ITSOLERA PVT LTD

INTERNSHIP TASKS BOOKLET

PRESENTED BY :
MUHAMMAD JARRAR HASSAN

TEAM SIGMA

Table of Contents:

Task 3: pfSense + Malware Detection + Wazuh Incident Response

Task 4: Malware Breach Report (Research & Analysis)

TASK#1 : Wazuh with FIM

Wazuh:

Wazuh is an open-source security monitoring platform designed to help organizations detect, respond to, and prevent cybersecurity threats. It provides a comprehensive solution for **threat detection**, **compliance monitoring**, and **incident response** across various operating systems including **Windows, Linux, and macOS**.

Wazuh works by collecting and analyzing data from monitored endpoints (such as servers, desktops, or cloud environments) through installed **agents**. This data is then processed by the **Wazuh Manager**, which identifies suspicious behavior or security policy violations. The results are presented in a user-friendly **web dashboard**, allowing security teams to take appropriate action.

Key Features of Wazuh:

Feature	Description
Intrusion Detection	Monitors systems to detect unauthorized or malicious activity.
Log Analysis	Collects and analyzes logs to identify threats or system issues.
File Integrity Monitoring (FIM)	Detects changes to critical files and directories.
Vulnerability Detection	Identifies weaknesses in systems that could be exploited.
Compliance Reporting	Helps meet regulatory standards like GDPR, HIPAA, and PCI-DSS.
Incident Response	Provides alerts and tools for quick investigation and response.

What is File Intergrity Monitoring(FIM):

File Integrity Monitoring (FIM) is a security process that checks and monitors files and directories on a system to detect any unauthorized or unexpected changes. It works by creating a **baseline** (original state) of critical files and then continuously **scanning for changes** such as:

- File modifications
- New file creations
- Deletions
- Changes in permissions or ownership

FIM tools (like Wazuh) generate alerts whenever such changes occur, helping system administrators detect potential threats or policy violations in real-time.

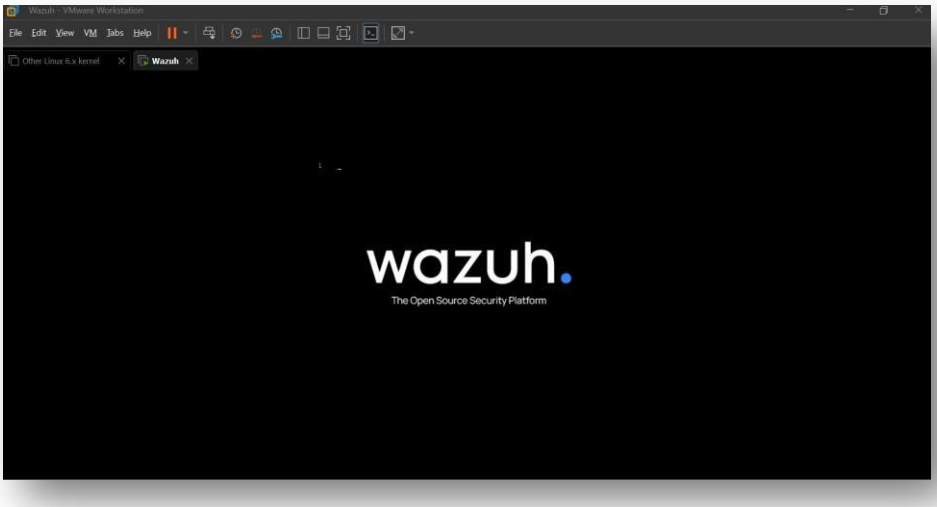
Setting File Integrity Monitoring(FIM) in Wazuh:

Step#1:Installing wazuh OVA File:

The first step involved downloading the **Wazuh OVA (Open Virtual Appliance)** file from the official Wazuh website. This pre-configured image simplifies the deployment process by bundling Wazuh components into a ready-to-use virtual machine.

Once the download was complete, the OVA file was **imported into VMware**. During the import process, system resources were allocated based on the official Wazuh documentation:

- **RAM:** 4 GB
- **Disk Storage:** 50 GB
- **CPU Cores:** 4



After successfully starting the Wazuh virtual machine, I accessed the Wazuh web interface and logged in using the **default credentials** provided by the official documentation:

- **Username:** `wazuh-user`
- **Password:** `wazuh`

Accessing the Wazuh Web Interface

After logging into the Wazuh virtual machine, I opened the terminal and executed the following command to retrieve the system's IP address:

ip a

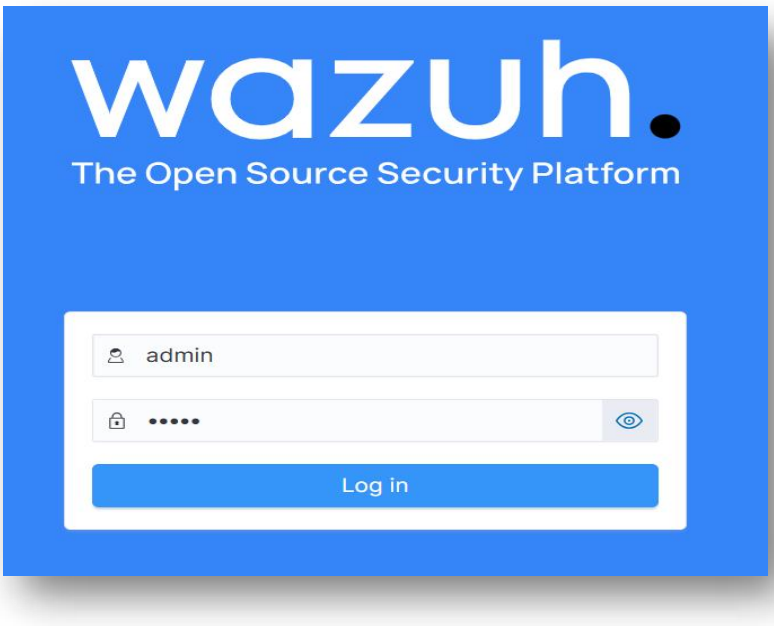
This command displayed the network interfaces and their assigned IP addresses. From the output, I identified the IP address assigned to the Wazuh VM.

Using this IP address, I accessed the **Wazuh web interface** through a web browser by entering the following URL:

https://192.168.1.20

Upon navigating to the URL, the Wazuh dashboard login page was displayed, allowing me to log in using the default credentials and begin the configuration and monitoring process.

Note: Since the connection uses HTTPS and is self-signed, the browser may show a security warning. I proceeded by choosing the "Advanced" option and continued to the site.



The default login credentials are:

- **Username:** admin
- **Password:** admin

Step#2:Installing wazuh agent on Windows:

To monitor a Windows system using Wazuh, I installed the **Wazuh agent** on the target machine. The agent is responsible for collecting logs, monitoring file changes, and sending security-related data to the Wazuh Manager.

I followed the official Wazuh documentation for Windows agent installation, available at:

https://documentation.wazuh.com/current/installation-guide/installing-wazuh-agent/win-agent.html

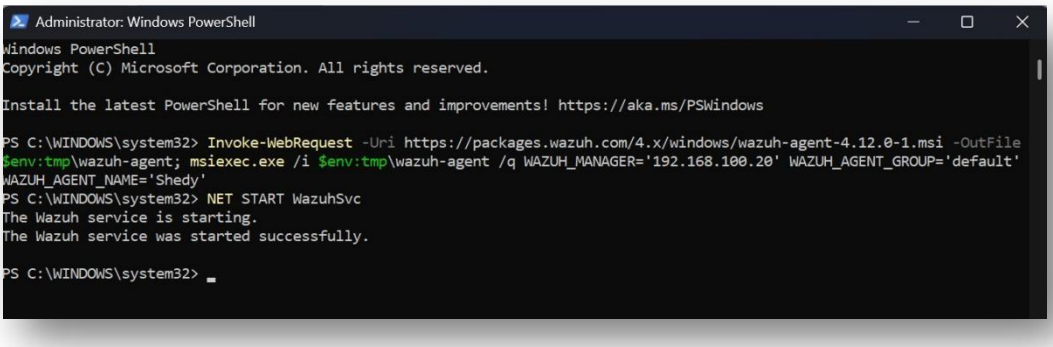
Installation Steps:

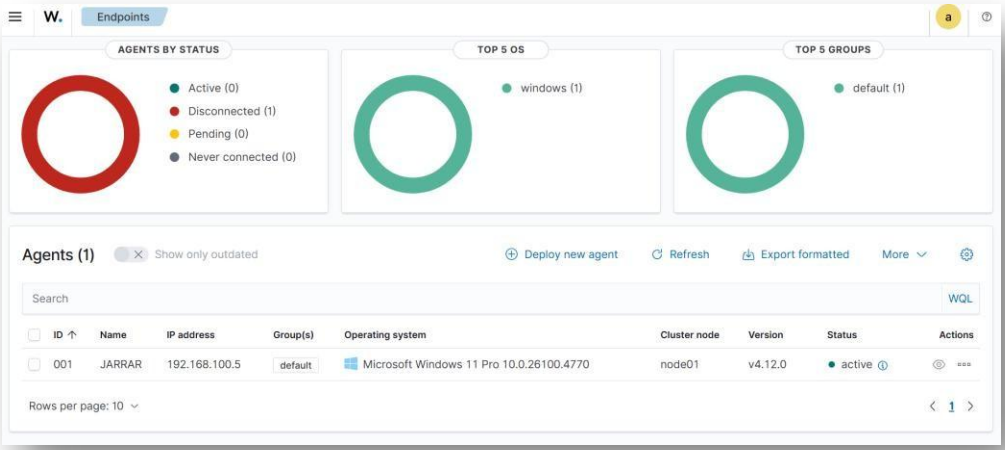
1. **Downloaded the Wazuh Agent** .msi installer from the official website.
2. Launched the installer and followed the step-by-step wizard.
3. During installation, I entered the following configuration:
    - **Wazuh Manager IP Address:** <Wazuh-Server-IP>
    - **Agent Name:** JARRAR
    - **Connection Type:** Direct registration (or via agent-auth, based on environment)
4. Completed the installation and ensured the **Wazuh Agent service** was running.

Post-Installation Verification:

- Opened **Wazuh Agent Manager** from the Start Menu.
- Verified that the agent named **JARRAR** was active and connected to the Wazuh Manager.
- Logged into the Wazuh web dashboard and confirmed that the agent JARRAR appeared in the list of connected agents.

This setup enabled real-time monitoring of the Windows endpoint under the unique agent identifier **JARRAR**.





Step#3:Configuring File Integrity Monitoring(FIM):

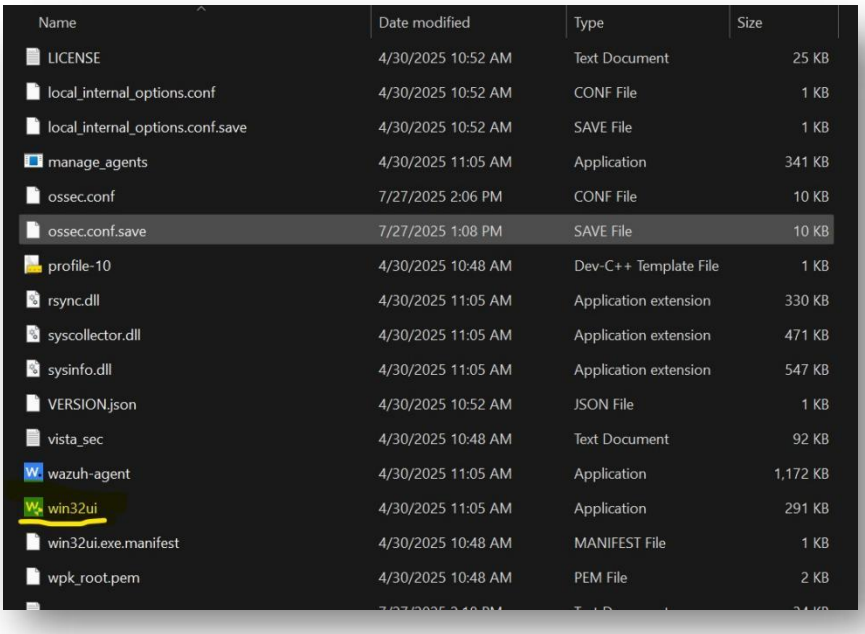
After successfully installing the Wazuh agent on the Windows machine (**Agent Name: JARRAR**), I proceeded to configure **File Integrity Monitoring (FIM)**. This feature allows Wazuh to monitor specified files and directories for any changes, additions, or deletions — helping detect unauthorized or suspicious activity on critical system files.

I followed the official Wazuh documentation for FIM configuration:
https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/index.html

Steps to Configure FIM:

1. **Edited the Wazuh Agent configuration file** on the Windows machine:
   Path:

   C:\Program Files (x86)\ossec-agent\ossec.conf



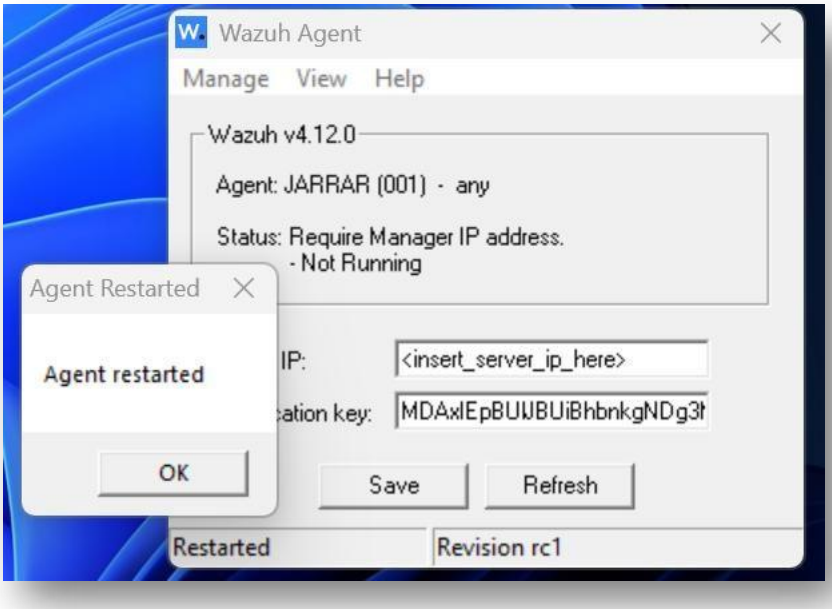
Name	Date modified	Type	Size
LICENSE	4/30/2025 10:52 AM	Text Document	25 KB
local_internal_options.conf	4/30/2025 10:52 AM	CONF File	1 KB
local_internal_options.conf.save	4/30/2025 10:52 AM	SAVE File	1 KB
manage_agents	4/30/2025 11:05 AM	Application	341 KB
ossec.conf	7/27/2025 2:06 PM	CONF File	10 KB
ossec.conf.save	7/27/2025 1:08 PM	SAVE File	10 KB
profile-10	4/30/2025 10:48 AM	Dev-C++ Template File	1 KB
rsync.dll	4/30/2025 11:05 AM	Application extension	330 KB
syscollector.dll	4/30/2025 11:05 AM	Application extension	471 KB
sysinfo.dll	4/30/2025 11:05 AM	Application extension	547 KB
VERSION.json	4/30/2025 10:52 AM	JSON File	1 KB
vista_sec	4/30/2025 10:48 AM	Text Document	92 KB
wazuh-agent	4/30/2025 11:05 AM	Application	1,172 KB
win32ui	4/30/2025 11:05 AM	Application	291 KB
win32ui.exe.manifest	4/30/2025 10:48 AM	MANIFEST File	1 KB
wpk_root.pem	4/30/2025 10:48 AM	PEM File	2 KB

2. **Added the FIM monitoring rules** inside the <ossec_config> block:

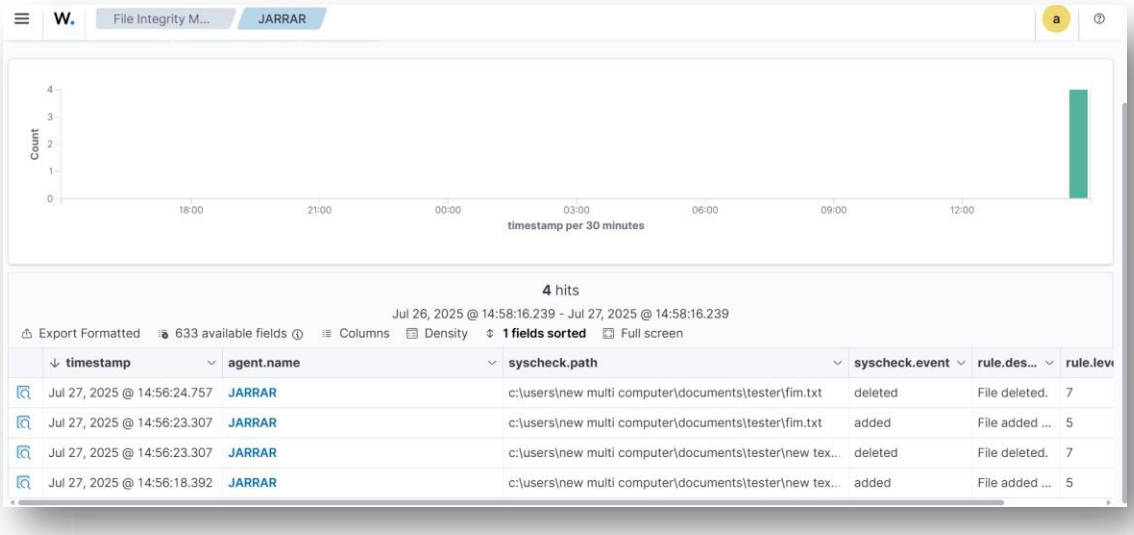
```
<syscheck>
  <directories check_all="yes" realtime="yes">C:\Users\JARRAR\Documents</directories>
  <directories check_all="yes" realtime="yes">C:\ImportantFiles</directories>
  <frequency>43200</frequency> <!-- Scans every 12 hours -->
</syscheck>
```

```
  <!-- File integrity monitoring -->
  <syscheck>

    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <!-- Default files to be monitored. -->
    <directories check_all = "yes"  realtime="yes">C:\Users\Documents</directories>
    <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe
$|reg.exe$|regedt32.exe|regsvr32.exe|runas.exe|sc.exe|schtasks.exe|sethc.exe|subst.exe$">%WINDIR%\SysNative</directories>
    <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

    <!-- 32-bit programs. -->
    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|net1.exe$|netsh.exe
$|reg.exe$|regedit.exe$|regedt32.exe$|regsvr32.exe$|runas.exe$|sc.exe$|schtasks.exe$|sethc.exe$|subst.exe$">%WINDIR%\System32</directories>
    <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

    <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
```

3. **Restarted the Wazuh agent service** to apply changes:



4. **Verified in the Wazuh Dashboard** that FIM was active and began detecting file changes (modification, addition, deletion) in the specified directories.



- In this dashboard we can see that I created a file and deleted it

Conclusion:

The deployment and configuration of the Wazuh security monitoring platform were successfully completed, providing a powerful and centralized solution for real-time threat detection and system monitoring. The installation of the Wazuh OVA in a virtualized environment, followed by agent installation on a Windows system named **JARRAR**, enabled a seamless flow of security data to the Wazuh Manager.

Through the implementation of **File Integrity Monitoring (FIM)**, critical directories were placed under active surveillance, ensuring that any unauthorized file modifications, additions, or deletions were promptly detected and reported. This significantly enhances the system's ability to detect potential security breaches and maintain compliance with cybersecurity standards.

Wazuh's open-source nature, ease of integration, and rich feature set make it a highly effective tool for both learning and enterprise-grade security operations. The insights gained from this setup can serve as a foundational step toward building a more robust and proactive cybersecurity infrastructure.

TASK#2 : Pfsense Firewall and Geoip/Website Blocking

Objectives:

1. **Implement pfSense.**

2. **Configure and create rule on firewall and test it with home lab**
   - BLOCK specific countries (example china Russia etc.) traffic
   - Create rules which restrict the user from specified websites
   - Administrator privileges rule

3. **Monitor the logs.**

Tools:

- **PfSense** – Open-source firewall and router software for network security, rule creation, and traffic filtering.
- **Wazuh** – Security Information and Event Management (SIEM) platform for log collection, intrusion detection, and real-time monitoring.
- **Oracle VirtualBox** – Virtualization software to host PfSense and Wazuh instances in a controlled lab environment.
- **Web Browser (e.g., Chrome/Firefox)** – For accessing PfSense web interface and Wazuh dashboard.

Setting pfSense Firewall:

1. Downloading PfSense

- Visit the official PfSense website: https://www.pfsense.org/download/.

Choose the following options:

Architecture: AMD64 (64-bit)

Installer: ISO Installer

- Download the **.iso** file.

2. Creating the Virtual Machine in VirtualBox

- Open **Oracle VirtualBox** → Click **New**.
- Name the VM (e.g., *PfSense Firewall*).
- Type: **BSD** → Version: **FreeBSD (64-bit)**.

Allocate **2 GB RAM** (or more).

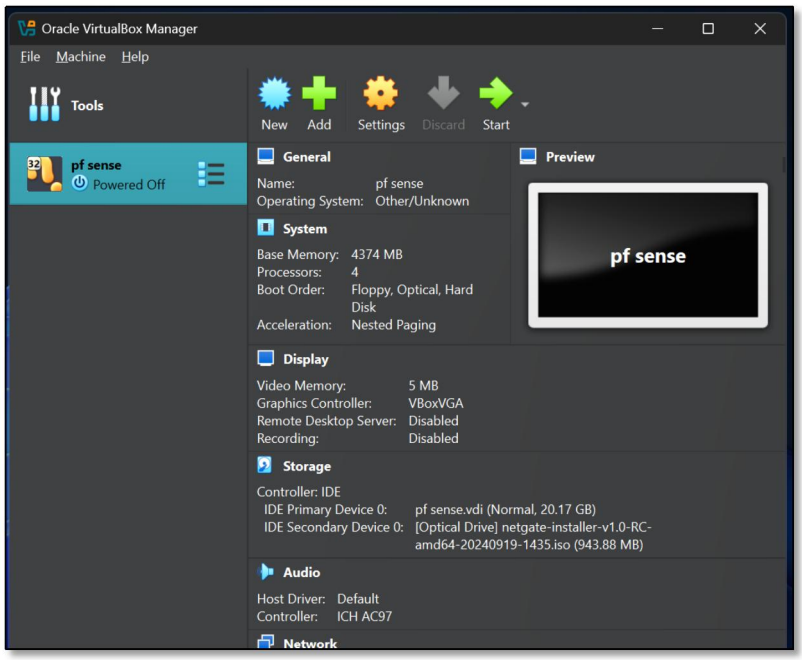
Assign **2 CPUs** (recommended for better performance).

Create a **Virtual Hard Disk** (10 GB minimum).

- Attach the **PfSense ISO**:

Go to **Settings** → **Storage**.

Under Controller IDE/SATA, choose **Add Optical Drive** and select the downloaded ISO.



3. Configuring Network Interfaces

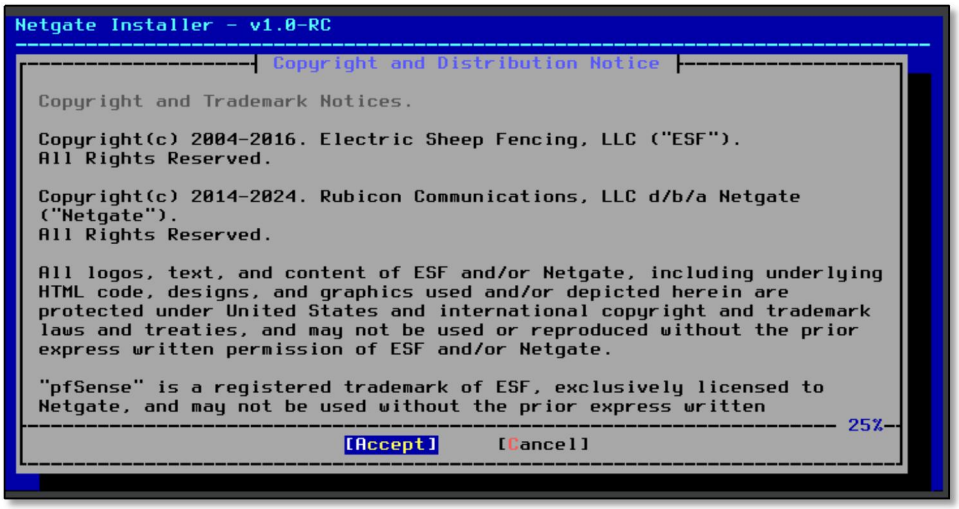
- In **VM Settings → Network**:

  Adapter 1: Set to *Bridged Adapter* (WAN connection).

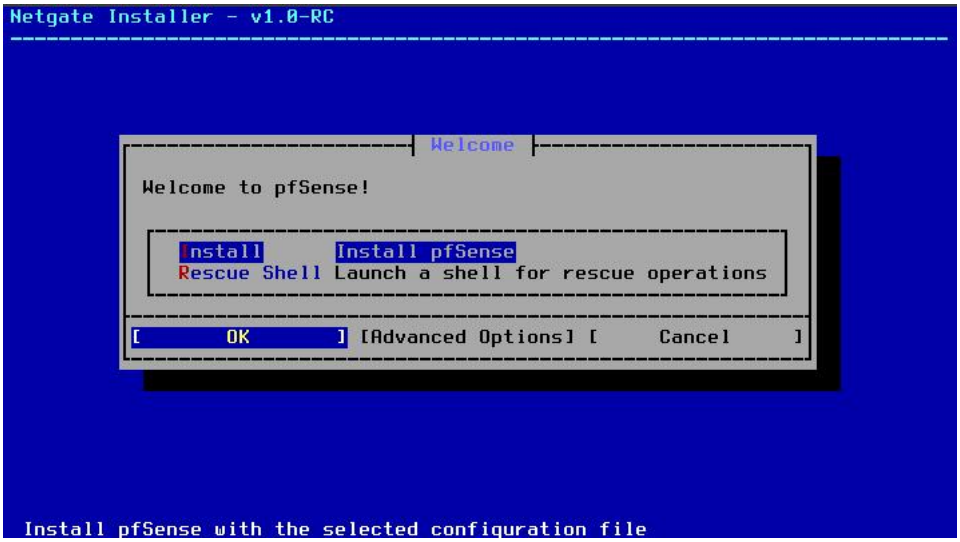
  Adapter 2: Set to *Internal Network* or *Host-only Adapter* (LAN connection).

4. Installing PfSense

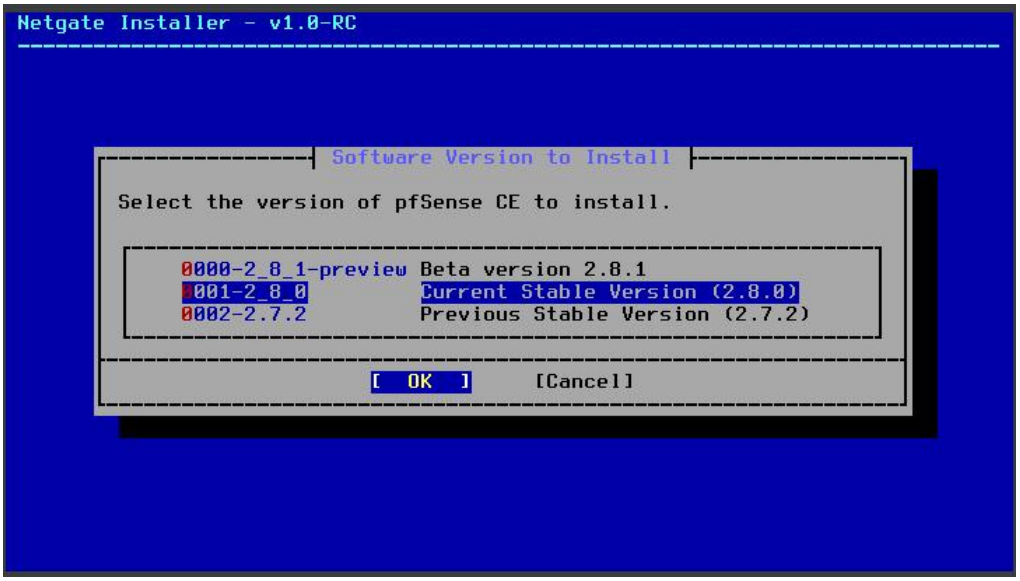
- Start the VM → The ISO will boot into the installer.



- Choose Install from the menu.



- Select the current stable version



- Installation will complete → Remove ISO from virtual drive → Reboot.

5. Assigning Interfaces

- After reboot, PfSense will ask to assign interfaces:

  WAN → Adapter 1.

  LAN → Adapter 2.

- The system will display assigned IP addresses — note down the **LAN IP**.

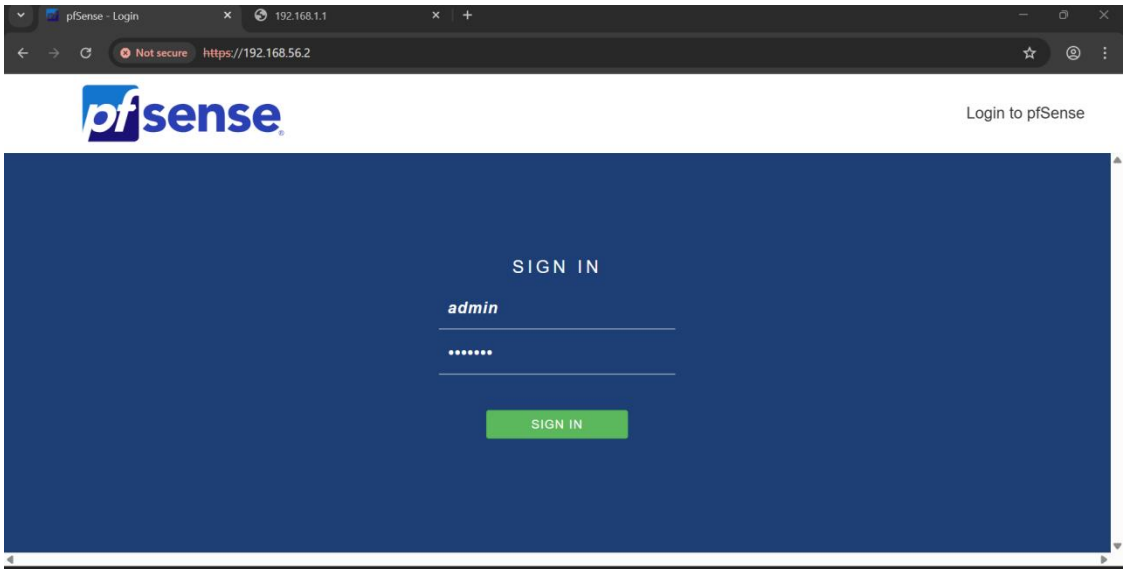
```
The IPv4 LAN address has been set to 192.168.56.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.56.2/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 0d7ad24c333d1e44a4a8

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

 WAN (wan) -> le0 -> v4/DHCP4: 10.0.2.15/24
                     v6/DHCP6: fd17:625c:f037:2:a00:27ff:fea5:a25e/64
 LAN (lan) -> le1 -> v4: 192.168.56.2/24

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

Enter an option:
```

6. Accessing the Web Interface

- From your host machine, open a web browser.
- Enter the **LAN IP** in the address bar (e.g., https://192.168.1.1).
- Login with default credentials:

Username: admin

Password: pfsense

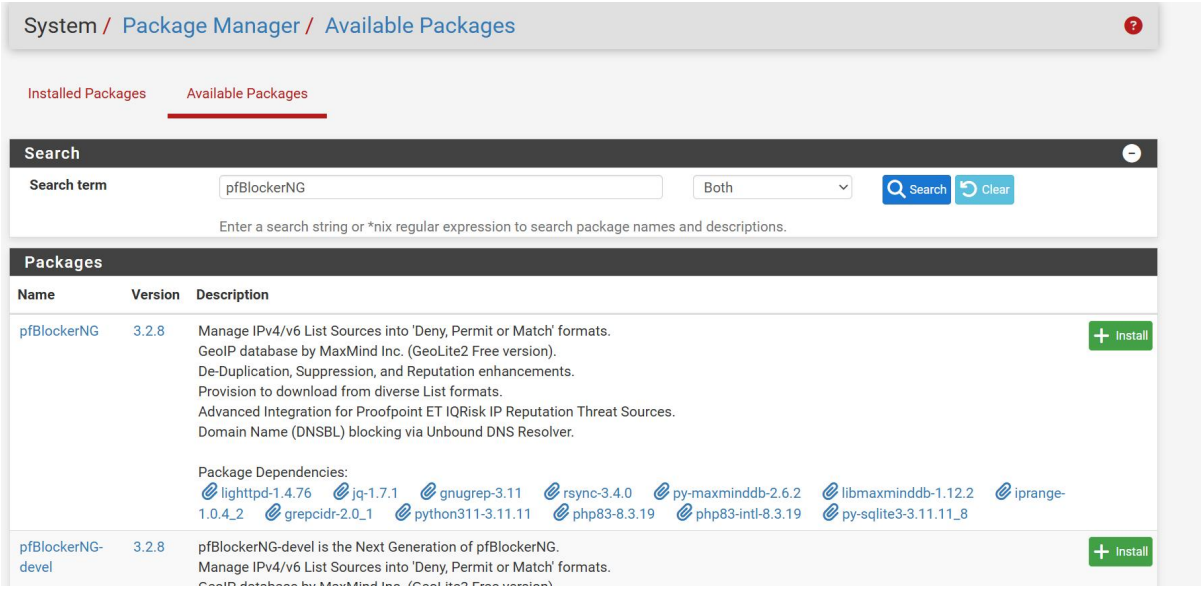


Setting pfBlockerNG:

1. Installing pfBlockerNG Package

- In PfSense web UI, go to: **System → Package Manager → Available Packages**.

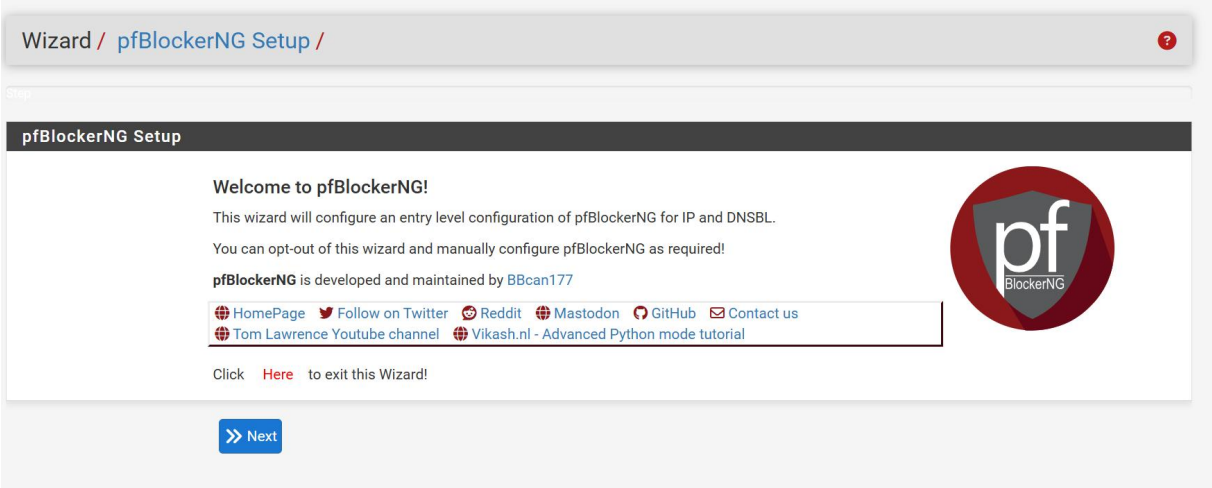
1. Search for **pfBlockerNG-devel** (recommended version with latest features).
2. Click **Install**, confirm, and wait until the installation completes.



2. Enabling pfBlockerNG

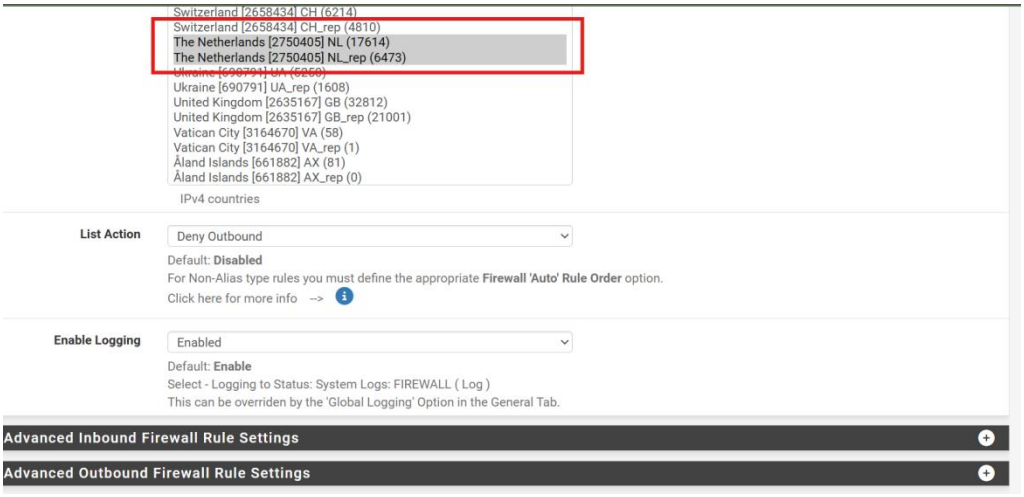
- After installation, navigate to **Firewall → pfBlockerNG**.
- In the **General** tab:

✓ Check **Enable pfBlockerNG**.
✓ Check **Keep Settings** (so configuration stays after upgrades).
✓ Click **Save**.

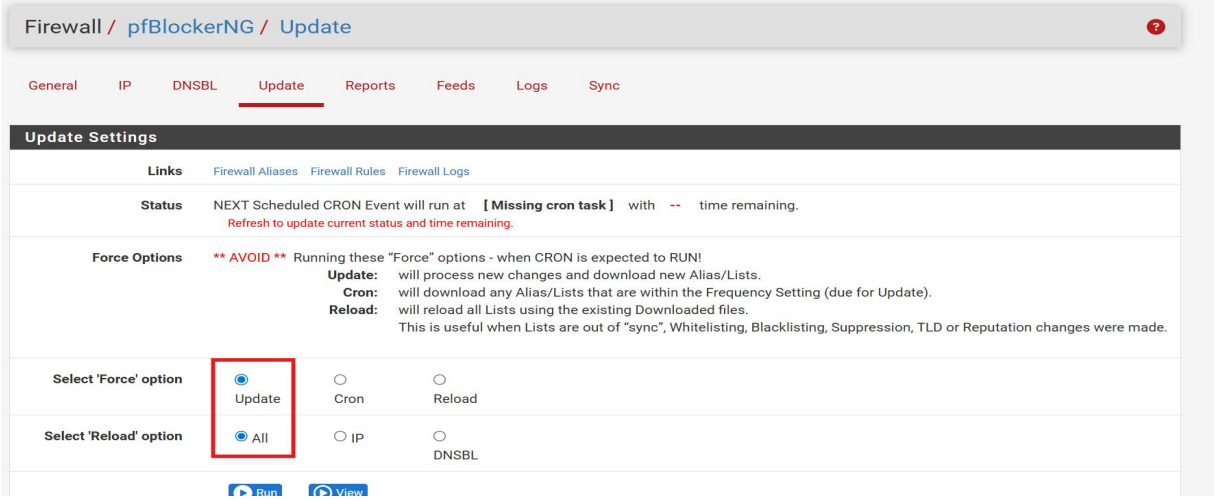


3. GeoIP Blocking (Blocking Netherlands)

- Go to **Firewall → pfBlockerNG → GeoIP**.
- Enable **GeoIP** by checking **Enable**.
- Under **Alias Name**, type something like `Blocked_Countries`.
- In **Country Selection**, scroll and select **Netherlands (NL)**.
    - Hold **Ctrl** to select multiple countries if needed.
- Under **List Action**, select **Deny Both** (blocks inbound and outbound).



- Click **Save**, then go to **Update** tab and click **Run** to apply rules.



4. Enabling DNSBL (Domain Blocking)

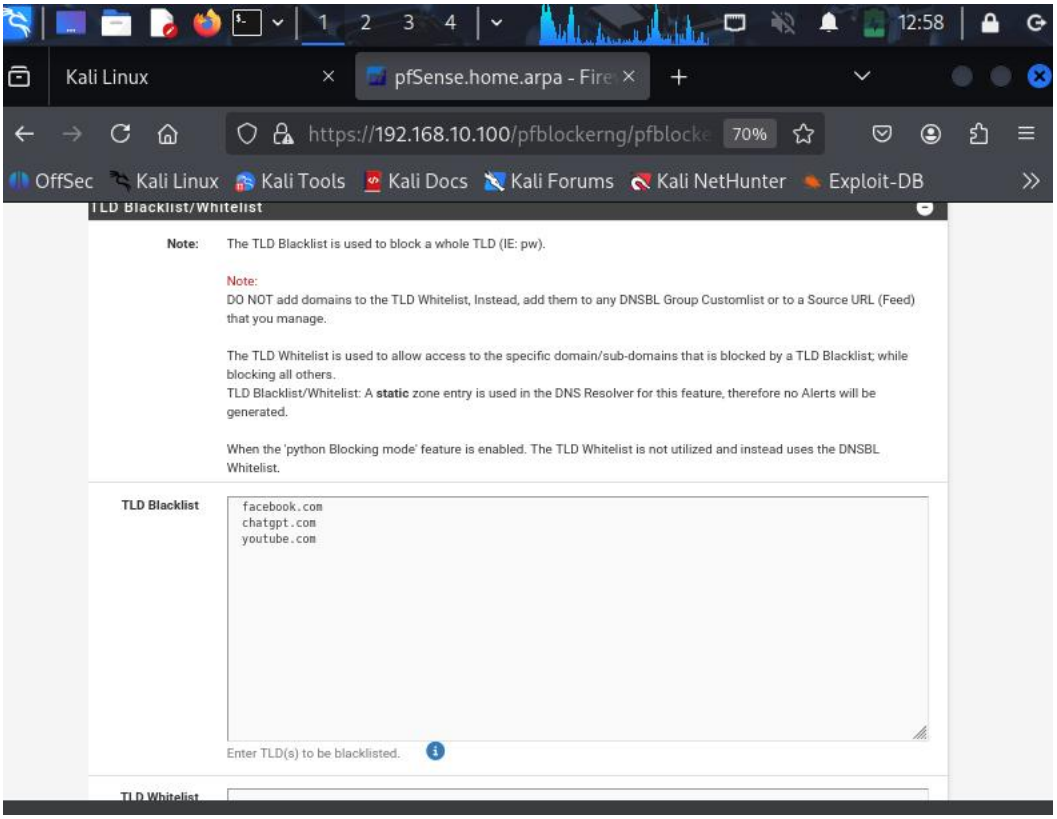
- Go to **Firewall → pfBlockerNG → DNSBL**.
- Check **Enable DNSBL**.
- Select **DNSBL Listening Interface** as `LAN`.
- Set **DNSBL Virtual IP** to `10.10.10.1` (default) unless changed.
- Check **DNSBL Blocking** to log blocked queries.
- Click **Save**.

5. Adding Websites to Block

- In **pfBlockerNG → DNSBL → DNSBL Custom Domain**, add:

✓ chatcom
✓ facebook. com

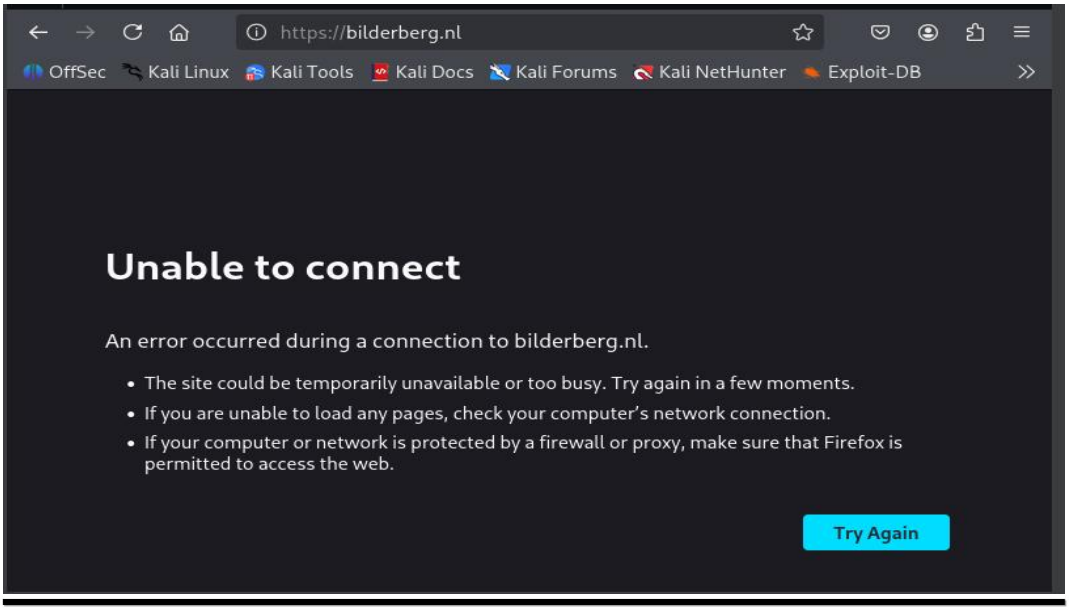
- Click **Save**.

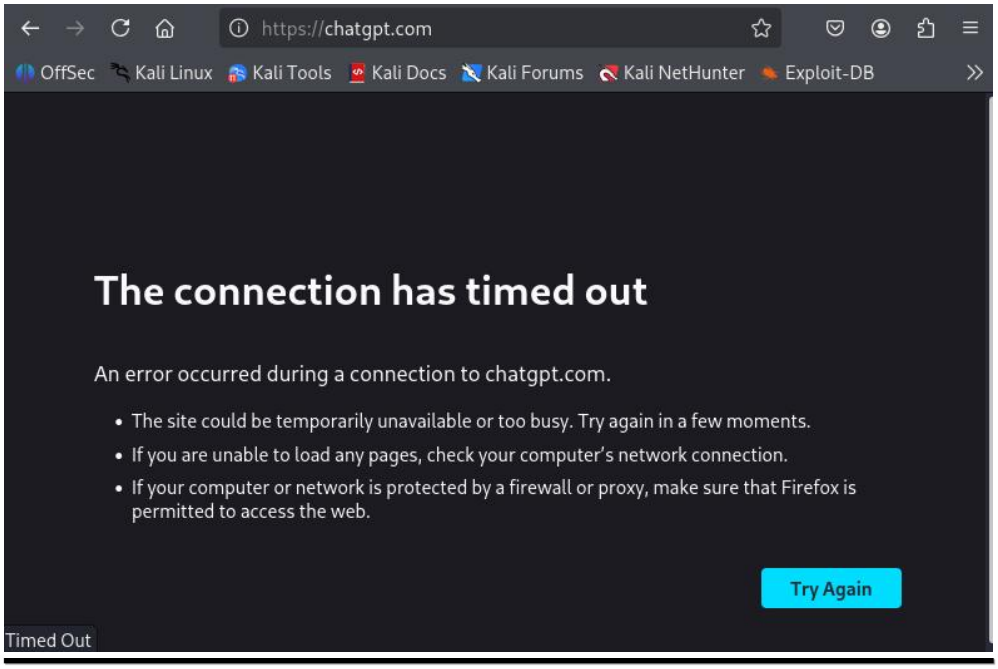


6. Reloading and Testing

- Go to **Firewall → pfBlockerNG → Update**.
- Click **Reload** to apply changes.
- From a client on the LAN:

Try visiting `facebook.com` or `chat.com` → It should be blocked.



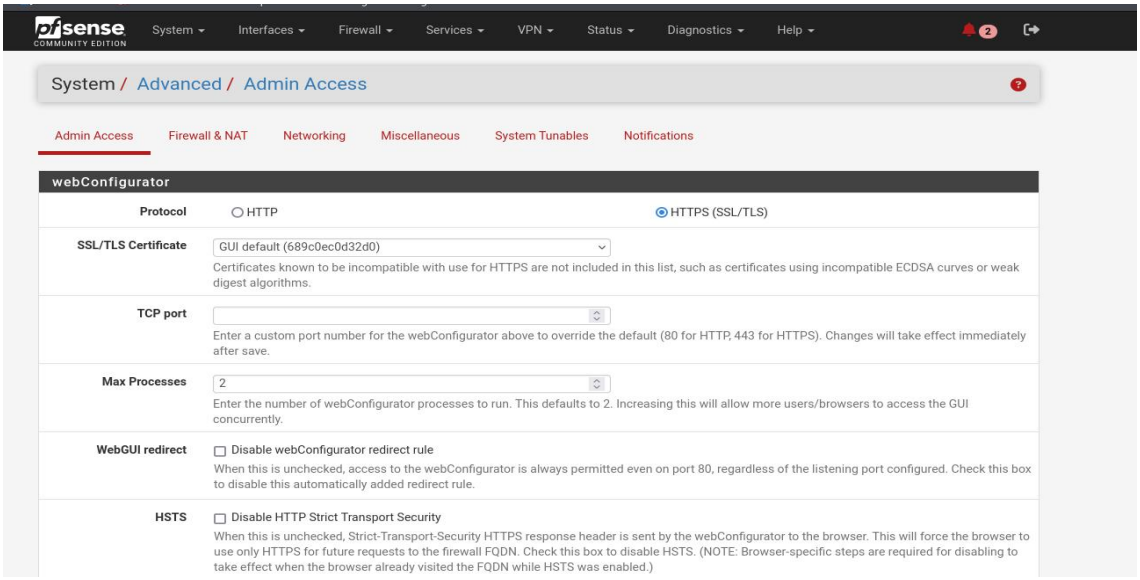


Applying Administrator privileges rule:

Part 1: Securing Web Interface via Admin Access Settings

In the PfSense web UI, go to: **System → Advanced → Admin Access**.

- In **Protocol**:
- Select **HTTPS (SSL/TLS)**.
- Ensure **HTTP** is unchecked for security.
- In **SSL/TLS Certificate**:
- Keep **GUI default** unless using a custom certificate.
- (Optional) In **TCP Port**:
- Enter a **custom port** (e.g., `8443`) to make access less predictable.
- Set **Max Processes** to `2` (default) — keeps resource usage low.
- Ensure **WebGUI redirect** is **unchecked** so HTTP doesn't auto-redirect to HTTPS.
- Leave **HSTS** enabled unless you have a reason to disable it.
- Click **Save** — changes apply immediately.



Part 2: Allow Only Admin VM to Access the Web Interface

Identify your **Admin VM's IP address** (e.g., `192.168.10.5`).

Create an alias:

- Go to **Firewall → Aliases → IP → Add**.
- Name: `Admin_VM`.
- Type: Host(s).
- IP: `192.168.10.5`.
- Save and Apply.

Create Allow Rule in LAN:

- Go to **Firewall → Rules → LAN → Add** (place at top).
- Action: Pass.
- Source: `Admin_VM`.
- Destination: This firewall (self).
- Port: 443 (or your custom port).
- Save and Apply.

Create Block Rule for everyone else:

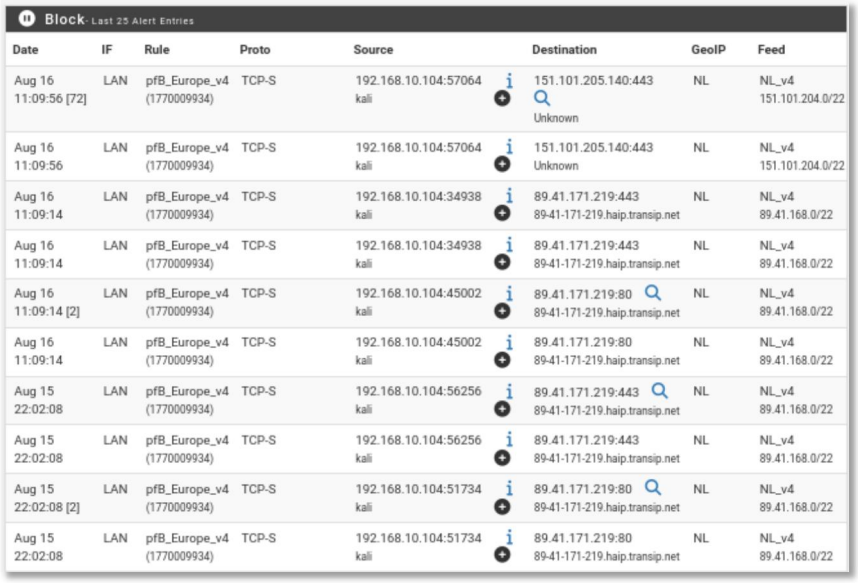
- Add a new rule **below** the allow rule.
- Action: Block.
- Source: LAN subnet (e.g., `192.168.10.0/24`).
- Destination: This firewall (self).
- Port: 443 (or your custom port).
- Save and Apply.

Monitoring logs:

Accessing pfBlockerNG Logs

- Log in to the pfSense web interface (e.g., https://192.168.1.1).
- Navigate to **Firewall > pfBlockerNG > Reports** to view blocked domains and traffic details.
- Check the **DNSBL Logs** tab for a list of blocked domain queries.
- Review the **GeoIP Logs** tab to see traffic blocked by country.

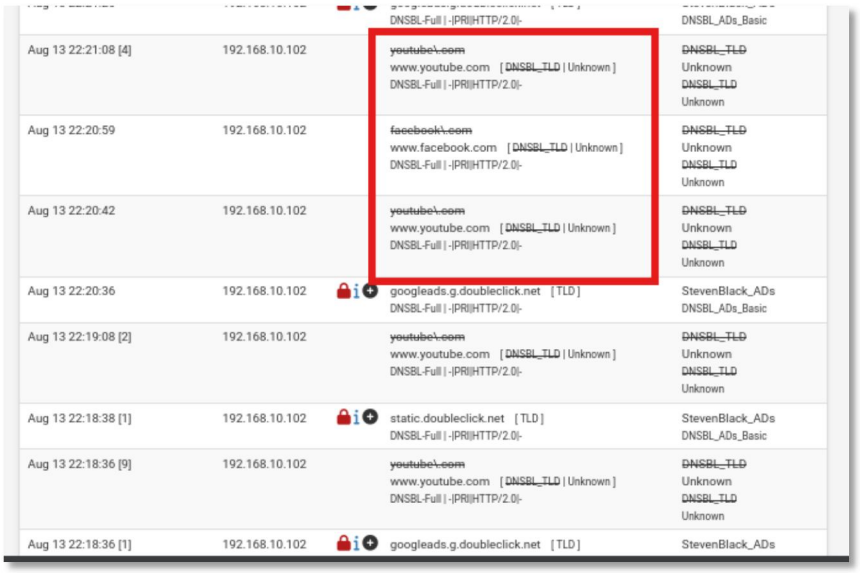
GeoIp Blocking Log screenshot:



Block - Last 25 Alert Entries

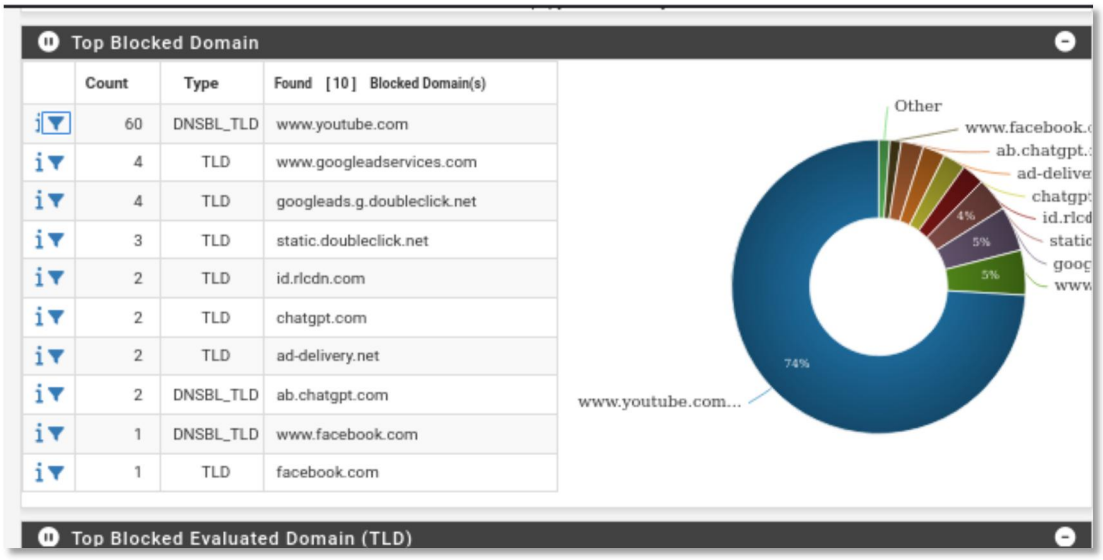
Date	IF	Rule	Proto	Source	Destination	GeoIP	Feed
Aug 16 11:09:56 [72]	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:57064 kali	151.101.205.140:443 Unknown	NL	NL_v4 151.101.204.0/22
Aug 16 11:09:56	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:57064 kali	151.101.205.140:443 Unknown	NL	NL_v4 151.101.204.0/22
Aug 16 11:09:14	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:34938 kali	89.41.171.219:443 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22
Aug 16 11:09:14	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:34938 kali	89.41.171.219:443 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22
Aug 16 11:09:14 [2]	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:45002 kali	89.41.171.219:80 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22
Aug 16 11:09:14	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:45002 kali	89.41.171.219:80 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22
Aug 15 22:02:08	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:56256 kali	89.41.171.219:443 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22
Aug 15 22:02:08	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:56256 kali	89.41.171.219:443 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22
Aug 15 22:02:08 [2]	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:51734 kali	89.41.171.219:80 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22
Aug 15 22:02:08	LAN	pfB_Europe_v4 (1770009934)	TCP-S	192.168.10.104:51734 kali	89.41.171.219:80 89-41-171-219.haip.transip.net	NL	NL_v4 89.41.168.0/22

Website Blocking Log screenshot:

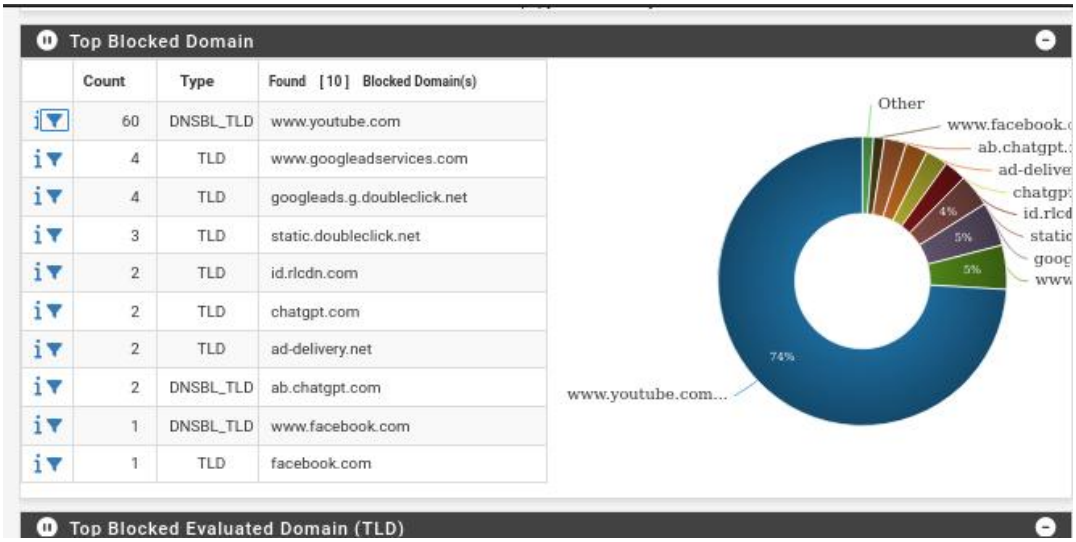


		DNSBL-Full | -IPRI|HTTP/2.0|-		DNSBL_ADs_Basic
Aug 13 22:21:08 [4]	192.168.10.102	youtube\.com www.youtube.com [DNSBL_TLD | Unknown] DNSBL-Full | -IPRI|HTTP/2.0|-		DNSBL_TLD Unknown DNSBL_TLD Unknown
Aug 13 22:20:59	192.168.10.102	facebook\.com www.facebook.com [DNSBL_TLD | Unknown] DNSBL-Full | -IPRI|HTTP/2.0|-		DNSBL_TLD Unknown DNSBL_TLD Unknown
Aug 13 22:20:42	192.168.10.102	youtube\.com www.youtube.com [DNSBL_TLD | Unknown] DNSBL-Full | -IPRI|HTTP/2.0|-		DNSBL_TLD Unknown DNSBL_TLD Unknown
Aug 13 22:20:36	192.168.10.102	googleads.g.doubleclick.net [TLD] DNSBL-Full | -IPRI|HTTP/2.0|-		StevenBlack_ADs DNSBL_ADs_Basic
Aug 13 22:19:08 [2]	192.168.10.102	youtube\.com www.youtube.com [DNSBL_TLD | Unknown] DNSBL-Full | -IPRI|HTTP/2.0|-		DNSBL_TLD Unknown DNSBL_TLD Unknown
Aug 13 22:18:38 [1]	192.168.10.102	static.doubleclick.net [TLD] DNSBL-Full | -IPRI|HTTP/2.0|-		StevenBlack_ADs DNSBL_ADs_Basic
Aug 13 22:18:36 [9]	192.168.10.102	youtube\.com www.youtube.com [DNSBL_TLD | Unknown] DNSBL-Full | -IPRI|HTTP/2.0|-		DNSBL_TLD Unknown DNSBL_TLD Unknown
Aug 13 22:18:36 [1]	192.168.10.102	googleads.g.doubleclick.net [TLD]		StevenBlack_ADs

Report of GeoIp:



Report of Website Blocking:



Conclusion:

The implementation of pfSense, coupled with pfBlockerNG, successfully achieved the objectives of blocking specific country traffic (e.g., Netherlands), restricting access to designated websites (e.g., facebook.com), and securing administrator privileges. Monitoring via pfBlockerNG logs and reports confirmed effective traffic filtering, with detailed insights into blocked domains and activities. This setup provides a scalable and secure solution for network management.

Thanks:

TASK#3 : Pfsense Firewall/Squid Proxy and Malware download prevention

Objectives:

- **Download a freely available malware via a VM with an active pf Sense firewall, observe detection and log**
- **Activities, analyze logs and malware, and create an incident response plan.**

Steps:

1. Setup and Download Malware
• Preparation:
- Ensure pfSense firewall is configured and running.
- Set up a VM for malware download.
• Download Malware:
- Download a freely available malware sample from a reputable site (e.g., theZoo, VirusShare)**.**

2. Detection and Observation
• pfSense Monitoring:
- Check pfSense logs for detection of the malicious download.
- Document any alerts or blocks.

• Wazuh Dashboard:
- Observe Wazuh for alerts/log entries related to the malware.
- Gather detailed log entries.

3. Log and Malware Analysis
• Log Details Collection:
- Collect comprehensive logs from Wazuh.
- Identify Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
• Analysis Report:
- Create a report analyzing the logs and malware behavior.

4. Incident Response Plan
• Create Incident Response Plan:
- Develop an incident response plan based on industry standards.
- Include steps for detection, analysis, containment, eradication, and recovery.
• Share Incident Response Plan:
- Compile the report and incident response plan.
- Share the document for review and implementation.

Tools:

- **PfSense** – Open-source firewall and router software for network security, rule creation, and traffic filtering.
- **Wazuh** – Security Information and Event Management (SIEM) platform for log collection, intrusion detection, and real-time monitoring.
- **Oracle VirtualBox** – Virtualization software to host PfSense and Wazuh instances in a controlled lab environment.
- **Web Browser (e.g., Chrome/Firefox)** – For accessing PfSense web interface and Wazuh dashboard.
- **Squid Proxy (on pfSense) --** Deployed as a transparent proxy to log and monitor web traffic and Captured details of the malware download request.

Setting pfSense Firewall:

1. Downloading PfSense

- Visit the official PfSense website: https://www.pfsense.org/download/.

Choose the following options:

Architecture: AMD64 (64-bit)

Installer: ISO Installer

- Download the **.iso** file.

2. Creating the Virtual Machine in VirtualBox

- Open **Oracle VirtualBox** → Click **New**.
- Name the VM (e.g., *PfSense Firewall*).
- Type: **BSD** → Version: **FreeBSD (64-bit)**.

Allocate **2 GB RAM** (or more).

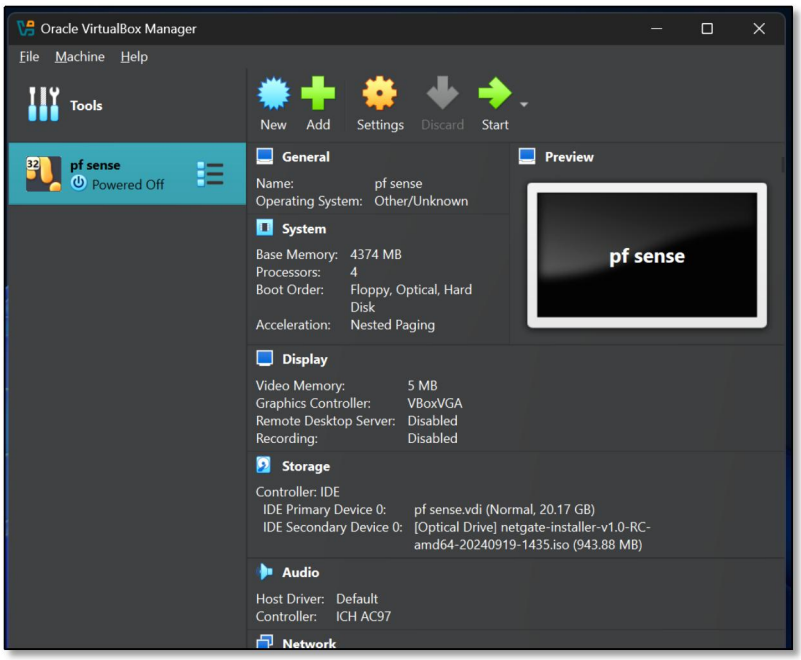
Assign **2 CPUs** (recommended for better performance).

Create a **Virtual Hard Disk** (10 GB minimum).

- Attach the **PfSense ISO**:

Go to **Settings** → **Storage**.

Under Controller IDE/SATA, choose **Add Optical Drive** and select the downloaded ISO.



3. Configuring Network Interfaces

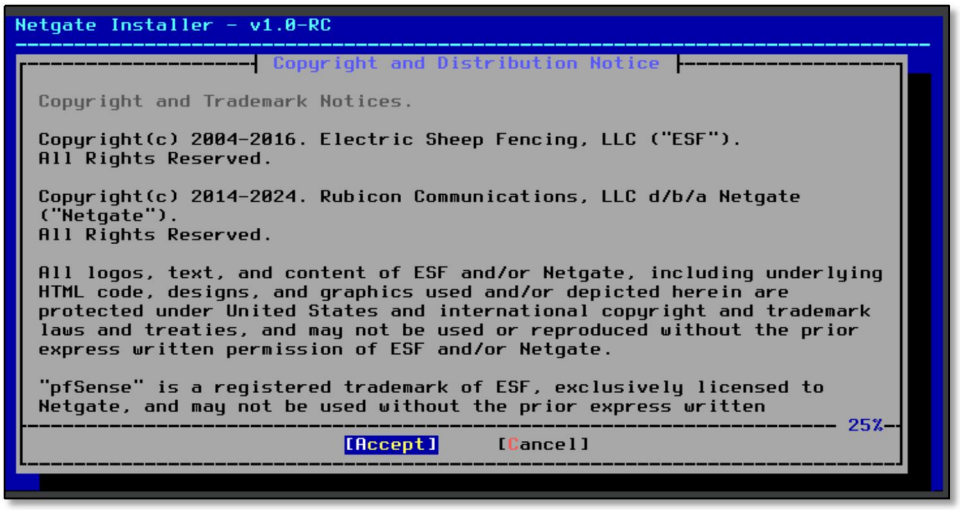
- In **VM Settings → Network**:

  Adapter 1: Set to *Bridged Adapter* (WAN connection).

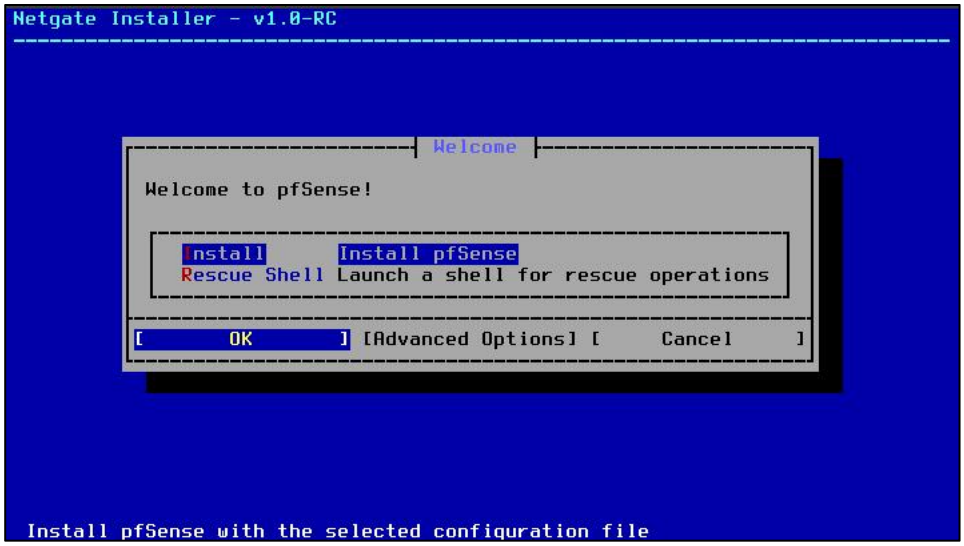
  Adapter 2: Set to *Internal Network* or *Host-only Adapter* (LAN connection).

4. Installing PfSense

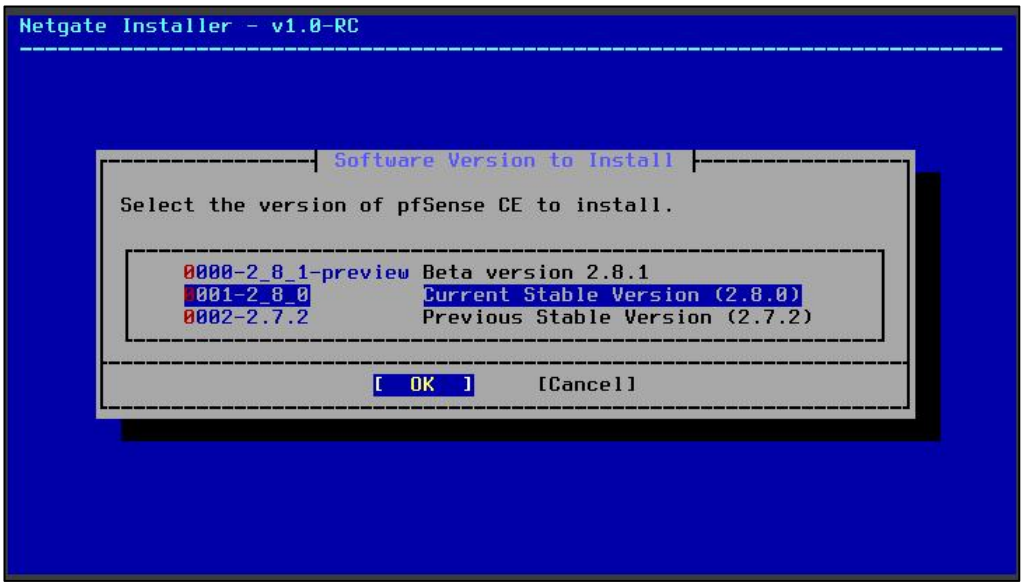
- Start the VM → The ISO will boot into the installer.



- Choose Install from the menu.



- Select the current stable version



- Installation will complete → Remove ISO from virtual drive → Reboot.

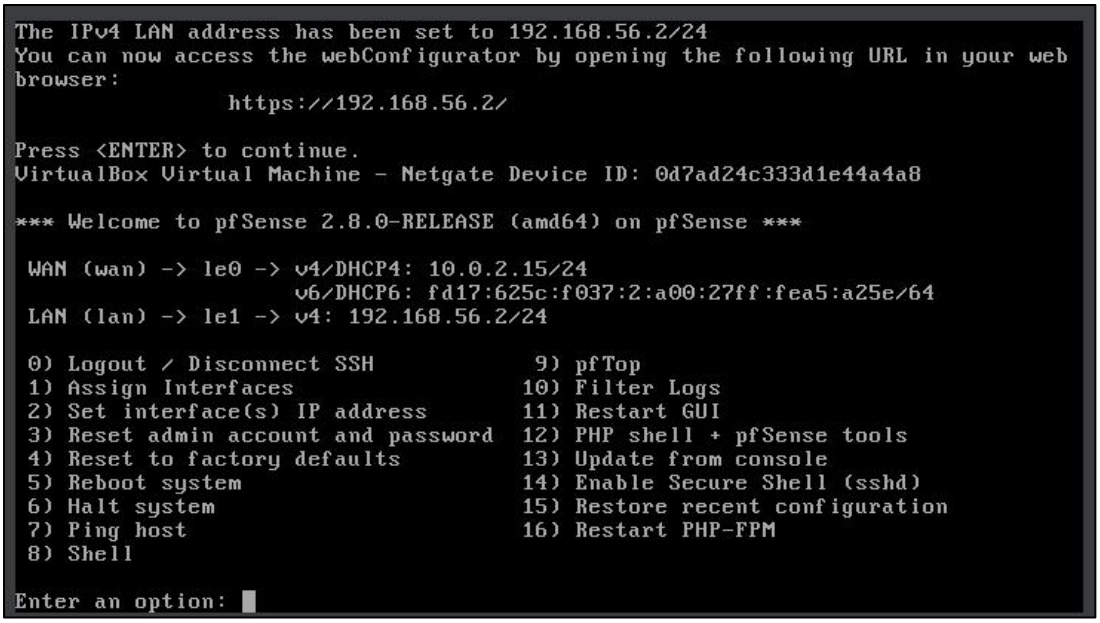
5. Assigning Interfaces

- After reboot, PfSense will ask to assign interfaces:

  WAN → Adapter 1.

  LAN → Adapter 2.

- The system will display assigned IP addresses — note down the **LAN IP**.

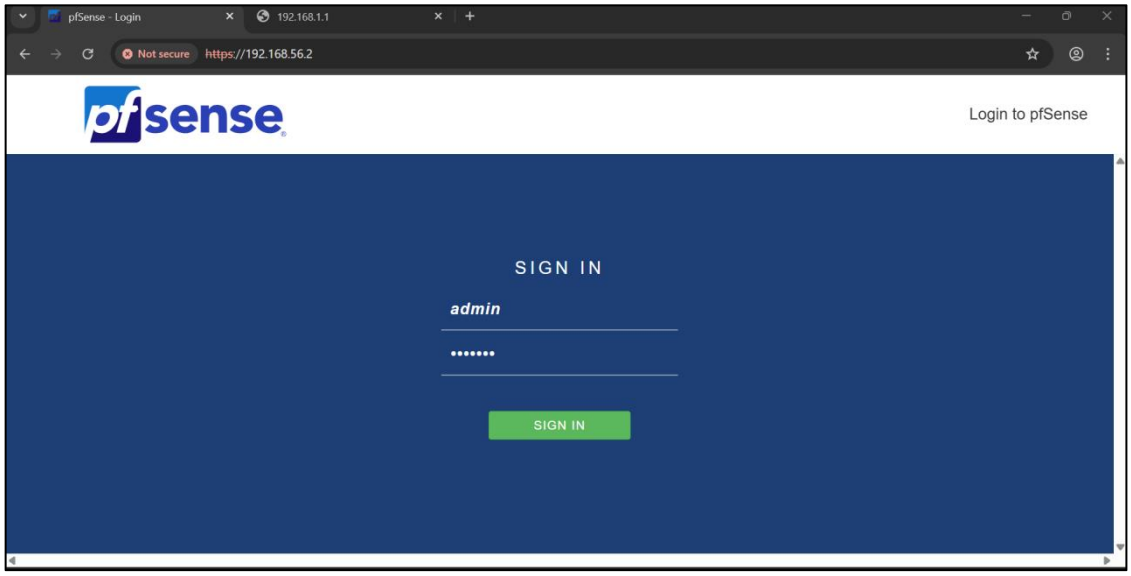


6. Accessing the Web Interface

- From your host machine, open a web browser.
- Enter the **LAN IP** in the address bar (e.g., https://192.168.1.1).
- Login with default credentials:

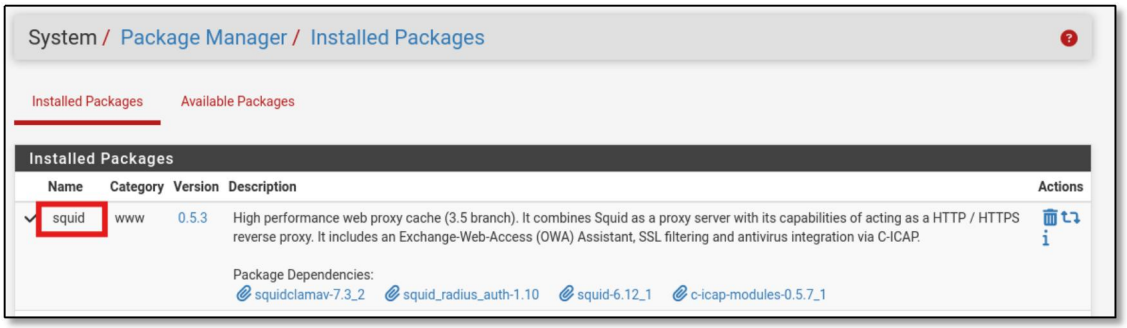
Username: admin

Password: pfsense



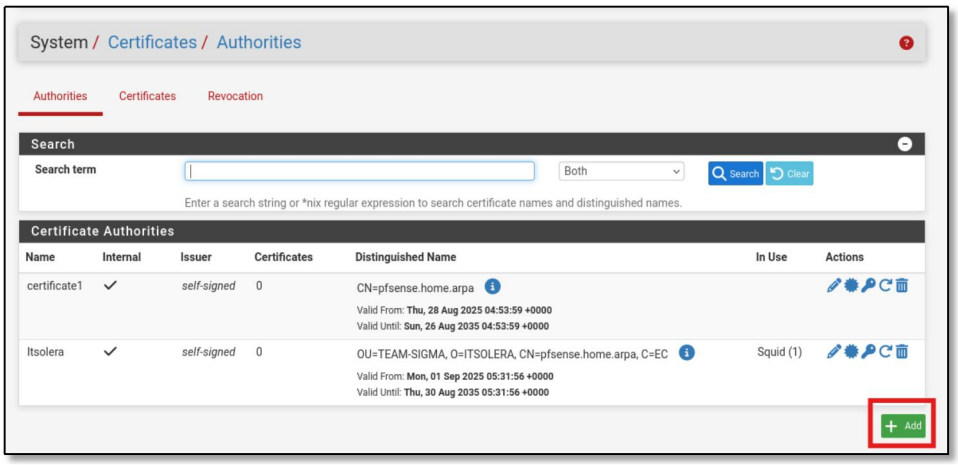
Installing Squid Package on pfSense:

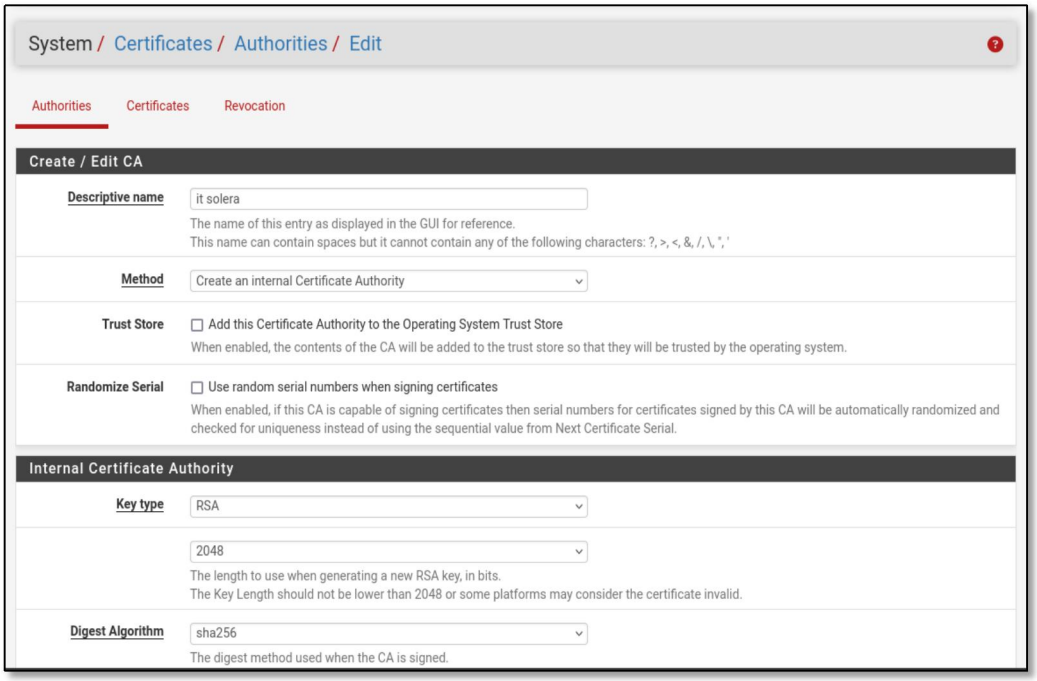
- Navigate to **System → Package Manager → Available Packages**.
- Search for **Squid**.
- Click **Install** and confirm the installation.
- Once installed, verify that Squid appears under **Services → Squid Proxy Server**.

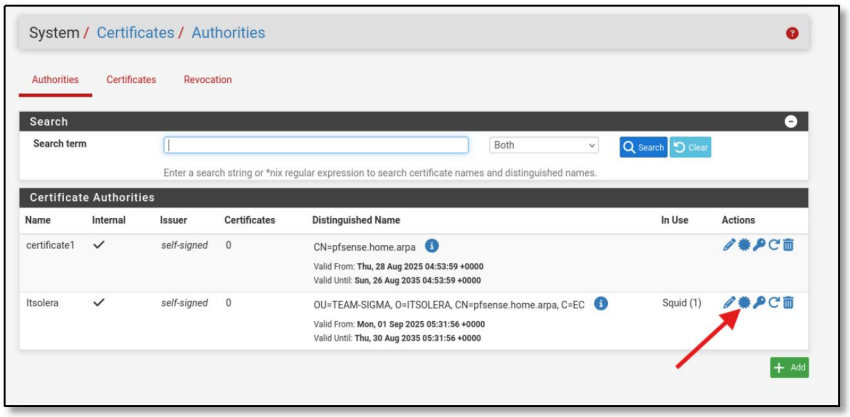


Creating SSL Certificate for HTTPS Filtering:

- Go to **System → Cert. Manager → CAs**
- Click **Add** to create a new **Certificate Authority (CA)**.
- Provide a descriptive name (e.g., *Squid_CA*).
- Save the CA.
- Next, navigate to **Certificates** tab and click **Add/Sign**.
- Select the newly created CA as the signer.
- Create a new server certificate for Squid.
- Save the certificate.
- Apply the certificate in **Services → Squid Proxy Server → General → SSL/MITM**



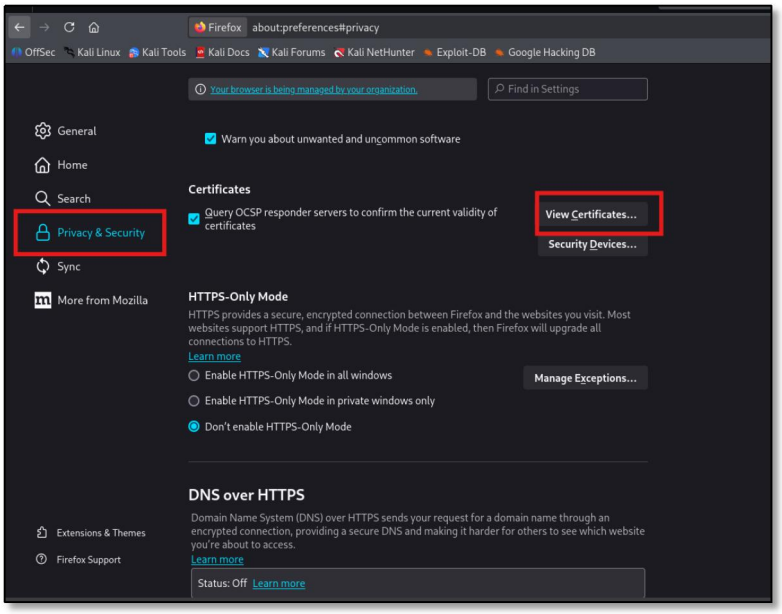


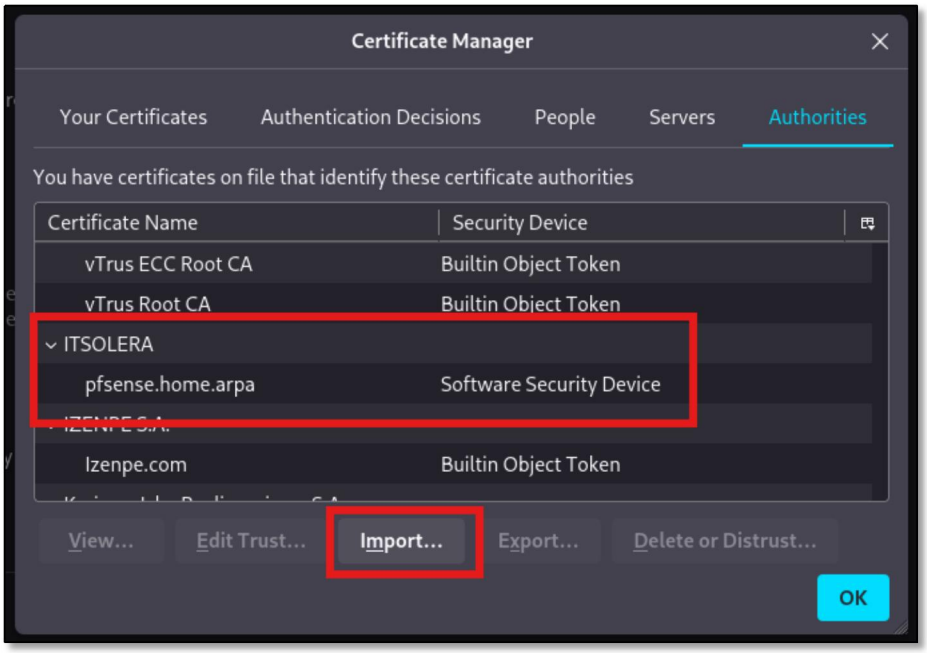


Integrating Certificate in Browser:

- Export the CA certificate from pfSense **Cert. Manager**.
- On the client VM, open the browser (e.g., Chrome/Firefox)

- Go to **Settings → Privacy & Security → Certificates**.
- Import the downloaded **CA certificate** into the browser's **Trusted Root Authorities**.
- Restart the browser to apply changes.

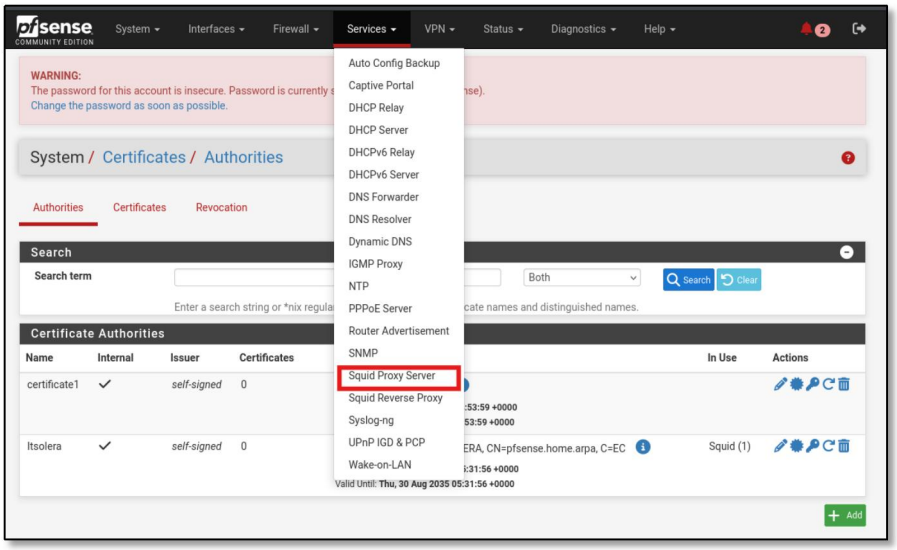




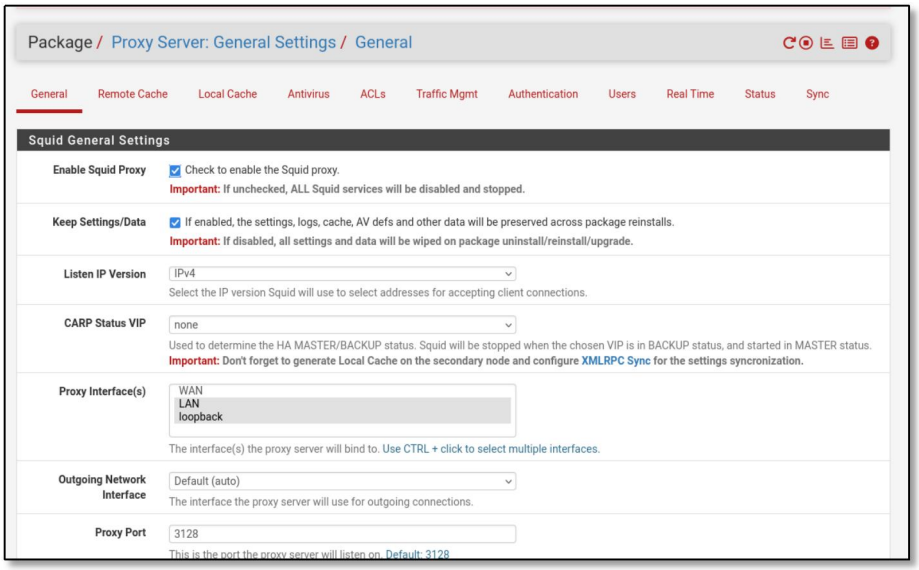
Configuration of Squid Proxy:

General Settings of Squid

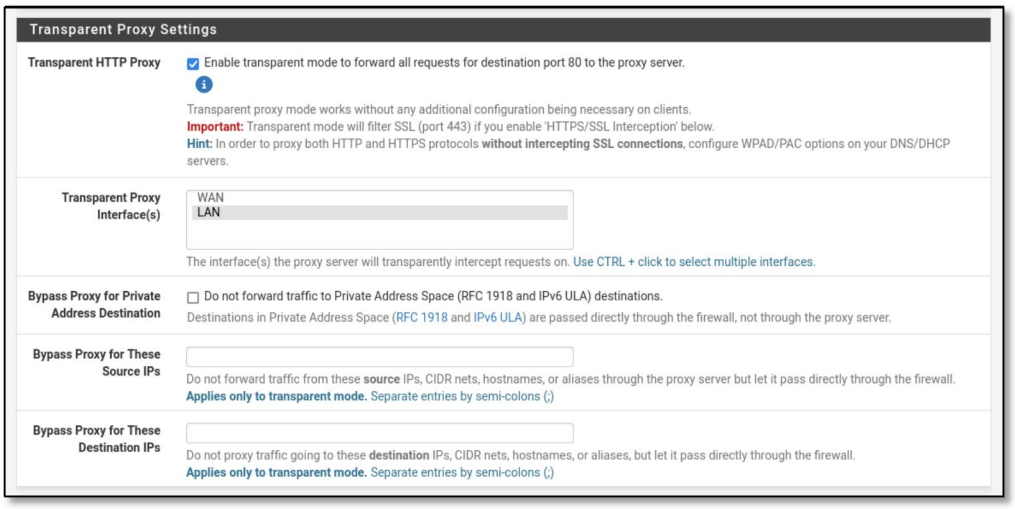
- Navigate to **Services → Squid Proxy Server → General**.



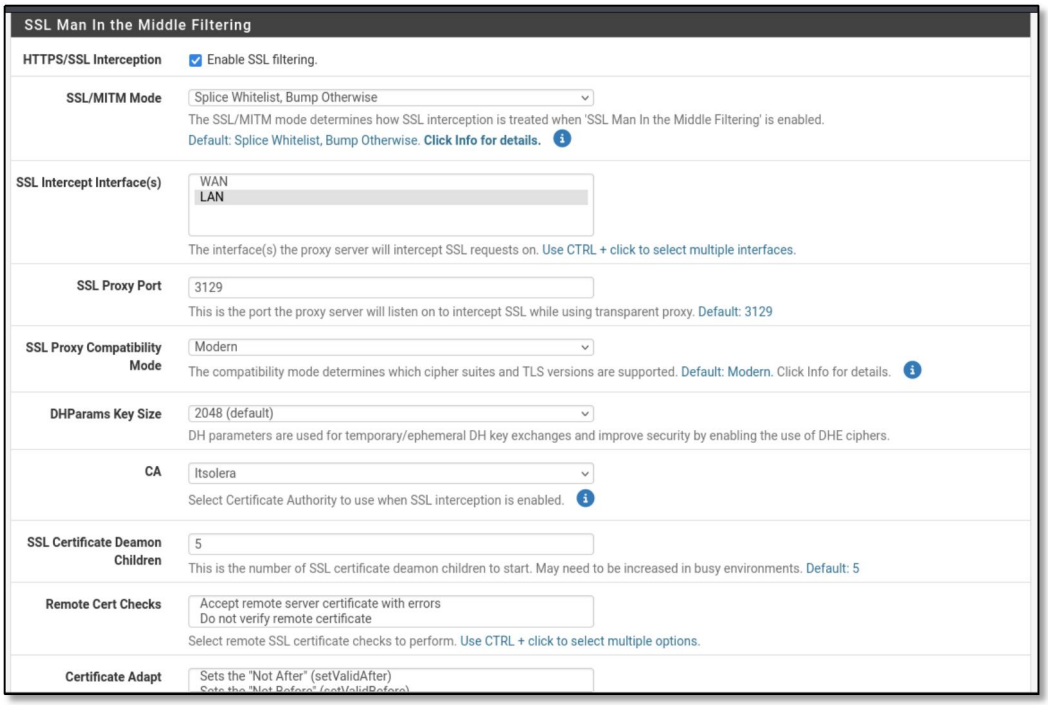
- Enable **Proxy Interface** → Select the desired LAN interface.
- Set **Allow Users on Interface** → Enabled.
- Configure **Proxy Port** (default: 3128).



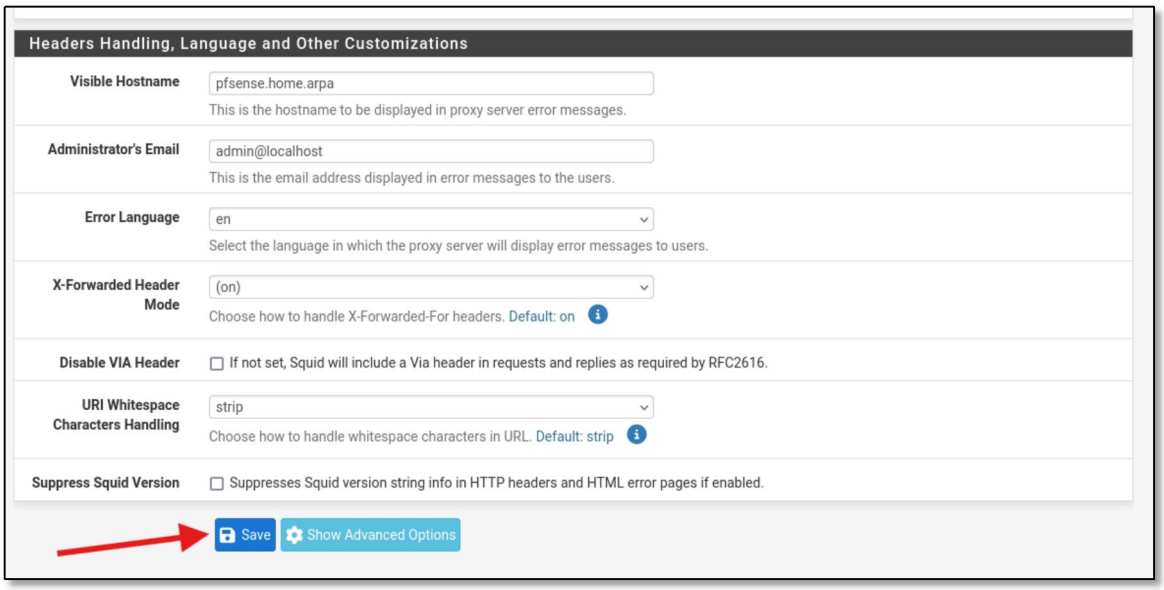
- Enable **Transparent HTTP Proxy** for seamless interception of web traffic.



- If HTTPS inspection is required:
  - Enable **SSL Filtering/MITM**.
  - Select the previously created **SSL Certificate.**

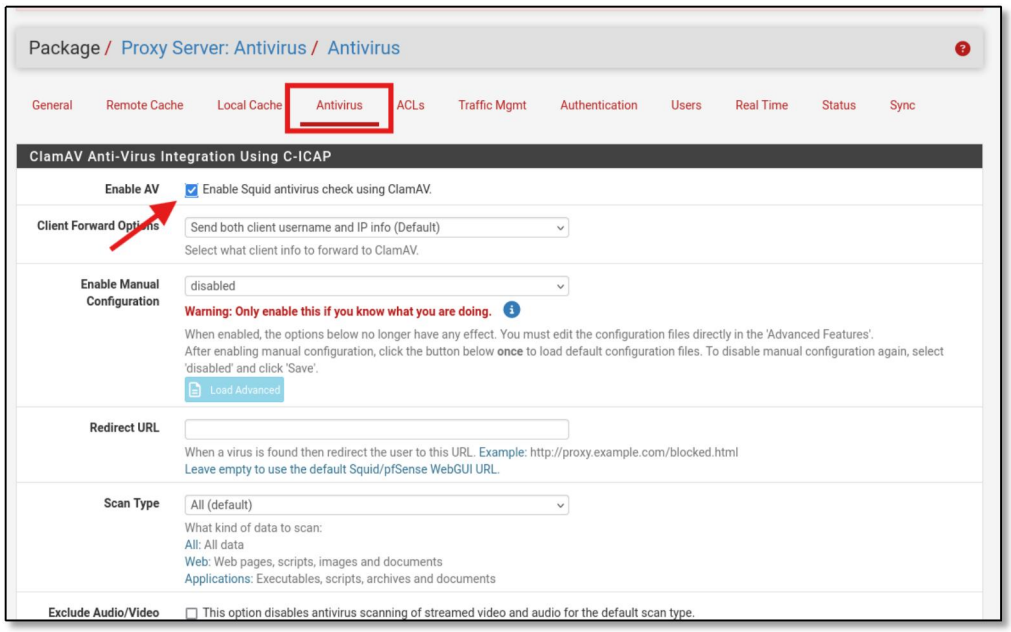


- Save and Apply settings.



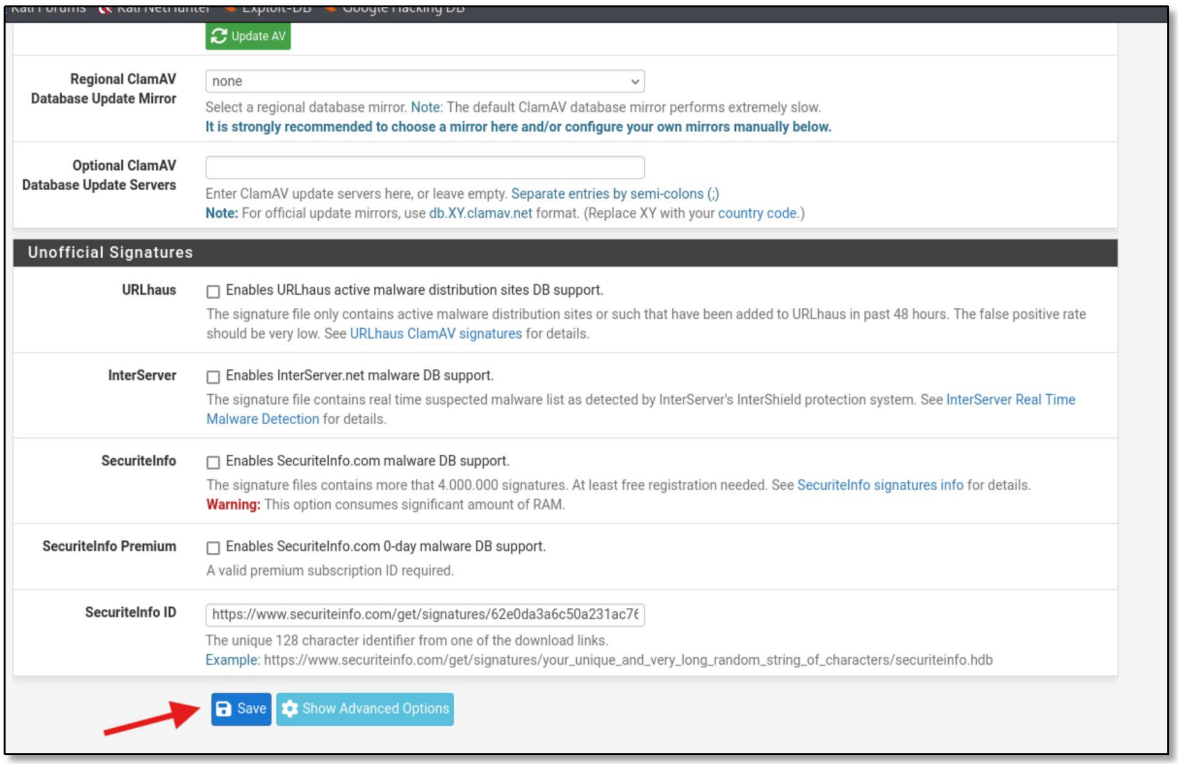
Antivirus Integration (SquidClamAV)

- Go to **Services → Squid Proxy Server → Antivirus**.
- Enable **Antivirus** .



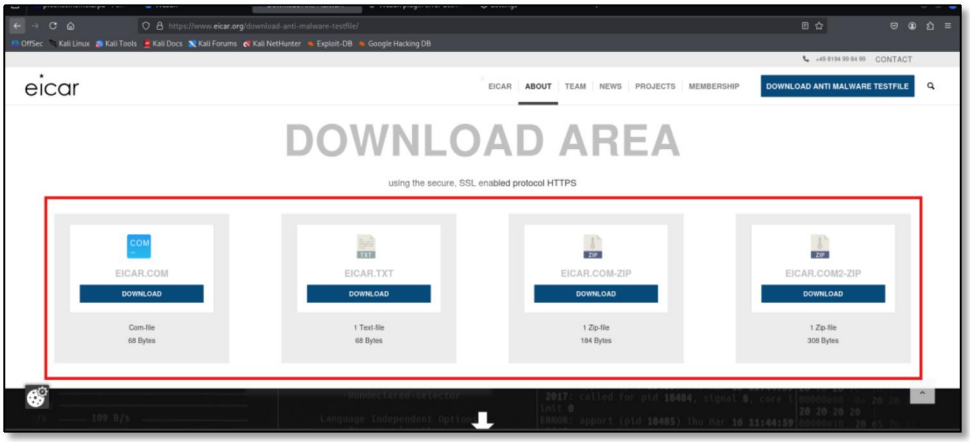
- Under **ClamAV Engine Settings**:
- Select **Enable ClamAV**.
- Ensure **Freshclam** service updates signatures regularly.

- Save and Apply settings.



Testing Malware Detection with EICAR File

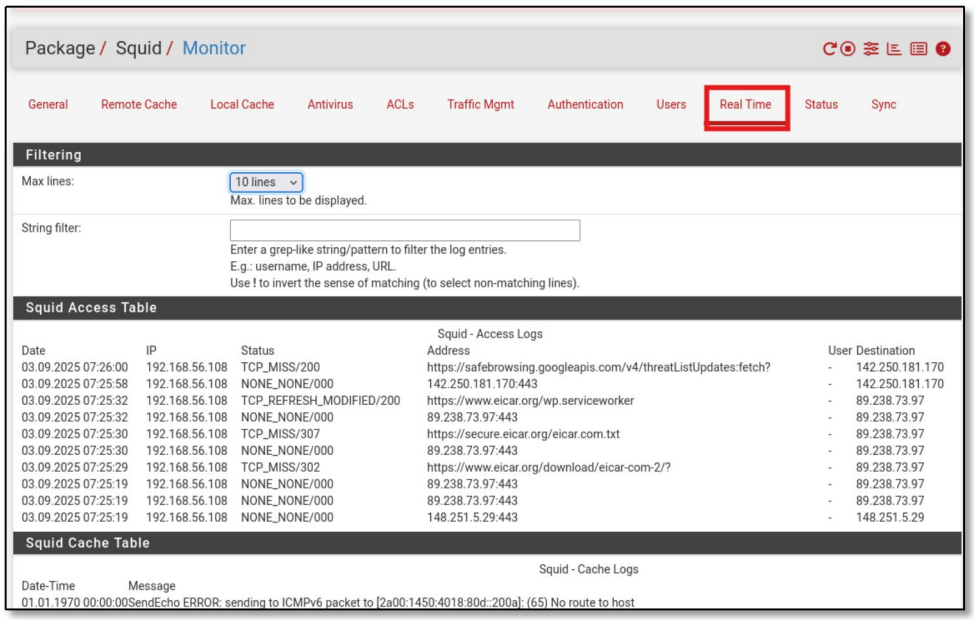
- On the client VM, open a browser configured with Squid.
- Navigate to the **EICAR test file website** (e.g., https://www.eicar.org/download-anti-malware-testfile/).).
- Attempt to download the EICAR test file.



- **Expected Behavior**:
- The download should be blocked by **Squid + ClamAV**.
- The browser should display an access denied or virus detected message.

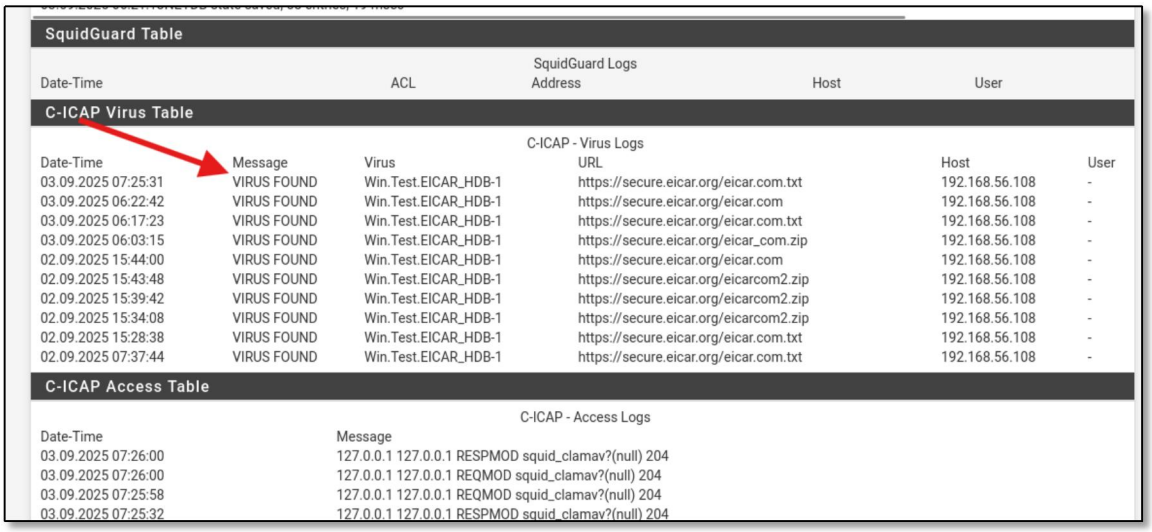
Viewing Logs in pfSense

- Go to **Status → System Logs → Proxy Filter (or Squid logs)**.



- Review logs for:
- Blocked EICAR file requests.
- ClamAV virus scan results.
- Client IP and request details.

- Confirm that the EICAR detection entry is logged.



SquidGuard Table

SquidGuard Logs

Date-Time	ACL	Address	Host	User

C-ICAP Virus Table

C-ICAP - Virus Logs

Date-Time	Message	Virus	URL	Host	User
03.09.2025 07:25:31	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicar.com.txt	192.168.56.108	-
03.09.2025 06:22:42	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicar.com	192.168.56.108	-
03.09.2025 06:17:23	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicar.com.txt	192.168.56.108	-
03.09.2025 06:03:15	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicar_com.zip	192.168.56.108	-
02.09.2025 15:44:00	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicar.com	192.168.56.108	-
02.09.2025 15:43:48	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicarcom2.zip	192.168.56.108	-
02.09.2025 15:39:42	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicarcom2.zip	192.168.56.108	-
02.09.2025 15:34:08	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicarcom2.zip	192.168.56.108	-
02.09.2025 15:28:38	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicar.com.txt	192.168.56.108	-
02.09.2025 07:37:44	VIRUS FOUND	Win.Test.EICAR_HDB-1	https://secure.eicar.org/eicar.com.txt	192.168.56.108	-

C-ICAP Access Table

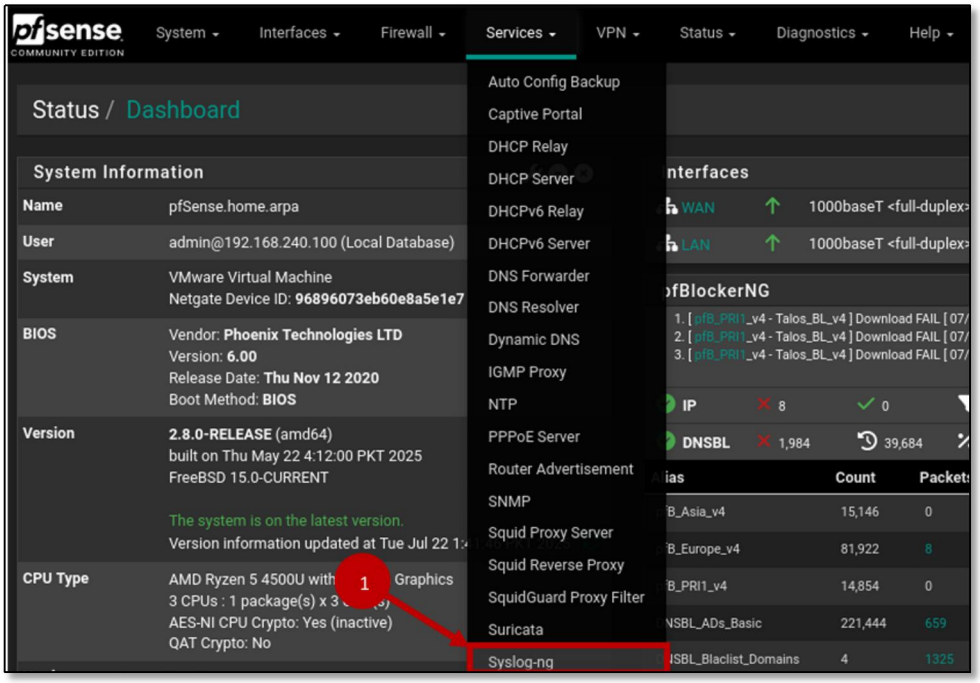
C-ICAP - Access Logs

Date-Time	Message
03.09.2025 07:26:00	127.0.0.1 127.0.0.1 RESPMOD squid_clamav?(null) 204
03.09.2025 07:26:00	127.0.0.1 127.0.0.1 REQMOD squid_clamav?(null) 204
03.09.2025 07:25:58	127.0.0.1 127.0.0.1 REQMOD squid_clamav?(null) 204
03.09.2025 07:25:32	127.0.0.1 127.0.0.1 RESPMOD squid_clamav?(null) 204

Integration of pfSense with Wazuh using Syslog-NG:

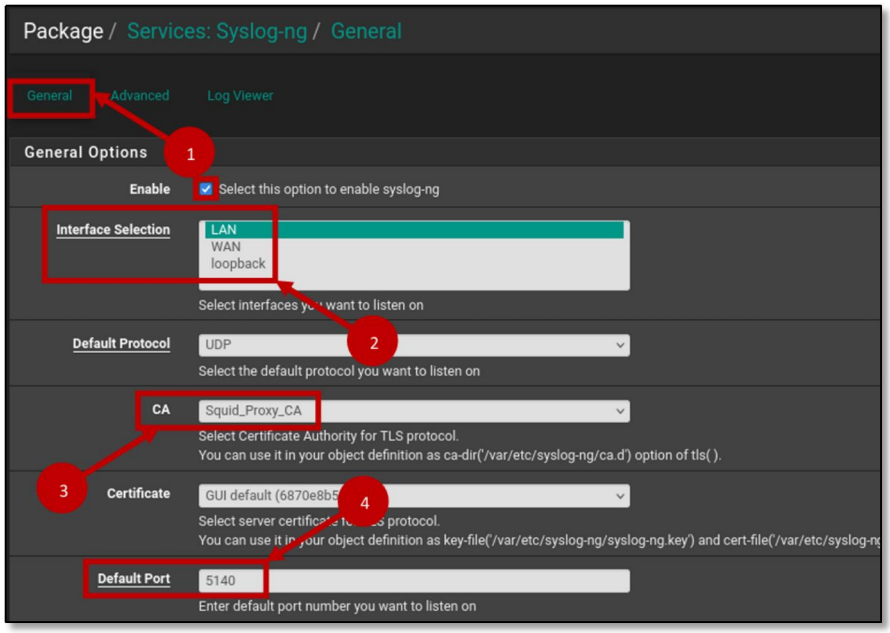
Installing Syslog-NG on pfSense:

- **Navigate to System → Package Manager → Available Packages.**
- Search for **syslog-ng**.
- Install the package and confirm its presence under **Installed Packages**.



Configuring Syslog-NG on pfSense:

- Go to **Services → Syslog-NG**.
- In the **Destinations** section:
- Add a new destination.
- Enter the **IP address of the Wazuh Manager**.
- Set the default syslog port **5514/UDP** (or TCP if configured).
- In the **Sources** section:
- Select system logs (firewall logs, Squid proxy logs, etc.) that should be forwarded.
- In the **Log Paths** section:
- Define a log path that links the selected source to the Wazuh Manager destination.
- Save and Apply changes.



Configuring Wazuh Manager to Receive Logs:

- On the **Wazuh Manager**, edit the configuration file:
- Add a new <remote> block to accept logs:
- Restart the Wazuh Manager service

```
<remote>
  <connection>syslog</connection>
  <port>5514</port>
  <protocol>udp</protocol>
  <allowed-ips>192.168.56.1</allowed-ips>
  <local_ip>192.168.56.109</local_ip>
</remote>
<!-- Policy monitoring -->
```

Adding Custom Decoders and Rules:

To properly parse pfSense and Squid logs, **custom decoders and rules** were created in Wazuh:

- Navigate to the Wazuh Manager configuration directory:
- Create or edit the **local_decoder.xml** file:
- Create or edit the **local_rules.xml** file to generate alerts:

local_rules_clamav.xml

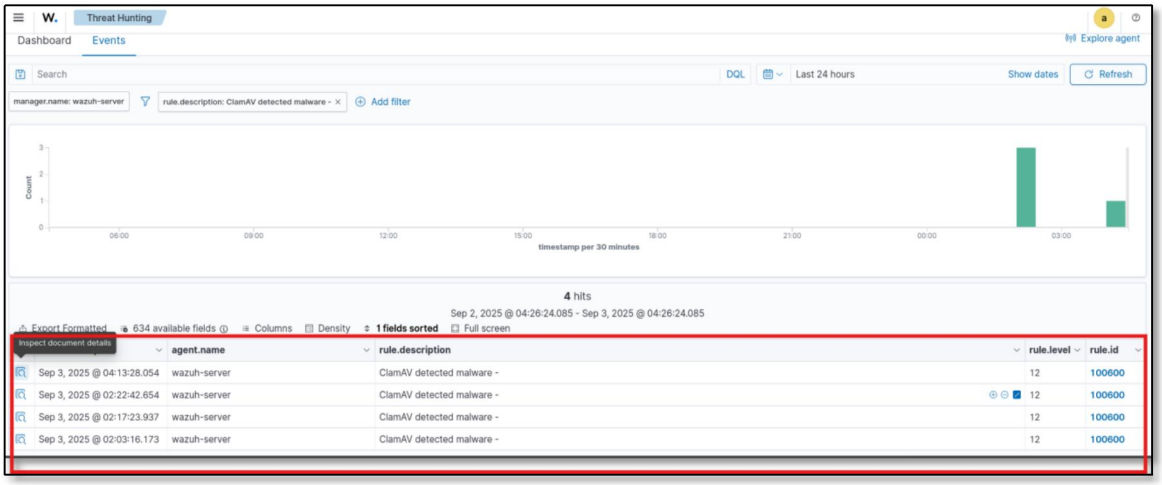
```
1  <!-- Modify it at your will. -->
2
3  <group name="clamav">
4    <rule id="100600" level="12">
5      <decoded_as>clamav_detector</decoded_as>
6      <description>ClamAV detected malware - $(2)</description>
7      <group>clamav,malware,antivirus</group>
8    </rule>
9  </group>
```

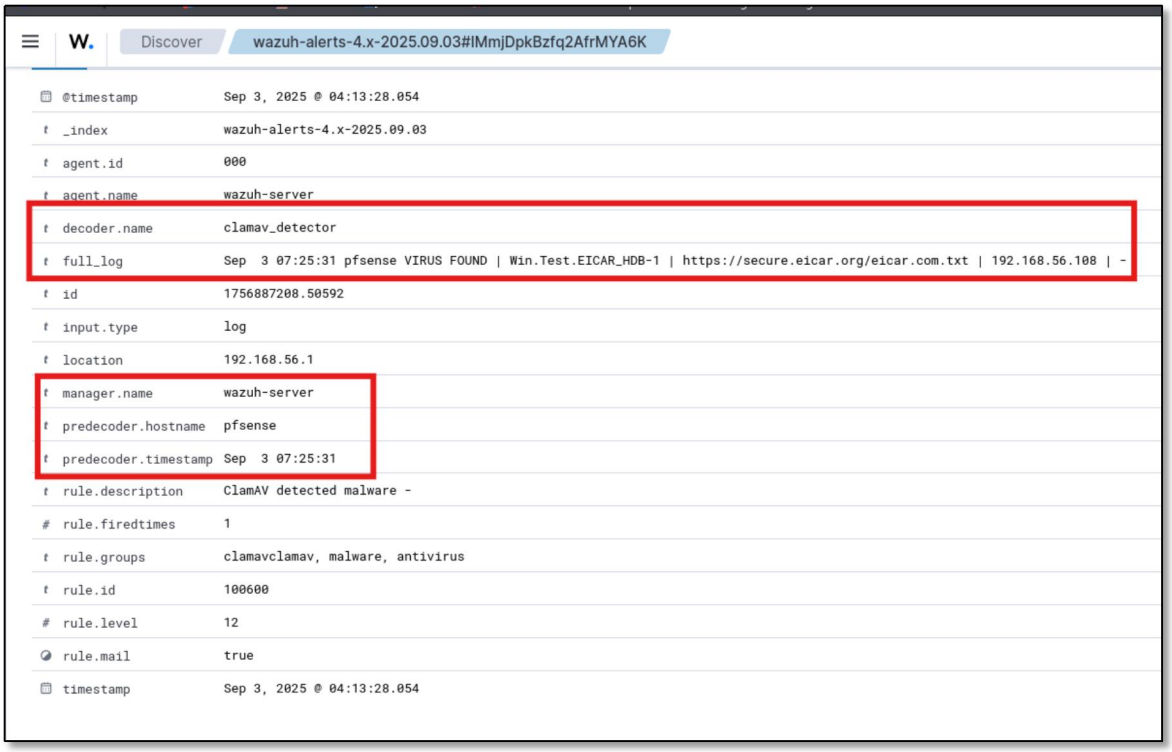
- Restart the Wazuh Manager service to apply changes:

This ensures that Squid and pfSense logs forwarded by **syslog-ng** are decoded correctly and that **custom alerts** are triggered when specific log patterns are detected.

Logs in Wazuh:

- Client attempts to download a malicious file.
- Squid proxy blocks or logs the download attempt.
- Squid sends logs to Wazuh via syslog or directly.
- Wazuh uses custom rules to detect malware-related activity.





Incident Report and Response Plan for Malware Detection Event

- **Date of Report:** September 4, 2025
- **Incident Date:** September 3, 2025
- **Status:** Closed

Executive Summary:

- On September 3, 2025, a network security incident was detected involving an attempt to download a malicious file onto a virtual machine within the lab environment. The download was successfully intercepted and blocked at the network gateway by the pfSense firewall utilizing the Squid proxy and ClamAV antivirus integration. The event was logged and forwarded to the Wazuh SIEM, which generated a high-severity alert, demonstrating the effectiveness of the integrated security monitoring system.
- This document provides a detailed analysis of the incident, including all relevant Indicators of Compromise (IOCs), and outlines the formal Incident Response (IR) Plan executed to manage the event. This plan is presented for review and adoption as a standard operating procedure for future, similar incidents.

Log and Malware Analysis

Log Details Collection:

Comprehensive logs were successfully collected in the Wazuh dashboard, originating from the pfSense firewall after being forwarded by

syslog-ng. The critical alert details are as follows:

Timestamp: Sep 3, 2025 @ 07:25:31

Agent Name: wazuh-server

Rule ID: 100600 (Custom ClamAV rule)

Rule Level: 12 (High Severity)

Rule Description: ClamAV detected malware

Full Log Entry: Sep 3 07:25:31 pfsense VIRUS FOUND | Win.Test.EICAR_HDB-1 | https://secure.eicar.org/eicar.com.txt | 192.166.56.108 | -

Decoder: clamav_detector

Indicators of Compromise and Indicators of Attack

From the collected logs, the following indicators were identified:

Indicators of Compromise (IOCs):

Malware Signature: Win.Test.EICAR_HDB-1

Malicious URL: https://secure.eicar.org/eicar.com.txt

Source IP Address of Client: 192.168.56.108

Indicators of Attack (IOAs):

- An attempt was made to download a file from a known malicious source over the network.
- The user-agent (browser) on the client VM initiated a GET request for a file identified as malware by signature-based detection.

Analysis Report:

- The experiment successfully demonstrated a layered security approach using pfSense and Wazuh. The pfSense firewall, configured with the Squid package as a transparent proxy , intercepted a download request from the client VM (IP: 192.168.56.108). The integrated ClamAV antivirus engine scanned the traffic and identified the EICAR test file as malicious, matching the signature

  Win.Test.EICAR_HDB-1.

- The download was immediately blocked at the gateway, and the client browser was served a "Virus detected!" notification page. Simultaneously, the detection event was logged by Squid's C-ICAP service on pfSense. The syslog-ng service on pfSense forwarded this log entry to the Wazuh manager.Within the Wazuh SIEM, a custom decoder

(clamav_detector) and rule (id: 100600) parsed the incoming log, recognized the malware detection event, and generated a high-severity alert (Level 12). The Wazuh dashboard provided a centralized view of the threat, clearly displaying the timestamp, the malware signature, the source URL, and the client IP address, proving the effectiveness of the integrated system for real-time threat detection and logging.

Incident Response Plan:

This incident response plan is developed based on the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) and is tailored to the malware detection event observed in this report.

IR-1: Preparation:

Tools: Ensure pfSense , Wazuh , Squid Proxy , and ClamAV are operational, updated, and correctly configured.

Roles & Responsibilities: The Security Analyst is responsible for monitoring Wazuh alerts and initiating the incident response process. The Network Administrator is responsible for managing the pfSense firewall and network configurations.

Training: All personnel involved should be trained on this response plan.

IR-2: Detection and Analysis:

Step 2.1: Detection: The incident is detected via a high-severity alert (Rule ID 100600) in the Wazuh dashboard, indicating that "ClamAV detected malware".

Step 2.2: Initial Analysis: The Security Analyst will review the alert details in Wazuh to identify the core IOCs:

Confirm the client IP address (192.168.56.108).

Identify the malware signature (Win.Test.EICAR_HDB-1).

Note the destination URL (https://secure.eicar.org/eicar.com.txt).

Step 2.3: Verification: The analyst will cross-reference the alert by checking the Squid Proxy logs directly within the pfSense web

interface (Status > System Logs > Proxy Filter) to confirm that the download was indeed blocked.

Step 2.4: Scope Assessment: Determine if other devices on the network attempted to access the same URL or download similar malware by querying Wazuh logs for the identified IOCs. In this scenario, the impact is confined to a single, blocked attempt.

IR-3: Containment:

Step 3.1: Immediate Containment: Although the malware was blocked at the gateway, isolate the source VM (192.168.56.108) from the network as a precaution. This can be done by disabling its virtual network adapter in VirtualBox or creating a firewall rule in pfSense to block all traffic from its IP.

Step 3.2: Network Containment: Add the malicious URL (https://secure.eicar.org/eicar.com.txt) and its domain (secure.eicar.org) to a blocklist in pfSense (e.g., using pfBlockerNG or Squid's ACLs) to prevent future connection attempts from any device on the network.

IR-4: Eradication:

Step 4.1: Threat Removal: Since the malware download was blocked, the primary threat never reached the endpoint. Eradication focuses on the client VM.

Step 4.2: System Sanitization: On the isolated VM:

- Clear the browser cache, history, and temporary files to remove any remnants of the download attempt.
- Perform a full antivirus scan on the VM using an up-to-date endpoint security solution to ensure no other malicious files are present.

IR-5: Recovery:

Step 5.1: System Restoration: Once the client VM has been scanned and confirmed clean, reconnect it to the network.

Step 5.2: Monitoring: Closely monitor the traffic from the restored VM and the entire network for any unusual activity or subsequent alerts related to the incident. Monitor Wazuh and pfSense logs for a 24-hour period.

Step 5.3: Normal Operations: If no further malicious activity is detected, the incident is considered resolved, and the system is returned to normal operations.

IR-6: Post-Incident Activity (Lessons Learned):

Step 6.1: Reporting: Compile a detailed incident report summarizing the detection, actions taken, and resolution. The report should include all identified IOCs and IOAs.

Step 6.2: Review and Improvement: Hold a post-incident meeting to review the effectiveness of the response plan. Discuss potential improvements, such as:

- Automating the blocking of malicious URLs based on Wazuh alerts.
- Refining Wazuh rules for better fidelity and faster detection.
- Evaluating the need for additional security layers (e.g., endpoint detection and response - EDR).

Step 6.3: Documentation Update: Update the incident response plan, security policies, and system configurations based on the lessons learned.

Thanks:

Muhammad Jarrar Hassan

TASK#4 : Malware Breaches Report

Malware Breaches:

Objectives:

- **Research and create a report on recent or current malware attacks, breaches, and the well-known companies affected by these incidents.**
- **Instructions:**

1. Research at least 10 major breaches that occurred recently.
2. Analyze the details of each breach, focusing on the nature of the attack, the company affected,
3. and the aftermath.
4. Read articles from credible sources and summarize the findings.
5. The report should be clear, concise, and insightful.

1) Change Healthcare (UnitedHealth) — Ransomware + patient data exposure

Date / discovery:

February 2024 (escalated disclosures through 2024–Jan 2025).
Nature:

Ransomware attack (AlphV / BlackCat reportedly involved); attackers used compromised credentials and insufficient MFA on a server; double-extortion concerns.
Affected:

Change Healthcare (UnitedHealth subsidiary); ultimately reported affecting ~190M people (largest U.S. healthcare breach).
Aftermath:

Massive operational disruption for claims processing; UHG reported large remediation costs and paid a reported ransom ($22M disclosed by some reports); ongoing breach notifications and Congressional attention.
Key lesson:

Enforce MFA everywhere, isolate critical claim-processing systems, assume credential theft + double-extortion; rebuild and segmentation are often required after large ransomware incidents.

2) National Public Data (NPD) — Massive data-broker leak (reported ~2.9B rows)

Date / discovery:

Breach activity traced to April 2024; public confirmations mid-Aug 2024.
Nature:

Data-broker repository exposed/stolen (public-record aggregation) — extremely large volume of PII (names, addresses, SSNs reported in analysis).
Affected:

Potentially hundreds of millions (reports of ~2.9 billion rows; legal actions followed).

Aftermath:

Class-action lawsuits, company bankruptcy filings, major risk to identity theft victims; remediation limited since historical public record data are hard to revoke.

Key lesson:

Data brokers holding aggregated PII are high-value targets — minimize data retention, encrypt strongly, monitor dark web for exfiltrated sets.

3) Snowflake customer environment compromises (mid-2024)

Date / discovery:

June 2024 (public reporting through late 2024).

Nature:

Attackers used stolen credentials (from infostealer malware / poor credential hygiene) to access customer Snowflake accounts and exfiltrate datasets — used for extortion/sales.

Affected:

Many Snowflake customers (reported victims included AT&T, Ticketmaster/Live Nation, LendingTree, Advance Auto Parts, Neiman Marcus, others).

Aftermath:

Data exfiltration and ransom/blackmail demands; arrests and indictments later for individuals tied to extortion; highlighted cloud misconfiguration and lack of enforced MFA.

Key lesson:

Cloud data platforms require enforced strong identity controls (MFA, credential hygiene, least privilege, session monitoring); endpoint infostealers are common initial vectors.

4) United Natural Foods Inc. (UNFI) — Operational cyberattack (June 2025)

Date / discovery:

Detected June 5, 2025.
Nature:

Unauthorized activity on internal systems (likely ransomware-type incident causing outage); UNFI took systems offline.
Affected:

UNFI (major grocery distributor) — disruption cascaded to retailers (Whole Foods and others) causing temporary shortages and order/delivery delays.
Aftermath:

Sales/earnings impact; stock dip; restoration of systems over weeks; supply-chain attention.
Key lesson:

Cyber incidents at distributors produce real-world supply chain effects — business continuity planning and alternate logistics channels are critical.

5) Ivanti Connect Secure & other Ivanti products — Zero-days exploited (2024–2025)

Date / discovery:

Multiple waves (notable exploitation mid-Dec 2024 → Jan 2025; continued advisories through 2025).
Nature:

Critical VPN / EPMM zero-days exploited in the wild by threat actors, enabling remote unauthenticated RCE and access to internal networks.
Affected:

Organizations with exposed Ivanti appliances; many instances remained unpatched leading to real compromises.

Aftermath:

Emergency mitigations, broad scanning/attacks, and numerous incident responses. Demonstrated patching lag risk for network appliances.

Key lesson:

Network appliances (VPNs, gateways) are high-value attack vectors — prioritize patching, implement network segmentation, MFA, and compensating controls.

6) Microsoft SharePoint "ToolShell" (July 2025) — chained zero-day exploitation

Date / discovery:

Exploitation observed in July 2025 (reports trace exploitation back to early July).

Nature:

Zero-day chain (ToolShell) targeting on-prem SharePoint servers, allowing remote code execution, webshells, credential theft and potential ransomware deployment. CISA and Microsoft published analyses/advice.

Affected:

Hundreds of organizations globally (government, energy, education, and private sector reported).

Aftermath:

Emergency patches and guidance; evidence of malware (webshells, key-stealers) used in follow-on activity; high urgency for on-prem customers.

Key lesson:

On-prem legacy platforms can present "wormable" or broadly exploitable surface even in an era of cloud; isolate, patch, rotate keys, and hunt for webshells.

7) Kettering Health — Interlock ransomware (May 2025)

Date / discovery:

Attack began May 20, 2025 (public disclosures late May–June).
Nature:

Interlock ransomware: data exfiltration + encryption; Epic EHR access impacted, phone lines and other services disrupted.
Affected:

Kettering Health system (14 hospitals + many clinics) — cancellation of elective procedures, backlog, manual workarounds.
Aftermath:

Staged restoration of EHR systems, patient notice and monitoring, law enforcement involvement; FBI/CISA advisories about Interlock.
Key lesson:

Healthcare remains a high-priority target; robust backups, offline recovery, and tabletop response plans for patient care continuity are vital.

8) Optima Tax Relief — Chaos ransomware (May–June 2025)

Date / discovery:

May–June 2025 (data leakage/claims in June).
Nature:

Double-extortion Chaos ransomware — threat actors claimed ~69 GB stolen (tax documents, SSNs, bank details).
Affected:

Optima Tax Relief clients — sensitive tax and personal financial documents exposed.

Aftermath:

Notifications to affected individuals and investigations; reputational and legal exposure.

Key lesson:

Firms handling highly sensitive PII (tax, finance) must treat data protection as top priority (encryption at rest, least privilege, EDR + logging).

9) DaVita — Interlock ransomware (Mar–Apr 2025)

Date / discovery:

March–April 2025 (public disclosures in April/May).

Nature:

Interlock ransomware exfiltrated patient data (PII and clinical records) across the dialysis provider.

Affected:

DaVita patients (nearly 1M records reported in some coverage); state-level notifications for many patients.

Aftermath:

Notifications, credit monitoring offers for affected individuals, forensic investigation and remediation.

Key lesson:

Recurrent groups (Interlock here) target multiple healthcare entities with similar TTPs — detecting early signs of their artifacts and blocking delivery vectors is crucial.

10) The North Face / Scattered Spider — credential stuffing (June 2025)

Date / discovery:

June 2025 (reports compiled in June).
Nature:

Credential-stuffing / account takeover incidents (attacker used reused credentials obtained elsewhere); resulted in ~3,000 customer accounts exposed in one wave.
Affected:

Retail customer accounts — names, addresses, purchase history and possibly financial metadata.
Aftermath:

Account resets, customer notices; emphasizes the threat of credential reuse and the need for rate-limiting & MFA for customer accounts.
Key lesson:

E-commerce players must adopt strong customer auth (MFA, password hygiene encouragement), bot/rate-limiting, credential-stuffing detection.

Sources (selected, credible reading):

- UnitedHealth / Change Healthcare coverage and HHS updates. Reuters+2AP News+2
- National Public Data reporting (The Verge, Troy Hunt analysis). The Verge+1
- Snowflake breach analyses and community reporting. Wikipedia+1
- UNFI cyber incident — Reuters, CyberScoop. Reuters+1
- Ivanti zero-day reporting (Mandiant/Google Cloud blog, CyberScoop). Google Cloud+1
- Microsoft SharePoint "ToolShell" (Microsoft blog, news outlets). Microsoft+1
- Kettering Health and Interlock reporting (official Kettering notices, HIPAA Journal). Kettering Health+1
- Optima Tax Relief / Chaos ransomware reporting. SC Media+1
- DaVita / Interlock reporting. TechRadar
- Retail credential stuffing (North Face) and other monthly incident trackers. CM Alliance