kali

2. Save → Apply.

⚠ Order matters! The Allow Kali rule must be on top.

◊ Step 3 — Block Ping (ICMP) from everyone except Kali

1. Add a new Pass rule (top):

- Action: Pass
- Protocol: ICMP
- Source: 192.168.0.101 (Kali)
- Destination: This Firewall (self)
- Description: Allow Ping from Kali

2. Add a Block rule (below):

- Action: Block
- Protocol: ICMP
- Source: any
- Destination: This Firewall (self)
- Log packets: enabled
- Description: Block Ping from others

.

Phase:3- Configure Wazuh To Receive Alerts

A) on pfsense side :

We setup syslog-ng package but its faild (not updating with gui)

Installed Packages		Available Packages		
Name	Category	Version	Description	Actions
✓ pfBlockerNG-devel	net	3.2.8	pfBlockerNG-devel is the Next Generation of pfBlockerNG. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.	 
✓ syslog-ng	sysutils	1.16.2	Syslog-ng syslog server. This service is not intended to replace the default pfSense syslog server but rather acts as an independent syslog server.	 

Package Dependencies:

 = Update  = Current
 = Remove  = Information  = Reinstall

So here we choose ,

pfSense Built-In Remote Syslog (no extra packages)

1. Go to: Status → System Logs → Settings.
2. Scroll down to Remote Logging Options.
3. Set:
 - Remote log servers:
192.168.0.100:514

Log Categories to send: check at least:

- Firewall Events
 - System Events
 - Authentication
 - pfBlockerNG / DNSBL (if available in your list)
- Save & Apply.

B) on wazuh side: (we can directly use agent for pfsense FreeBSD but we use syslog here)

- 1) sudo yum install -y rsyslog
- 2) sudo systemctl enable rsyslog –now

Check : sudo systemctl status rsyslog

- 3) Replace file content with below , (sudo nano /etc/rsyslog.d/10-pfsense.conf)

```
$ModLoad imuxsock
$ModLoad imklog
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514

if $fromhost-ip == "192.168.0.1" then
/var/log/pfsense.log
& stop
```

```
$ModLoad imuxsock
$ModLoad imklog
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514

if $fromhost-ip == "192.168.0.1" then /var/log/pfsense.log
& stop
```

- 4) sudo touch /var/log/pfsense.log
- 5) sudo chown root:root /var/log/pfsense.log
- 6) sudo chmod 0640 /var/log/pfsense.log
- 7) sudo systemctl restart rsyslog
- 8) Check that rsyslog is listening: sudo ss -tulpn | grep 514

```
[wazuh-user@wazuh-server ~]$ sudo ss -tulpn | egrep "514"
udp  UNCONN 0      0          0.0.0.0:514          0.0.0.0:*      users:(("r
syslogd",pid=1651,fd=5))
udp  UNCONN 0      0          [::]:514           [::]:*        users:(("r
syslogd",pid=1651,fd=6))
tcp   LISTEN 0     25         0.0.0.0:514          0.0.0.0:*      users:(("r
syslogd",pid=1651,fd=7))
tcp   LISTEN 0     128        0.0.0.0:1514         0.0.0.0:*      users:(("w
azuh-remoted",pid=2799,fd=4))
tcp   LISTEN 0     25         [::]:514           [::]:*        users:(("r
syslogd",pid=1651,fd=8))
[wazuh-user@wazuh-server ~]$
```

- 9) Edit /var/ossec/etc/ossec.conf and add inside <ossec_config>:

```
<localfile>
<log_format>syslog</log_format>
<location>/var/log/pfsense.log</location>
</localfile>
```

- 10) sudo systemctl restart wazuh-manager

- 11) Verify Logs Coming on Wazuh using below Commands :

```
sudo tail -f /var/log/pfsense.log
sudo tail -n 100 /var/ossec/logs/ossec.log
sudo tail -n 50 /var/ossec/logs/alerts/alerts.log
```

```
sudo tail -n 200 /var/ossec/logs/alerts/alerts.json
```

```
Aug 20 09:06:07 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8
Aug 20 09:08:12 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8
Aug 20 09:09:55 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0x0,,128,1724,0,none,17,udp,229,192.168.0.105,192.168.0.255,138,138,209
Aug 20 09:10:17 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8
Aug 20 09:12:10 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8
Aug 20 09:12:21 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8
Aug 20 09:13:09 pfsense.home.arpa php-fpm[47998]: /status_logs_settings.php: Configuration Change: admin@192.168.0.101 (Local Database): Changed system logging options.
Aug 20 09:13:09 pfsense.home.arpa sshguard[62960]: Exiting on signal.
Aug 20 09:13:09 pfsense.home.arpa sshguard[62960]: Exiting on signal.
Aug 20 09:13:10 pfsense.home.arpa sshguard[61284]: Exiting on signal.
Aug 20 09:13:10 pfsense.home.arpa sshguard[61284]: Exiting on signal.
Aug 20 09:13:10 pfsense.home.arpa check_reload_status[512]: Syncing firewall
Aug 20 09:13:10 pfsense.home.arpa syslogd: exiting on signal 15
Aug 20 09:13:10 pfsense.home.arpa syslogd: kernel boot file is /boot/kernel/kernel
Aug 20 09:13:10 pfsense.home.arpa sshguard[66480]: Now monitoring attacks.
Aug 20 09:13:10 pfsense.home.arpa sshguard[66480]: Now monitoring attacks.
Aug 20 09:14:27 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8
Aug 20 09:16:32 pfsense.home.arpa filterlog[41627]: 69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8
```

```
2025/08/20 07:53:09 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2025/08/20 07:53:13 wazuh-modulesd:vulnerability-scanner: INFO: Vulnerability scanner module started.
2025/08/20 07:53:43 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2025/08/20 07:53:43 wazuh-syscheckd: INFO: FIM sync module started.
2025/08/20 07:54:06 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/cis_amazon_linux_2023.yml'
2025/08/20 07:54:06 sca: INFO: Security Configuration Assessment scan finished.
Duration: 61 seconds.
2025/08/20 07:54:10 wazuh-modulesd:vulnerability-scanner: INFO: Initiating update feed process.
2025/08/20 07:54:18 sca: INFO: Integration checksum failed for policy '/var/ossec/ruleset/sca/cis_amazon_linux_2023.yml'. Resending scan results in 80 seconds.
2025/08/20 07:55:12 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-vulnerabilities-wazuh-server.
2025/08/20 07:55:13 rootcheck: INFO: Ending rootcheck scan.
2025/08/20 07:55:48 sca: INFO: Integration checksum failed for policy '/var/ossec/ruleset/sca/cis_amazon_linux_2023.yml'. Resending scan results in 210 seconds.
2025/08/20 07:59:27 sca: INFO: Integration checksum failed for policy '/var/ossec/ruleset/sca/cis_amazon_linux_2023.yml'. Resending scan results in 198 seconds.
2025/08/20 08:04:15 wazuh-modulesd:vulnerability-scanner: INFO: Triggered a re-scan after content update.
2025/08/20 08:04:15 wazuh-modulesd:vulnerability-scanner: INFO: Feed update process completed.
2025/08/20 08:07:42 wazuh-logcollector: INFO: (9204): 'Journald' timestamp was refreshed due to rotation.
2025/08/20 08:53:10 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2025/08/20 08:53:21 wazuh-modulesd:syscollector: INFO: Evaluation finished.
[wazuh-user@wazuh-server ~]$
```

```

_AC.7,nist_800_53_AC.6,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Aug 20 09:18:30 wazuh-server->journald
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
User: root
Aug 20 09:18:28 wazuh-server sudo[4846]: wazuh-user : TTY=tty1 : PWD=/home/wazuh
:user : USER=root : COMMAND=/usr/bin/tail -n 50 /var/ossec/logs/ossec.log
tty: tty1
pwd: /home/wazuh-user
command: /usr/bin/tail -n 50 /var/ossec/logs/ossec.log

** Alert 1755681510.90851: - pam,syslog,authentication_success,pci_dss_10.2.5,gp
g13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.
7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Aug 20 09:18:30 wazuh-server->journald
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: root(uid=0)
Aug 20 09:18:28 wazuh-server sudo[4846]: pam_unix(sudo:session): session opened
for user root(uid=0) by wazuh-user(uid=1000)
uid: 1000

** Alert 1755681510.91295: - pam,syslog,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_
IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,t
sc_CC7.3,
2025 Aug 20 09:18:30 wazuh-server->journald
Rule: 5502 (level 3) -> 'PAM: Login session closed.'
User: root
Aug 20 09:18:28 wazuh-server sudo[4846]: pam_unix(sudo:session): session closed
for user root

```

12) decoders and rules verification using (sudo /var/ossec/bin/wazuh-logtest):

We check 3 logs,

Aug 20 13:27:14 pfsense.home.arpa filterlog[39598]:

69,,,12004,em0,match,block,in,4,0x0,,128,1752,0,none,17,udp,229,192.168.0.105,192.168.0.255,138,1
38,209

Aug 20 13:36:57 pfsense.home.arpa filterlog[39598]:

69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8

Aug 20 13:44:19 pfsense.home.arpa filterlog[39598]:

91,,,1770009033,em1,match,block,in,4,0x0,,64,20443,0,DF,1,icmp,84,192.168.0.101,123.125.115.110,r
equest,1,164

Result:

**Phase 1: Completed pre-decoding.

full event: 'Aug 20 13:36:57 pfsense.home.arpa filterlog[39598]:'

69,,,12004,em0,match,block,in,4,0xc0,,1,0,0,DF,2,igmp,32,192.168.0.1,224.0.0.1,datalength=8'

timestamp: 'Aug 20 13:36:57'

hostname: 'pfsense.home.arpa'

program_name: 'filterlog'

**Phase 2: Completed decoding.

```
name: 'pf'
action: 'block'
dstip: '224.0.0.1'
id: '12004'
length: '8'
protocol: 'igmp'
srcip: '192.168.0.1'
```

**Phase 3: Completed filtering (rules).

```
id: '87701'
level: '5'
description: 'pfSense firewall drop event.'
groups: '['pfsense', 'firewall_block']'
firetimes: '1'
gpg13: '['4.12']'
hipaa: '['164.312.a.1']'
mail: 'False'
nist_800_53: '['SC.7']'
pci_dss: '['1.4']'
tsc: '['CC6.7', 'CC6.8']'
```

**Alert to be generated.

We can also use custom rules & decoders:

```
sudo nano /var/ossec/etc/decoders/local_decoder.xml
```

```
sudo nano /var/ossec/etc/rules/local_rules.xml
```

Refrence Building : <https://socfortress.medium.com/understanding-wazuh-decoders-4093e8fc242c>

ISSUE: Everything is Fine & Done Till Now , Receiving Logs and All Stuff Just Perfect . BUT Cant See Alerts in Wazuh DashBoard . Spending 3 Days on Debugging, some of Snippets Below and Mainly Fixing Ways.

Phase 4 : Debugging

(Not Putting Outputs here, the report will be too lengthy)

1) Check whether your Wazuh alerts are indexed in the indexer (Elasticsearch / Wazuh Indexer).

```
curl -s 'http://localhost:9200/_cat/indices?v' | egrep 'wazuh-alerts|wazuh' || echo "no-indices-found"
```

```
curl -s -u user:pass 'https://localhost:9200/_cat/indices?v' -k | egrep 'wazuh-alerts|wazuh' || echo "no-indices-found"
```

manager is generating alerts, but nothing is being indexed into the Wazuh Indexer.

We now need to confirm whether the service that ships alerts (Filebeat, or wazuh-indexer output module

2) sudo systemctl status filebeat --no-pager -l

Filebeat is running That means it *should* be forwarding alerts from /var/ossec/logs/alerts/alerts.json into your Wazuh Indexer.

3) Check Filebeat logs for errors: sudo tail -n 50 /var/log/filebeat/filebeat

Filebeat **was failing to connect** (connect: connection refused, 503 Service Unavailable: OpenSearch Security not initialized).

Later it finally established a connection (Connection to backoff(elasticsearch(<https://127.0.0.1:9200>)) established).

Now it's harvesting /var/ossec/logs/alerts/alerts.json.

4) Verify new indices: curl -s -u user:pass 'https://localhost:9200/_cat/indices?v' -k | grep wazuh-alerts still **no wazuh-alerts-* index**, even though Filebeat says it connected, then the alerts are not being written to the Indexer. That points to a **Filebeat → Elasticsearch/Wazuh Indexer config issue**.

5) Inspect Filebeat output configuration : grep -A5 "^output.elasticsearch" /etc/filebeat/filebeat.yml
filebeat.yml is misconfigured But in YAML, output.elasticsearch.hosts: and output.elasticsearch: are separate, so Filebeat is confused. It's not applying username/password properly, which explains why indices aren't being created.

6) Fix steps: sudo nano /etc/filebeat/filebeat.yml (Replace full code with below code)

```
# Wazuh - Filebeat configuration file
```

```
output.elasticsearch:
```

```
hosts: ["https://127.0.0.1:9200"]
```

```
username: "admin"
```

```
password: "admin"
```

```
ssl.certificateAuthorities:
```

```
- /etc/filebeat/certs/root-ca.pem  
ssl.certificate: "/etc/filebeat/certs/wazuh-server.pem"  
ssl.key: "/etc/filebeat/certs/wazuh-server-key.pem"  
  
setup.template.json.enabled: true  
setup.template.json.path: '/etc/filebeat/wazuh-template.json'  
setup.template.json.name: 'wazuh'  
setup.ilm.overwrite: true  
setup.ilm.enabled: false  
  
filebeat.modules:  
- module: wazuh  
  alerts:  
    enabled: true  
  archives:  
    enabled: false  
  
logging.level: info  
logging.to_files: true  
logging.files:  
  path: /var/log/filebeat  
  name: filebeat  
  keepfiles: 7  
  permissions: 0644  
  
logging.metrics.enabled: false  
  
seccomp:  
  default_action: allow  
  syscalls:  
    - action: allow
```

names:

- rseq

7) sudo systemctl restart filebeat

8) Verifying,

Check Filebeat status (make sure no errors): sudo systemctl status filebeat -l --no-pager

Test Indexer connection: curl -u admin:admin https://127.0.0.1:9200 -k (should return JSON with cluster_name.)

See if Wazuh indices appear: curl -u admin:admin https://127.0.0.1:9200/_cat/indices?v -k | grep wazuh

- Filebeat is running fine.
- Indexer (https://127.0.0.1:9200) is reachable with admin/admin.
- Wazuh indices are created (wazuh-alerts-4.x-2025.08.20 and others).

That means **alerts are indeed flowing into the Indexer.**

9) The missing piece is the **Wazuh Dashboard → Indexer connection**. If the Dashboard isn't pointing to the Indexer with correct credentials, it won't show alerts.

Check Dashboard config: sudo nano /etc/wazuh-dashboard/opensearch_dashboards.yml

Replace code With below Code :

```
server.host: "0.0.0.0"
server.port: 443
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/wazuh-dashboard.pem"
```

```
opensearch.hosts: ["https://127.0.0.1:9200"]
```

```
opensearch.username: "admin"
```

```
opensearch.password: "admin"
```

```
# If you have working CA certs and want strict verification, set to "certificate"
```

```
opensearch.ssl.verificationMode: none
```

```
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
```

```
opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]
```

```
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
```

```
uiSettings.overrides.defaultRoute: /app/wz-home
opensearch_security.cookie.secure: true
10) sudo systemctl restart wazuh-dashboard
sudo systemctl status wazuh-dashboard -l --no-pager
# Quick test that the dashboard can reach OpenSearch
curl -u admin:admin https://127.0.0.1:9200/_cluster/health -k
backend-wise looks healthy now (indices exist, dashboard running).
```

11) on wazuh dashboard :

Click the blue chip that says virus (001) (top bar, right of Threat Hunting).

Unpin and it changes to All (also 000 wazuh server)

Click **Add filter** (next to existing filter chips).

Field: type rule.groups and choose it.

Operator: is

Value: pfSense

12) Final check again on wazuh VM : sudo curl -s -u admin:admin -k https://127.0.0.1:9200/wazuh-alerts-4.x-*/_search?q=rule.groups:pfSense&size=10&pretty

Yes — it's working.

That single hit is a **grouped pf/pfSense alert** (rule 87702) that represents many blocked packets from the same source — the previous_output in that document contains the multiple raw filterlog lines. Now I'll give you one precise reproduce / verify workflow (teacher style) so you can generate firewall traffic from your Kali VM, confirm pfSense logged it, and confirm Wazuh indexed it.

Why you only see 1 hit

- The alert you saw (id: 87702) is a **grouping rule** (“Multiple pfSense firewall blocks events from same source”).
- Wazuh groups repeated filterlog drops from the same source into one alert to reduce noise — that alert’s previous_output field already contains multiple raw log lines.
- So one alert can map to many firewall drop events (that’s why previous_output shows many lines).

13) From Kali linux generate UDP traffic:

```
sudo python3 - <<'PY'
import socket, time
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)
for i in range(10):
    s.sendto(b'TEST-PF', ('192.168.0.255', 137))
    time.sleep(0.2)
print("Done sending 10 UDP packets to 192.168.0.255:137")
```

PY

FINAL RESULTS

The screenshot shows a web browser window displaying pfSense statistics and pfBlockerNG rules. The browser address bar shows `https://192.168.0.1`. The page content includes:

- Kernel PTI:** Enabled
- MDS Mitigation:** Inactive
- Uptime:** 02 Hours 31 Minutes 54 Seconds
- Current date/time:** Thu Aug 21 11:23:08 UTC 2025
- DNS server(s):**
 - 127.0.0.1
 - ::1
 - 192.168.0.1
- Last config change:** Wed Aug 20 12:54:44 UTC 2025
- State table size:** 0% (65/199000) [Show states](#)
- MBUF Usage:** 0% (3556/1000000)
- Load average:** 0.87, 0.89, 0.82
- CPU usage:** 30%
- Memory usage:** 20% of 1992 MiB
- SWAP usage:** 0% of 1024 MiB
- Disks:**

Mount	Used	Size	Usage
> /	972M	16G	[progress bar]
- Interfaces:**

Interface	Status	Description	IP Address
WAN	Up	1000baseT <full-duplex>	192.168.0.108
LAN	Up	1000baseT <full-duplex>	192.168.0.1
- pfBlockerNG:**

Category	Count	Actions
IP	15	[green checkmark] [red X] [refresh] [trash]
DNSBL	68	[green checkmark] [red X] [refresh] [trash] [info icon]

Log entries:

 - 1. [pfB_PRI1_v4 - Talos_BL_v4] Download FAIL [08/21/25 10:00:26]
 - 2. [pfB_PRI1_v4 - Talos_BL_v4] Download FAIL [08/21/25 09:01:49]

Alias	Count	packets	Updated
pfB_Asia_v4	8,494	15	Aug 20 08:00:25
pfB_PRI1_v4	14,531	0	Aug 21 11:01:31
DNSBL_Ados_Basic	230,046	28	Aug 19 10:59:28
DNSBL_blocked_web	4	40	Aug 19 10:59:29

Screenshot of the Wazuh Threat Hunting interface showing event details for pfSense firewall blocks.

Events Overview:

- Count: 2
- Time Range: 2025-08-15 00:00 - 2025-08-21 00:00
- Timestamp per 3 hours

Event Details:

3 hits (Aug 14, 2025 @ 07:29:36.935 - Aug 21, 2025 @ 07:29:36.936)

timestamp	agent.name	rule.description	rule.level	rule.id
Aug 21, 2025 @ 07:27:03.5...	wazuh-server	Multiple pfSense firewall blocks events from same source.	10	87702
Aug 21, 2025 @ 07:08:24.9...	wazuh-server	Multiple pfSense firewall blocks events from same source.	10	87702
Aug 20, 2025 @ 11:57:46.8...	wazuh-server	Multiple pfSense firewall blocks events from same source.	10	87702

Screenshot of the Wazuh Threat Hunting interface showing document details for pfSense firewall blocks.

Document Details:

3 hits (Aug 14, 2025 @ 07:27:45.594)

timestamp	agent.name	rule.description
Aug 21, 2025 @ 07:27:03.5...	wazuh-server	Multiple pfSense firewall blocks ev...
Aug 21, 2025 @ 07:08:24.9...	wazuh-server	Multiple pfSense firewall blocks ev...
Aug 20, 2025 @ 11:57:46.8...	wazuh-server	Multiple pfSense firewall blocks ev...

Document Fields (Table View):

Field	Value
_index	wazuh-alerts-4.x-2025.08.21
agent.id	000
agent.name	wazuh-server
data.action	block
data.dstip	123.125.115.110
data.dstport	7
data.id	1770009033
data.length	364
data.protocol	icmp
data.srcip	192.168.0.101
data.report	
decoder.name	pf
full_log	Aug 21 11:27:02 pfsense.home.arpa filterlog[33250]: 91,,,1770009033,em1,match,block,in,4,0x0,,64,3261,0,DF,1,icmp,84,192.168.0.101,123.125.115.110,request,7,364

The screenshot shows the Wazuh Threat Hunting interface. On the left, there's a search bar with filters: "manager.name: wazuh-server" and "rule-groups: pfsense". Below it is a chart showing event counts over time from August 15 to 17, 2025. On the right, the "Document Details" section displays a table of event fields:

Table	JSON
<code>t _index</code>	wazuh-alerts-4.x-2025.08.21
<code>t agent.id</code>	000
<code>t agent.name</code>	wazuh-server
<code>t data.action</code>	block
<code>t data.dstip</code>	192.168.0.255
<code>t data.dstport</code>	137
<code>t data.id</code>	12014
<code>t data.length</code>	76
<code>t data.protocol</code>	udp
<code>t data.srchip</code>	192.168.0.106
<code>t data.srport</code>	137
<code>t decoder.name</code>	pf
<code>t full_log</code>	Aug 21 11:08:24 pfsense.home.arpa filterlog[33250]: 69,,12014@R [REDACTED] h,block,in,4,0x0,,128,34167,0,none,17,udp,96,192.168.0.106,192.168.0.255,137,137,76

The screenshot shows the Wazuh Rules manager interface. On the left, a list of rules is shown with IDs 1 through 201. Rule 87702 is selected and detailed on the right:

Multiple pfSense firewall blocks events from same source.

Information

ID	Level	File	Path
87702	10	0540-pfsense_rules.xml	ruleset/rules

Groups
multiple_blocks, pfsense

Details

Frequency	Timeframe	Ignore	If_matched_sid
18	45	240	87701

Same_source_ip
true

Compliance

GPG	HIPAA	TSC
13 4.12	164.312.a.1, 164.312.b	CC6.7, CC6.8, CC7.2, CC7.3

THE END