# 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 .

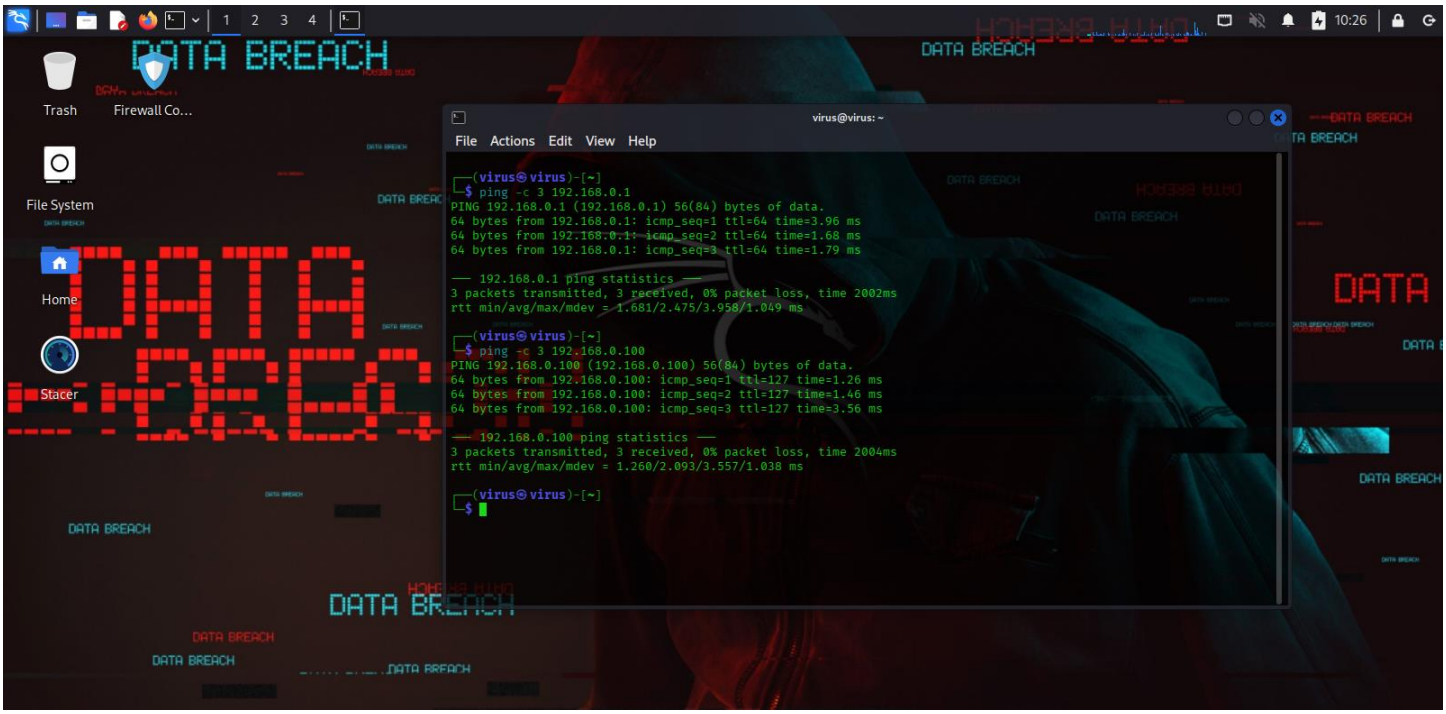
```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
TYPE=Ethernet
IPADDR=192.168.0.100
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
DNS1=8.8.8.8
DNS2=1.1.1.1
```

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.

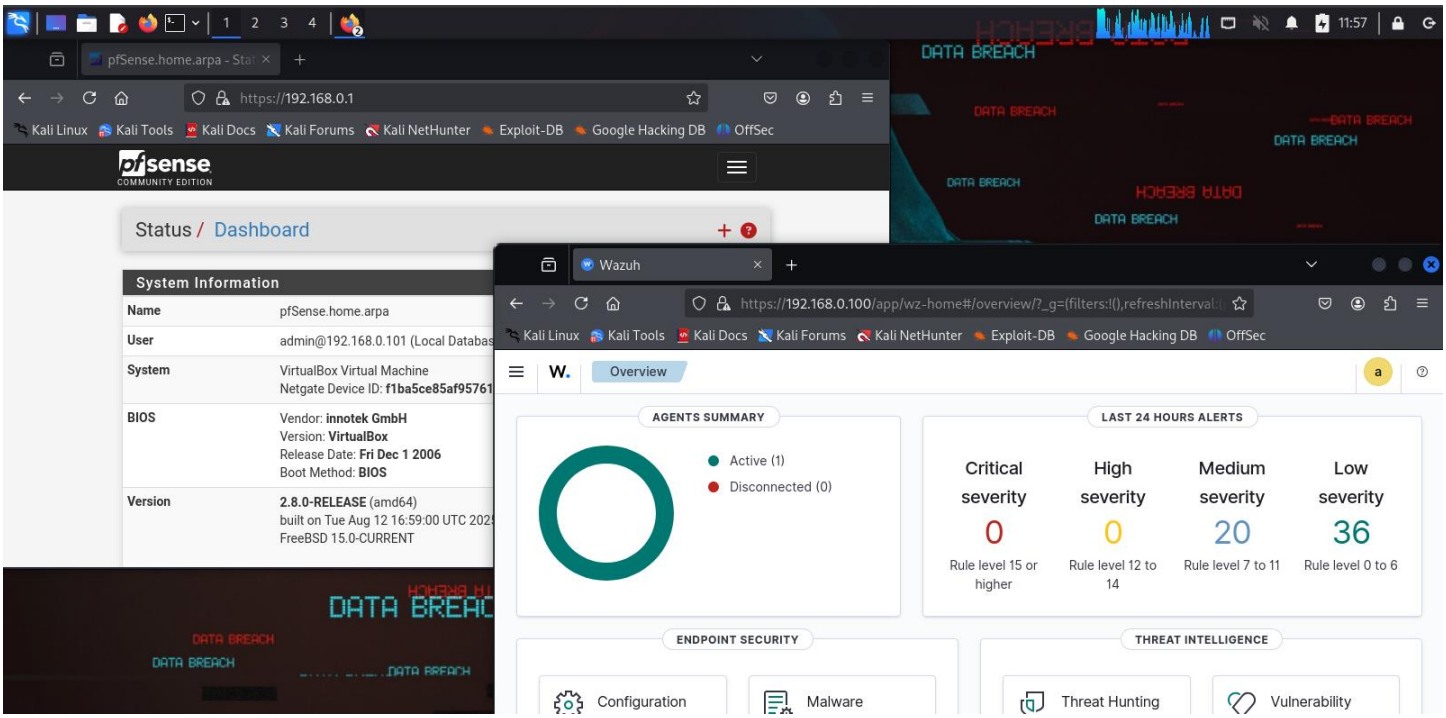
Under *Protocol*, choose HTTPS (default is HTTP on fresh installs).

Save & apply.

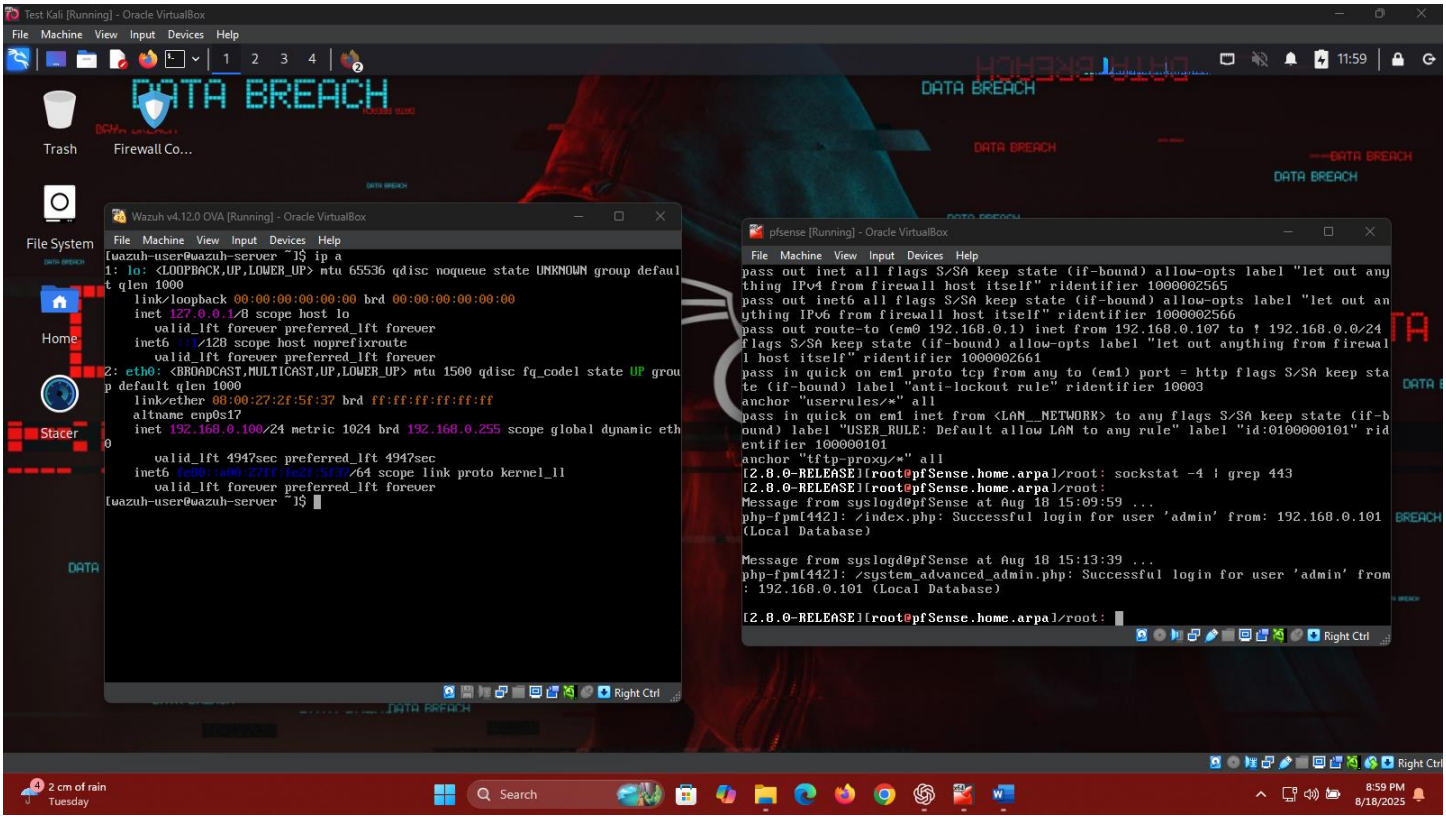
Now access properly (https://192.168.0.1)

**For Wazuh** is Already Same Setup in Task 1 .

https://192.168.0.100



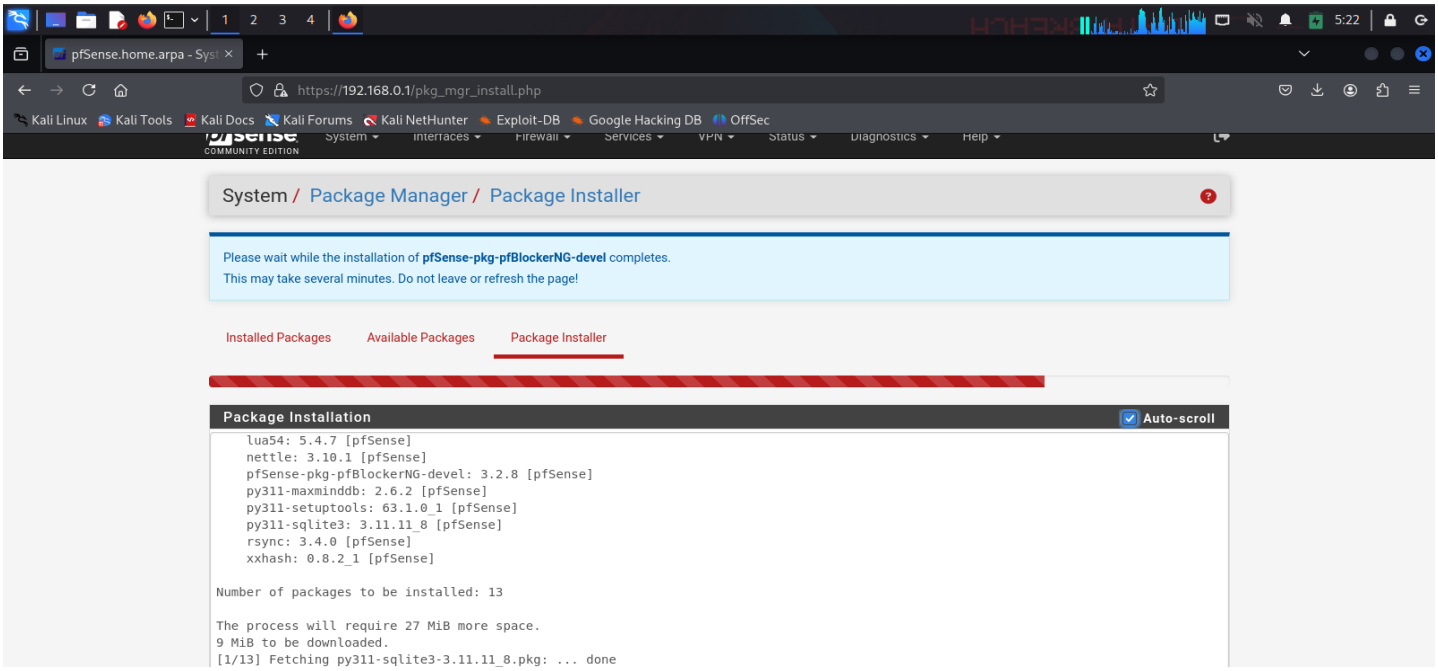

Running Machines Check.

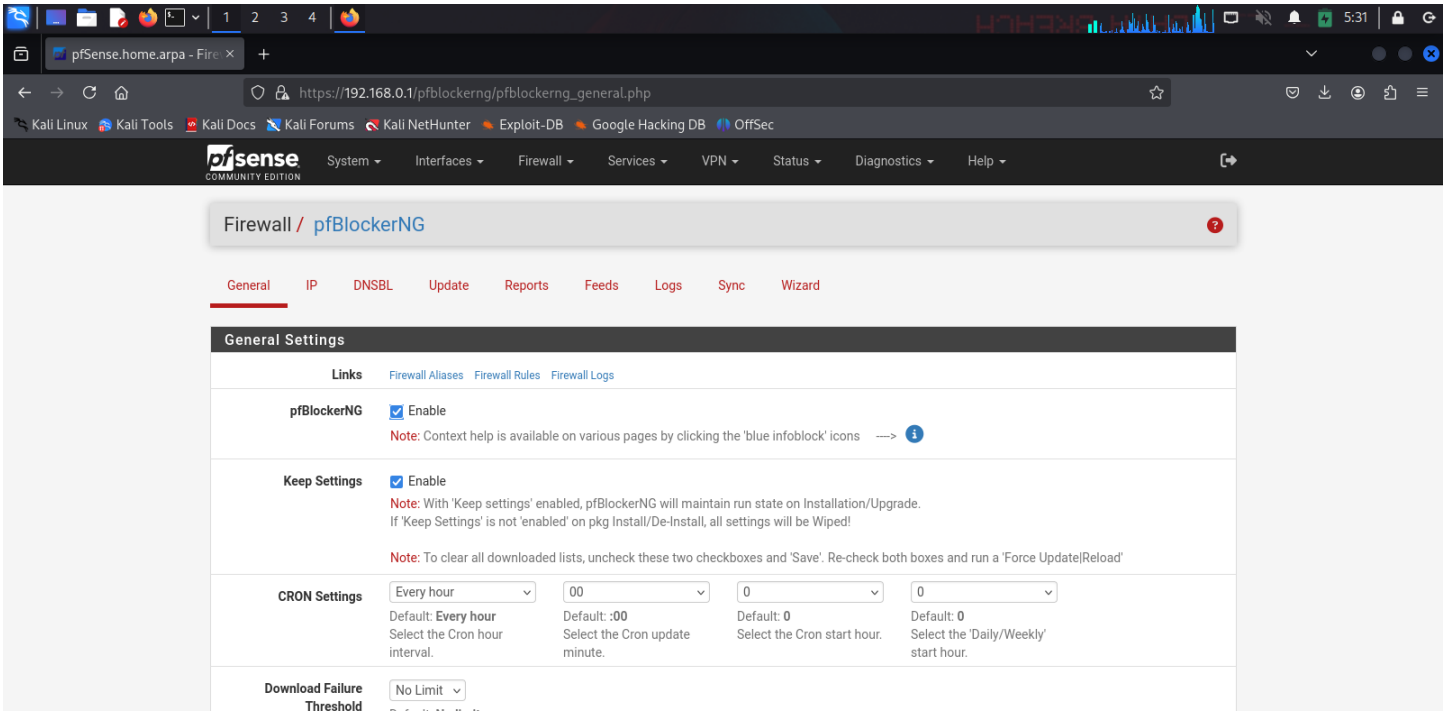



## *Phase 2*

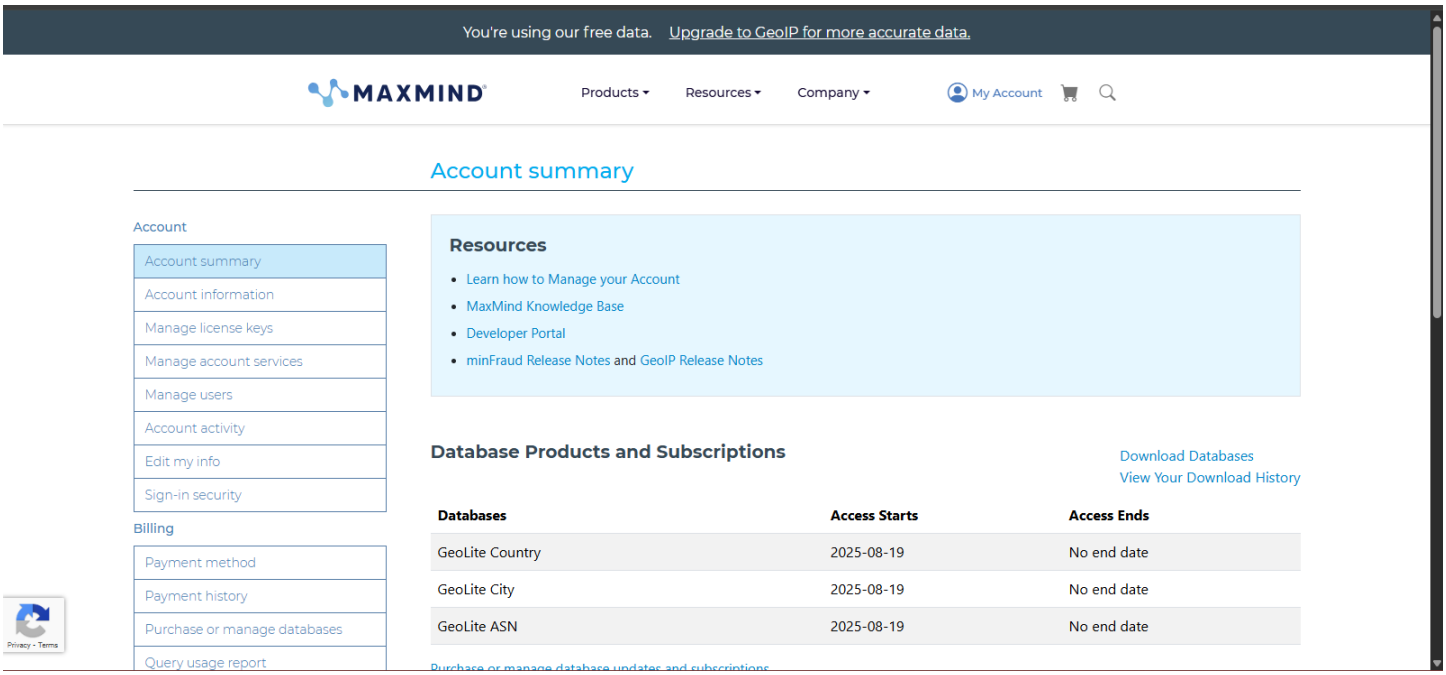
## A) Blocking Countries-Geoip

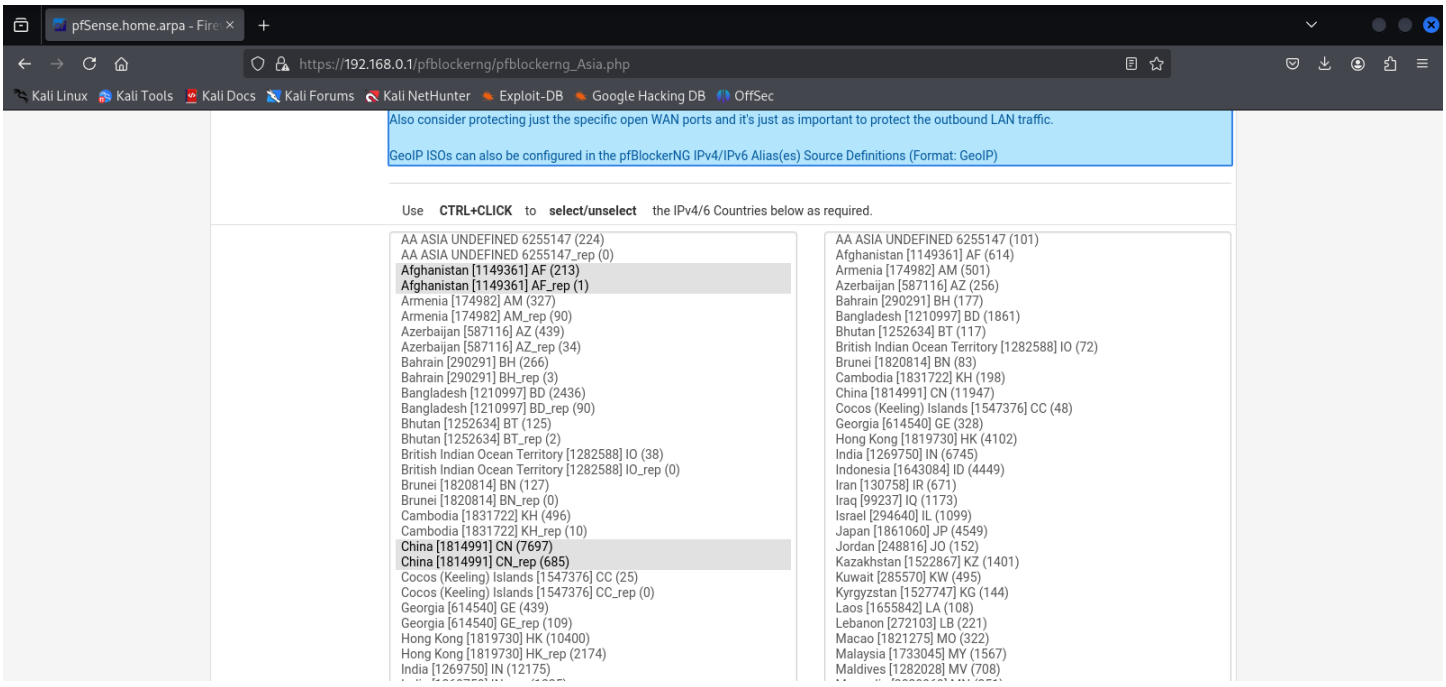
installed pfBlockerNG-devel.



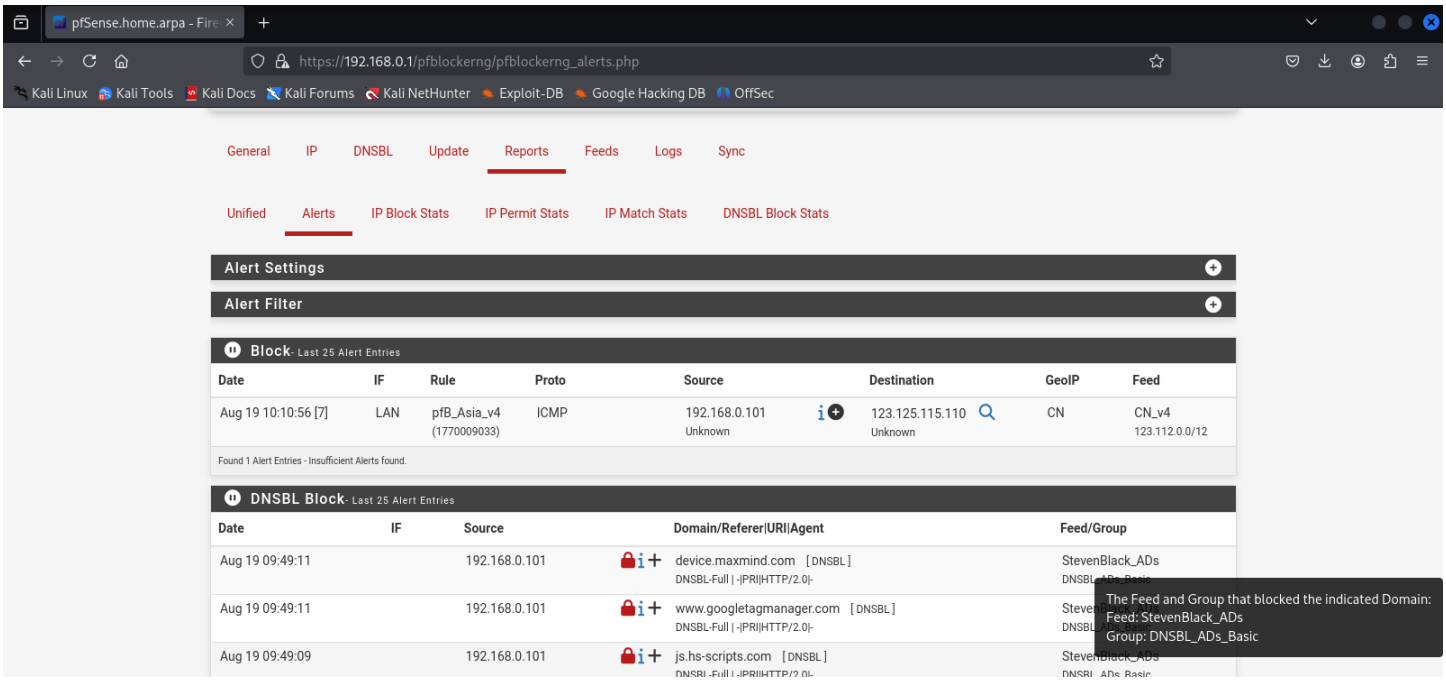
Update geoip database with maxmind license & added GeoIP blocking for Afghanistan & China.




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.



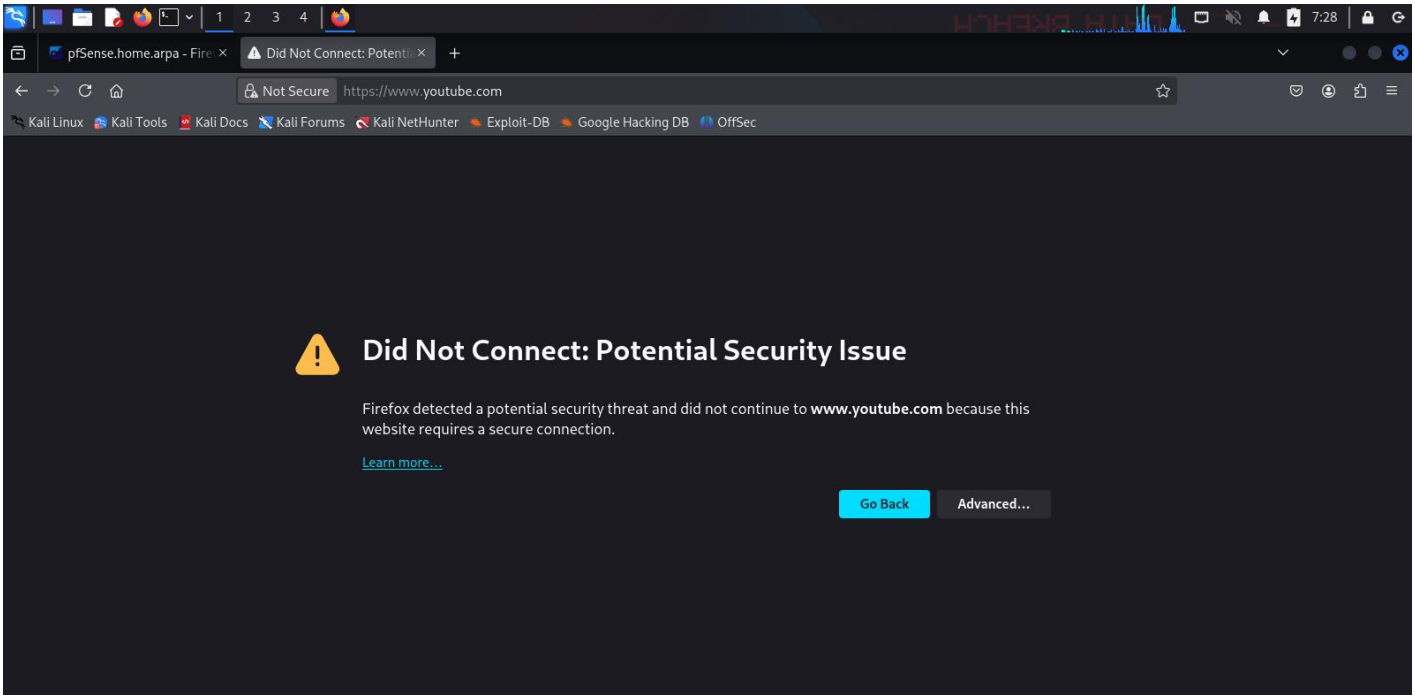

→ This proves your GeoIP block is working 🚀.

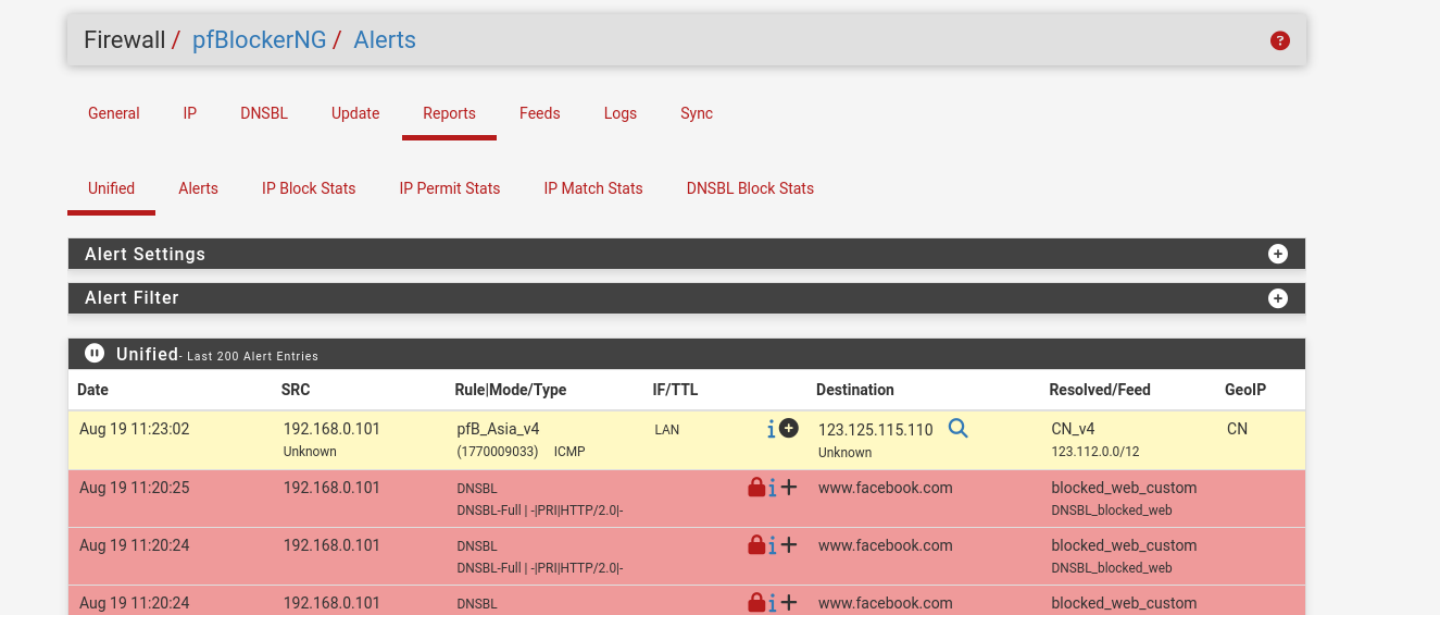
**B) Blocking Facebook & Youtube Website**

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






## 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

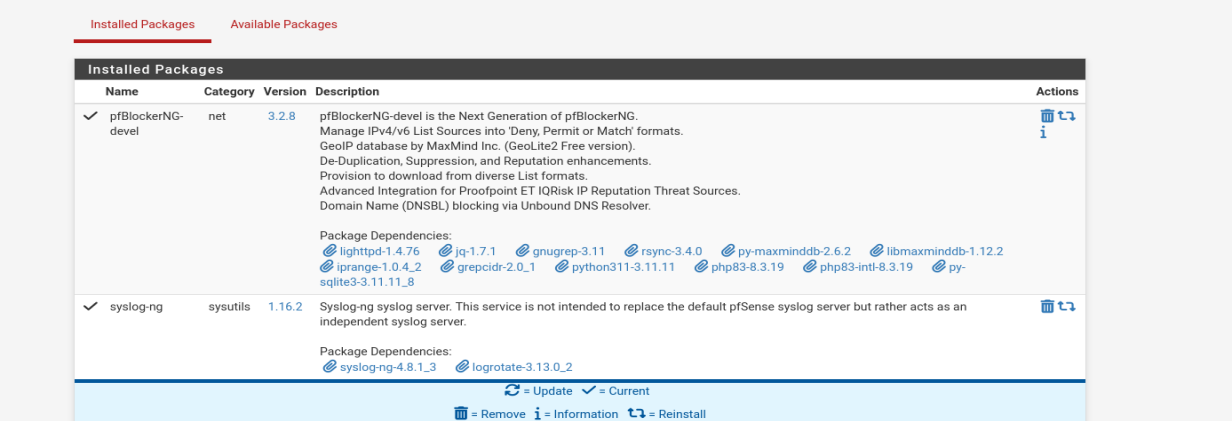
.

---

## Phase:3- Configure Wazuh To Receive Alerts

### A) on pfsense side :

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



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

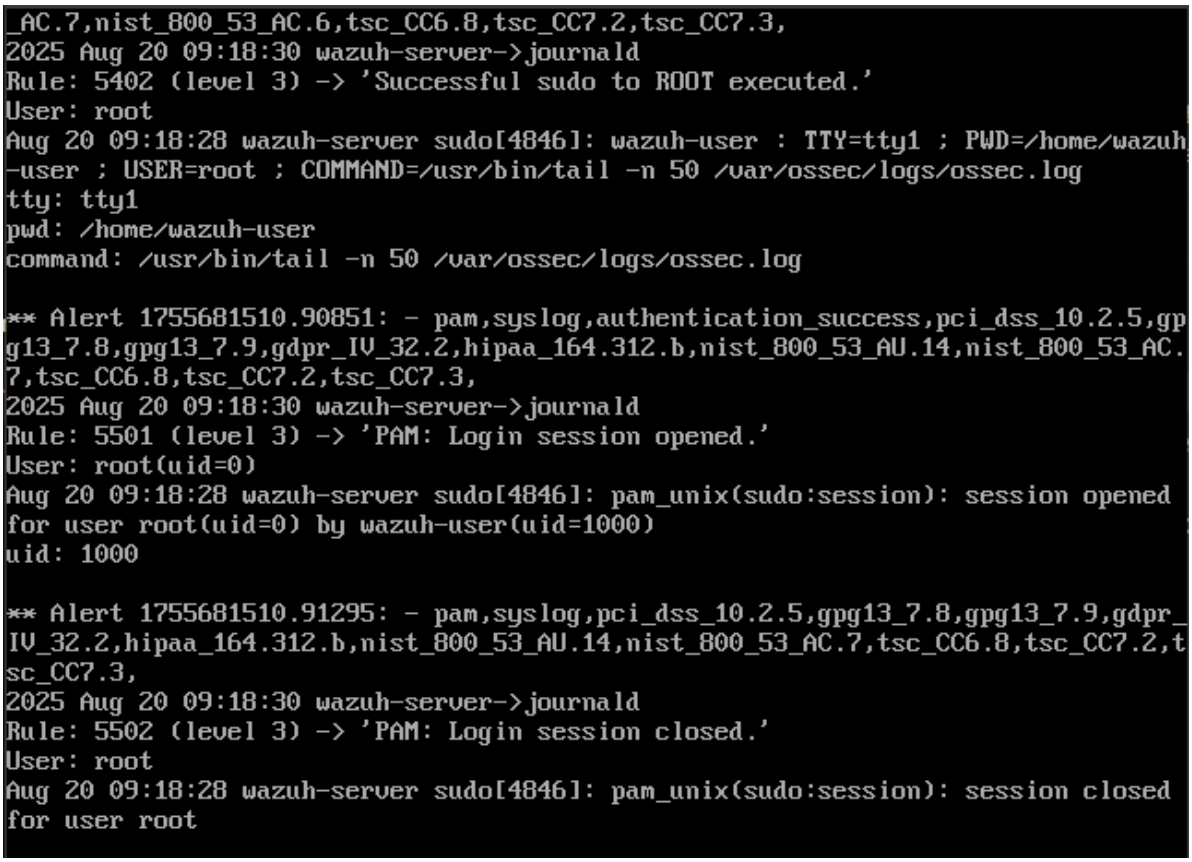
sudo tail -n 100 /var/ossec/logs/ossec.log

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,i
n,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,i
n,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,i
n,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,i
n,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,i
n,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,i
n,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: Con
figuration 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/kern
el
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,i
n,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,i
n,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 sc
anner module started.
2025/08/20 07:53:43 wazuh-syscheckd: INFO: (6009): File integrity monitoring sca
n 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/rulese
t/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 updat
e feed process.
2025/08/20 07:54:18 sca: INFO: Integration checksum failed for policy '/var/osse
c/ruleset/sca/cis_amazon_linux_2023.yml'. Resending scan results in 80 seconds.
2025/08/20 07:55:12 indexer-connector: INFO: IndexerConnector initialized succes
sfully 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/osse
c/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/osse
c/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-s
can after content update.
2025/08/20 08:04:15 wazuh-modulesd:vulnerability-scanner: INFO: Feed update proc
ess completed.
2025/08/20 08:07:42 wazuh-logcollector: INFO: (9204): 'Journald' timestamp was r
efreshed 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 ~]$
```




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,229,192.168.0.105,192.168.0.255,138,138,209

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,request,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']'

firedtimes: '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 lenghty)
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.certificate_authorities:
```

```
    - /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.

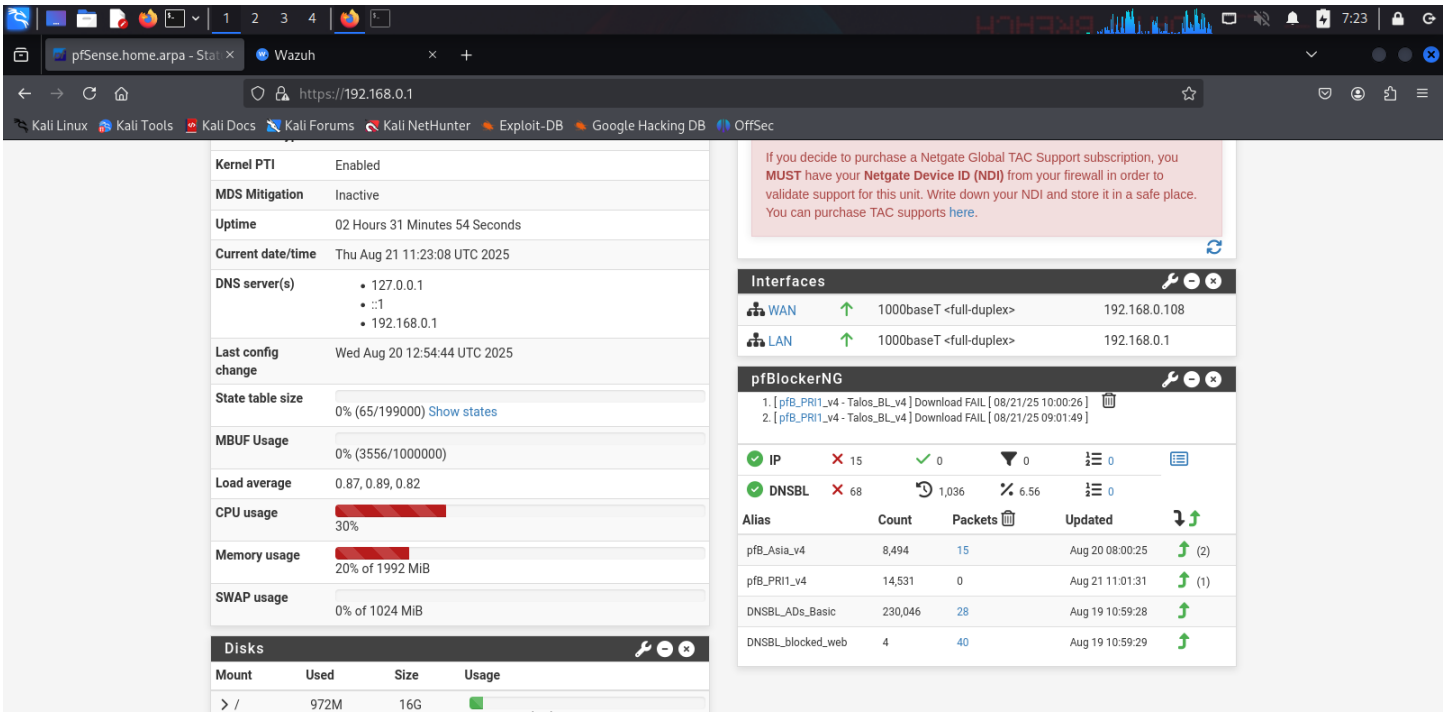
**Why you only see 1 hit**

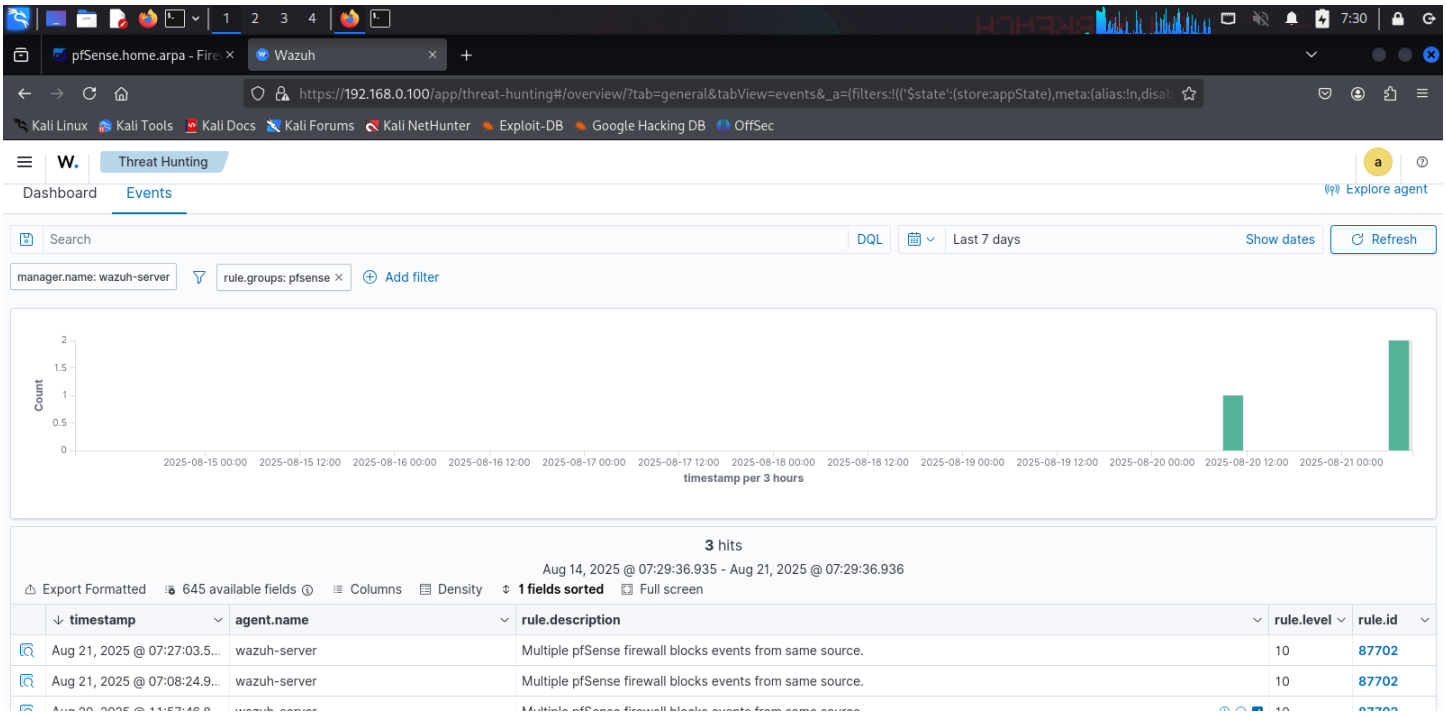
- The alert you saw (id: 87702) is a **grouping rule** ("Multiple pfSense firewall blocks events from same source").
- Wazuh groups repeated filterlog drops from the same source into one alert to reduce noise — that alert's previous_output field already contains multiple raw log lines.
- So one alert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

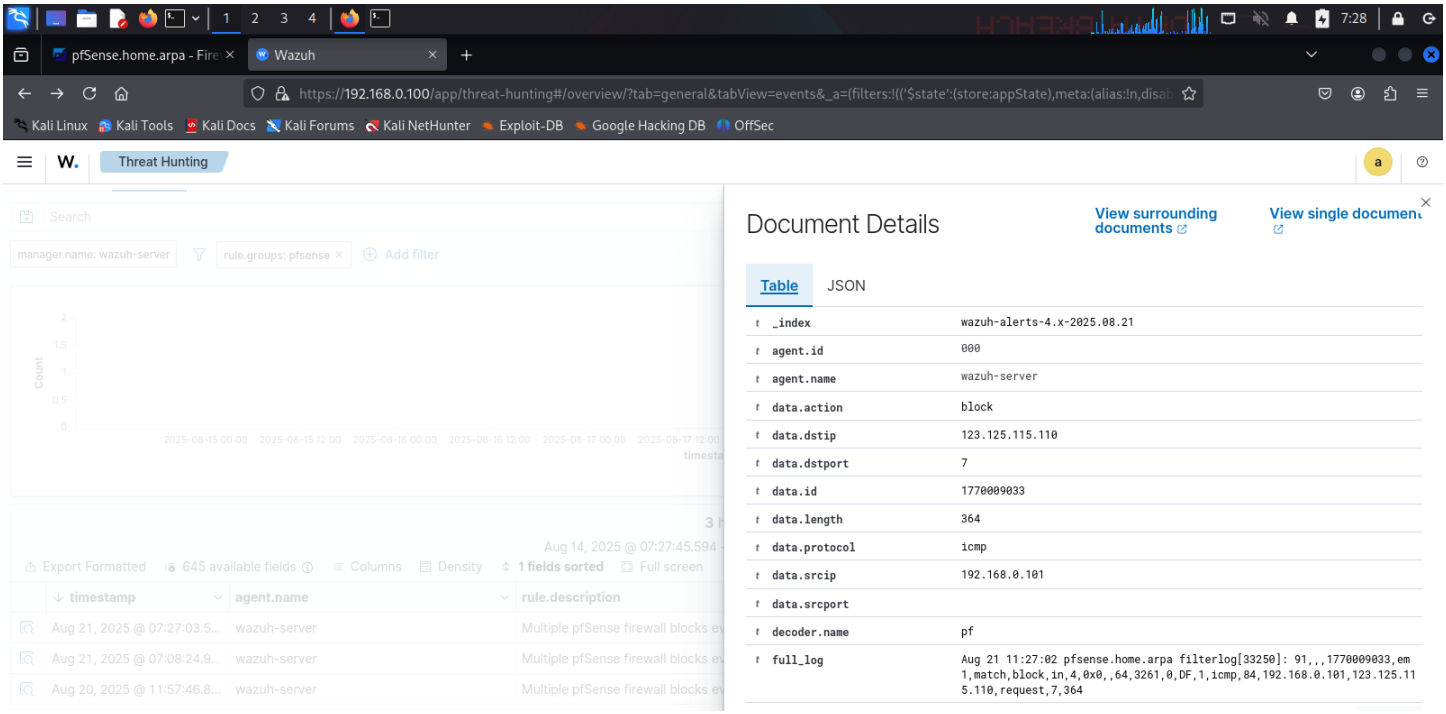
13) From Kali linux generate UDP traffic:

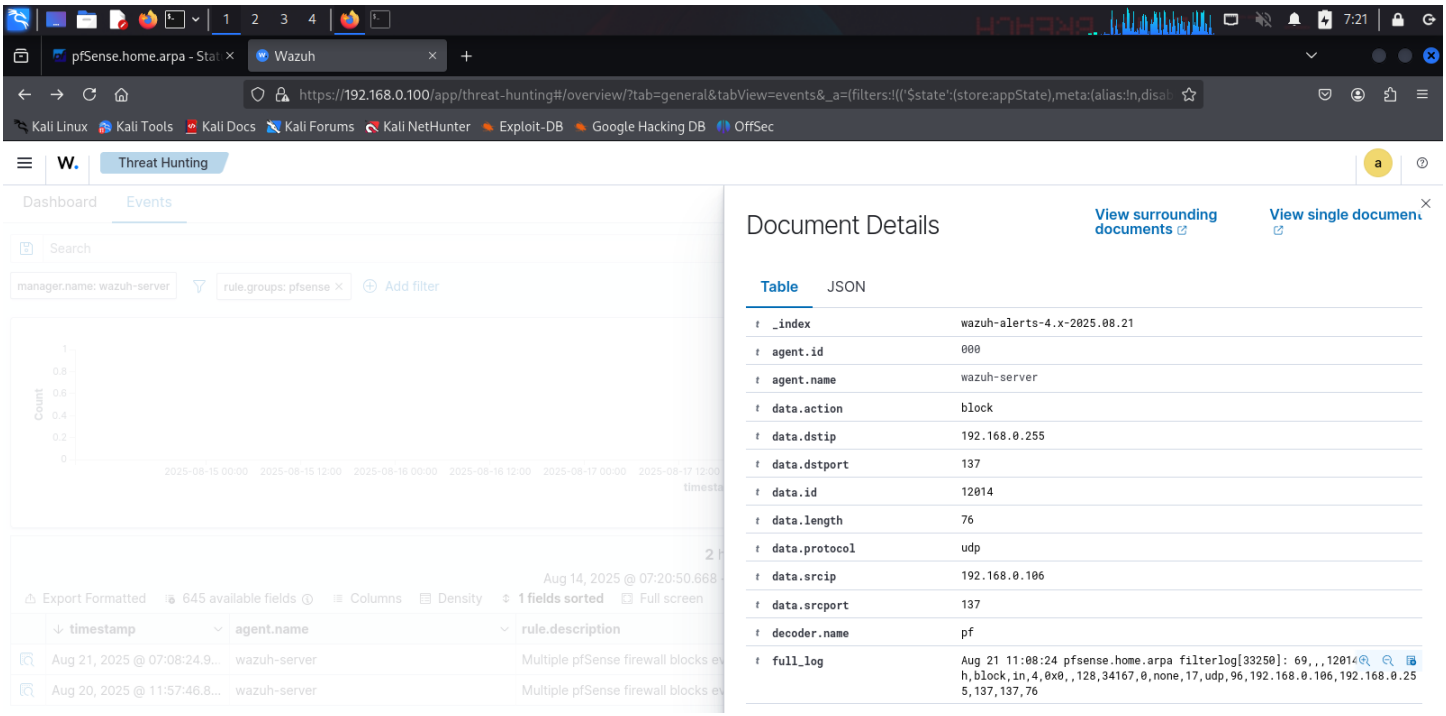
```
sudo python3 - <<'PY'
import socket, time
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)
for i in range(10):
   s.sendto(b'TEST-PF', ('192.168.0.255', 137))
   time.sleep(0.2)
print("Done sending 10 UDP packets to 192.168.0.255:137")
PY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

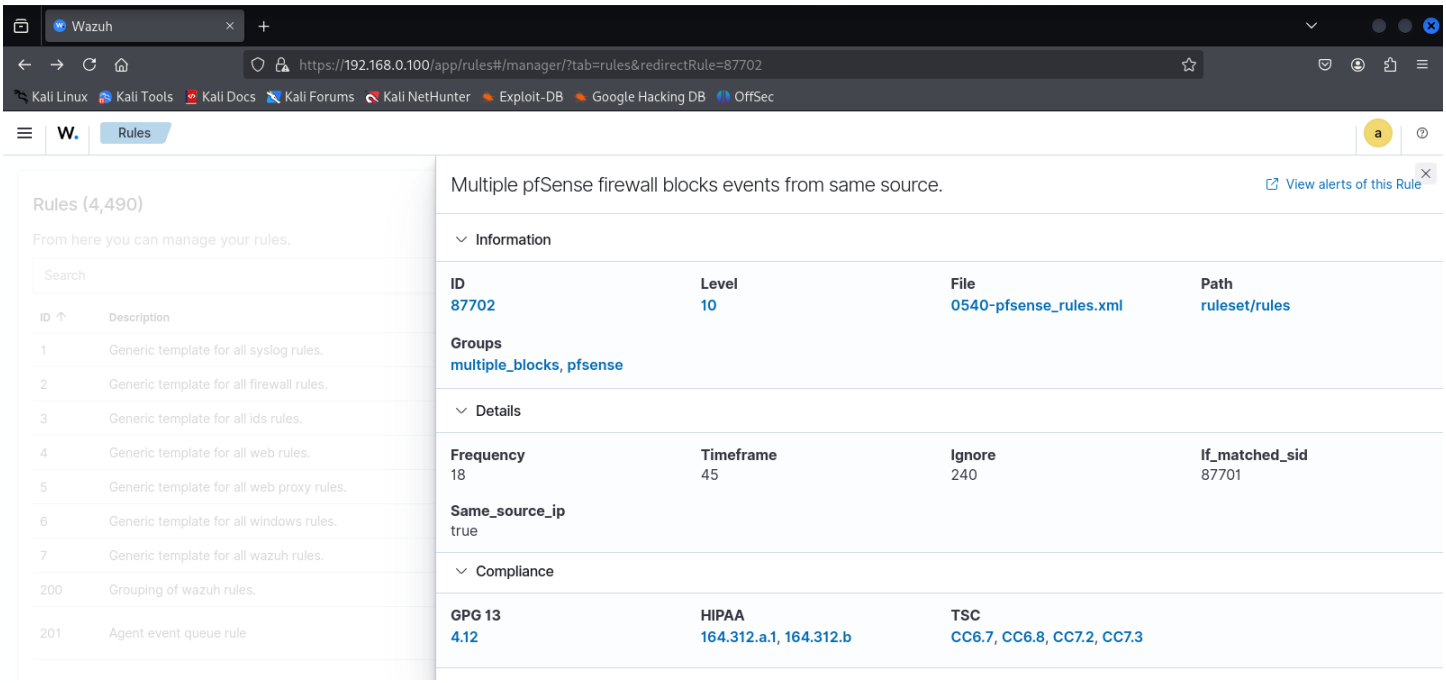
# FINAL RESULTS




pfSense.home.arpa - Firewall
Wazuh
https://192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(('$state':(store:appState),meta:(alias:!n,disab
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Threat Hunting
Dashboard
Events
Explore agent
Search
DQL
Last 7 days
Show dates
Refresh
manager.name: wazuh-server
rule.groups: pfsense
Add filter
Count
timestamp per 3 hours
3 hits
Aug 14, 2025 @ 07:29:36.935 - Aug 21, 2025 @ 07:29:36.936
Export Formatted
645 available fields
Columns
Density
1 fields sorted
Full screen
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


pfSense.home.arpa - Firewall
Wazuh
https://192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(('$state':(store:appState),meta:(alias:!n,disab
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Threat Hunting
Document Details
View surrounding documents
View single documen
Table
JSON
_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.srcport
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


pfSense.home.arpa - Stat
Wazuh
https://192.168.0.100/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(('$state':(store:appState),meta:(alias:!n,disab
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Threat Hunting
Dashboard
Events
Search
manager.name: wazuh-server
rule.groups: pfsense
Add filter
Export Formatted
645 available fields
Columns
Density
1 fields sorted
Full screen
timestamp
agent.name
rule.description
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 Details
View surrounding documents
View single documen
Table
JSON
_index
wazuh-alerts-4.x-2025.08.21
agent.id
000
agent.name
wazuh-server
data.action
block
data.dstip
192.168.0.255
data.dstport
137
data.id
12014
data.length
76
data.protocol
udp
data.srcip
192.168.0.106
data.srcport
137
decoder.name
pf
full_log
Aug 21 11:08:24 pfsense.home.arpa filterlog[33250]: 69,,,12014
h,block,in,4,0x0,,128,34167,0,none,17,udp,96,192.168.0.106,192.168.0.25
5,137,137,76


Wazuh
https://192.168.0.100/app/rules#/manager/?tab=rules&redirectRule=87702
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Rules
Rules (4,490)
From here you can manage your rules.
Search
ID
Description
1 Generic template for all syslog rules.
2 Generic template for all firewall rules.
3 Generic template for all ids rules.
4 Generic template for all web rules.
5 Generic template for all web proxy rules.
6 Generic template for all windows rules.
7 Generic template for all wazuh rules.
200 Grouping of wazuh rules.
201 Agent event queue rule
Multiple pfSense firewall blocks events from same source.
View alerts of this Rule
Information
ID
87702
Level
10
File
0540-pfsense_rules.xml
Path
ruleset/rules
Groups
multiple_blocks, pfsense
Details
Frequency
18
Timeframe
45
Ignore
240
If_matched_sid
87701
Same_source_ip
true
Compliance
GPG 13
4.12
HIPAA
164.312.a.1, 164.312.b
TSC
CC6.7, CC6.8, CC7.2, CC7.3

**THE END**