# Report Task No: 02

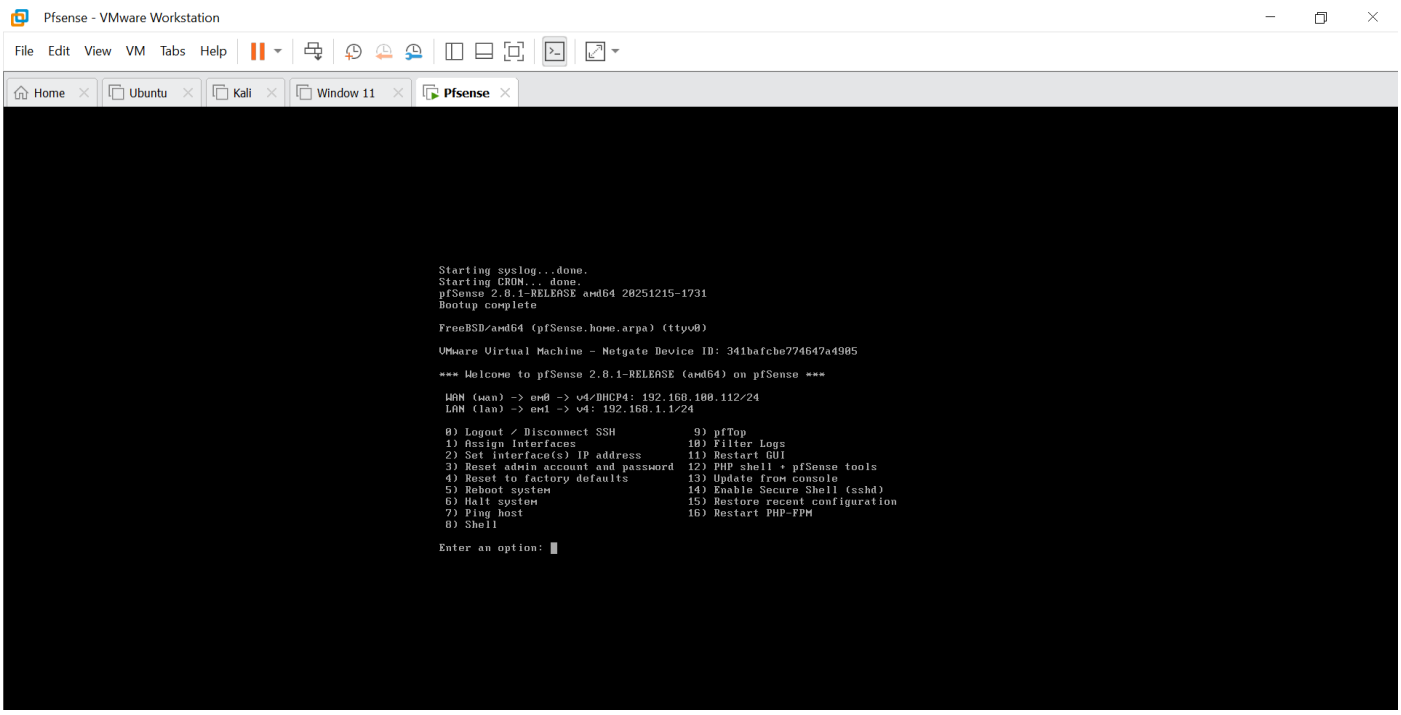
| | |
|---|---|
| Name | Saad |
| Internship | Itsolera |
| Team | Phi |

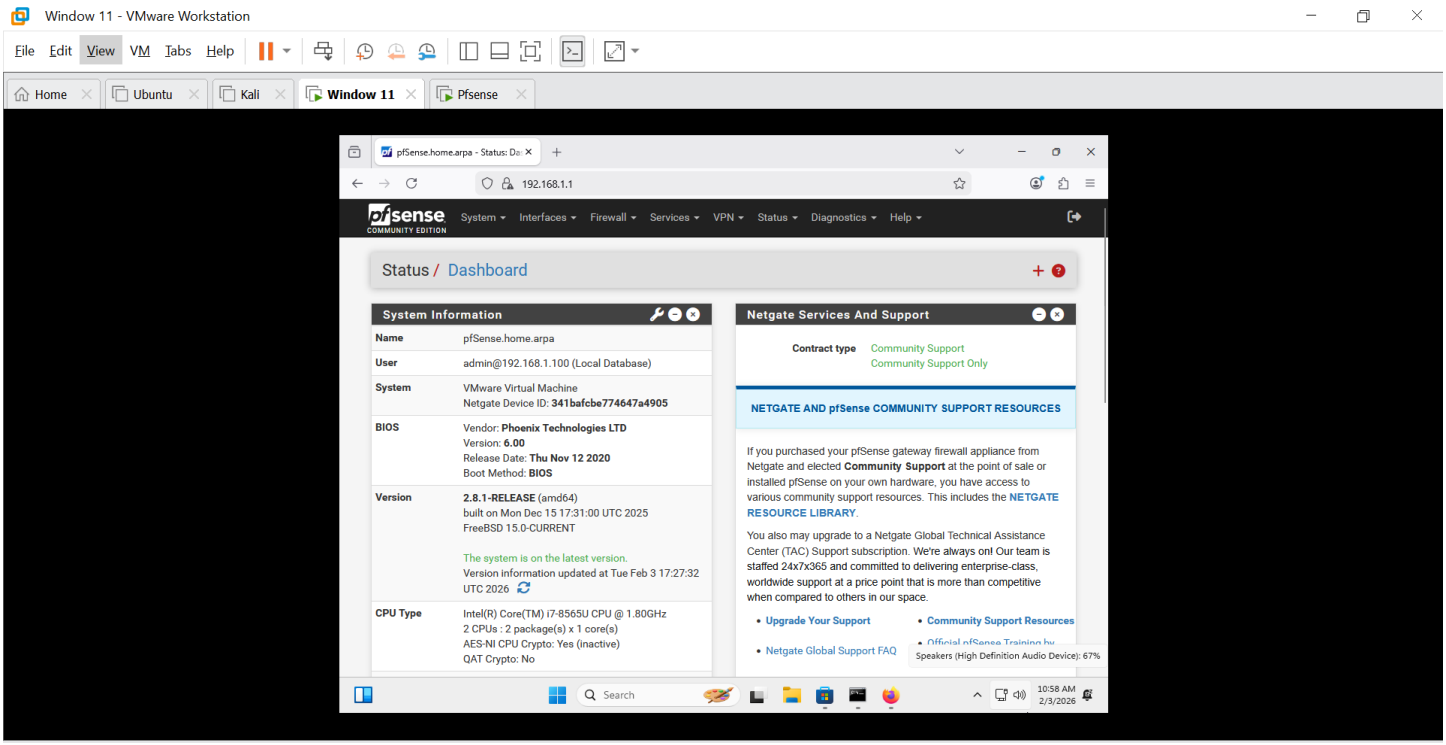
# Task:

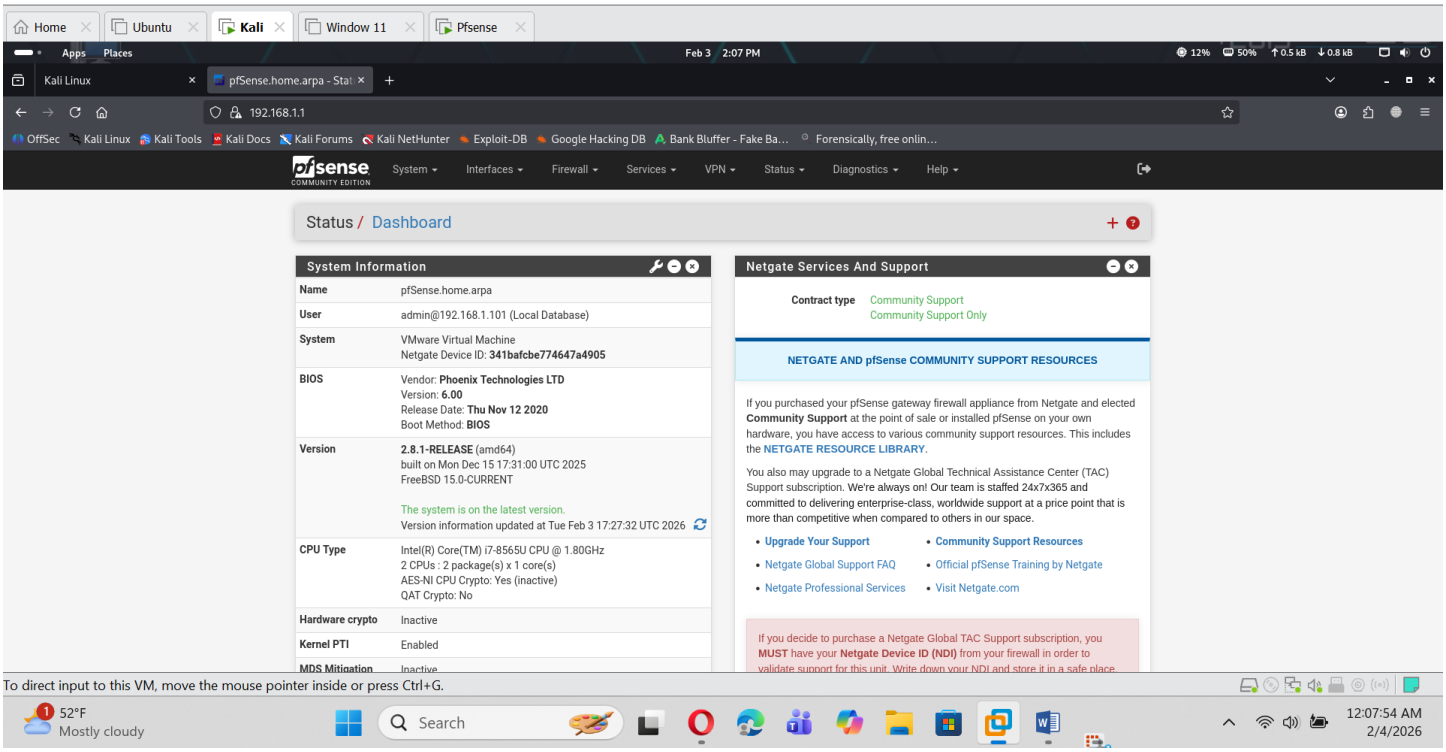
1. Implement a software-based firewall and connect it with wazuh
2. Configure and create rule on firewall and test it with home lab
    A. BLOCK specific countries (example china Russia etc.) traffic
    B. Create rules which restrict the user from specified websites
    C. Administrator privileges rule
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 Pfsene firewall in vm ware.




Window 11 - VMware Workstation
File Edit View VM Tabs Help
Home Ubuntu Kali Window 11 Pfsense
pfSense.home.arpa - Status: Da
192.168.1.1
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Status / Dashboard
System Information
Name pfSense.home.arpa
User admin@192.168.1.100 (Local Database)
System VMware Virtual Machine
Netgate Device ID: 341bafcbe774647a4905
BIOS Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
Boot Method: BIOS
Version 2.8.1-RELEASE (amd64)
built on Mon Dec 15 17:31:00 UTC 2025
FreeBSD 15.0-CURRENT
The system is on the latest version.
Version information updated at Tue Feb 3 17:27:32 UTC 2026
CPU Type Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
2 CPUs : 2 package(s) x 1 core(s)
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
Speakers (High Definition Audio Device): 67%
Search
10:58 AM
2/3/2026

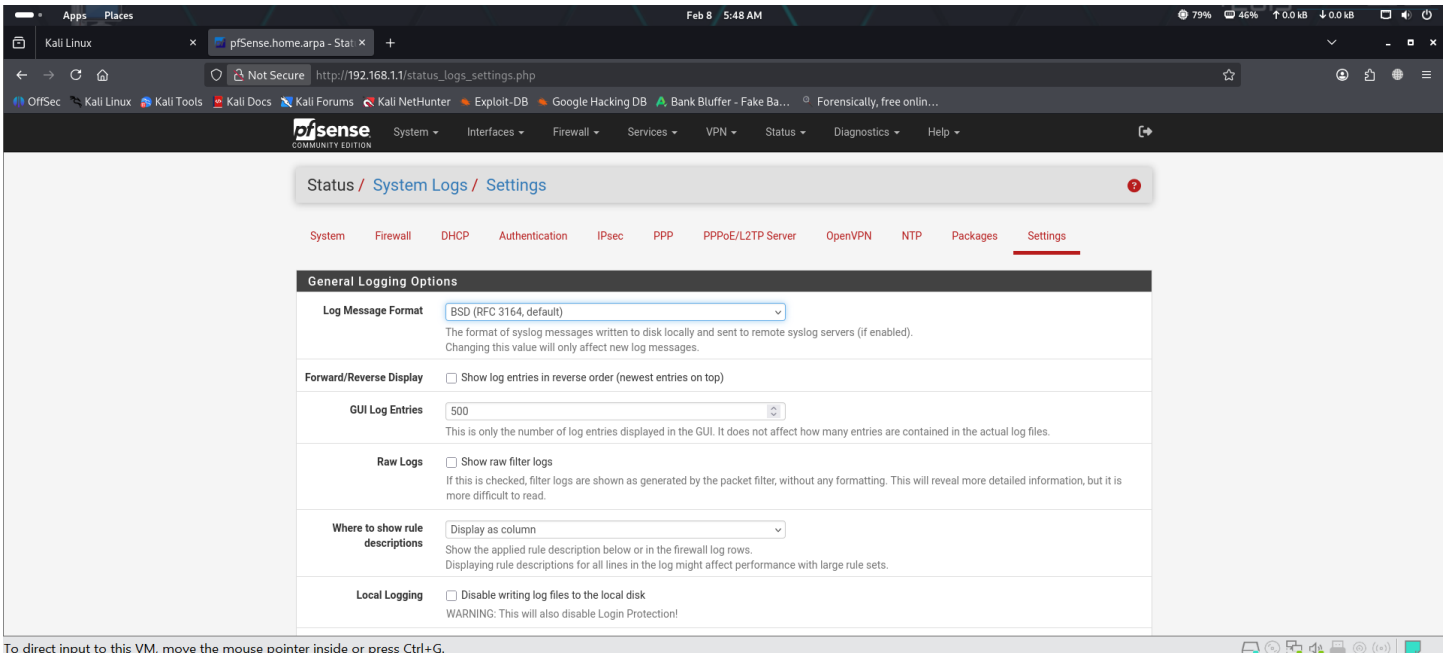

Home Ubuntu Kali Window 11 Pfsense
Apps Places
Feb 3 2:07 PM
Kali Linux
pfSense.home.arpa - Stat
192.168.1.1
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Bank Bluffer - Fake Ba... Forensically, free onlin...
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Status / Dashboard
System Information
Name pfSense.home.arpa
User admin@192.168.1.101 (Local Database)
System VMware Virtual Machine
Netgate Device ID: 341bafcbe774647a4905
BIOS Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
Boot Method: BIOS
Version 2.8.1-RELEASE (amd64)
built on Mon Dec 15 17:31:00 UTC 2025
FreeBSD 15.0-CURRENT
The system is on the latest version.
Version information updated at Tue Feb 3 17:27:32 UTC 2026
CPU Type Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
2 CPUs : 2 package(s) x 1 core(s)
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
Hardware crypto Inactive
Kernel PTI Enabled
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
If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
52°F
Mostly cloudy
Search
12:07:54 AM
2/4/2026

# Step 2:

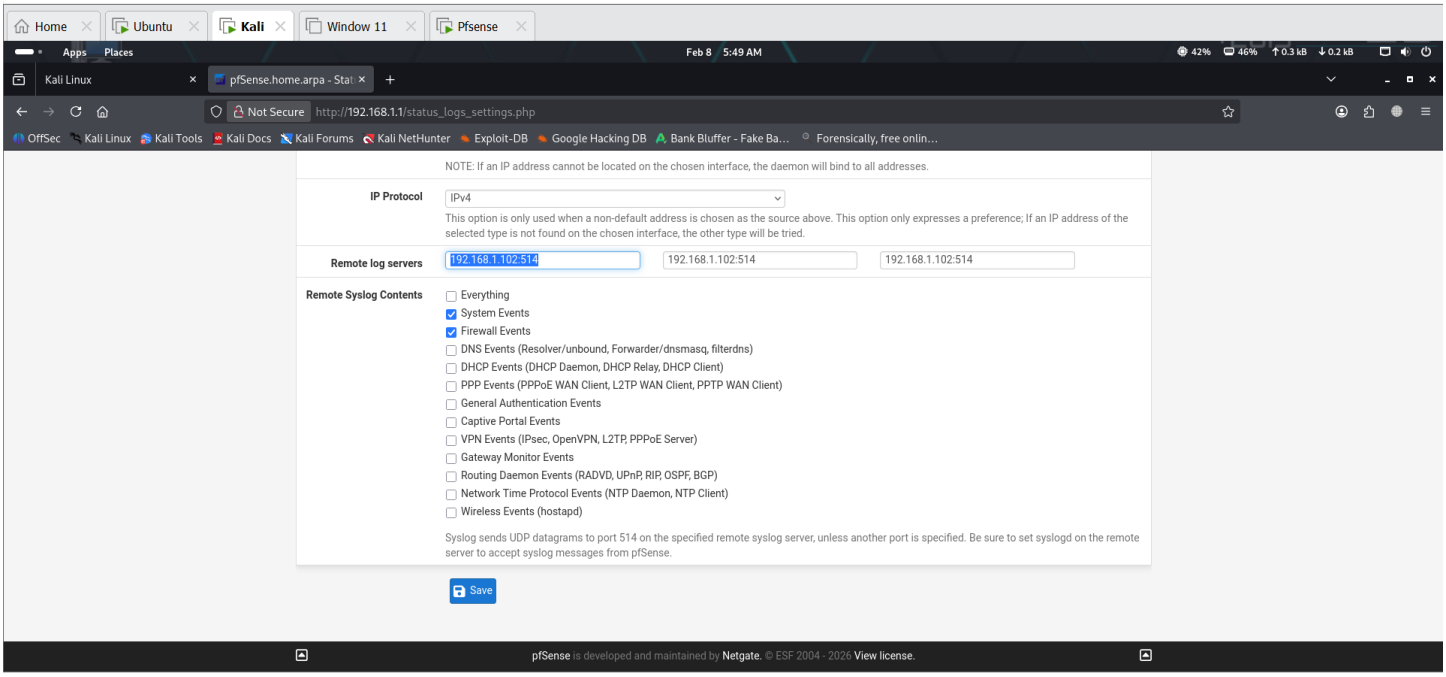
Configure pfsense with wazuh manager.

Login pfsense:

Status > Settings

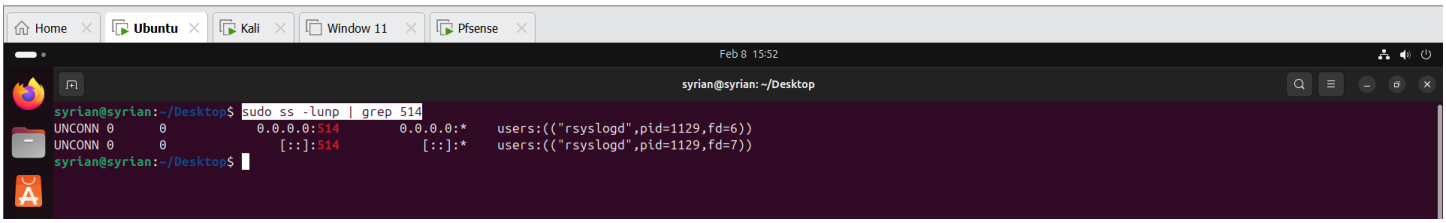



Set wazuh manager ip address.

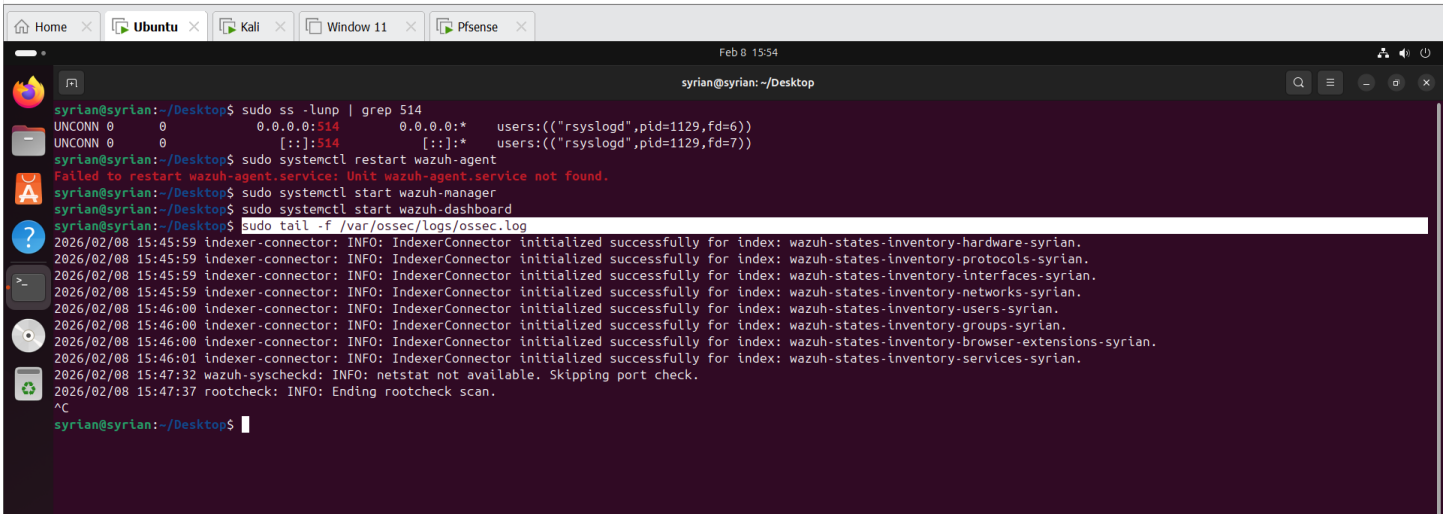



After assign wazuh server ip and then save. Now I check configuration confirmation in wazuh manager in Ubuntu.

Command: sudo ss -lunp | grep 514




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




# Step 3 (A):

## Configure and create rules:

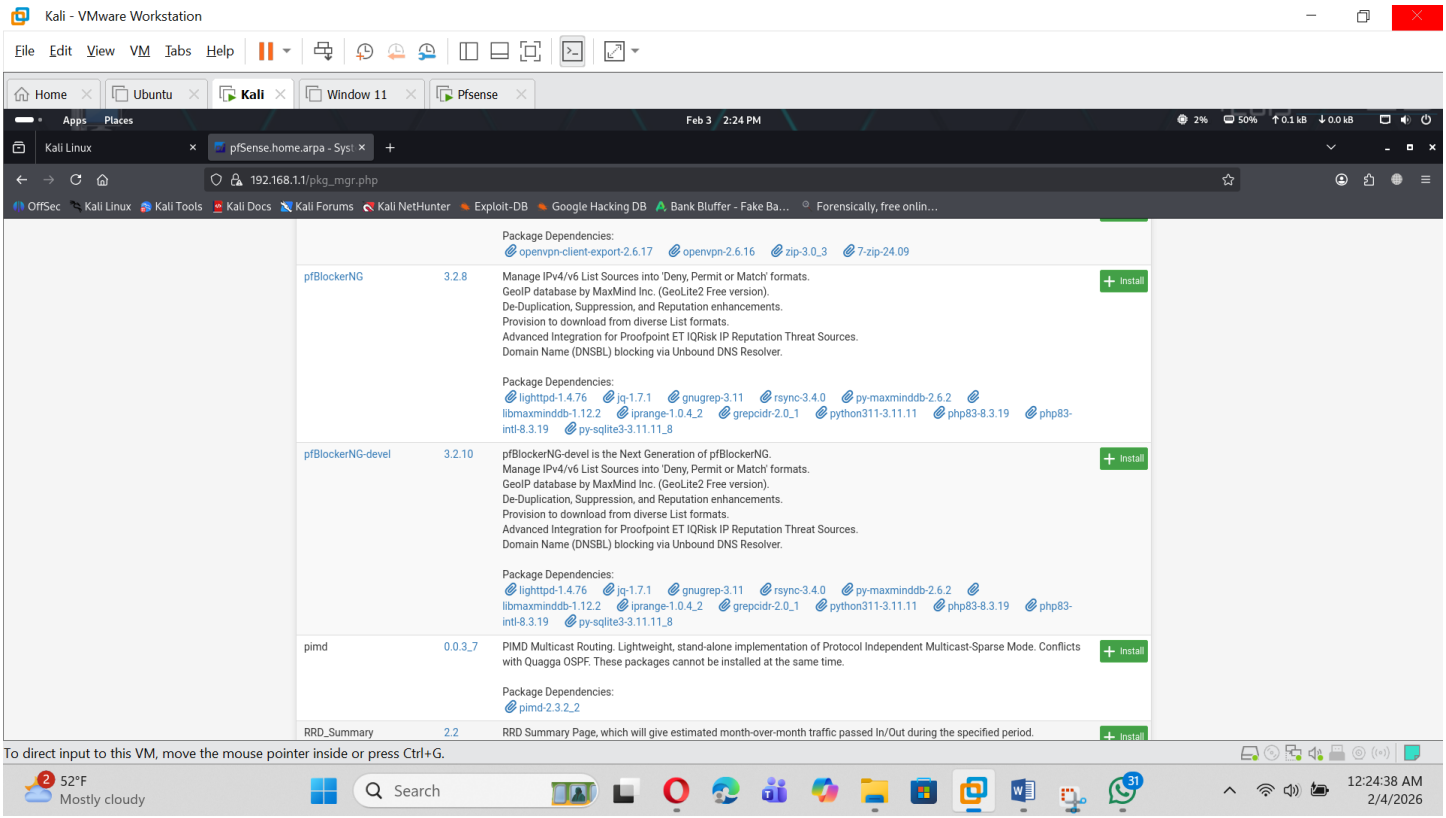
**Goal:** Block traffic from countries like China, Russia.

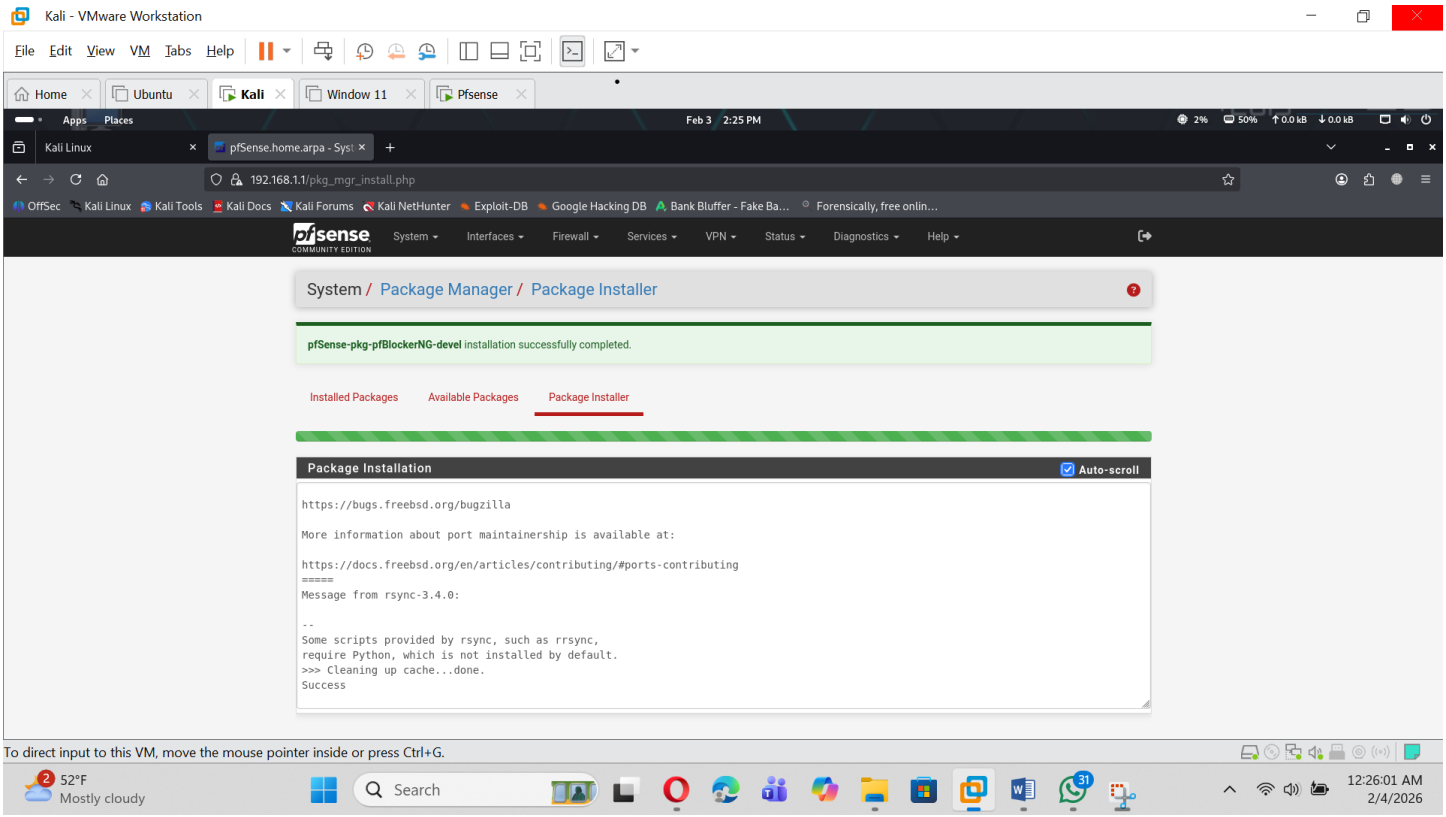
### Step 1: Install pfBlockerNG

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

System → Package Manager → Available Packages

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

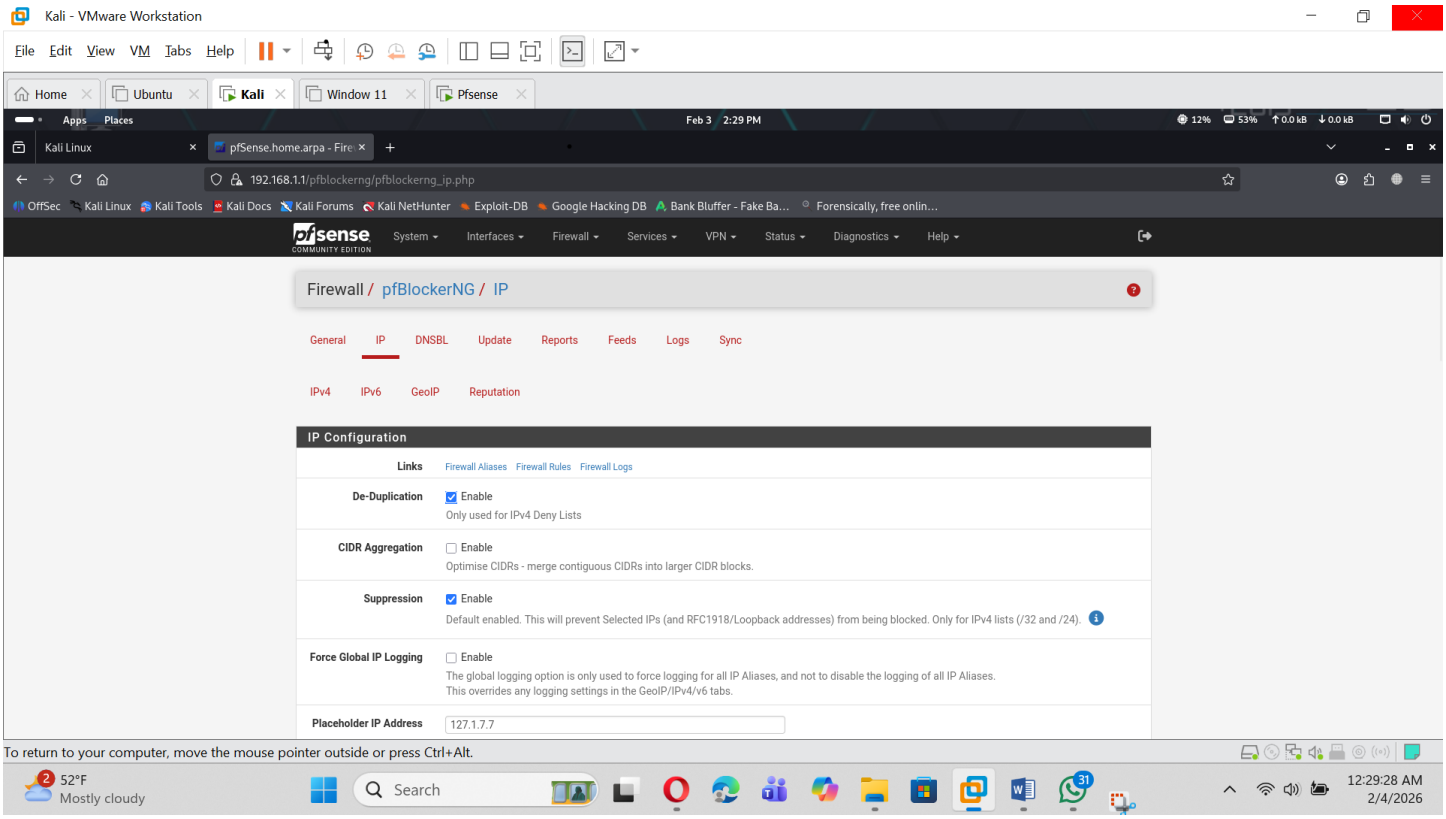


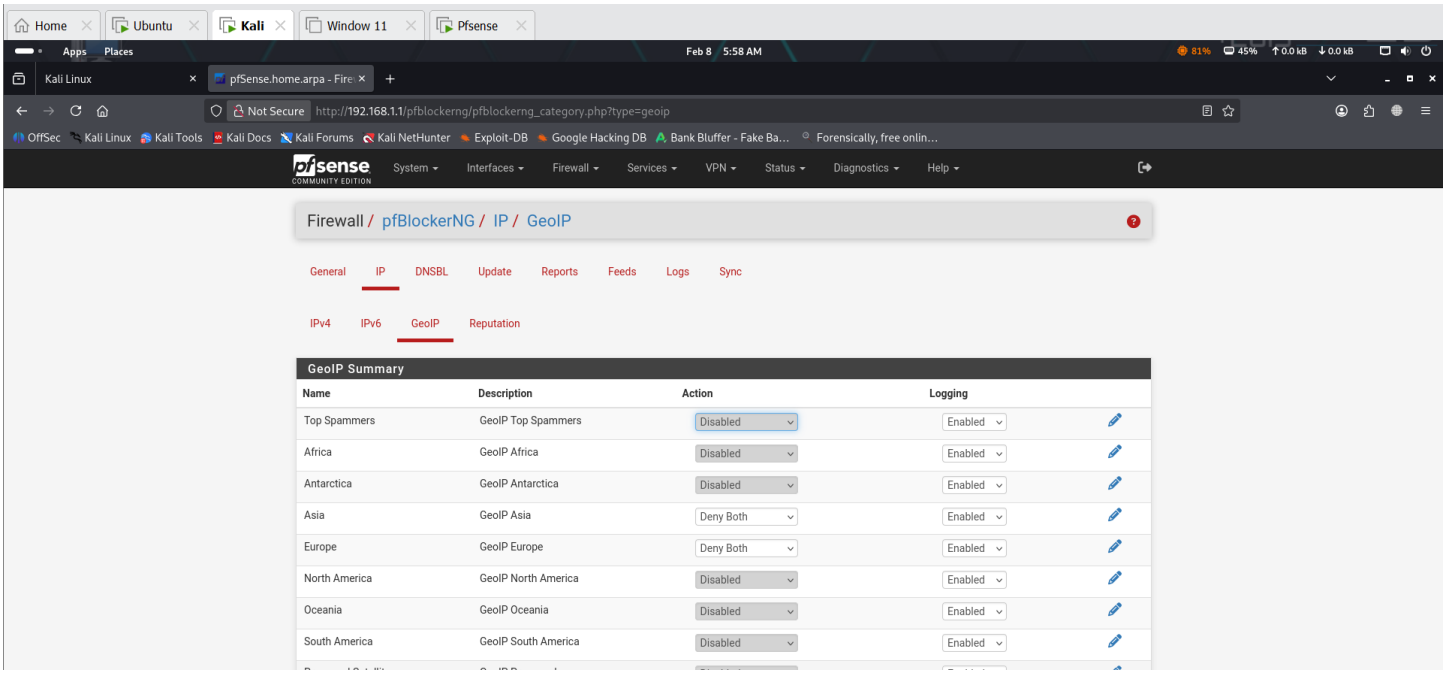




# Step 2: Enable GeoIP

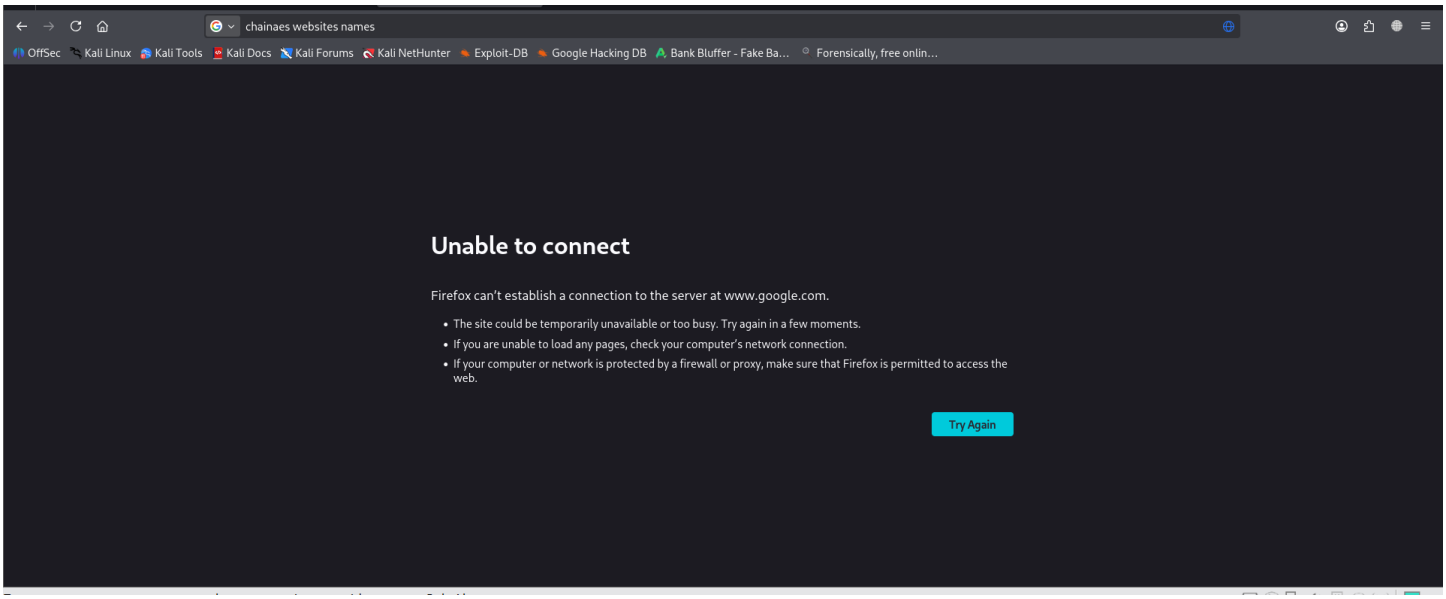
1. Go to:

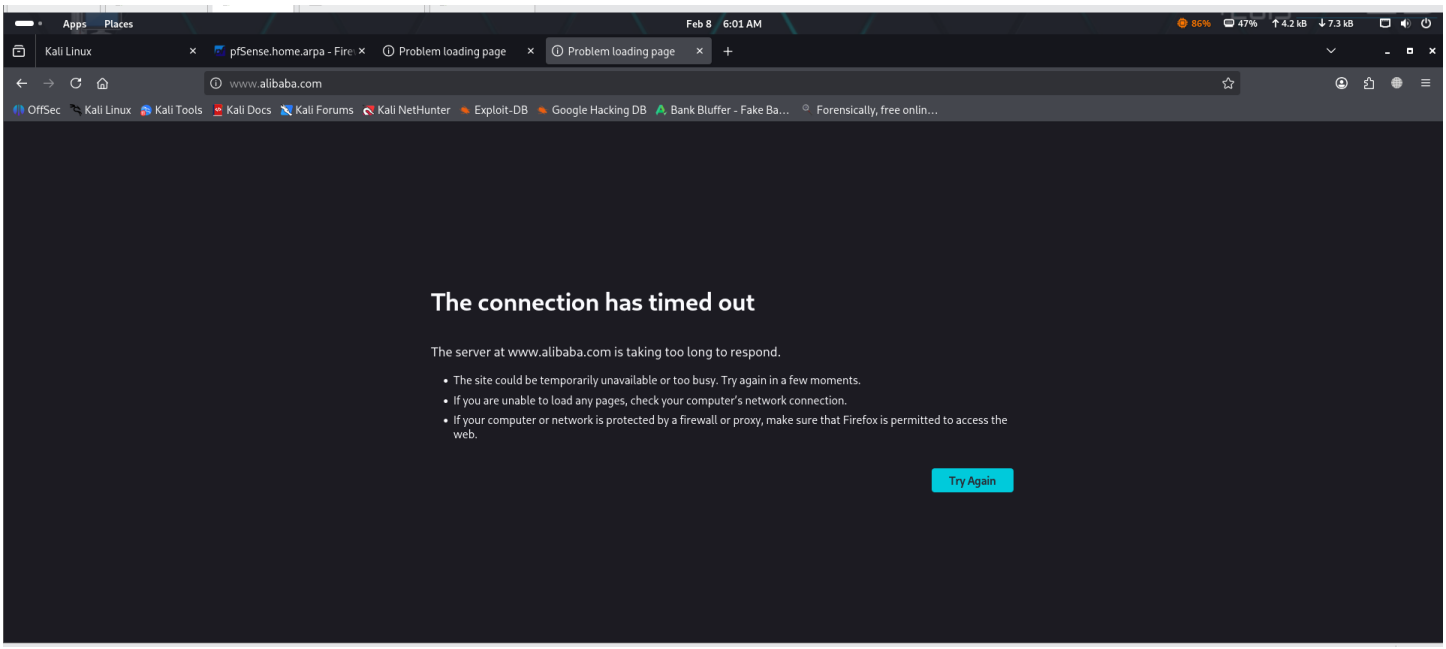
# Firewall → pfBlockerNG → IP



Now I check those countries traffic.



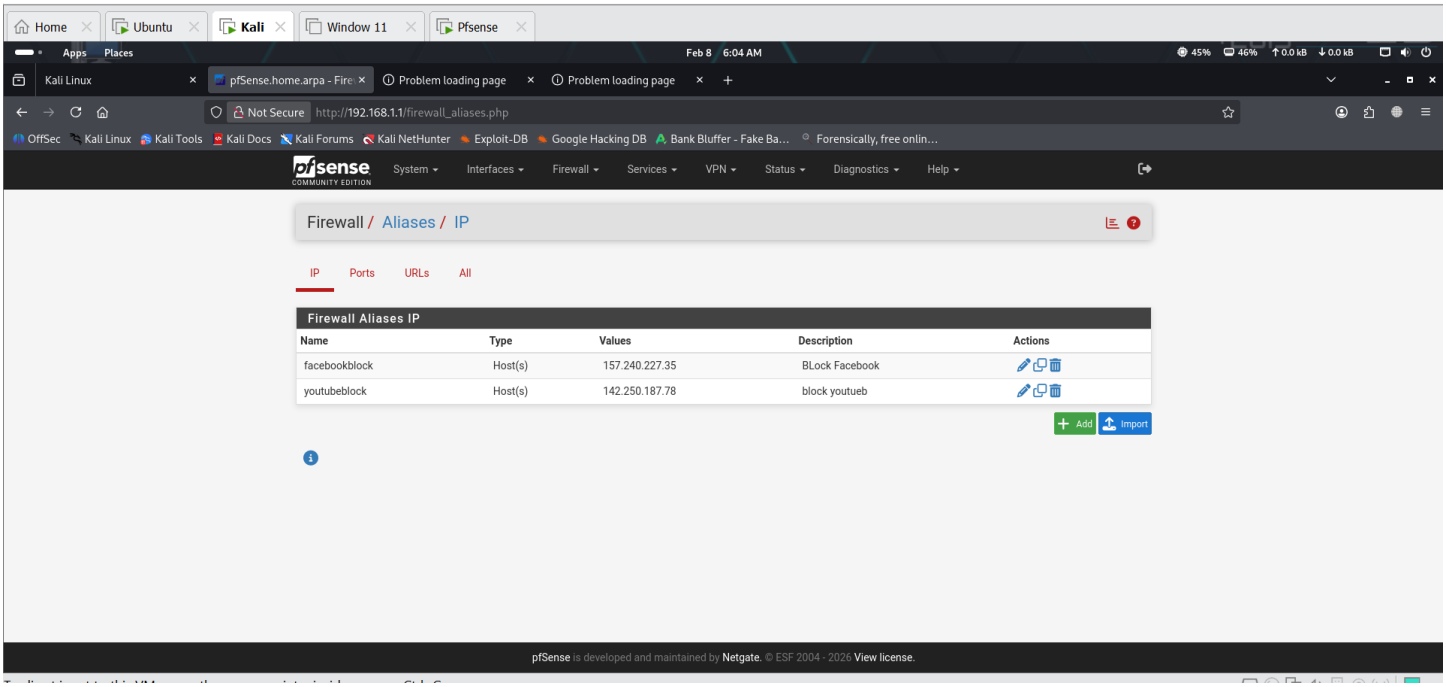




Step 4 (B):

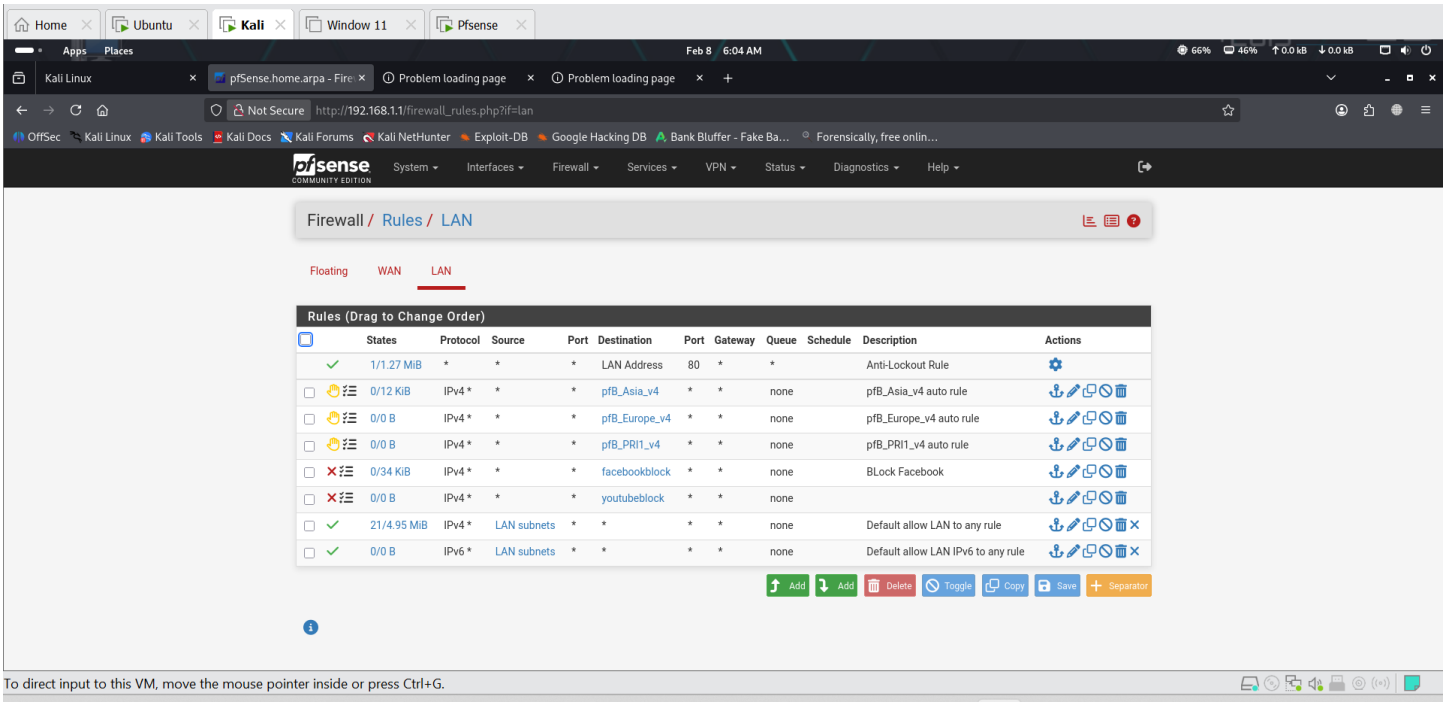
Specific websites block.

Go:

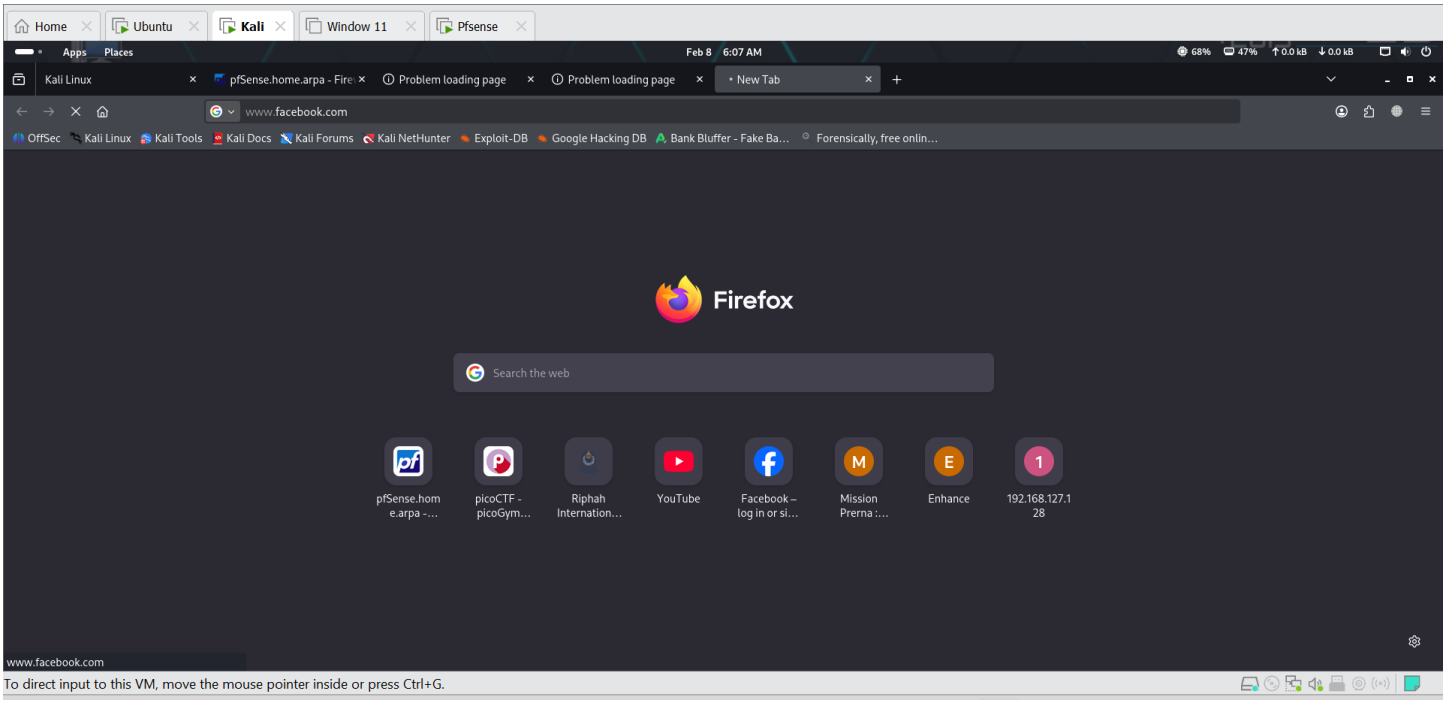
Firewall > Aliases and add websites.




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

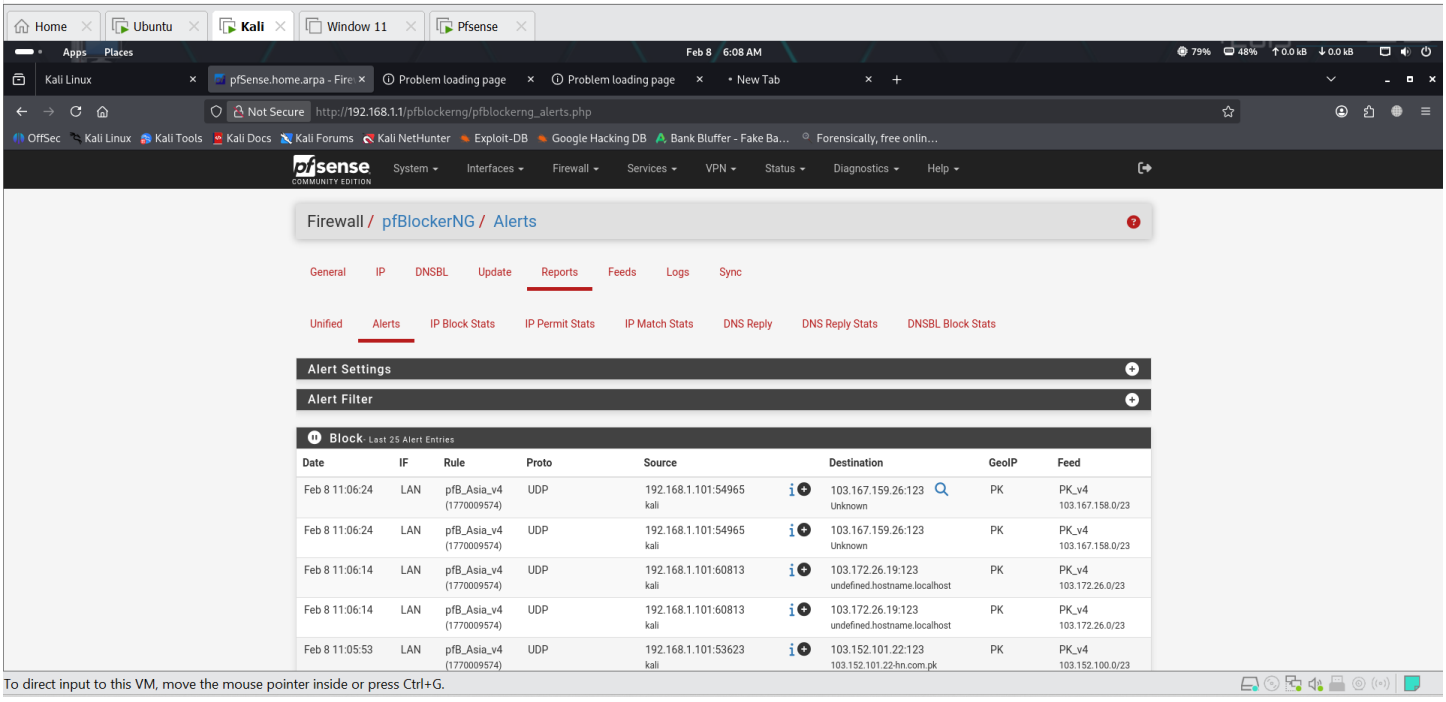


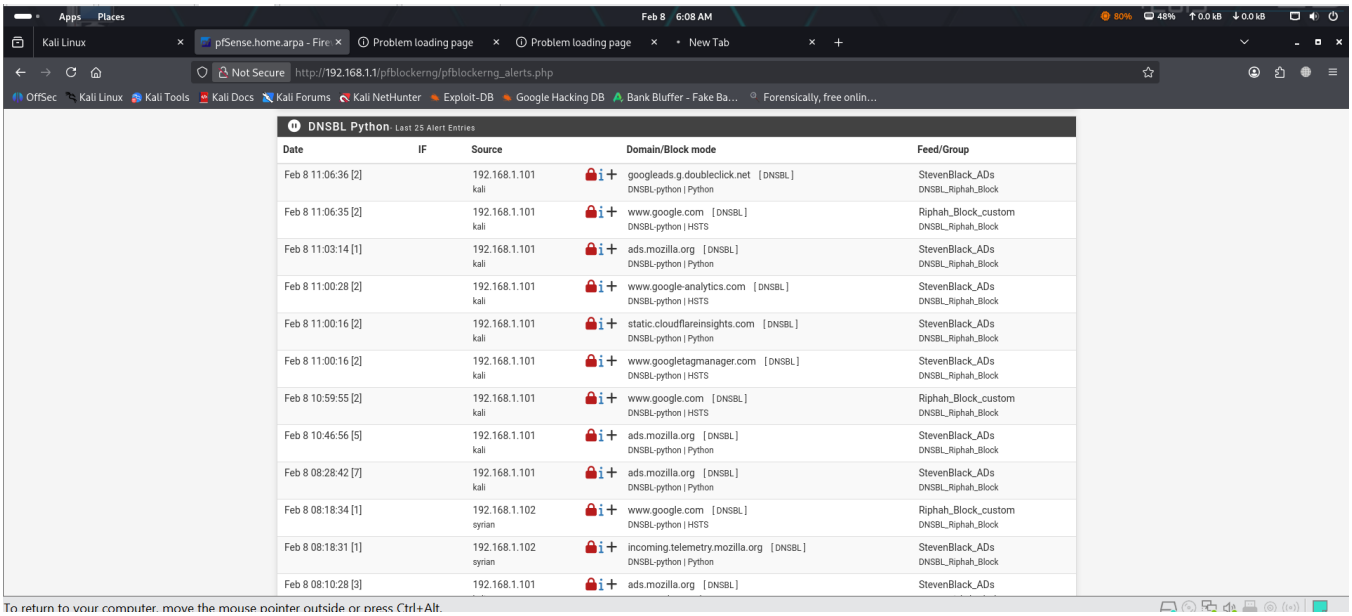

Now I checked.

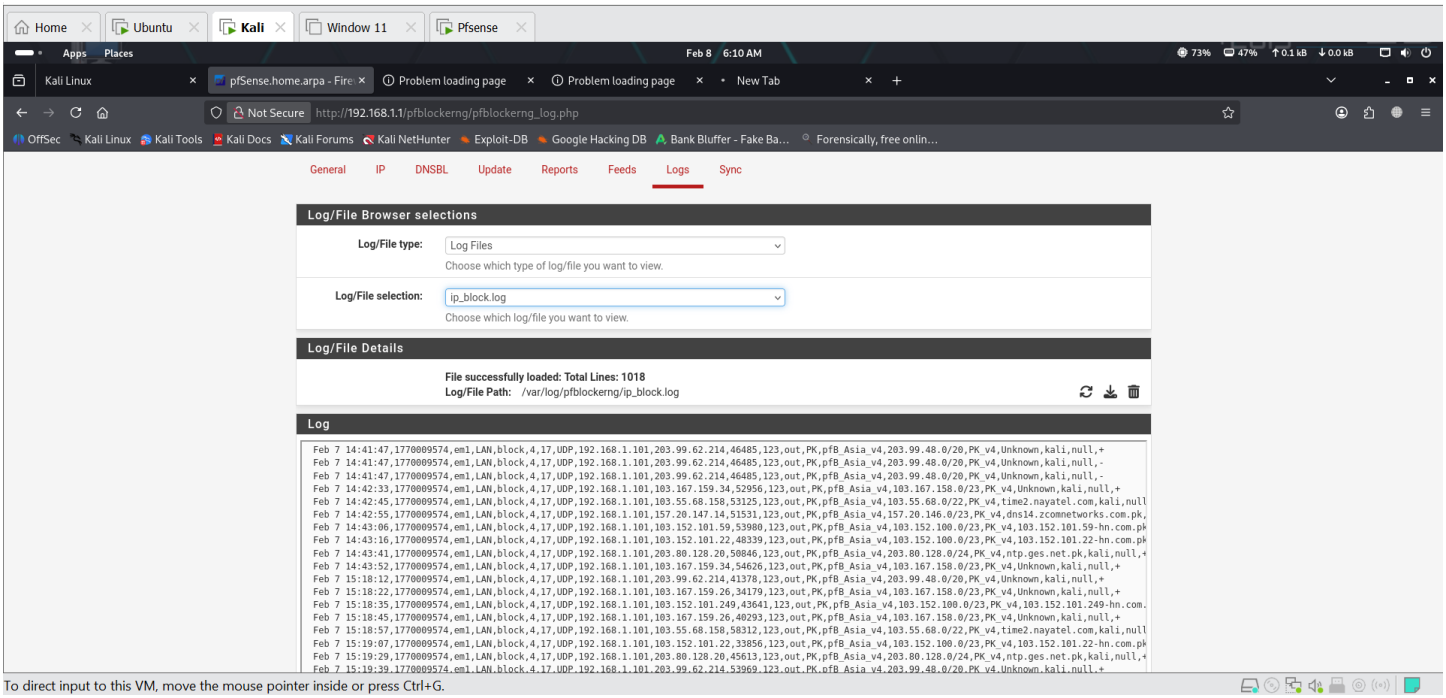



So not loading facebook page.

Alerts.




Apps Places
Feb 8 6:08 AM
Kali Linux
pfSense.home.arpa - Fire
Problem loading page
Problem loading page
New Tab
Not Secure
http://192.168.1.1/pfblockerng/pfblockerng_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 IF 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_Riphah_Block
Feb 8 11:06:35 [2] 192.168.1.101 kali www.google.com [DNSBL] DNSBL-python | HSTS Riphah_Block_custom DNSBL_Riphah_Block
Feb 8 11:03:14 [1] 192.168.1.101 kali ads.mozilla.org [DNSBL] DNSBL-python | Python StevenBlack_ADs DNSBL_Riphah_Block
Feb 8 11:00:28 [2] 192.168.1.101 kali www.google-analytics.com [DNSBL] DNSBL-python | HSTS StevenBlack_ADs DNSBL_Riphah_Block
Feb 8 11:00:16 [2] 192.168.1.101 kali static.cloudflareinsights.com [DNSBL] DNSBL-python | Python StevenBlack_ADs DNSBL_Riphah_Block
Feb 8 11:00:16 [2] 192.168.1.101 kali www.googletagmanager.com [DNSBL] DNSBL-python | HSTS StevenBlack_ADs DNSBL_Riphah_Block
Feb 8 10:59:55 [2] 192.168.1.101 kali www.google.com [DNSBL] DNSBL-python | HSTS Riphah_Block_custom DNSBL_Riphah_Block
Feb 8 10:46:56 [5] 192.168.1.101 kali ads.mozilla.org [DNSBL] DNSBL-python | Python StevenBlack_ADs DNSBL_Riphah_Block
Feb 8 08:28:42 [7] 192.168.1.101 kali ads.mozilla.org [DNSBL] DNSBL-python | Python StevenBlack_ADs DNSBL_Riphah_Block
Feb 8 08:18:34 [1] 192.168.1.102 syrian www.google.com [DNSBL] DNSBL-python | HSTS Riphah_Block_custom DNSBL_Riphah_Block
Feb 8 08:18:31 [1] 192.168.1.102 syrian incoming.telemetry.mozilla.org [DNSBL] DNSBL-python | Python StevenBlack_ADs DNSBL_Riphah_Block
Feb 8 08:10:28 [3] 192.168.1.101 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
Apps Places
Feb 8 6:10 AM
Kali Linux
pfSense.home.arpa - Fire
Problem loading page
Problem loading page
New Tab
Not Secure
http://192.168.1.1/pfblockerng/pfblockerng_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/pfblockerng/ip_block.log
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.zcomnetworks.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,+
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

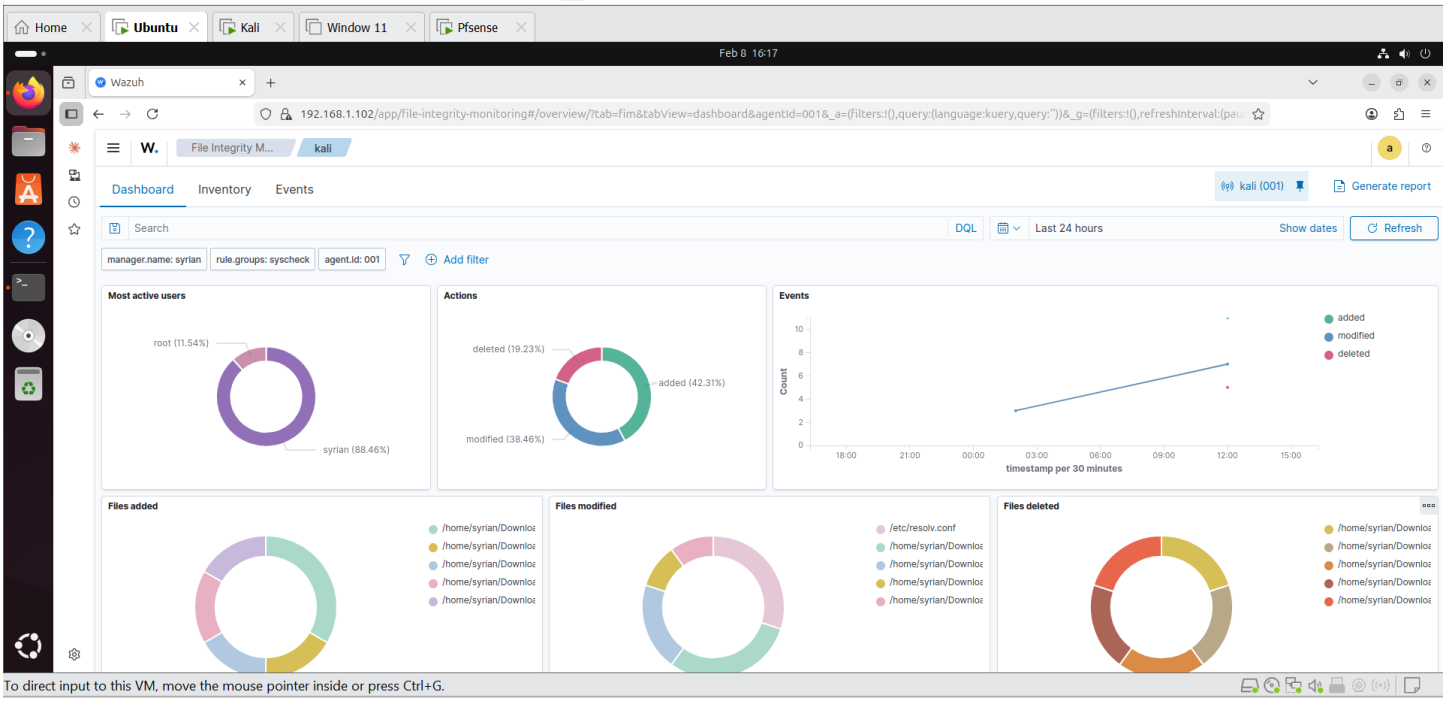
Log

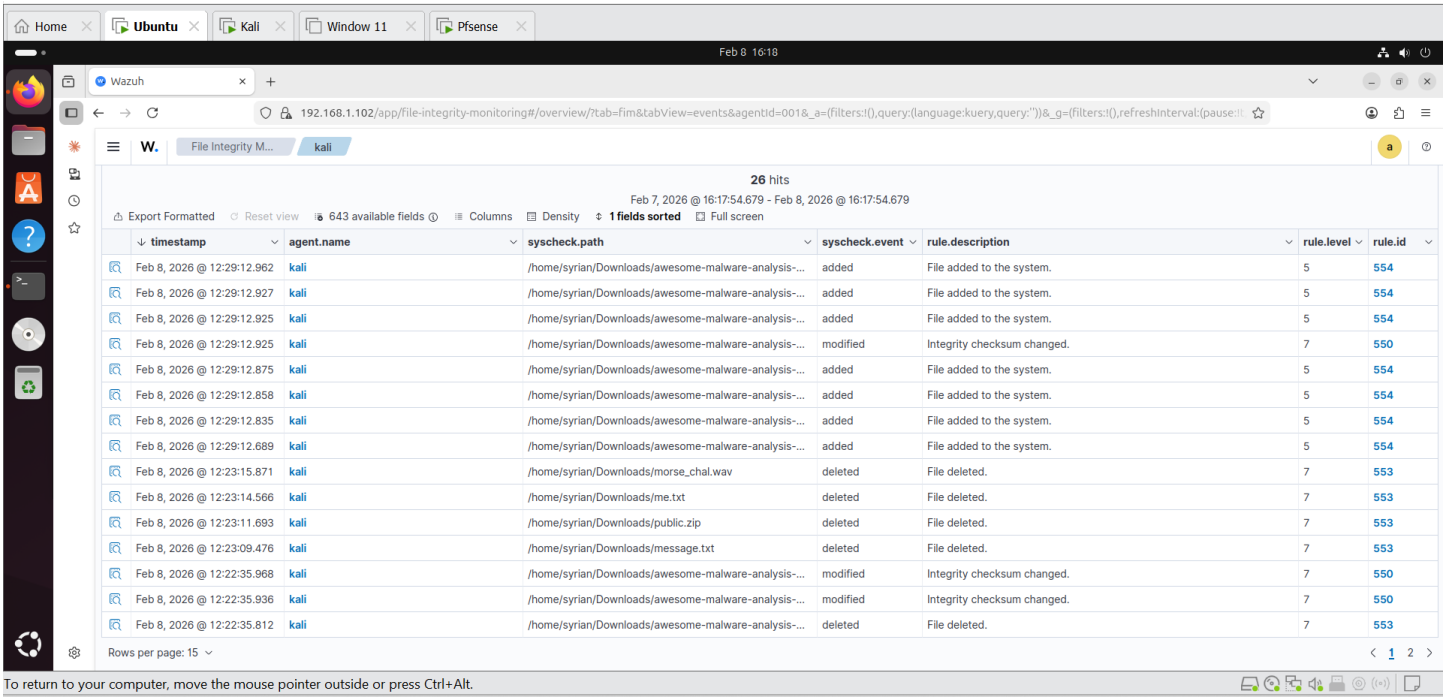
```
Feb 7 14:41:47,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,+
Feb 7 14:41:47,1770009574,em1,LAN,block,4,17,UDP,192.168.1.101,203.99.62.214,46485,123,out,PK,pfB_Asia_v4,203.99.48.0/20,PK_v4,Unknown,kali,null,-
Feb 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.zcomnetworks.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,+
```

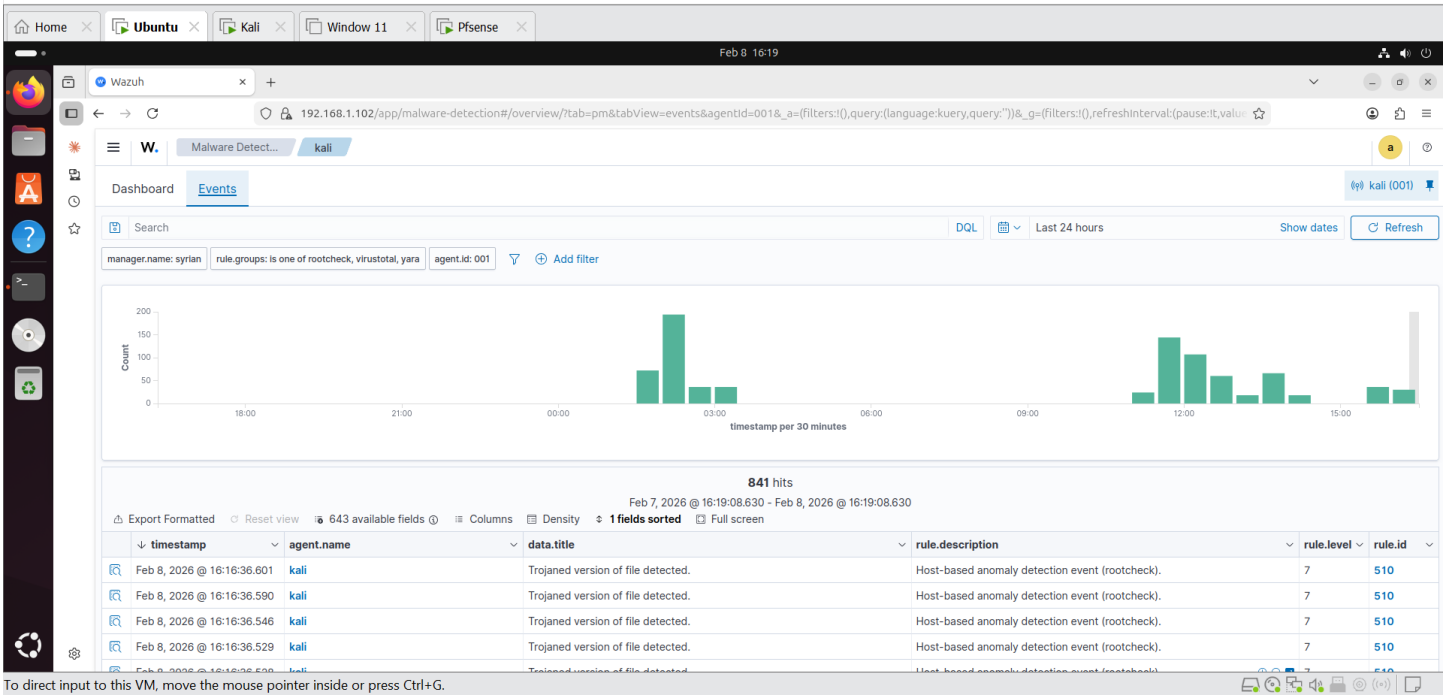
# Step 4:

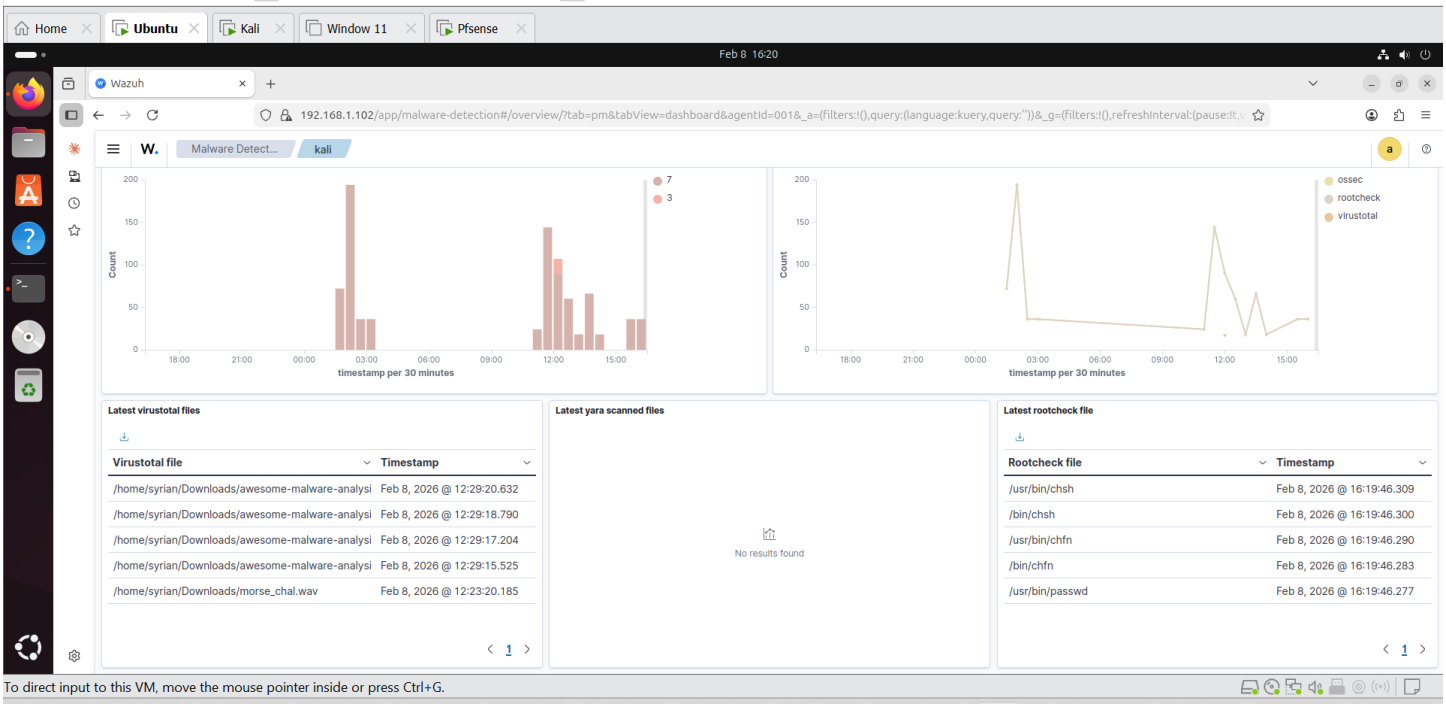
Monitor logs through wazuh

Login wazuh manger




Home
Ubuntu
Kali
Window 11
Pfsense
Feb 8 16:18
Wazuh
192.168.1.102/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t
File Integrity M...
kali
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 @ 12:29:12.689 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 @ 12:22:35.968 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.


Home
Ubuntu
Kali
Window 11
Pfsense
Feb 8 16:19
Wazuh
192.168.1.102/app/malware-detection#/overview/?tab=pm&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:!t,valu
Malware Detect...
kali
Dashboard
Events
kali (001)
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: syrian
rule.groups: is one of rootcheck, virustotal, yara
agent.id: 001
Add filter
Count
200
150
100
50
0
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
timestamp per 30 minutes
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
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.