Blocking Malware Download and Incident Response Plan

Report Task # 03 (Team IOTA)

SUBMITTED TO :-

Mr. Zain

SUBMITTED BY :-

Nasir Sharif

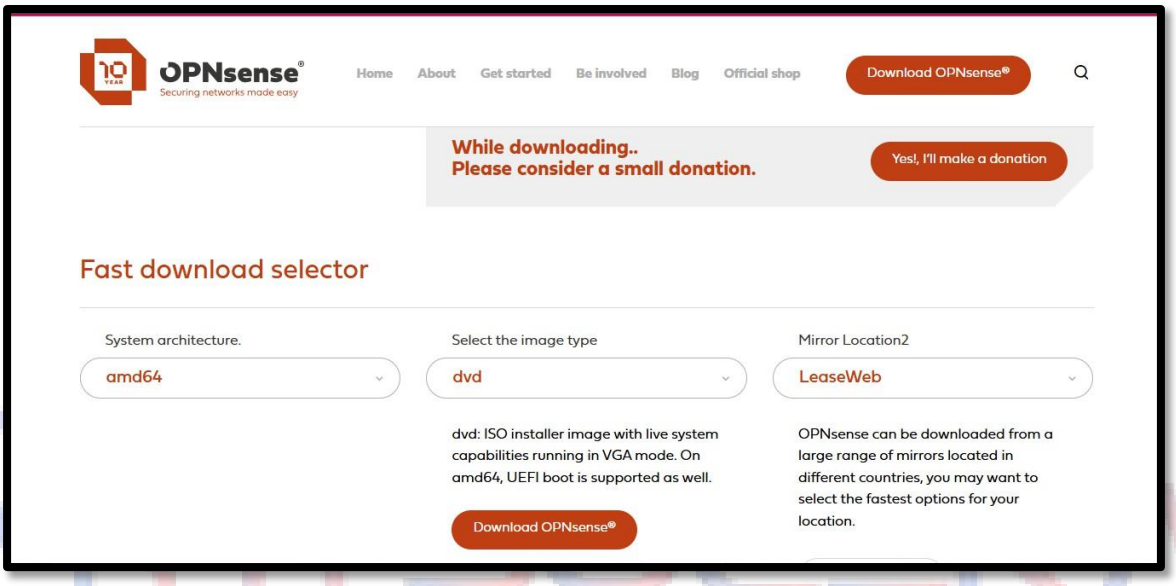
National University of Modern Languages H-9 Islamabad

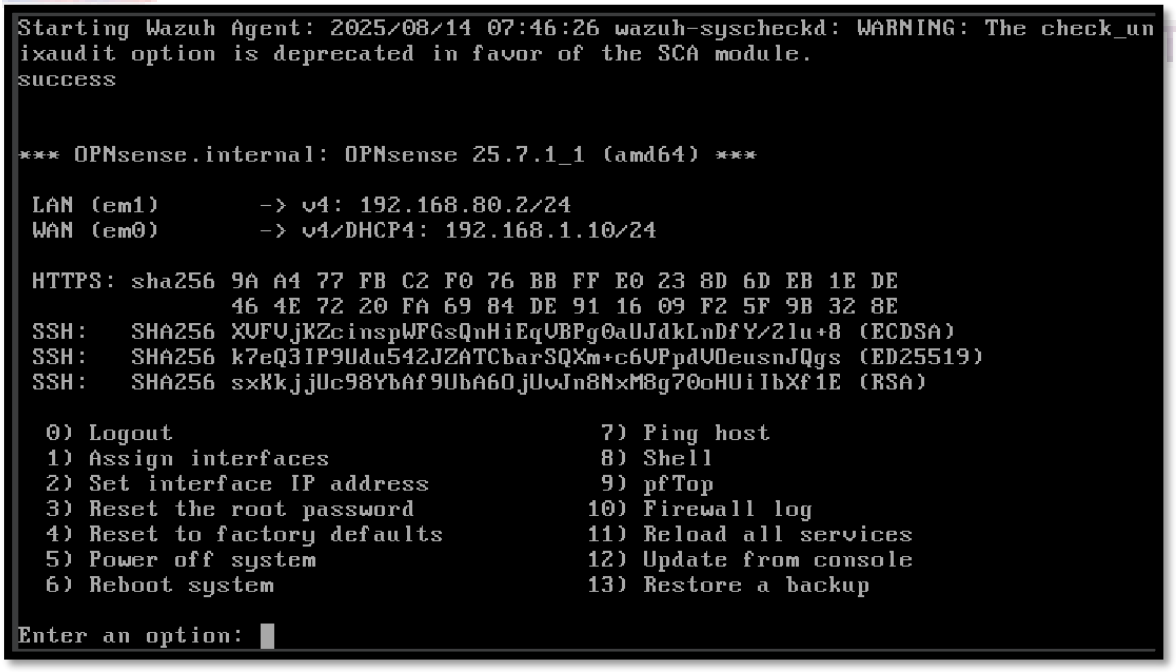
September 02, 2025

1. Firewall installation and setup

I am downloading a software-based firewall named "OPNsense" for this task. Following are the steps to download it:

- Go to the official site of OPNsense. https://opnsense.org/download/
- Select system architecture: amd64, image type: dvd and mirror location: LeaseWeb. Then click on download.





- Now, we have to set the interfaces and IP addresses.
- Type 1 and press enter.
- Set interfaces:

For WAN interface em0 For
LAN interface em1

Now you can access the web GUI using LAN IP.

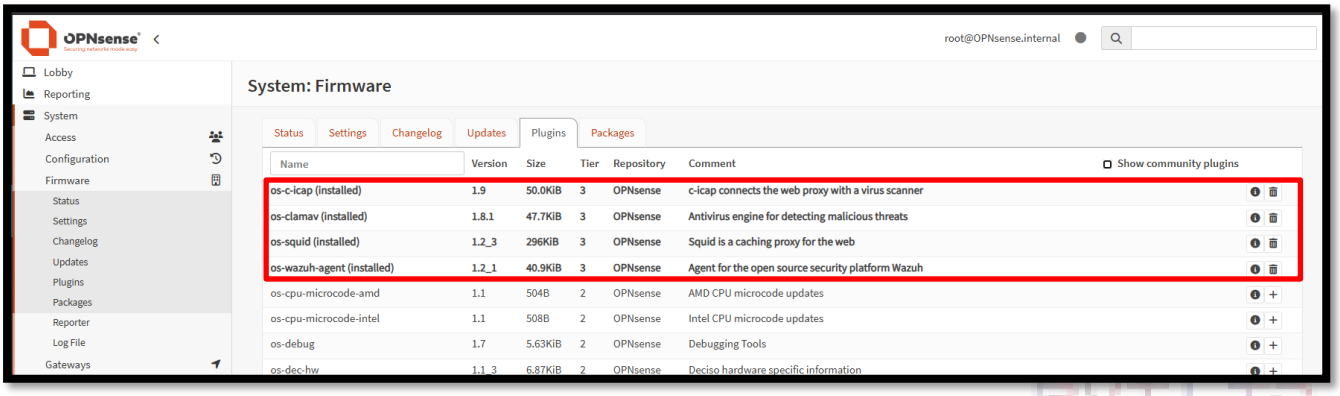
Firewall is now successfully installed.

2. Setting up the firewall:

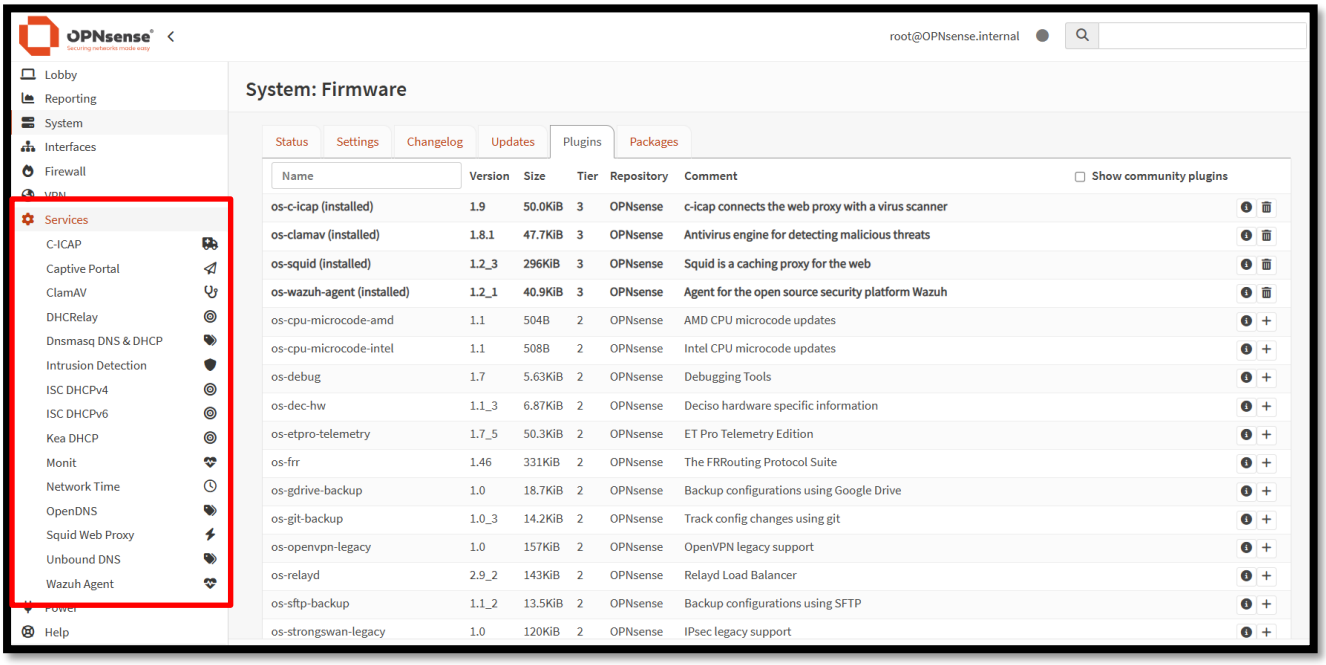
2.1 Installing required Plugins on Firewall:

To install them, follow the steps below:

- Go to system -> firmware -> plugins.
- Search squid and download os-squid plugin.
- Search clamav and download os-clamav plugin.
- Search c-icap and download os-c-icap plugin.

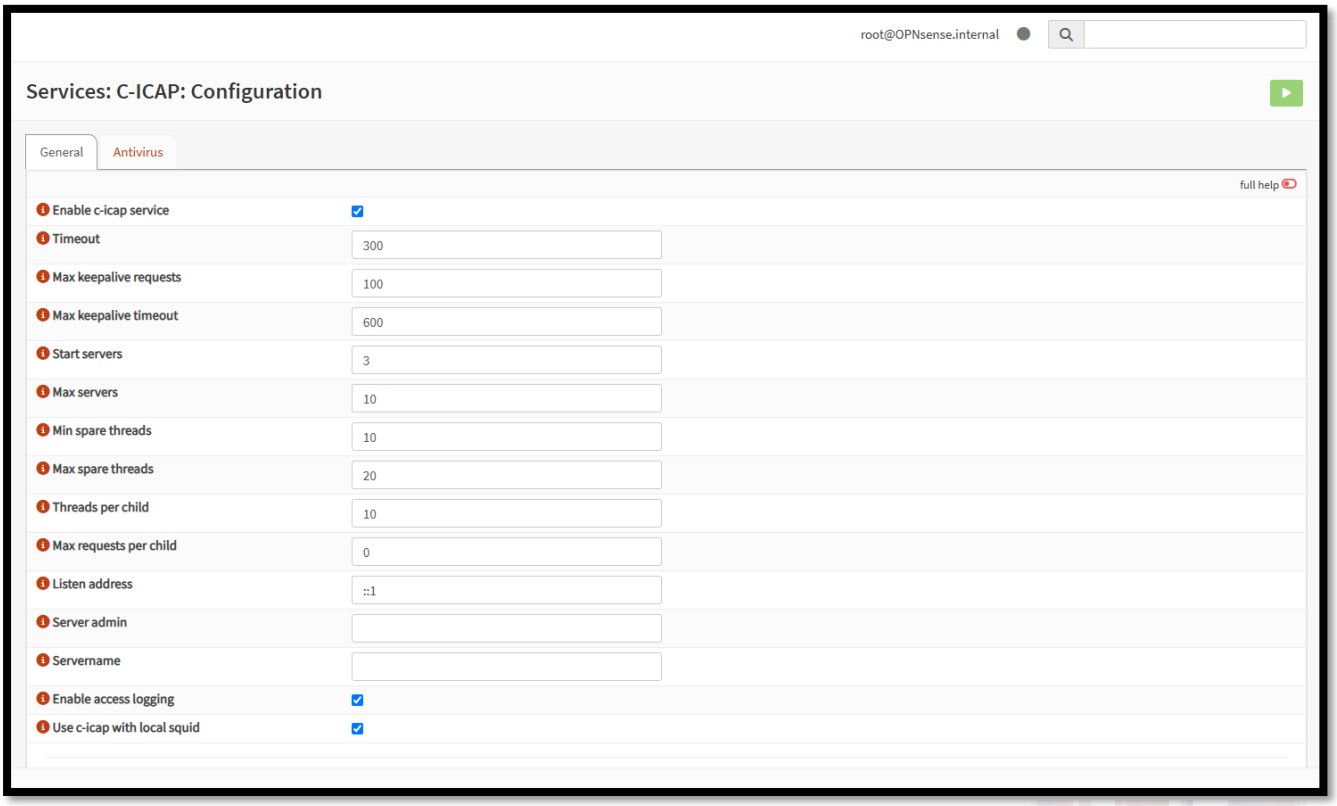


- After downloading, these plugins will be available in services tab.

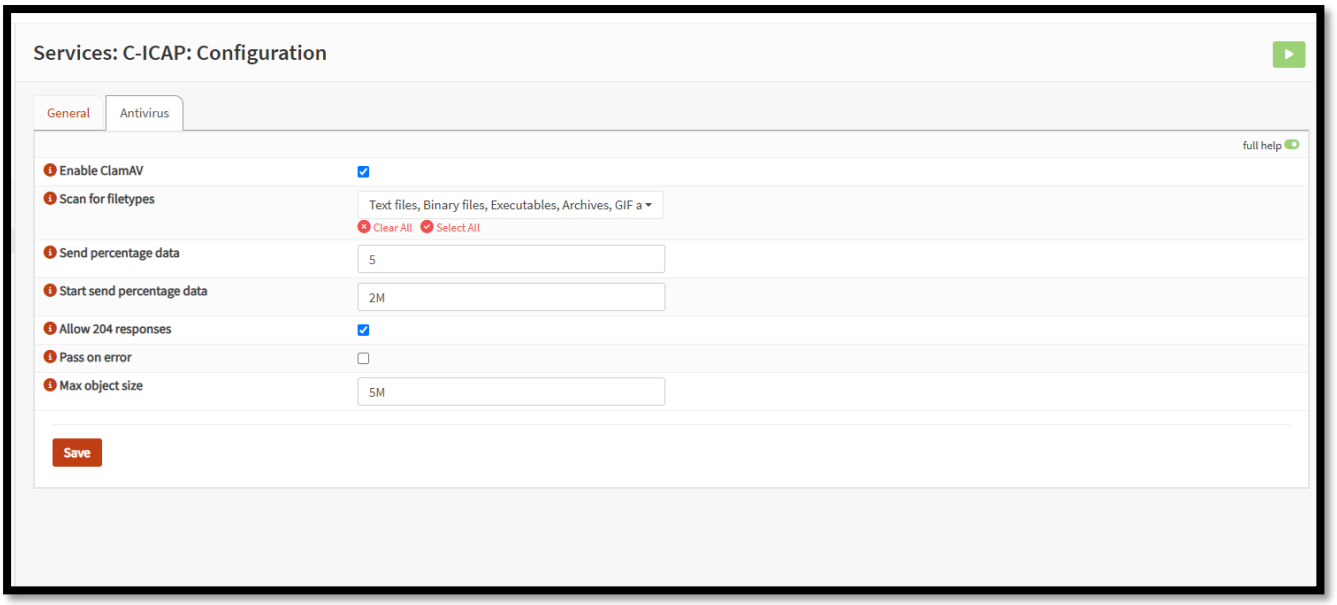


2.2 Configuring c-icap:

- Go to service -> c-icap -> configuration.
- Click on general.
- Enable c-icap services, access logging and use c-icap with local squid.

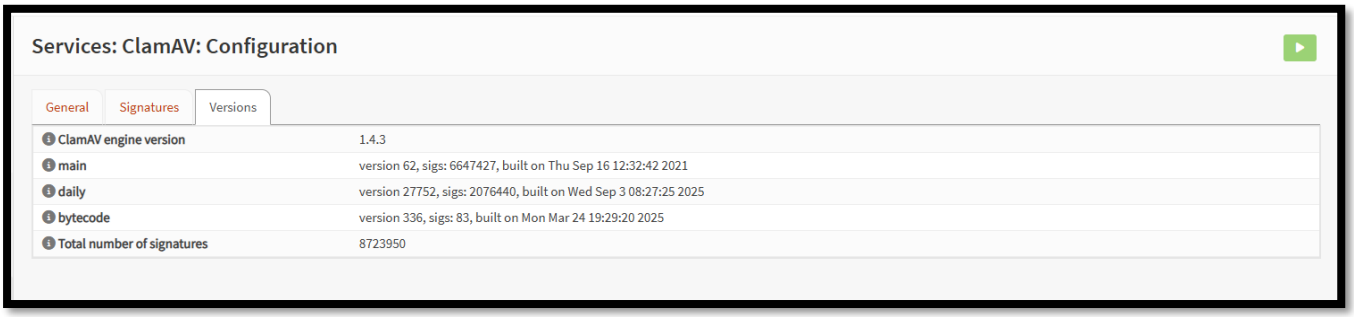


- Click on antivirus and enable ClamAV. Then save it.

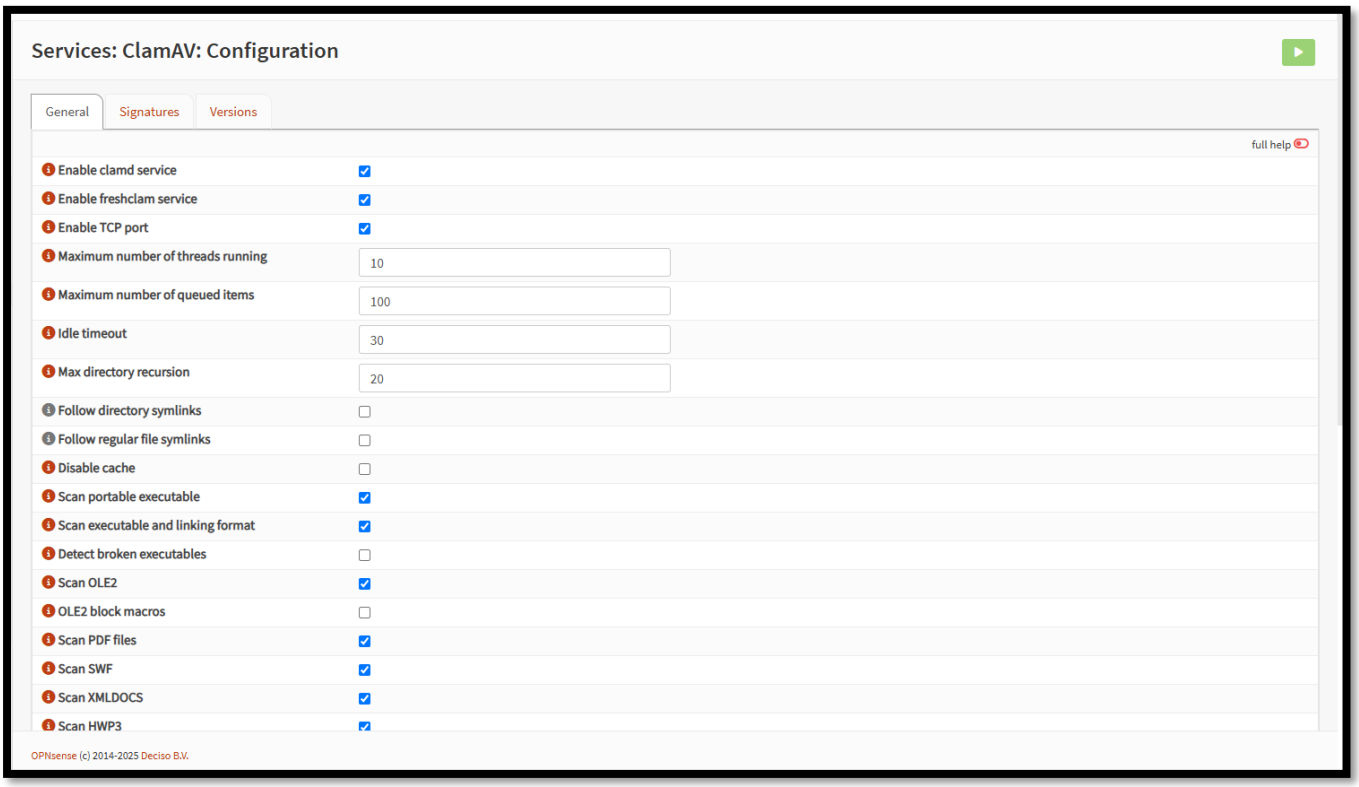


2.3 Configuring ClamAV:

- Go to services -> ClamAV -> configuration.
- Download signatures. It will take several minutes. After downloading, you can verify it by clicking on versions tab.



- Then click on general and enable clamd service, freshclam service, TCP port.



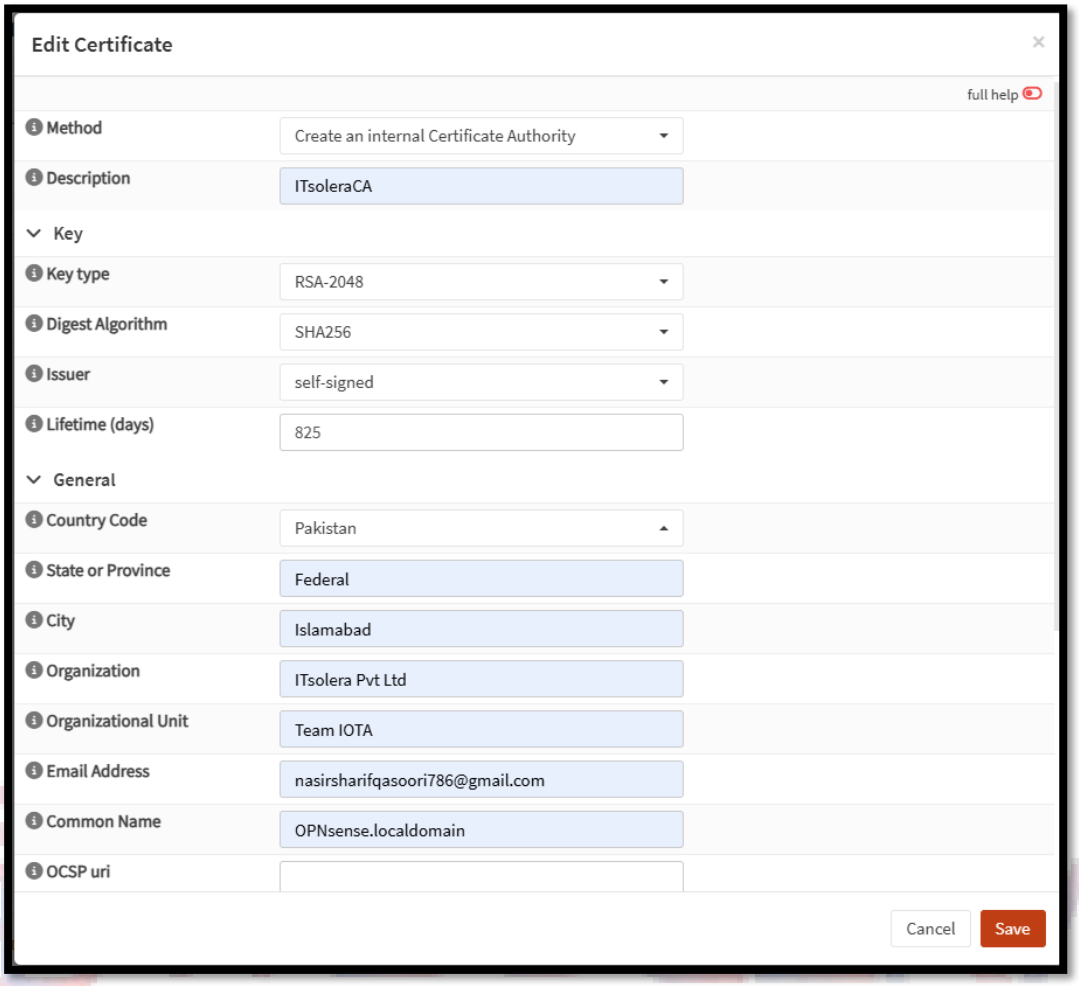
2.4 Configuring Squid proxy:

To configure squid proxy and make it to read HTTP, HTTPS traffic of our browser, first we need to create a self-signed certificate and integrate it with our browser and proxy.

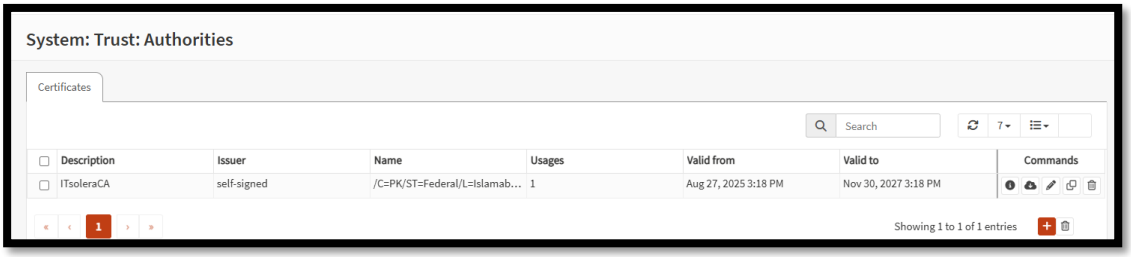
2.5 Creating and integrating self-signed certificate:

- On firewall GUI, go to system -> trust -> authorities.
- Click on '+' icon to create a new certificate.

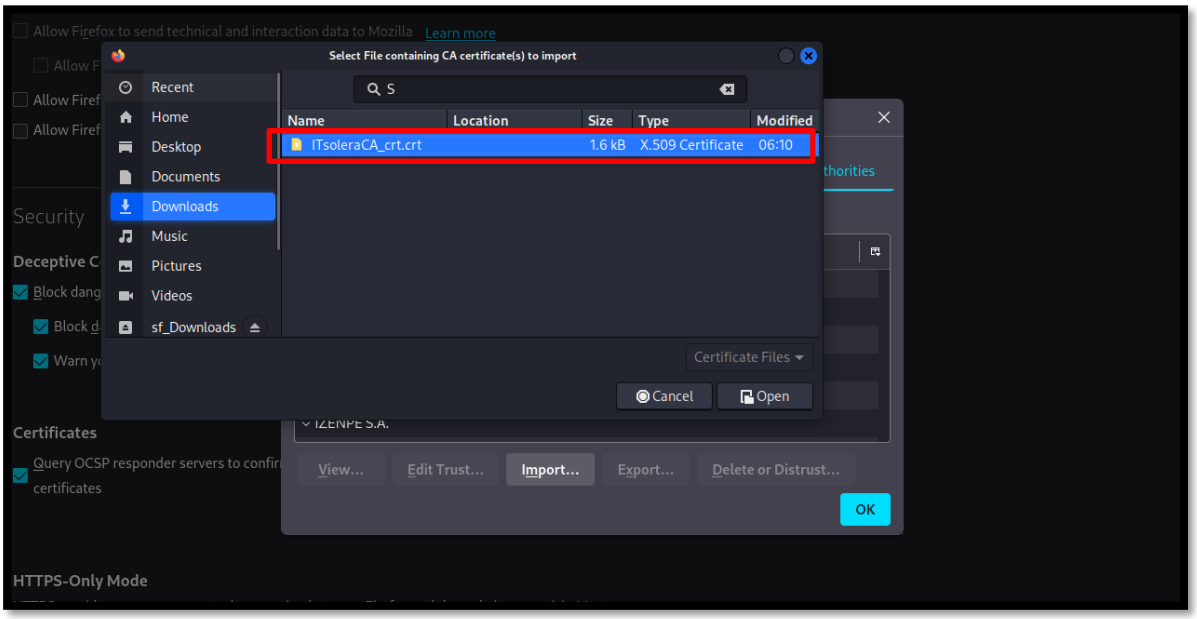
Enter the following and click on save.



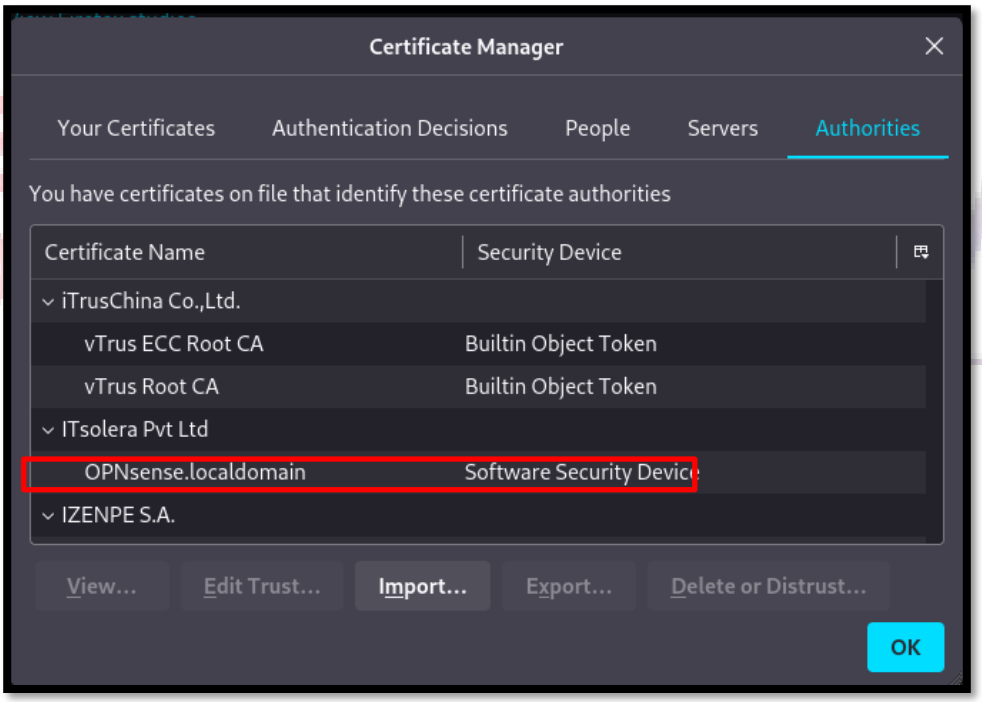
Then it will appear in system -> trust -> authorities.



Click on download.
While downloading, select type ‘certificate’.
Now send this certificate to your test device.
Then open browser on test device.
Go to settings -> certificate manager -> trusted root certificates.
Click on import.
Select the file and click on next.

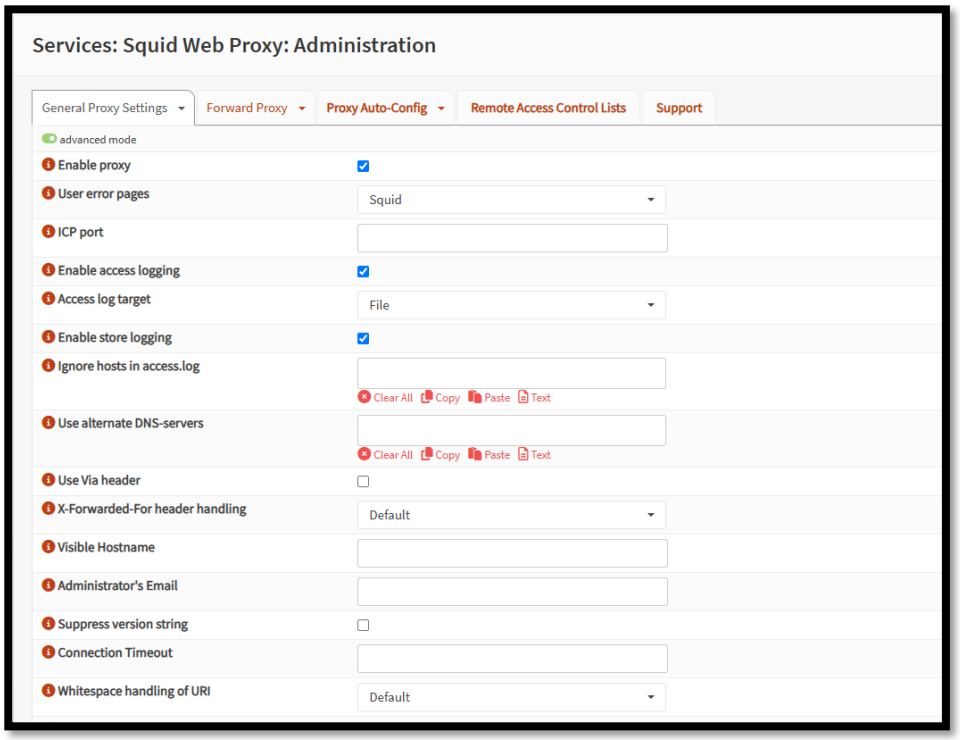


Then it will appear in certificate manager -> trusted root certificates.



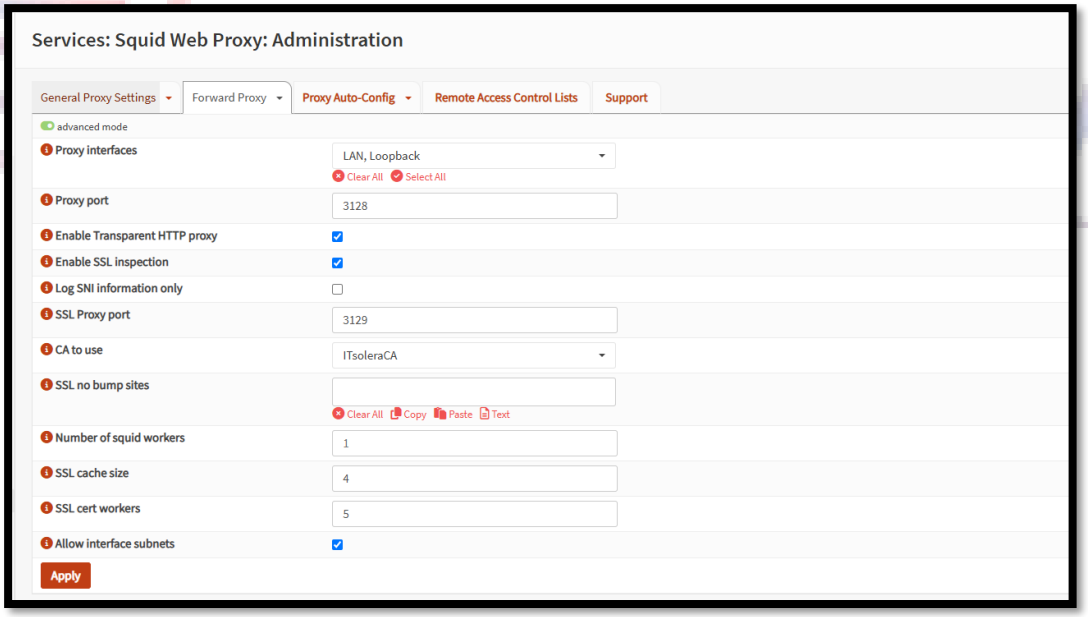
2.6 Configuring and integrating in Squid proxy:

- Go to services -> squid web proxy -> administration.
- Click on general proxy settings.
- Enable proxy. Then click on save.

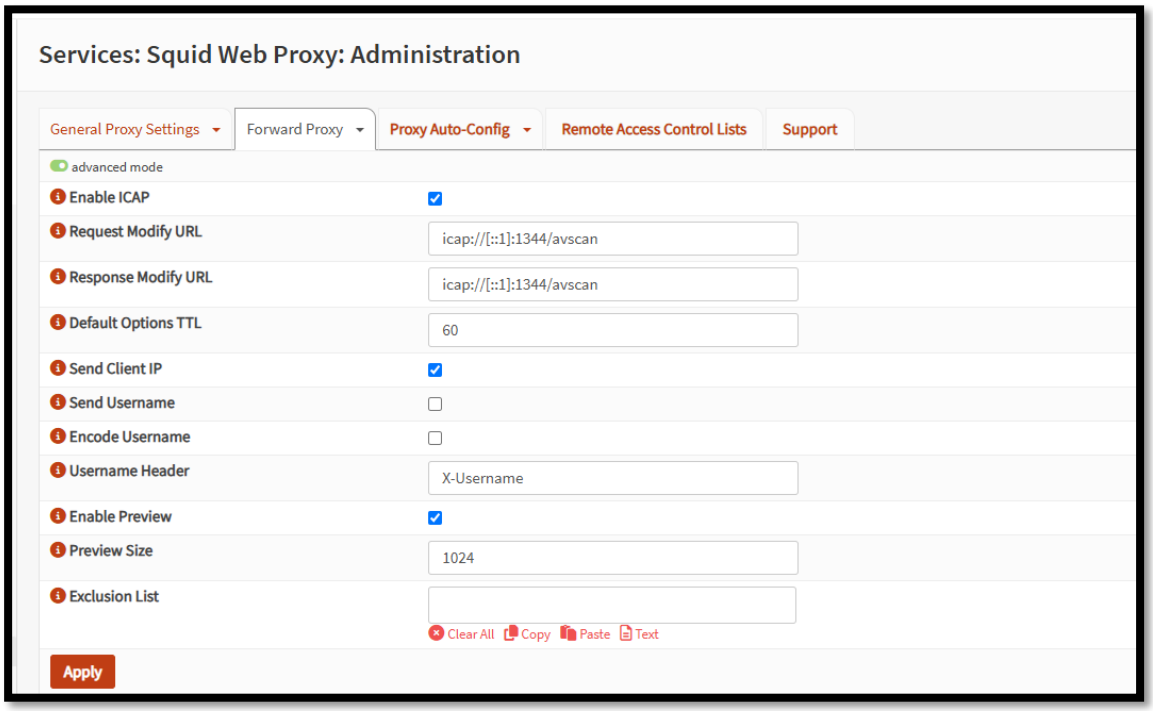


- Click on forward proxy.
- Select your required interfaces.
- Enable transparent HTTP proxy, SSL inspection.
- Under 'CA to use' select the self-signed certificate created earlier.

- Click on apply.

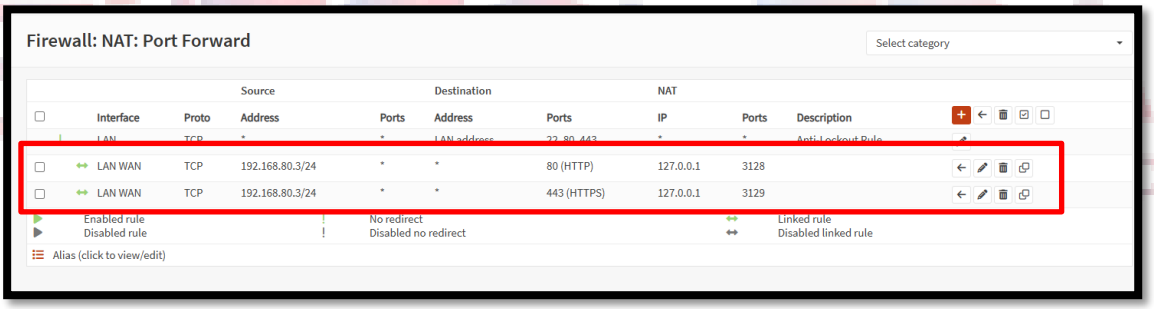


- Click on the arrow near forward proxy and select ICAP settings.
- Enable ICAP and enter request modify URL and response modify URL as shown.



- Click on apply.

  To redirect traffic from test PC to the proxy, we have to make two NAT port forwarding rules, one for HTTP and one for HTTPS traffic.



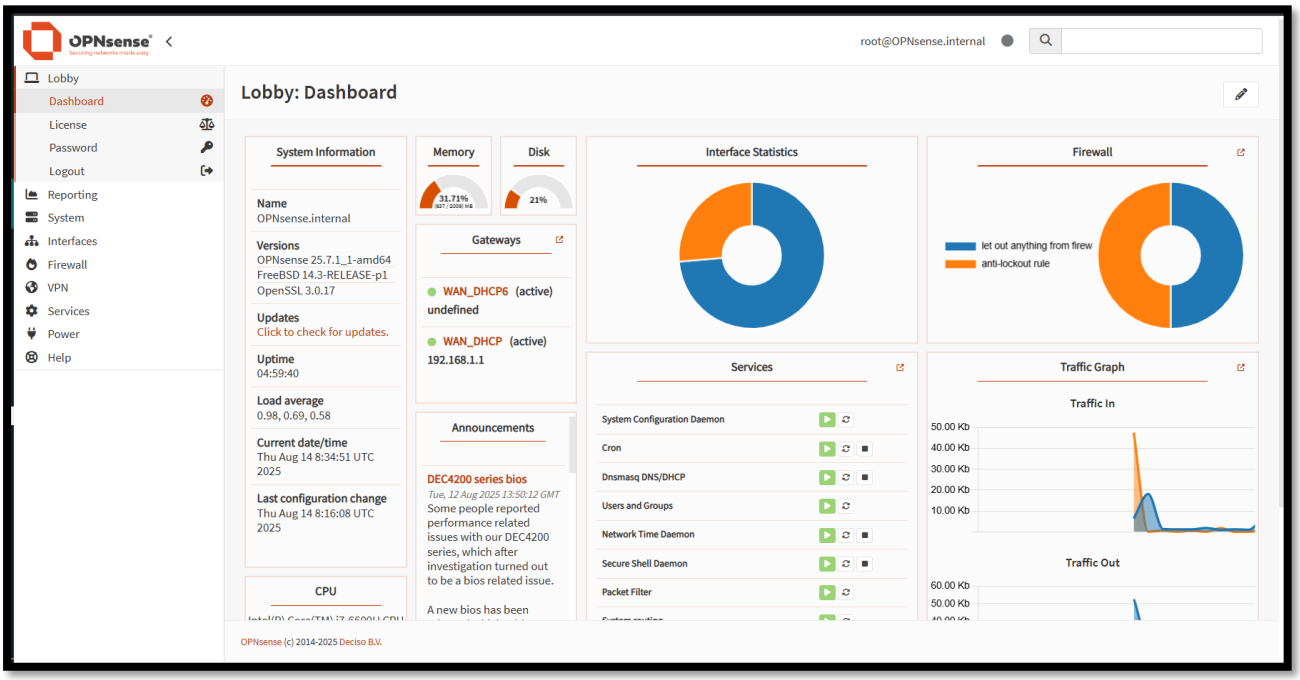
  - Select **protocol TCP**
  - **Source address** is the IP address of the test PC
  - **Destination address**: any, ports 80 and 443 (one for each rule)
  - **Redirect IP** is the loopback IP and redirect ports is 3128 for HTTP rule and 3129 for HTTPS rule

3. Configuring Wazuh To Receive Logs:

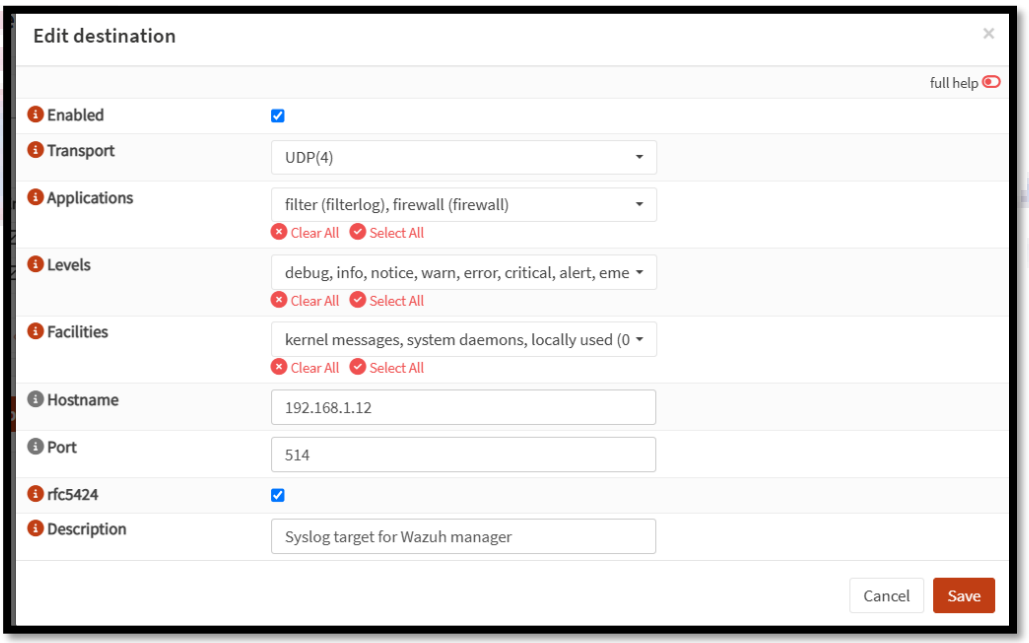
To integrate the firewall with Wazuh to see the logs, there are two options to do so:

Option: 1) Remote logging:

- Go to firewall Web GUI.



- Then on system -> settings -> logging -> remote, create a new destination to send remote logs and enter the following:



- Here hostname is Wazuh manager IP that is (192.168.1.12) and port is 514 through which it gets logs from firewall.

Now, we have to do some configuration on Wazuh manager.

- Open Wazuh dashboard.
- Go to server management -> settings.
- Click on edit configuration.

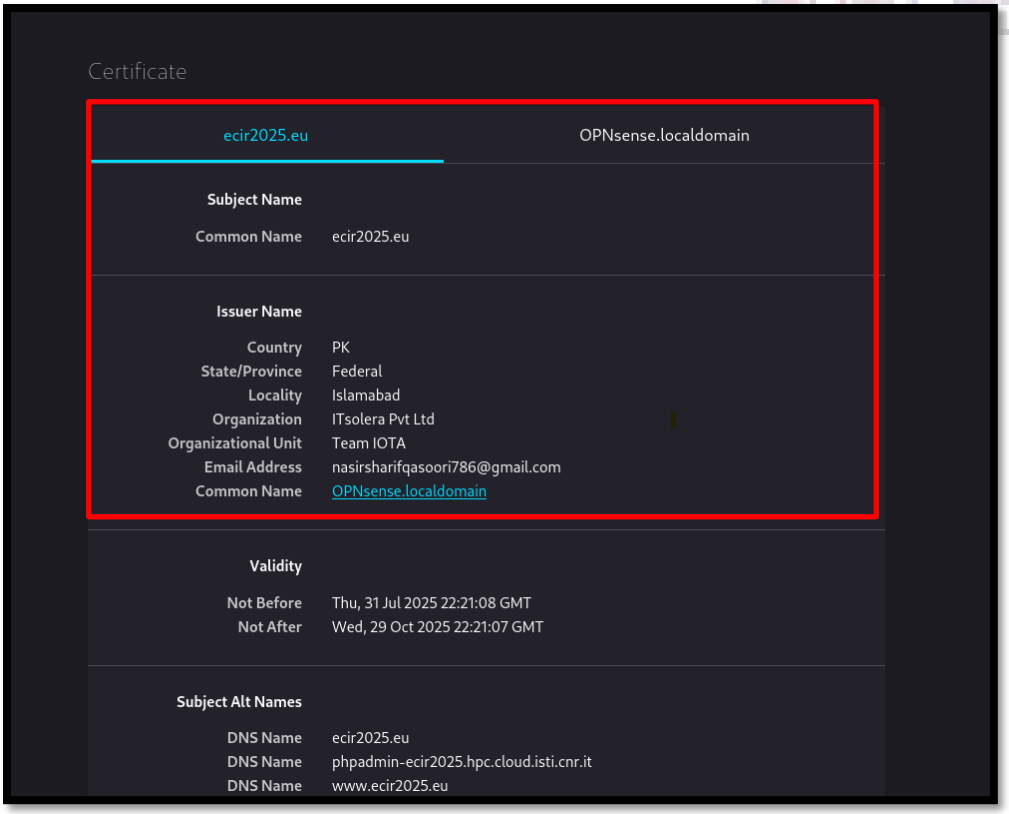
- Save it and restart Wazuh manager.

4. Testing:

Check if browser shows your certificate:

After you have integrated certificate on your browser and setup the proxy, verify if certificate is Displayed on your browser.

- Open your browser on test machine.
- Search any website.
- Open it.
- On top left corner next to URL bar.
- Click on the lock icon and check certificate detail.
- It should show this:



4.1 Downloading test malware and checking logs on firewall:

To download test malware, there are many sources on like EICAR, IKarussecurityetc.

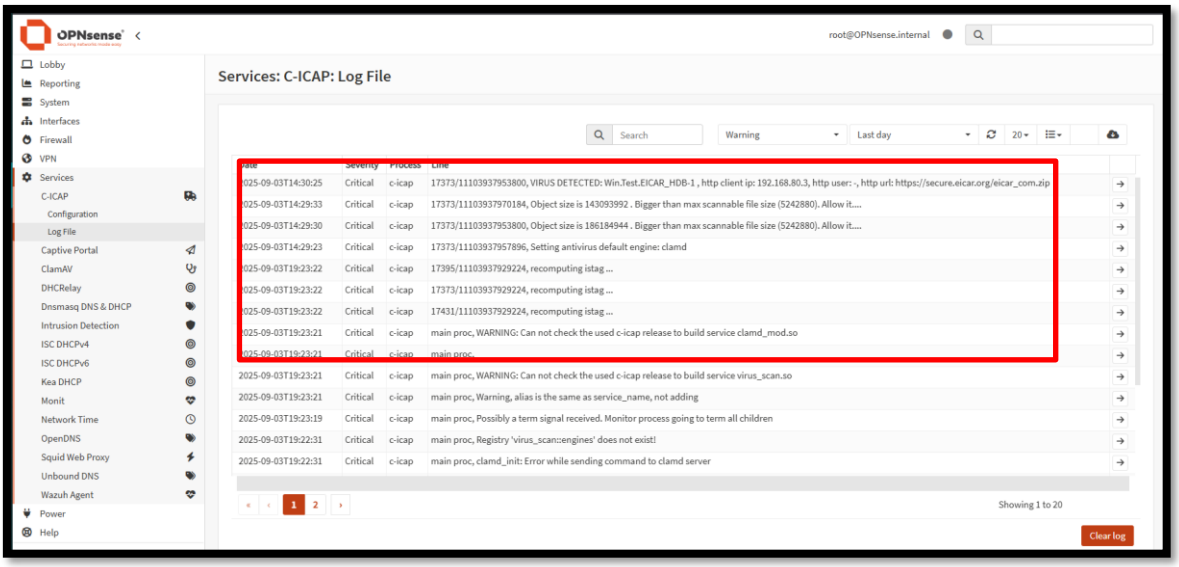
Source: 1

On the test machine, open browser and search EICAR. (Download any one of these for testing)

- Click on download. (I downloaded EICAR.COM2-ZIP).
- When you try to download it, the firewall will block it if configurations are done properly.

- This will also generate logs on firewall.
- Open firewall GUI. Go to services -> C-ICAP -> log file.

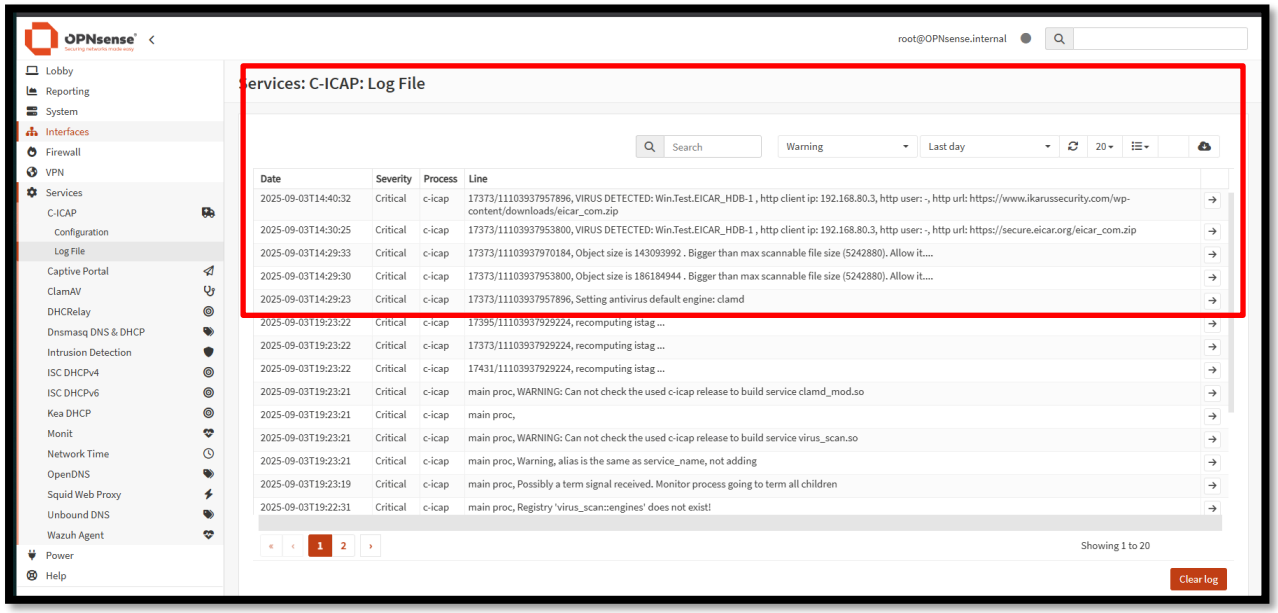
- The following log is shown:



Testing: The another File from Ikarussecurity.com

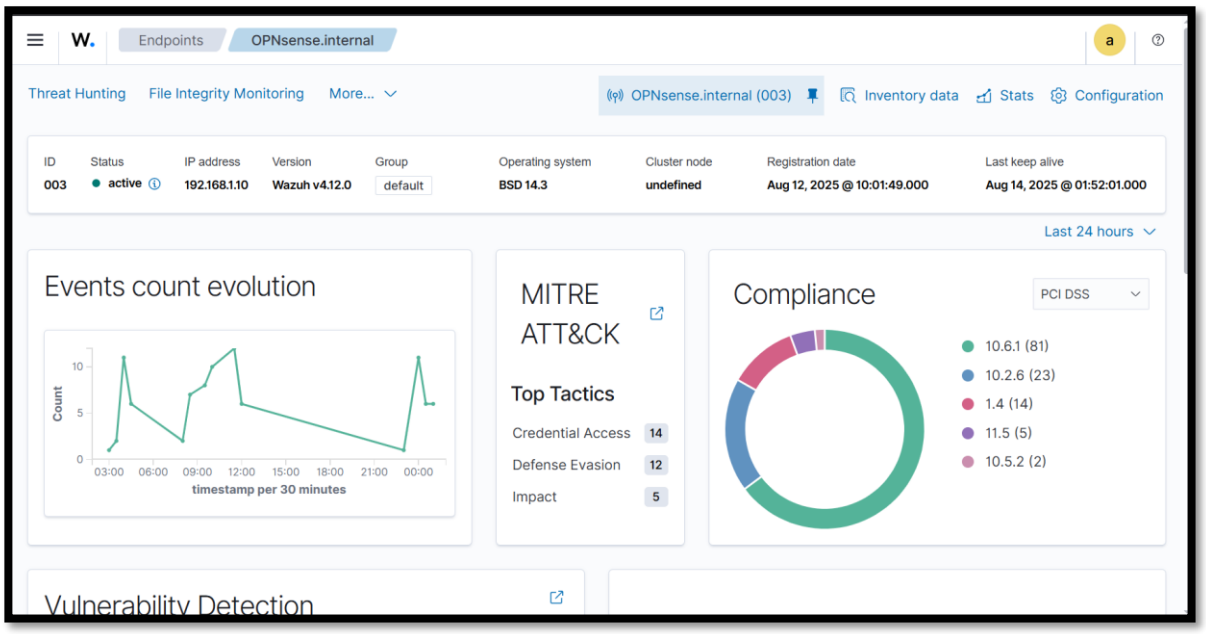
- When you try to download it, the firewall will block it if configurations are done properly.

- This will also generate logs on firewall.
- Open firewall GUI. Go to services -> C-ICAP -> log file.



4.2 Viewing logs on dashboard:

- After all the above configurations, download the malware files again to generate logs.
- Open Wazuh dashboard.
- Go to explore -> discover.
- Apply filters as needed (by IP, or virus name).
- Logs will appear on dashboard.



Forwarding & Decoding OPNsense c-icap Logs into Wazuh

1. Log Source Identification

- The OPNsense firewall was configured with the **c-icap service** (integrated with ClamAV) for malware scanning.
- All virus detection and blocking events were being logged locally on OPNsense.

2. Log Forwarding Configuration

- Used **Syslog-ng / rsyslog** on OPNsense to forward logs to the Wazuh Manager.
- Configured **remote log forwarding** (UDP/TCP, usually port 514) with proper formatting to ensure c-icap messages were transmitted.
- Ensured logs included critical fields: timestamp, event type, client IP, URL, and detection result.

3. Wazuh Manager Integration

- On the Wazuh side, the manager was configured to **listen for logs** from OPNsense's IP.
- Added the OPNsense node in the **ossec.conf** file under the <remote> section for proper agentless log collection.

4. Decoding c-icap Log Format

a) Since raw c-icap logs have a specific format, a **custom Wazuh decoder** was created.

b) The decoder extracted important fields:

c) **Virus Name / Signature** (e.g., Win.Test.EICAR_HDB-1)

d) **Client IP Address** (192.168.80.3)

e) **Requested URL** (e.g., https://secure.eicar.org/eicarcom2.zip)

f) **Event Type** (VIRUS DETECTED)

5. Rule Creation for Alerts

a. Wazuh rules were implemented to **match decoder output**.

b. Rules categorized events as **High Severity** when a real trojan/malware was detected and **Low Severity** when only the EICAR test file was detected.

c. Mapped detections to **MITRE ATT&CK techniques** such as:

   i. **T1566 (Delivery via Malicious Files)**

   ii. **T1071 (C2 over HTTPS)**

6. Visualization on Wazuh Dashboard

a. Once decoded, logs appeared in **structured JSON format** in Wazuh.
b. Dashboards were built to show:
c. Malware detections by **signature**
d. Malware detections by **client IP**
e. Timeline of attempted downloads
f. Severity levels (EICAR test vs. real malware)

7. Validation

a. Tested by downloading the **EICAR test file** and a **sample trojan (ELF)**.
b. Confirmed events were blocked at OPNsense and forwarded correctly to Wazuh with proper parsing and alerting.

Malware Download and Incident Response Analysis Report

1. Overview

- **Date of Incident:** September 02, 2025
- **Time Frame:** 15:07:41 – 15:09:47
- **System:** OPNsense Firewall (c-icap with ClamAV)
- **Host IP (Affected Client):** 192.168.80.3
- **Reported By:** c-icap Antivirus Service
- **Event Type:** Virus Detection and Mitigation (Malware Download Attempt)
- **Affected Systems:** Local network client device with IP 192.168.80.3

2. Incident Summary

On **September 02, 2025**, two malicious files were downloaded using separate links. Both attempts were intercepted and blocked by the **c-icap antivirus service on the OPNsense firewall**.

- The first detection corresponded to **Win.Test.EICAR_HDB-1**, a harmless test file used globally to validate antivirus functionality.
- The second detection was **Win.Test.EICAR_HDB-1**, an **actual malware sample** targeting Unix-based systems.

The malicious attempts originated from a client device (**192.168.80.3**) attempting to download files via **HTTPS**.

- While the EICAR test file is benign, the Unix Trojan represents a **genuine security risk**, capable of enabling remote access, persistence, or data exfiltration if executed.

Key Observation:
The firewall correctly identified and blocked the files before they entered the protected network, demonstrating effective **Deep Packet Inspection (DPI)** and **inline antivirus scanning.**

3. Indicators of Compromise (IOCs)

Malware Signatures Detected:

- **Win.Test.EICAR_HDB-1** → Harmless test file (used for AV validation).
- **Win.Test.EICAR_HDB-2**→ Malicious Malware capable of remote access or data theft.

Malware Download URLs:

- https://secure.eicar.org/eicarcom2.zip
- https://www.ikarussecurity.com/en/download-test-viruses-for-free/

Host Involved (Client IP):

- 192.168.80.3 → internal device initiating the download requests.

Firewall Log Excerpts:

- **2025-09-02 T15:07:41 - Critical** – Virus Detected: Win.Test.EICAR_HDB-1
  - Client IP: 192.168.80.3
  - URL: https://secure.eicar.org/eicarcom2.zip
- **2025-09-02 T15:09:47 - Critical** – Virus Detected: Win.Test.EICAR_HDB-2
  - Client IP: 192.168.80.3
  - URL: https://www.ikarussecurity.com/en/download-test-viruses-for-free/

4. Indicators of Attack (IOAs)

Tactic 1: Delivery

- **Technique:** Malicious File Download
- **Details:** Host 192.168.80.3 attempted to download known-malicious files (test + real malware).

Tactic 2: Defense Evasion

- **Technique:** Use of Benign-Looking or Test Malware
- **Details:** Use of EICAR file and Palo Alto ELF sample suggests attempts to bypass AV or to simulate adversarial behavior in a controlled environment.

Tactic 3: Command and Control (C2) Preparation

- **Technique:** Remote File Retrieval from External Servers
- **Details:** The files were hosted on legitimate domains but carried malicious signatures, mimicking real-world adversaries retrieving malware from C2 infrastructure.

5. Analysis

- **Detection:** OPNsense firewall (c-icap + ClamAV) intercepted and blocked both downloads before they reached the client system.
- **Threat Severity:**
  - EICAR file = **no threat** (validation test).
  - Unix Trojan = **medium-to-high threat** (capable of execution on Unix/Linux hosts).
- **Possible Scenarios:**
  1. The device (192.168.80.3) was used by a security analyst conducting malware testing.
  2. An automated script/tool attempted the downloads for reconnaissance.
  3. A user unknowingly accessed malware links.

Result:
No evidence of malware execution or compromise. Firewall protection was effective.

Incident Response Plan

1. Immediate Containment

- Isolated **host 192.168.80.3** from the internal LAN until verified safe.
- Blocked domains:
  - secure.eicar.org
  - https://www.ikarussecurity.com

2. Investigation

- Conducted forensic review of the affected host.
- Verified **system logs, browser cache, and memory** for signs of execution.
- Confirmed whether downloads were for **internal testing or unauthorized activity.**

3. Eradication and Recovery

- No active malware found on the host.
- System cleaned and restored to a **known-good state**.
- Rotated **network credentials** as a precaution.
- Re-applied **endpoint hardening policies** (application whitelisting, restricted privileges).

4. Post-Incident Review

- Confirmed first detection was intentional EICAR test.
- Second detection was a **live malware sample**, requiring tighter controls.
- Updated **firewall policies** to:
  - Block all **malware test repositories** unless pre-approved.
  - Generate **alerts to SOC team** on any attempt to access such domains.

5. Conclusion

The OPNsense firewall with **c-icap antivirus scanning** successfully prevented malware downloads. While one file was harmless (EICAR), the Unix Trojan could have posed a **significant risk** if executed.

Key Takeaways:

- Perimeter defenses are functioning effectively.
- Malware testing within production networks must follow **strict isolation and approval** processes.
- Integration with SIEM (e.g., Wazuh) enhances **real-time detection, correlation, and response.**

6. Lessons Learned

- **Firewall-based malware scanning** effectively neutralized threats.
- **Malware testing policies** must be formalized and restricted to sandboxed environments.
- **SIEM integration** accelerates detection and reduces investigation time.
- **Blocking known malware repositories** prevents accidental exposure.

7. Reference to Standards

This report and response plan were developed following **cybersecurity incident handling best practices**:

1. **NIST SP 800-61 Revision 2** – Computer Security Incident Handling Guide (NIST, 2012).
    - Framework: Preparation → Detection → Analysis → Containment → Eradication → Recovery → Lessons Learned.
2. **ISO/IEC 27035** – Information Security Incident Management (ISO, 2016).
    - Emphasizes structured responses to incidents and continual improvement.
3. **SANS Incident Handler's Handbook (2018)**
    - Provides operational guidelines for SOC teams on containment, eradication, and reporting.