

## Report Task No: 02

Name Saad  
Internship Itsolera  
Team Phi

---

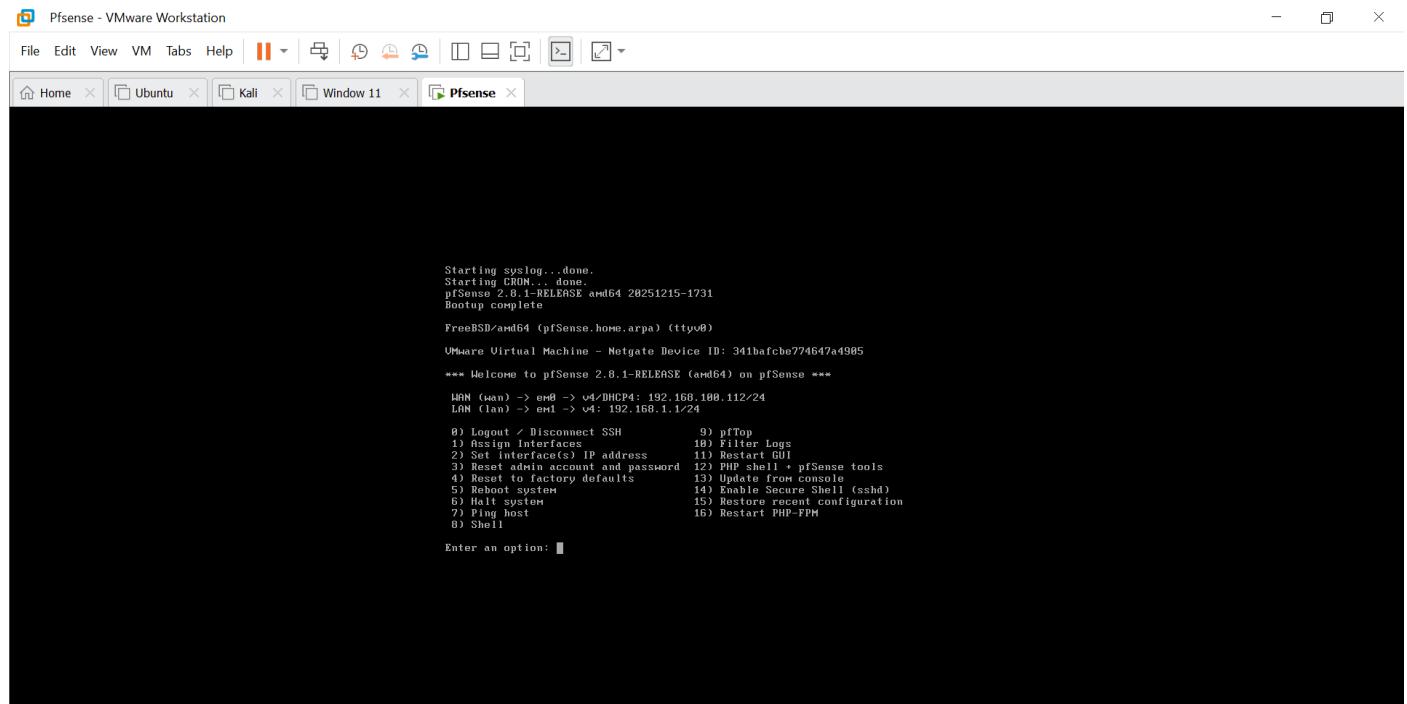


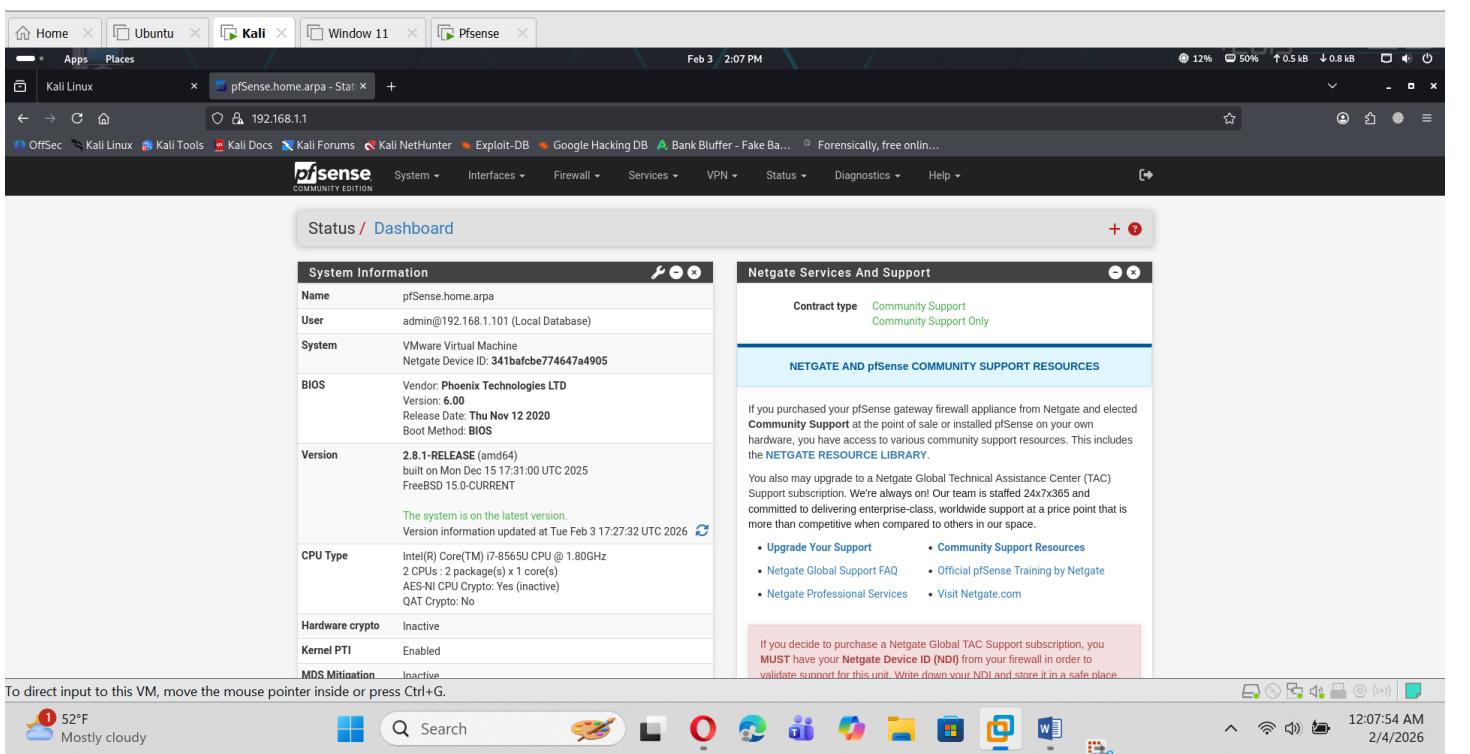
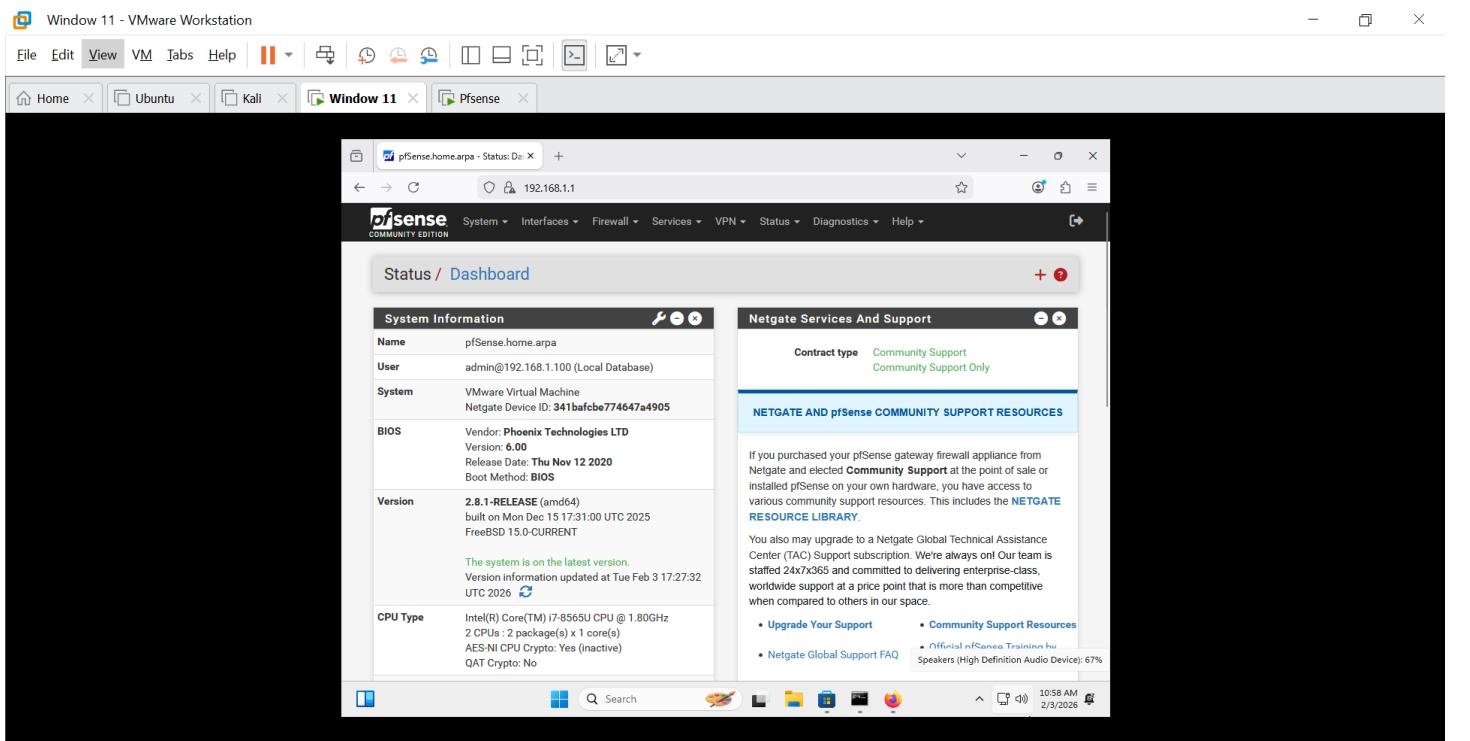
## Task:

1. Implement a software-based firewall and connect it with wazuh
2. Configure and create rule on firewall and test it with home lab
  - A. BLOCK specific countries (example china Russia etc.) traffic
  - B. Create rules which restrict the user from specified websites
  - C. Administrator privileges rule
3. Try to Monitor the files and logs on wazuh
4. create reports put analysis on the report regarding the traffic you have observed

## Step 1:

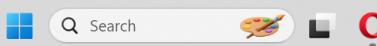
In the first step I configure Pfsense firewall in vm ware.





To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Cloudy 52°F  
Mostly cloudy



12:07:54 AM  
2/4/2026

## Step 2:

Configure pfSense with Wazuh Manager.

Login pfSense:

Status > Settings

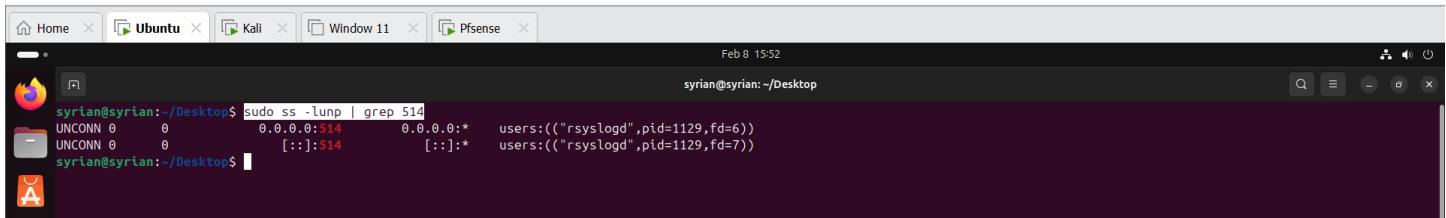
The screenshot shows the pfSense web interface with the URL [http://192.168.1.1/status\\_logs\\_settings.php](http://192.168.1.1/status_logs_settings.php). The page title is "Status / System Logs / Settings". The "Settings" tab is selected. The main section is titled "General Logging Options". It includes fields for "Log Message Format" (set to "BSD (RFC 3164, default)"), "Forward/Reverse Display" (checkbox for "Show log entries in reverse order (newest entries on top)"), "GUI Log Entries" (set to 500), "Raw Logs" (checkbox for "Show raw filter logs"), "Where to show rule descriptions" (set to "Display as column"), and "Local Logging" (checkbox for "Disable writing log files to the local disk"). A note at the bottom of this section states: "WARNING: This will also disable Login Protection!". Below this section, a note says: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

Set Wazuh Manager IP address.

The screenshot shows the pfSense web interface with the URL [http://192.168.1.1/status\\_logs\\_settings.php](http://192.168.1.1/status_logs_settings.php). The page title is "Status / System Logs / Settings". The "Settings" tab is selected. The main section is titled "Remote log servers". It includes a dropdown for "IP Protocol" (set to "IPv4") and three input fields for "Remote log servers": "192.168.1.102:514", "192.168.1.102:514", and "192.168.1.102:514". Below this, the "Remote Syslog Contents" section contains a list of checkboxes for various event types, with most being checked. A note at the bottom states: "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." At the bottom of the page is a "Save" button and a footer note: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2026 View license."

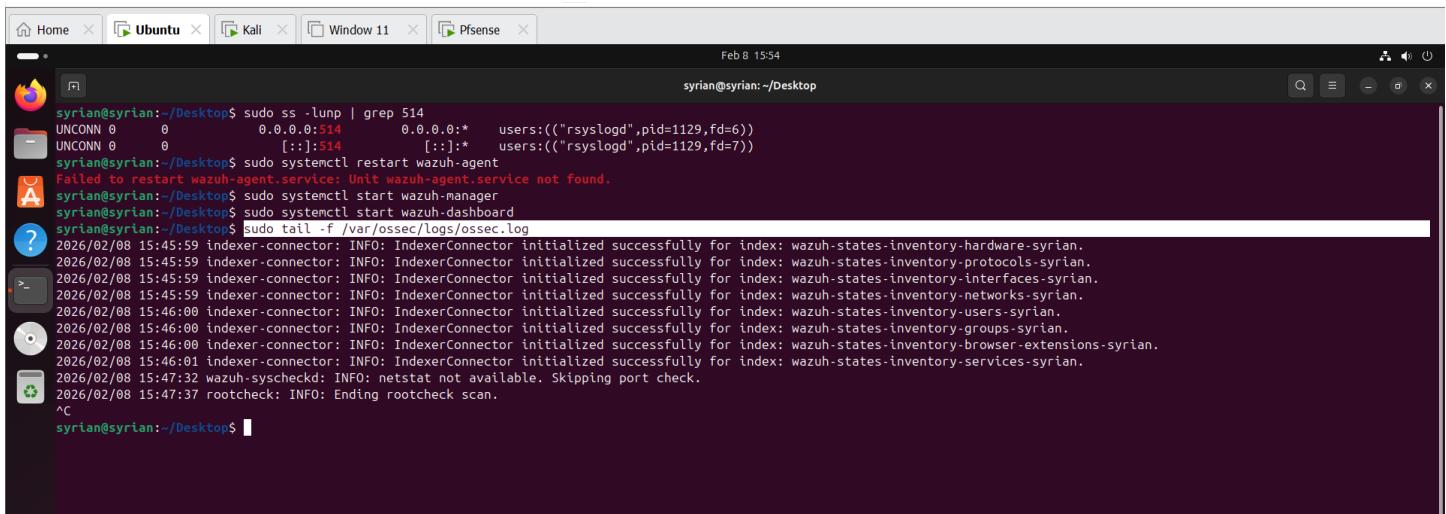
After assign Wazuh server IP and then save. Now I check configuration confirmation in Wazuh manager in Ubuntu.

Command: sudo ss -lunp | grep 514



```
Feb 8 15:52
syrian@syrian:~/Desktop$ sudo ss -lunp | grep 514
UNCONN 0      0      0.0.0.0:514      0.0.0.0:*      users:(("rsyslogd",pid=1129,fd=6))
UNCONN 0      0      [::]:514      [::]:*      users:(("rsyslogd",pid=1129,fd=7))
syrian@syrian:~/Desktop$
```

Command: sudo tail -f /var/ossec/logs/ossec.log



```
Feb 8 15:54
syrian@syrian:~/Desktop$ sudo ss -lunp | grep 514
UNCONN 0      0      0.0.0.0:514      0.0.0.0:*      users:(("rsyslogd",pid=1129,fd=6))
UNCONN 0      0      [::]:514      [::]:*      users:(("rsyslogd",pid=1129,fd=7))
syrian@syrian:~/Desktop$ sudo systemctl restart wazuh-agent
Failed to restart wazuh-agent.service: Unit wazuh-agent.service not found.
syrian@syrian:~/Desktop$ sudo systemctl start wazuh-manager
syrian@syrian:~/Desktop$ sudo systemctl start wazuh-dashboard
syrian@syrian:~/Desktop$ sudo tail -f /var/ossec/logs/ossec.log
2026/02/08 15:45:59 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-hardware-syrian.
2026/02/08 15:45:59 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-protocols-syrian.
2026/02/08 15:45:59 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-interfaces-syrian.
2026/02/08 15:45:59 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-networks-syrian.
2026/02/08 15:46:00 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-users-syrian.
2026/02/08 15:46:00 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-groups-syrian.
2026/02/08 15:46:00 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-browser-extensions-syrian.
2026/02/08 15:46:01 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-inventory-services-syrian.
2026/02/08 15:47:32 wazuh-syscheckd: INFO: netstat not available. Skipping port check.
2026/02/08 15:47:37 rootcheck: INFO: Ending rootcheck scan.
^C
syrian@syrian:~/Desktop$
```

## Step 3 (A):

Configure and create rules:

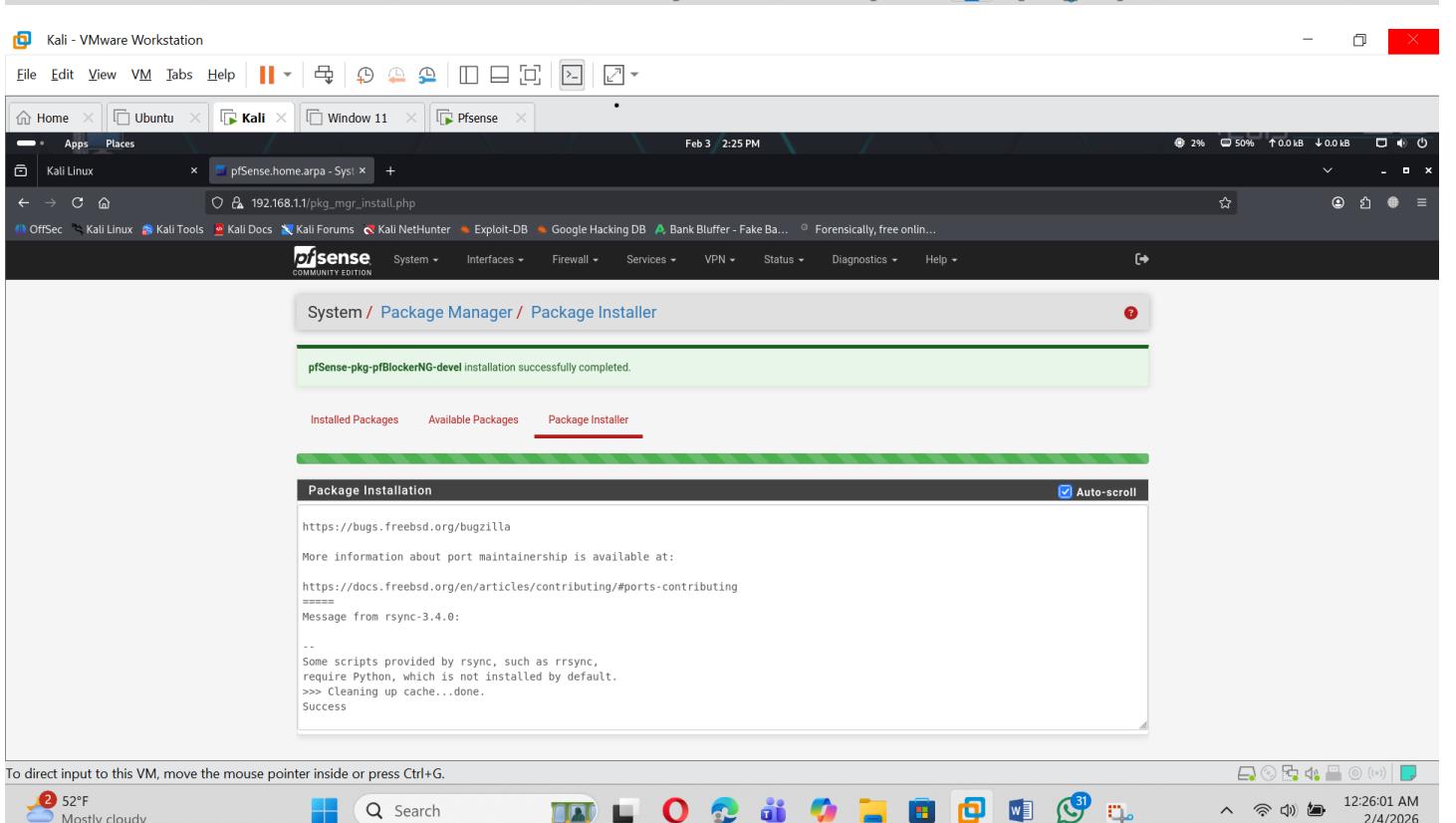
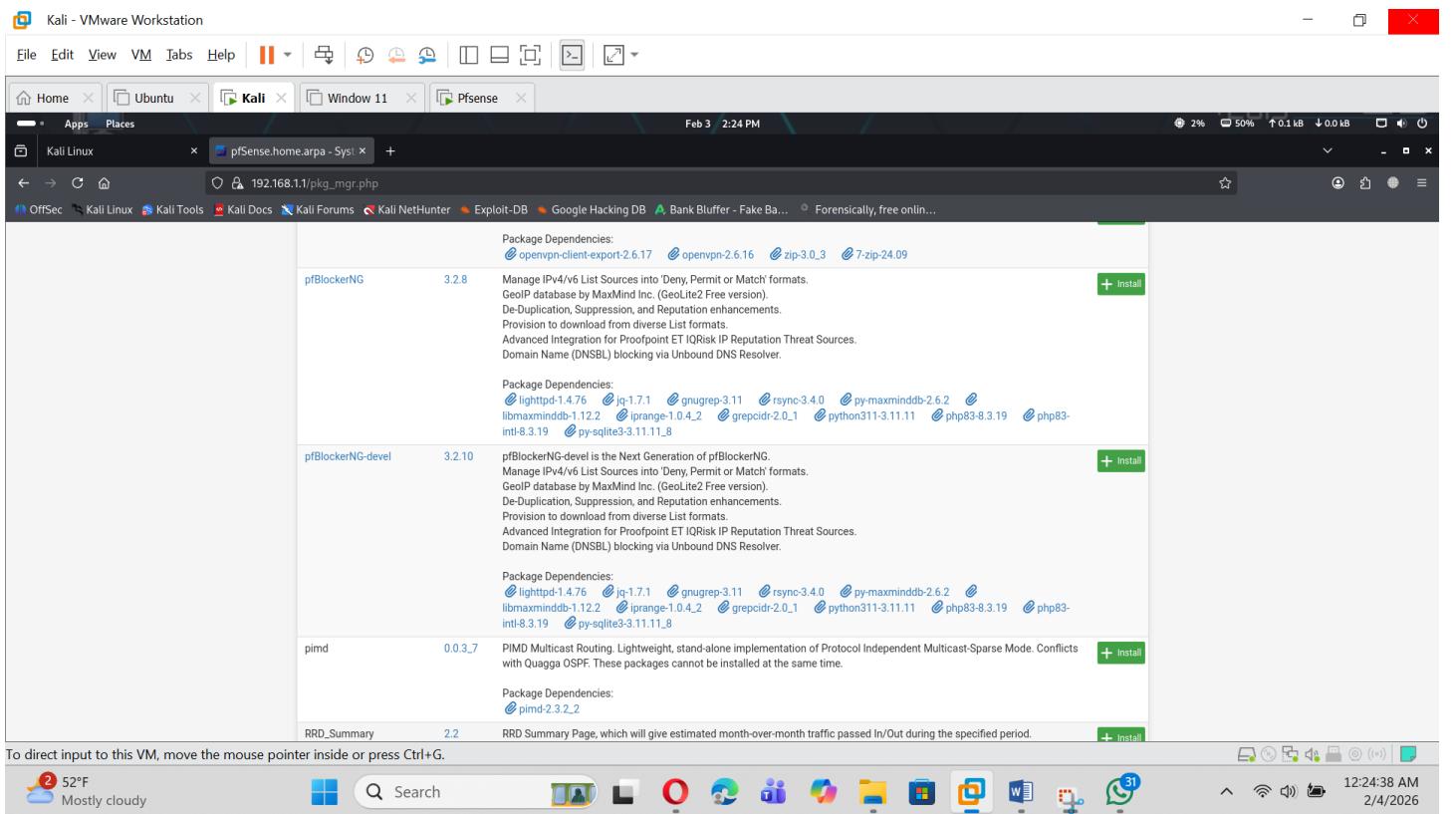
**Goal:** Block traffic from countries like China, Russia.

### Step 1: Install pfBlockerNG

1. Login to **pfSense Web GUI**
2. Go to:

System → Package Manager → Available Packages

- Search **pfBlockerNG**
- Install **pfBlockerNG-devel** (recommended)



## Step 2: Enable GeoIP

1. Go to:

## Firewall → pfBlockerNG → IP

The screenshot shows a Kali Linux VM interface with several tabs open: Home, Ubuntu, Kali, Window 11, and PfSense. The PfSense tab is active, displaying the pfSense Firewall configuration. The main navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a breadcrumb trail: Firewall / pfBlockerNG / IP.

The IP Configuration section is currently selected. It contains the following settings:

- De-Duplication:** Enabled (checkbox checked)
- CIDR Aggregation:** Not enabled (checkbox unchecked)
- Suppression:** Enabled (checkbox checked)
- Force Global IP Logging:** Not enabled (checkbox unchecked)

A placeholder IP address of 127.1.7.7 is listed at the bottom.

The status bar at the bottom indicates "To return to your computer, move the mouse pointer outside or press Ctrl+Alt."

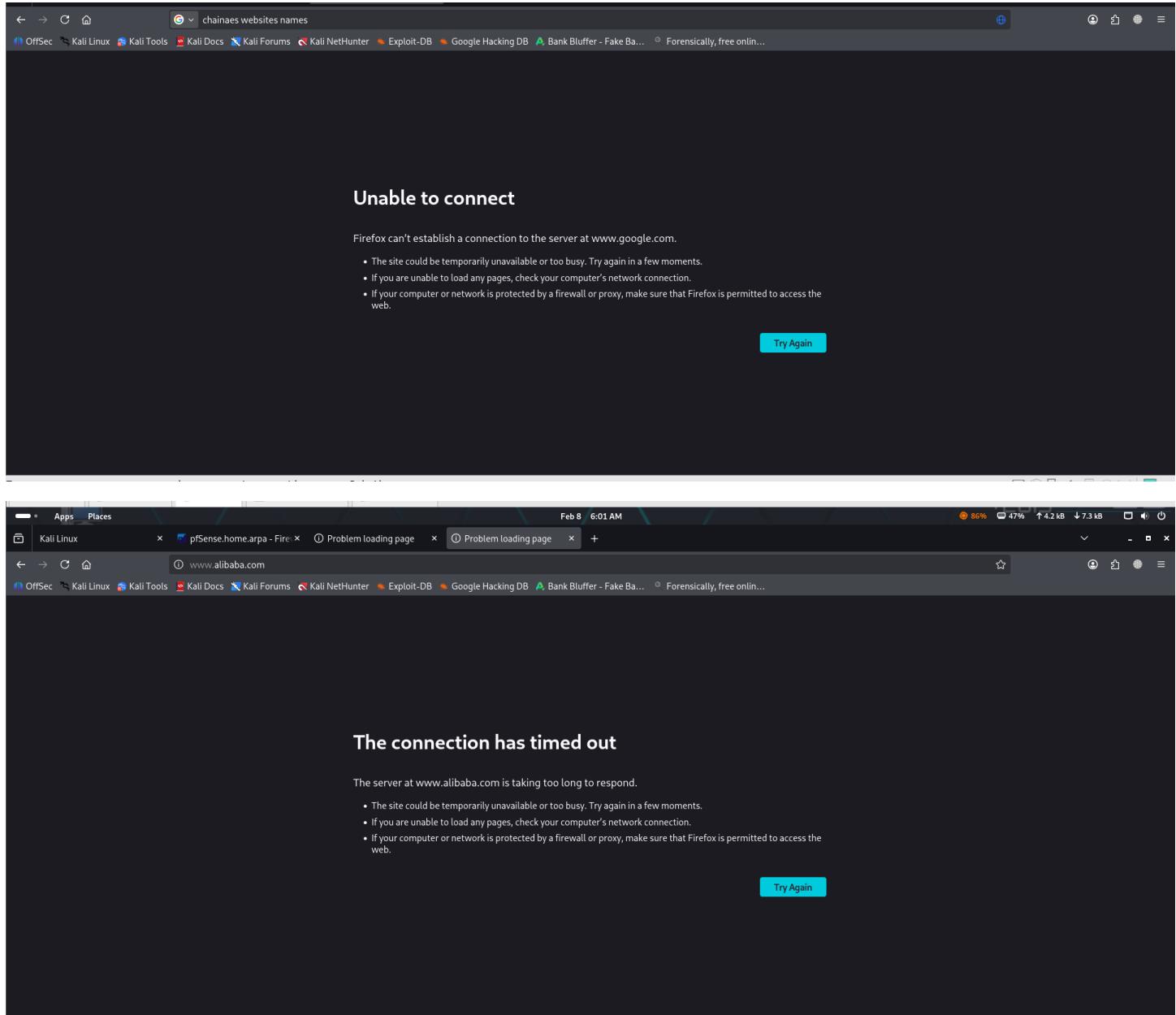
The taskbar at the bottom shows various icons for Windows applications like File Explorer, Task View, and Control Panel, along with system status indicators for battery level (53%), signal strength, and network activity.

The screenshot shows the same Kali Linux VM interface as the previous one, but the pfSense Firewall configuration has changed. The GeoIP tab is now selected under the IP section.

The GeoIP Summary table lists the following entries:

Name	Description	Action	Logging
Top Spammers	GeoIP Top Spammers	Disabled	Enabled
Africa	GeoIP Africa	Disabled	Enabled
Antarctica	GeoIP Antarctica	Disabled	Enabled
Asia	GeoIP Asia	Deny Both	Enabled
Europe	GeoIP Europe	Deny Both	Enabled
North America	GeoIP North America	Disabled	Enabled
Oceania	GeoIP Oceania	Disabled	Enabled
South America	GeoIP South America	Disabled	Enabled

Now I check those countries traffic.



Step 4 (B):

Specific websites block.

Go:

Firewall > Aliases and add websites.

The screenshot shows the pfSense Firewall / Aliases / IP configuration page. It lists two entries under 'Firewall Aliases IP':

Name	Type	Values	Description	Actions
facebookblock	Host(s)	157.240.227.35	Block Facebook	<a href="#">Edit</a> <a href="#">Delete</a>
youtubeblock	Host(s)	142.250.187.78	block youtube	<a href="#">Edit</a> <a href="#">Delete</a>

At the bottom right, there are buttons for '+ Add' and 'Import'.

Then again click firewall > click Rules , click LAN add and save.

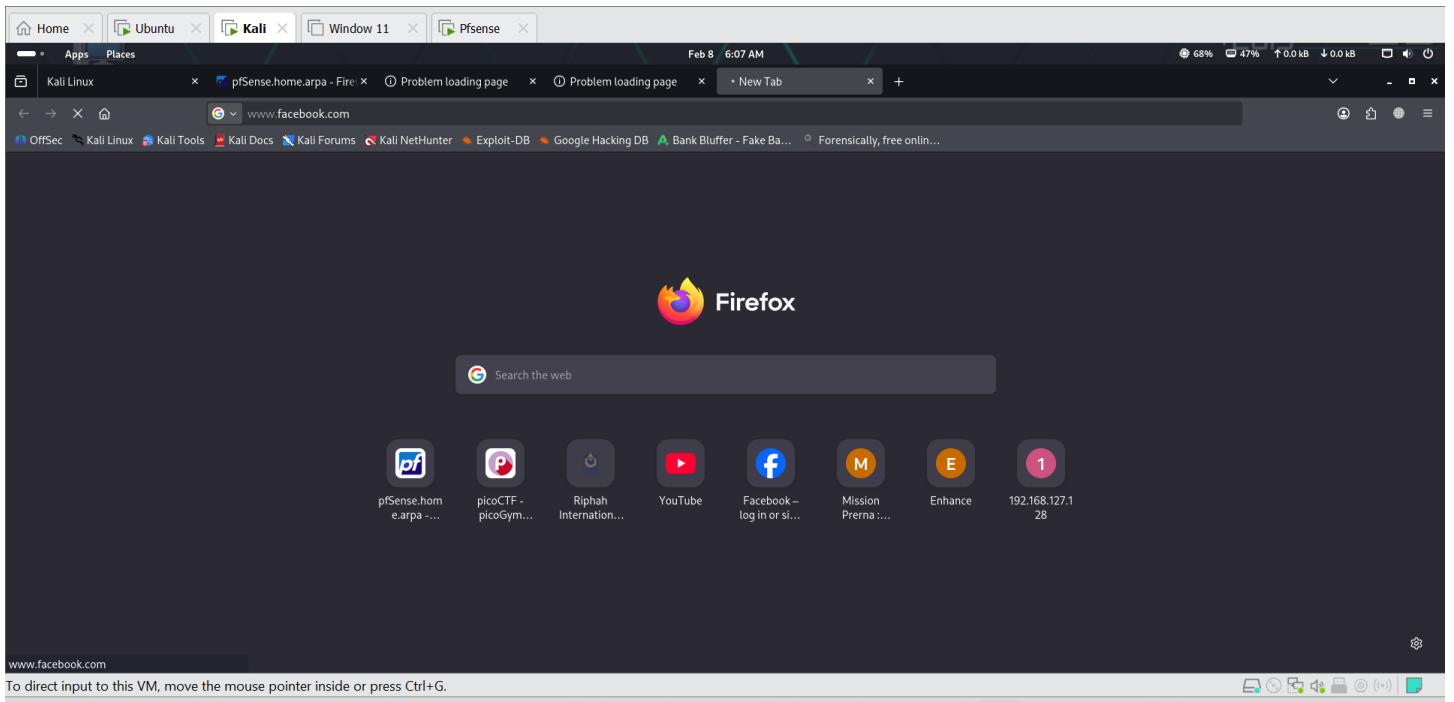
The screenshot shows the pfSense Firewall / Rules / LAN configuration page. It displays a list of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/1.27 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	<a href="#">Edit</a>
✗ 0/12 KiB	IPv4	*	*	pfB_Asia_v4	*	*	none		pfB_Asia_v4 auto rule	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a>
✗ 0/0 B	IPv4	*	*	pfB_Europe_v4	*	*	none		pfB_Europe_v4 auto rule	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a>
✗ 0/0 B	IPv4	*	*	pfB_PRI1_v4	*	*	none		pfB_PRI1_v4 auto rule	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a>
✗ 0/34 KiB	IPv4	*	*	facebookblock	*	*	none		Block Facebook	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a>
✗ 0/0 B	IPv4	*	*	youtubeblock	*	*	none			<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a>
✓ 21/4.95 MiB	IPv4	*	LAN subnets	*	*	*	*		Default allow LAN to any rule	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a>
✓ 0/0 B	IPv6	*	LAN subnets	*	*	*	*		Default allow LAN IPv6 to any rule	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Save</a>

At the bottom right, there are buttons for '+ Add', 'Add', 'Delete', 'Toggle', 'Copy', 'Save', and 'Separate'.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Now I checked.



So not loading facebook page.

## Alerts.

A screenshot of the pfSense Firewall / pfBlockerNG / Alerts interface. The 'Alerts' tab is selected. The table displays the following data:

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Kali Linux pfSense.home.arpa - Fire □ Problem loading page □ Problem loading page □ New Tab

Not Secure http://192.168.1.1/pfblockeng/pfblockeng\_alerts.php

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Bank Bluffer - Fake Ba... Forensically, free onlin...

**DNSBL Python - Last 25 Alert Entries**

Date	IP	Source	Domain/Block mode	Feed/Group
Feb 8 11:06:36 [2]	192.168.1.101	kali	googleads.g.doubleclick.net [DNSBL] DNSBL-python   Python	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 11:06:35 [2]	192.168.1.101	kali	www.google.com [DNSBL] DNSBL-python   HSTS	Ripah_Block_custom DNSBL_Ripah_Block
Feb 8 11:03:14 [1]	192.168.1.101	kali	ads.mozilla.org [DNSBL] DNSBL-python   Python	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 11:00:28 [2]	192.168.1.101	kali	www.google-analytics.com [DNSBL] DNSBL-python   HSTS	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 11:00:16 [2]	192.168.1.101	kali	static.cloudflareinsights.com [DNSBL] DNSBL-python   Python	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 11:00:16 [2]	192.168.1.101	kali	www.googletagmanager.com [DNSBL] DNSBL-python   HSTS	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 10:59:55 [2]	192.168.1.101	kali	www.google.com [DNSBL] DNSBL-python   HSTS	Ripah_Block_custom DNSBL_Ripah_Block
Feb 8 10:46:56 [5]	192.168.1.101	kali	ads.mozilla.org [DNSBL] DNSBL-python   Python	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 09:28:42 [7]	192.168.1.101	kali	ads.mozilla.org [DNSBL] DNSBL-python   Python	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 08:34 [1]	192.168.1.102	syrian	www.google.com [DNSBL] DNSBL-python   HSTS	Ripah_Block_custom DNSBL_Ripah_Block
Feb 8 08:31 [1]	192.168.1.102	syrian	incoming.telemetry.mozilla.org [DNSBL] DNSBL-python   Python	StevenBlack_ADs DNSBL_Ripah_Block
Feb 8 08:10:28 [3]	192.168.1.101	kali	ads.mozilla.org [DNSBL]	StevenBlack_ADs

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Home □ Ubuntu □ Kali □ Window 11 □ PfSense

Kali Linux pfSense.home.arpa - Fire □ Problem loading page □ Problem loading page □ New Tab

Not Secure http://192.168.1.1/pfblockeng/pfblockeng\_log.php

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Bank Bluffer - Fake Ba... Forensically, free onlin...

General IP DNSBL Update Reports Feeds Logs Sync

**Log/File Browser selections**

Log/File type: Log Files Choose which type of log/file you want to view.

Log/File selection: ip\_block.log Choose which log/file you want to view.

**Log/File Details**

File successfully loaded: Total Lines: 1018  
Log/File Path: /var/log/pfblockeng/ip\_block.log

**Log**

```
Feb 7 14:41:47,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia.v4,203.99.48.0/28,PK,v4,Unknown,kali,null,+  
Feb 7 14:41:47,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia.v4,203.99.48.0/28,PK,v4,Unknown,kali,null,-  
Feb 7 14:41:47,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia.v4,203.99.48.0/28,PK,v4,Unknown,kali,null,-  
Feb 7 14:42:33,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.167,159.34,52956,123,out,PK,pfB_Asia.v4,103.167,159.0/23,PK,v4,Unknown,kali,null,+  
Feb 7 14:42:45,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.55,68.158,53125,123,out,PK,pfB_Asia.v4,103.55,68.0/22,PK,v4,time2.nayatel.com,kali,null,+  
Feb 7 14:42:55,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.157,20.147,14,51531,123,out,PK,pfB_Asia.v4,103.157,20.146.0/23,PK,v4,dns14.zcomnetworks.com.pk,  
Feb 7 14:43:06,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.152,101.59,53980,123,out,PK,pfB_Asia.v4,103.152,100.0/23,PK,v4,103.152.101.59-hn.com.pk  
Feb 7 14:43:16,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.152,101.29,48339,123,out,PK,pfB_Asia.v4,103.152.100.0/23,PK,v4,103.152.101.22-hn.com.pk  
Feb 7 14:43:27,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.157,128.20,58840,123,out,PK,pfB_Asia.v4,103.157.128.0/23,PK,v4,103.157.128.0/23,PK,v4,ges.net.pk,kali,null,+  
Feb 7 14:43:37,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.157,128.20,58840,123,out,PK,pfB_Asia.v4,103.157.128.0/23,PK,v4,103.157.128.0/23,PK,v4,ges.net.pk,kali,null,+  
Feb 7 15:18:12,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,41378,123,out,PK,pfB_Asia.v4,203.99.48.0/28,PK,v4,Unknown,kali,null,+  
Feb 7 15:18:23,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.167,150.26,34170,123,out,PK,pfB_Asia.v4,103.167,150.0/23,PK,v4,Unknown,kali,null,+  
Feb 7 15:18:35,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.152,101.101,43641,123,out,PK,pfB_Asia.v4,103.152.100.0/23,PK,v4,103.152.101.249-hn.com  
Feb 7 15:18:45,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.167,159.26,40293,123,out,PK,pfB_Asia.v4,103.167,159.0/23,PK,v4,Unknown,kali,null,+  
Feb 7 15:18:57,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.55,68.158,58312,123,out,PK,pfB_Asia.v4,103.55.68.0/22,PK,v4,time2.nayatel.com,kali,null  
Feb 7 15:19:07,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,103.152,101.22,33856,123,out,PK,pfB_Asia.v4,103.152.100.0/23,PK,v4,103.152.101.22-hn.com.pk  
Feb 7 15:19:29,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,203.80.128.20,45613,123,out,PK,pfB_Asia.v4,203.80.128.0/24,PK,v4,ntp.ges.net.pk,kali,null,+  
Feb 7 15:19:39,1770089574,en1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,53969,123,out,PK,pfB_Asia.v4,203.99.48.0/28,PK,v4,Unknown,kali,null,+
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

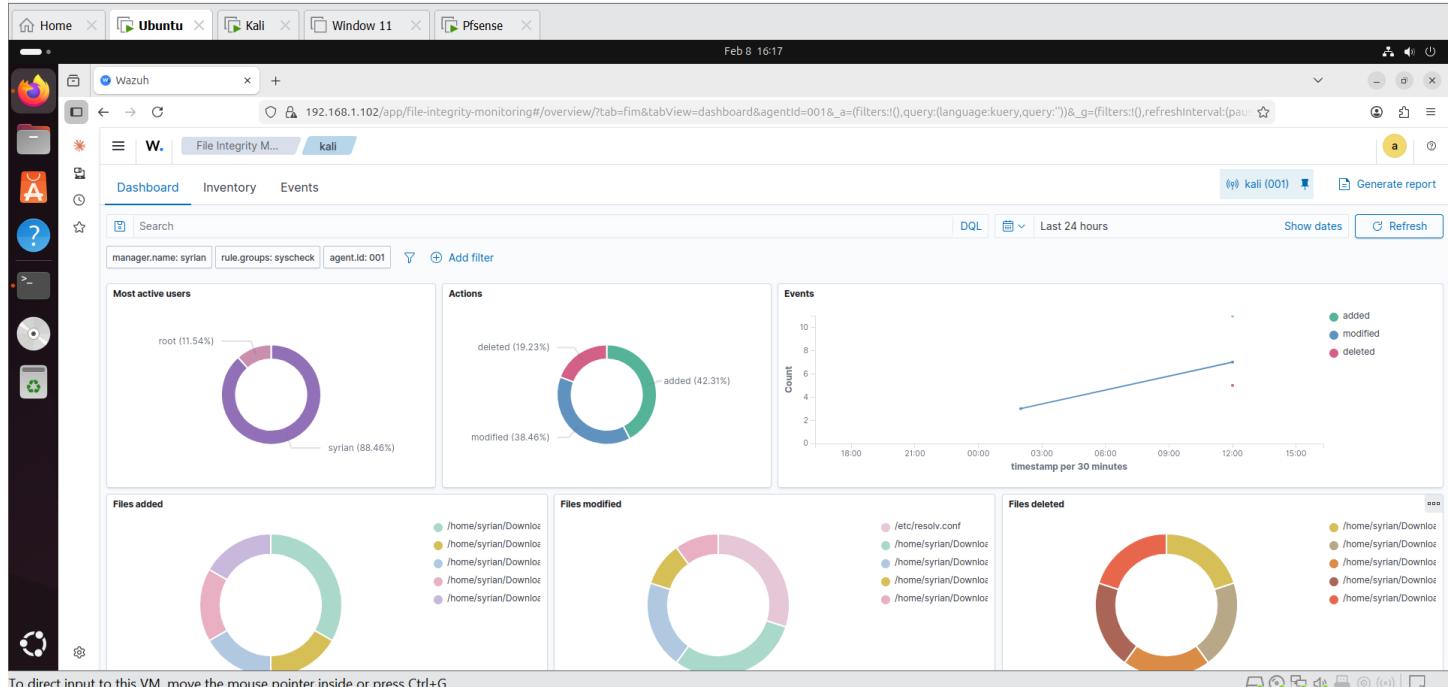
## Log

```
Feb 7 14:41:47,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,+  
Feb 7 14:41:47,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,-  
Feb 7 14:41:47,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,-  
Feb 7 14:42:33,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.167.159.34,52956,123,out,PK,pfB_Asia_v4,103.167.158.0/23,PK_v4,Unknown,kali,null,+  
Feb 7 14:42:45,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.55.68.158,53125,123,out,PK,pfB_Asia_v4,103.55.68.0/22,PK_v4,time2.nayatel.com,kali,null  
Feb 7 14:42:55,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,157.20.147.14,51531,123,out,PK,pfB_Asia_v4,157.20.146.0/23,PK_v4,dns14.zcommnetworks.com.pk,  
Feb 7 14:43:06,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.152.101.59,53980,123,out,PK,pfB_Asia_v4,103.152.100.0/23,PK_v4,103.152.101.59-hn.com.pk  
Feb 7 14:43:16,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.152.101.22,48339,123,out,PK,pfB_Asia_v4,103.152.100.0/23,PK_v4,103.152.101.22-hn.com.pk  
Feb 7 14:43:41,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.80.128.20,50846,123,out,PK,pfB_Asia_v4,203.80.128.0/24,PK_v4,ntp.ges.net.pk,kali,null,+  
Feb 7 14:43:52,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.167.159.34,54626,123,out,PK,pfB_Asia_v4,103.167.158.0/23,PK_v4,Unknown,kali,null,+  
Feb 7 15:18:12,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,41378,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,+  
Feb 7 15:18:22,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.167.159.26,34179,123,out,PK,pfB_Asia_v4,103.167.158.0/23,PK_v4,Unknown,kali,null,+  
Feb 7 15:18:35,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.152.101.249,43641,123,out,PK,pfB_Asia_v4,103.152.100.0/23,PK_v4,103.152.101.249-hn.com.  
Feb 7 15:18:45,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.167.159.26,40293,123,out,PK,pfB_Asia_v4,103.167.158.0/23,PK_v4,Unknown,kali,null,+  
Feb 7 15:18:57,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.55.68.158,58312,123,out,PK,pfB_Asia_v4,103.55.68.0/22,PK_v4,time2.nayatel.com,kali,null  
Feb 7 15:19:07,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,103.152.101.22,33856,123,out,PK,pfB_Asia_v4,103.152.100.0/23,PK_v4,103.152.101.22-hn.com.pk  
Feb 7 15:19:29,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.80.128.20,45613,123,out,PK,pfB_Asia_v4,203.80.128.0/24,PK_v4,ntp.ges.net.pk,kali,null,+  
Feb 7 15:19:39,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,53969,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,+  
Feb 7 15:19:39,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,53969,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,-  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,183.60.227.38,42678,443,out,CN,pfB_Asia_v4,183.0.0.0/10,CN_v4,Unknown,kali,null,+  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,183.60.227.38,42678,443,out,CN,pfB_Asia_v4,183.0.0.0/10,CN_v4,Unknown,kali,null,+  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,27.128.217.38,41528,443,out,CN,pfB_Asia_v4,27.128.0.0/15,CN_v4,Unknown,kali,null,+  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,27.128.217.38,41528,443,out,CN,pfB_Asia_v4,27.128.0.0/15,CN_v4,Unknown,kali,null,-  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,60.164.7.38,42196,443,out,CN,pfB_Asia_v4,60.160.0.0/11,CN_v4,Unknown,kali,null,+  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,60.164.7.38,42196,443,out,CN,pfB_Asia_v4,60.160.0.0/11,CN_v4,Unknown,kali,null,-  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,61.170.57.38,52370,443,out,CN,pfB_Asia_v4,61.160.0.0/11,CN_v4,Unknown,kali,null,+  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,61.170.57.38,52370,443,out,CN,pfB_Asia_v4,61.160.0.0/11,CN_v4,Unknown,kali,null,-  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,175.12.90.38,45810,443,out,CN,pfB_Asia_v4,175.0.0.0/12,CN_v4,Unknown,kali,null,+  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,175.12.90.38,45810,443,out,CN,pfB_Asia_v4,175.0.0.0/12,CN_v4,Unknown,kali,null,-  
Feb 7 16:12:16,1770009574,em1,LAN,block,4,6,TCP-S,192.168.1.101,182.106.158.38,36464,443,out,CN,pfB_Asia_v4,182.96.0.0/12,CN_v4,Unknown,kali,null,+
```

## Step 4:

Monitor logs through wazuh

Login wazuh manger



Feb 8 16:18

Wazuh - File Integrity Monitoring

26 hits

Feb 7, 2026 @ 16:17:54.679 - Feb 8, 2026 @ 16:17:54.679

Export Formatted | Reset view | 643 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Feb 8, 2026 @ 12:29:12.962	kali	/home/syrian/Downloads/awesome-malware-analysis...	added	File added to the system.	5	554
Feb 8, 2026 @ 12:29:12.927	kali	/home/syrian/Downloads/awesome-malware-analysis...	added	File added to the system.	5	554
Feb 8, 2026 @ 12:29:12.925	kali	/home/syrian/Downloads/awesome-malware-analysis...	added	File added to the system.	5	554
Feb 8, 2026 @ 12:29:12.925	kali	/home/syrian/Downloads/awesome-malware-analysis...	modified	Integrity checksum changed.	7	550
Feb 8, 2026 @ 12:29:12.875	kali	/home/syrian/Downloads/awesome-malware-analysis...	added	File added to the system.	5	554
Feb 8, 2026 @ 12:29:12.858	kali	/home/syrian/Downloads/awesome-malware-analysis...	added	File added to the system.	5	554
Feb 8, 2026 @ 12:29:12.835	kali	/home/syrian/Downloads/awesome-malware-analysis...	added	File added to the system.	5	554
Feb 8, 2026 @ 12:29:12.889	kali	/home/syrian/Downloads/awesome-malware-analysis...	added	File added to the system.	5	554
Feb 8, 2026 @ 12:23:15.871	kali	/home/syrian/Downloads/morse_chal.wav	deleted	File deleted.	7	553
Feb 8, 2026 @ 12:23:14.566	kali	/home/syrian/Downloads/me.txt	deleted	File deleted.	7	553
Feb 8, 2026 @ 12:23:11.693	kali	/home/syrian/Downloads/public.zip	deleted	File deleted.	7	553
Feb 8, 2026 @ 12:23:09.476	kali	/home/syrian/Downloads/message.txt	deleted	File deleted.	7	553
Feb 8, 2026 @ 12:23:35.968	kali	/home/syrian/Downloads/awesome-malware-analysis...	modified	Integrity checksum changed.	7	550
Feb 8, 2026 @ 12:22:35.936	kali	/home/syrian/Downloads/awesome-malware-analysis...	modified	Integrity checksum changed.	7	550
Feb 8, 2026 @ 12:22:35.812	kali	/home/syrian/Downloads/awesome-malware-analysis...	deleted	File deleted.	7	553

Rows per page: 15 < 1 2 >

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Feb 8 16:19

Wazuh - Malware Detection

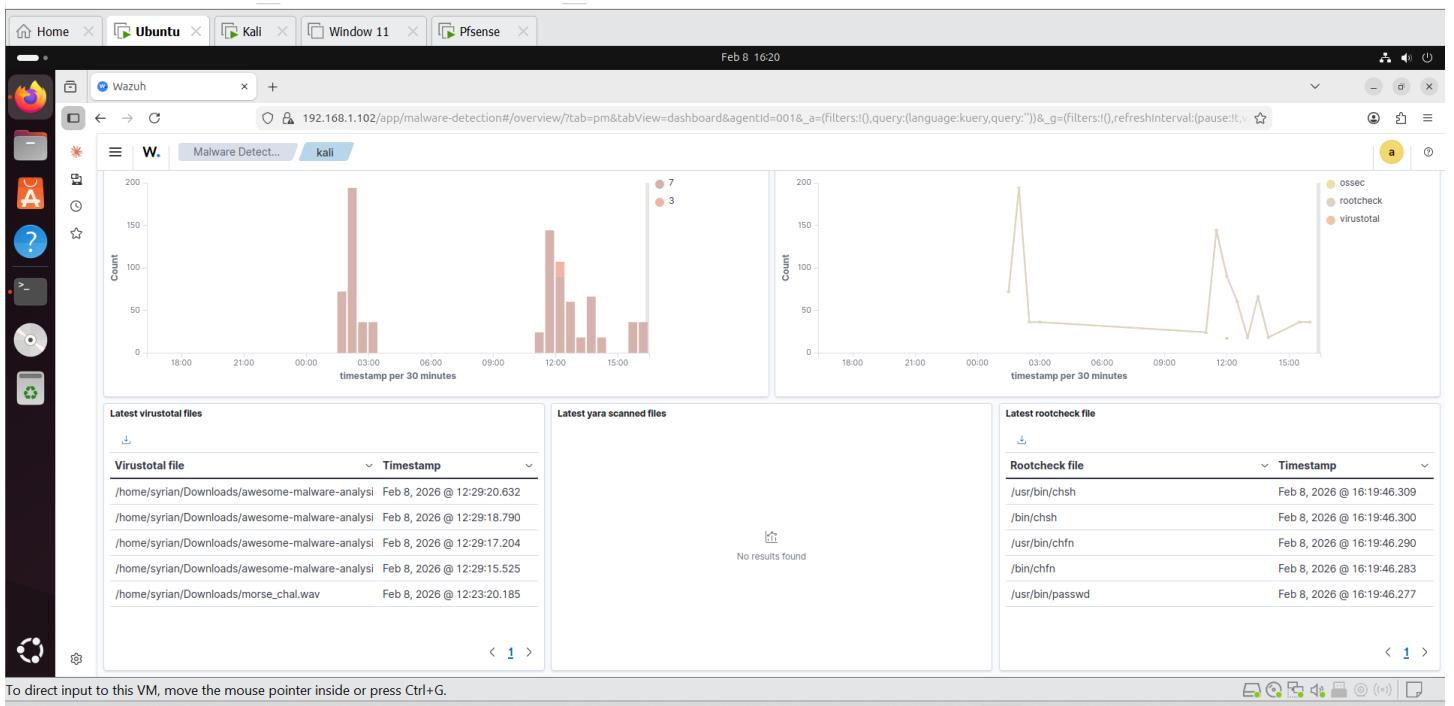
841 hits

Feb 7, 2026 @ 16:19:08.630 - Feb 8, 2026 @ 16:19:08.630

Export Formatted | Reset view | 643 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	data.title	rule.description	rule.level	rule.id
Feb 8, 2026 @ 16:16:36.601	kali	Trojaned version of file detected.	Host-based anomaly detection event (rootcheck).	7	510
Feb 8, 2026 @ 16:16:36.590	kali	Trojaned version of file detected.	Host-based anomaly detection event (rootcheck).	7	510
Feb 8, 2026 @ 16:16:36.546	kali	Trojaned version of file detected.	Host-based anomaly detection event (rootcheck).	7	510
Feb 8, 2026 @ 16:16:36.529	kali	Trojaned version of file detected.	Host-based anomaly detection event (rootcheck).	7	510
Feb 8, 2026 @ 16:16:36.500	kali	Trojaned version of file detected.	Host-based anomaly detection event (rootcheck).	7	510

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



## Final Summary:

During this task, I successfully:

- Configured pfSense firewall in VMware.
- Integrated pfSense with Wazuh Manager.
- Blocked traffic from high-risk countries using GeoIP.
- Blocked specific websites using firewall rules.
- Monitored and analyzed traffic logs using Wazuh.