



Blocking Malware Download and Incident Response Plan

Report Task # 03 (Team IOTA)

SUBMITTED TO :-

Mr. Zain

SUBMITTED BY :-

Nasir Sharif

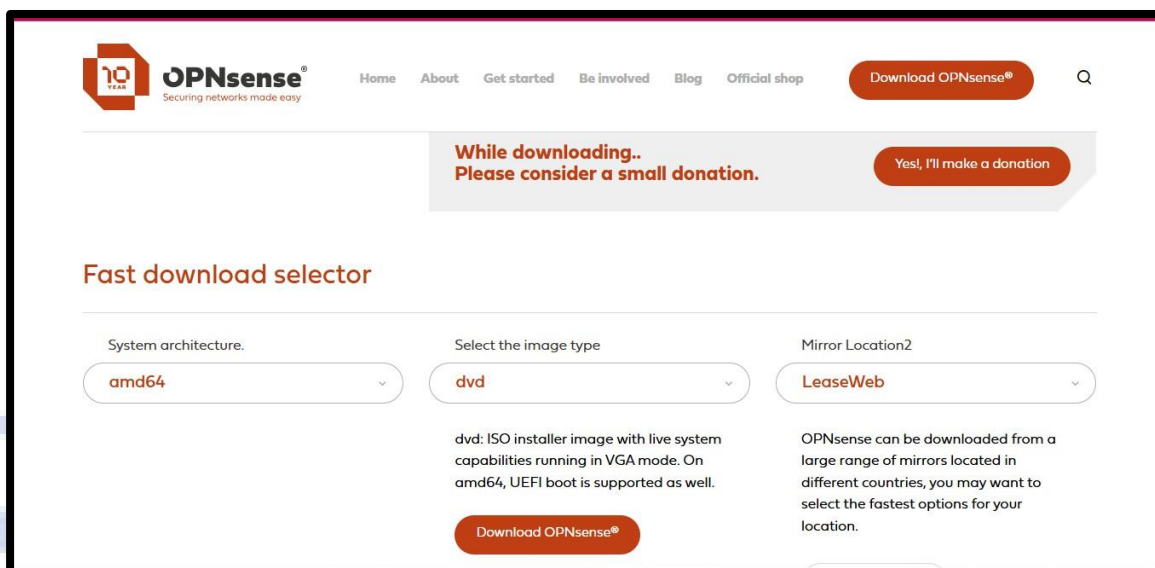
National University of Modern Languages H-9 Islamabad

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.



OPNsense®
Securing networks made easy

Home About Get started Be involved Blog Official shop Download OPNsense®

While downloading.. Please consider a small donation. Yes, I'll make a donation

Fast download selector

System architecture: **amd64** Select the image type: **dvd** Mirror Location2: **LeaseWeb**

dvd: ISO installer image with live system capabilities running in VGA mode. On amd64, UEFI boot is supported as well.

OPNsense can be downloaded from a large range of mirrors located in different countries, you may want to select the fastest options for your location.

Download OPNsense®

```
Starting Wazuh Agent: 2025/08/14 07:46:26 wazuh-syscheckd: WARNING: The check_unixaudit option is deprecated in favor of the SCA module.
success

*** OPNsense.internal: OPNsense 25.7.1_1 (amd64) ***

LAN (em1)      -> v4: 192.168.80.2/24
WAN (em0)      -> v4/DHCP4: 192.168.1.10/24

HTTPS: sha256 9A A4 77 FB C2 F0 76 BB FF E0 23 8D 6D EB 1E DE
          46 4E 72 20 FA 69 84 DE 91 16 09 F2 5F 9B 32 8E
SSH:  SHA256 XUFUjKZcinspWFGsQnHiEqUBPg0aUJdkLnDfY/2lu+8 (ECDSA)
SSH:  SHA256 k7eQ3IP9Udu542JZATCbarSQXm+c6UPpdU0eusnJQgs (ED25519)
SSH:  SHA256 sxKkjjUc98YbAf9UbA60jUvJn8NxmBg70oHUiIbXf1E (RSA)

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: █
```

- 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.

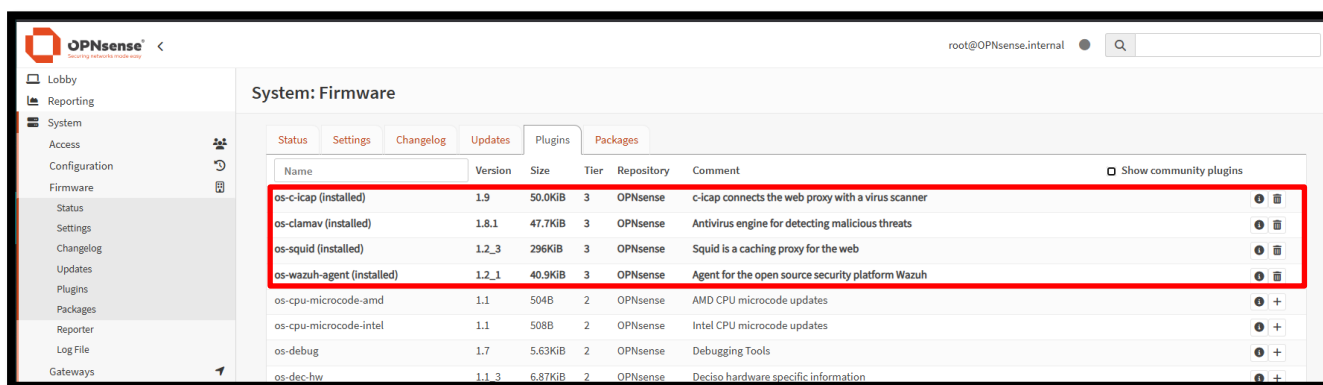
Firewall is now successfully installed.

2. Setting up the firewall:

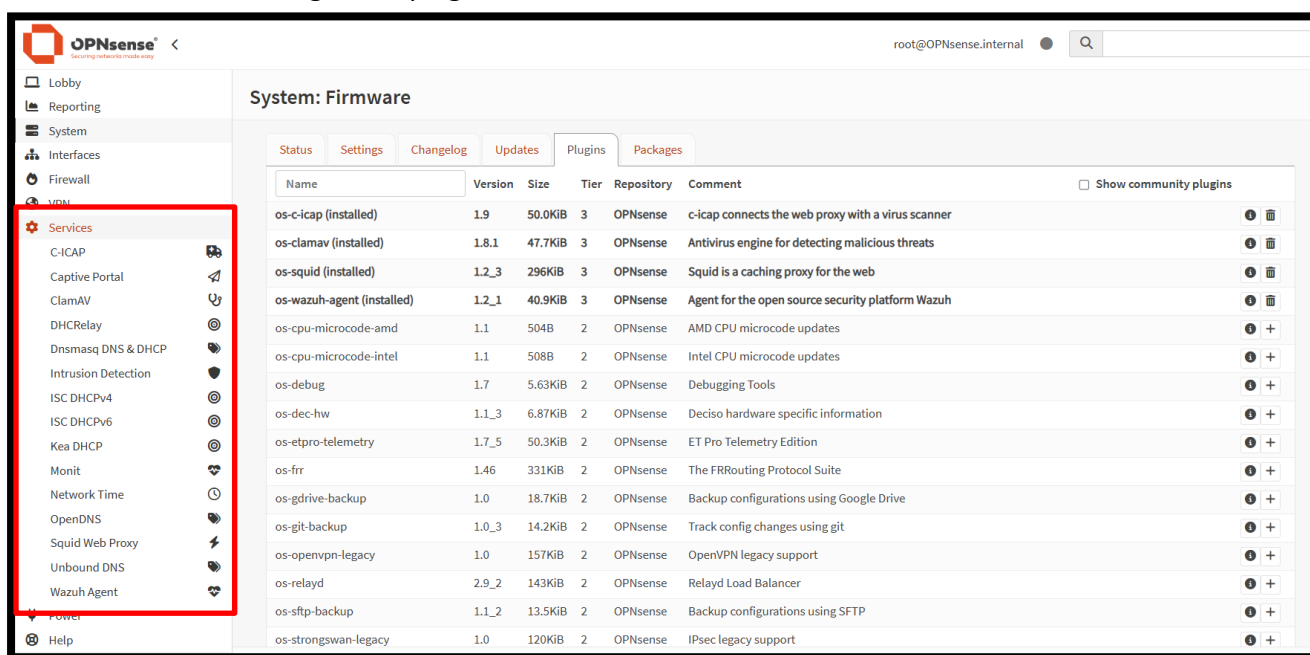
2.1 Installing required Plugins on Firewall:

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.

The screenshot shows the 'Services: C-ICAP: Configuration' page with the 'General' tab selected. The page has a header with 'root@OPNsense.internal' and a search bar. The configuration table includes the following settings:

Setting	Value
Enable c-icap service	☒
Timeout	300
Max keepalive requests	100
Max keepalive timeout	600
Start servers	3
Max servers	10
Min spare threads	10
Max spare threads	20
Threads per child	10
Max requests per child	0
Listen address	:::1
Server admin	
Servename	
Enable access logging	☒
Use c-icap with local squid	☒

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

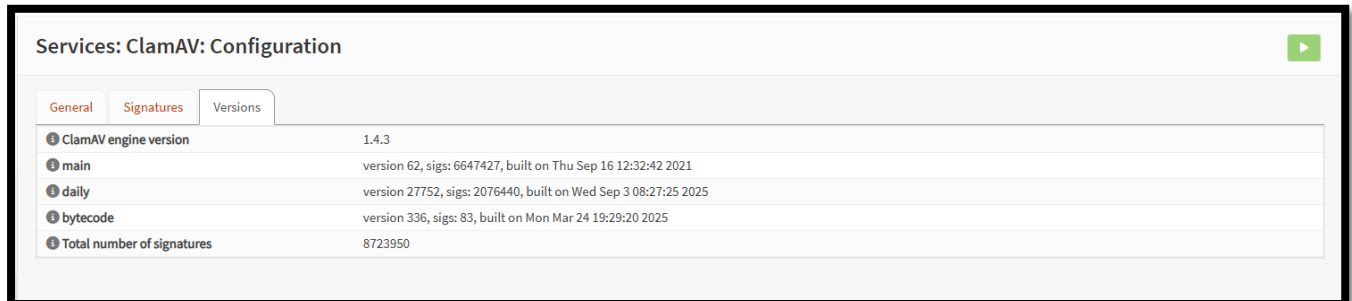
The screenshot shows the 'Services: C-ICAP: Configuration' page with the 'Antivirus' tab selected. The configuration table includes the following settings:

Setting	Value
Enable ClamAV	☒
Scan for filetypes	Text files, Binary files, Executables, Archives, GIF a
Send percentage data	5
Start send percentage data	2M
Allow 204 responses	☒
Pass on error	☐
Max object size	5M

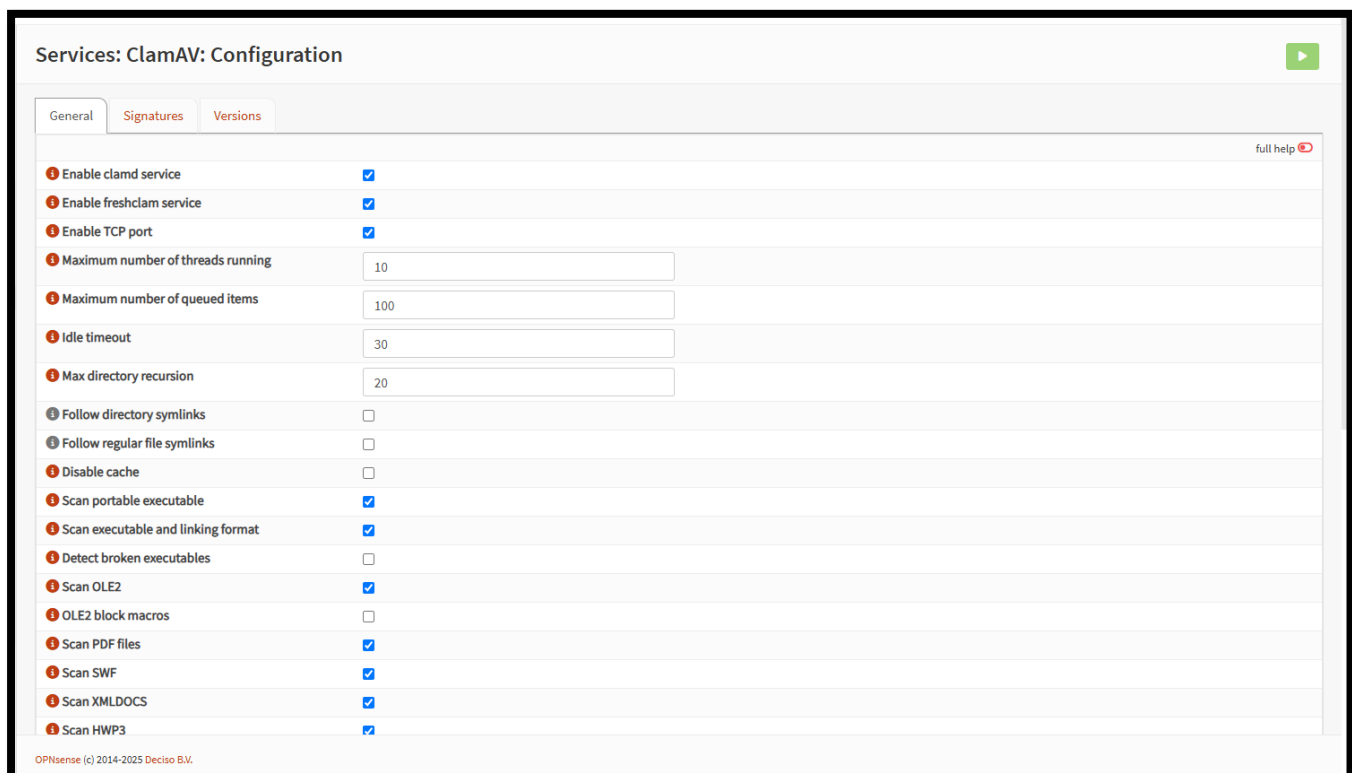
At the bottom of the configuration table, there is a 'Save' button.

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.

Edit Certificate

full help

1 Method: Create an internal Certificate Authority

1 Description: ITsoleraCA

Key

1 Key type: RSA-2048

1 Digest Algorithm: SHA256

1 Issuer: self-signed

1 Lifetime (days): 825

General

1 Country Code: Pakistan

1 State or Province: Federal

1 City: Islamabad

1 Organization: ITsolera Pvt Ltd

1 Organizational Unit: Team IOTA

1 Email Address: nasirsharifqasoori786@gmail.com

1 Common Name: OPNsense.localdomain

1 OSCP uri:

Cancel Save

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

System: Trust: Authorities

Certificates

Search

Description	Issuer	Name	Usages	Valid from	Valid to	Commands
ITsoleraCA	self-signed	/C=PK/ST=Federal/L=Islamab...	1	Aug 27, 2025 3:18 PM	Nov 30, 2027 3:18 PM	Download Edit Delete

Showing 1 to 1 of 1 entries

Click on download.

While downloading, select type 'certificate'.

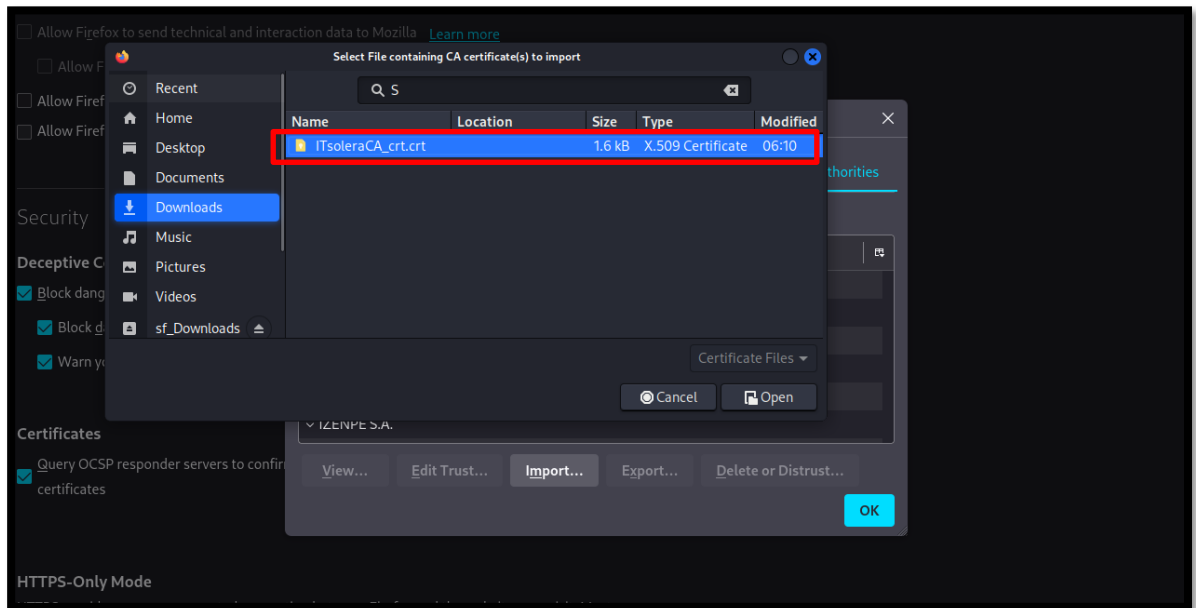
Now send this certificate to your test device.

Then open browser on test device.

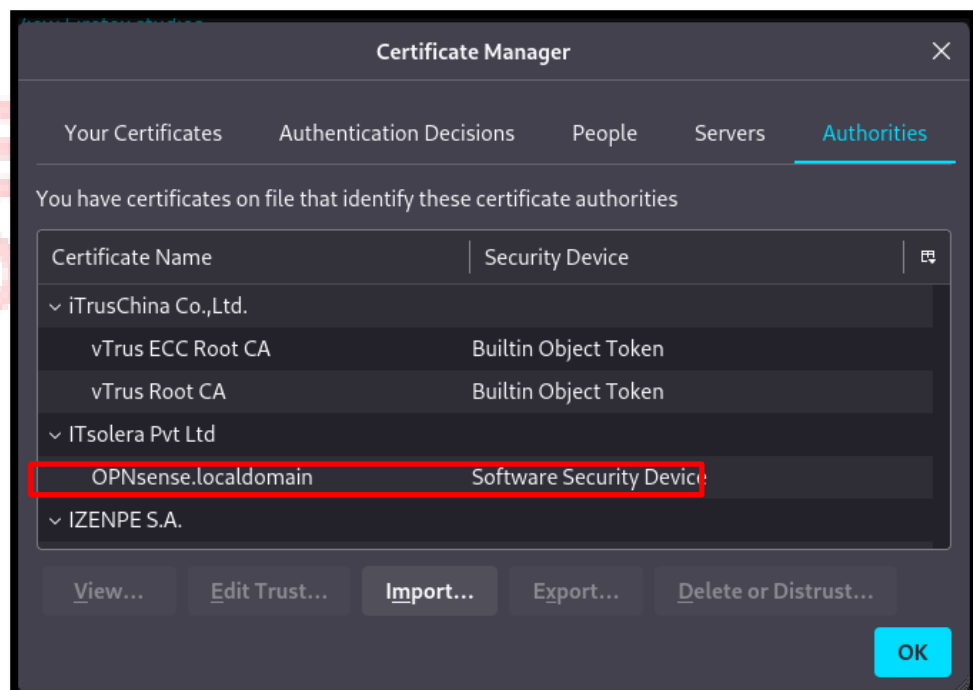
Go to settings -> certificate manager -> trusted root certificates.

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.

Services: Squid Web Proxy: Administration

General Proxy Settings ▾ Forward Proxy ▾ Proxy Auto-Config ▾ Remote Access Control Lists Support

advanced mode

1 Enable proxy ☒

1 User error pages Squid ▾

1 ICP port

1 Enable access logging ☒

1 Access log target File ▾

1 Enable store logging ☒

1 Ignore hosts in access.log

1 Use alternate DNS-servers

1 Use Via header ☐

1 X-Forwarded-For header handling Default ▾

1 Visible Hostname

1 Administrator's Email

1 Suppress version string ☐

1 Connection Timeout

1 Whitespace handling of URI Default ▾

- 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.

Services: Squid Web Proxy: Administration

General Proxy Settings ▾ Forward Proxy ▾ Proxy Auto-Config ▾ Remote Access Control Lists Support

advanced mode

1 Proxy interfaces LAN, Loopback ▾

1 Proxy port 3128

1 Enable Transparent HTTP proxy ☒

1 Enable SSL inspection ☒

1 Log SNI information only ☐

1 SSL Proxy port 3129

1 CA to use ITsoleraCA ▾

1 SSL no bump sites

1 Number of squid workers 1

1 SSL cache size 4

1 SSL cert workers 5

1 Allow interface subnets ☒

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.

Services: Squid Web Proxy: Administration

General Proxy Settings Forward Proxy Proxy Auto-Config Remote Access Control Lists Support

advanced mode

Enable ICAP ☒

Request Modify URL

Response Modify URL

Default Options TTL

Send Client IP ☒

Send Username ☐

Encode Username ☐

Username Header

Enable Preview ☒

Preview Size

Exclusion List

Clear All Copy Paste Text

Apply

- 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.

Firewall: NAT: Port Forward

Select category

		Source		Destination		NAT			
☐	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description
☐	LAN	TCP	*	*	LAN address	77-80, 443	*	*	Anti-lockout Rule
☐	↔ LAN WAN	TCP	192.168.80.3/24	*	*	80 (HTTP)	127.0.0.1	3128	
☐	↔ LAN WAN	TCP	192.168.80.3/24	*	*	443 (HTTPS)	127.0.0.1	3129	
☒	▶ Enabled rule		!	No redirect			↔		Linked rule
☐	▶ Disabled rule		!	Disabled no redirect			↔		Disabled linked rule

Alias (click to view/edit)

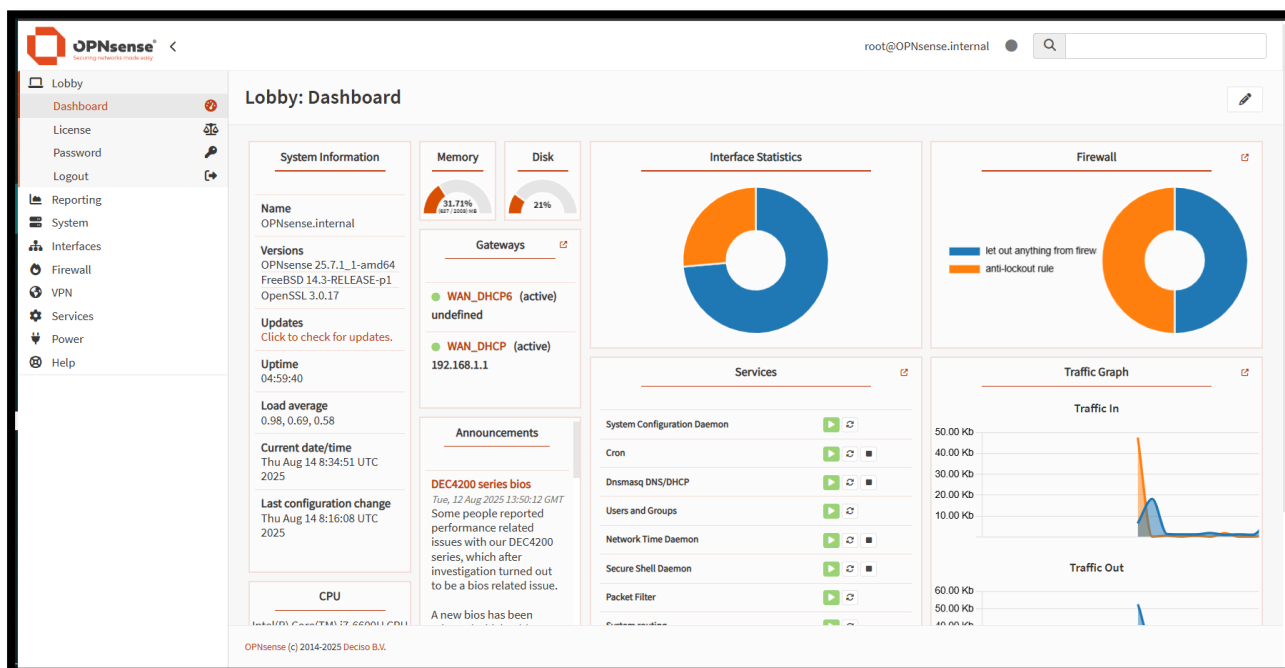
- Select **protocol TCP**
- Source address** is the IP address of the test PC
- Destination address:** any, ports 80 and 443 (one for each rule)
- Redirect IP** is the loopback IP and redirect ports is 3128 for HTTP rule and 3129 for HTTPS rule

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:

The 'Edit destination' form is shown with the following configuration:

- Enabled:** ☒
- Transport:** UDP(4)
- Applications:** filter (filterlog), firewall (firewall). Buttons: Clear All, Select All.
- Levels:** debug, info, notice, warn, error, critical, alert, eme. Buttons: Clear All, Select All.
- Facilities:** kernel messages, system daemons, locally used (0). Buttons: Clear All, Select All.
- Hostname:** 192.168.1.12
- Port:** 514
- rfc5424:** ☒
- Description:** Syslog target for Wazuh manager

Buttons at the bottom: Cancel, Save.

- 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.



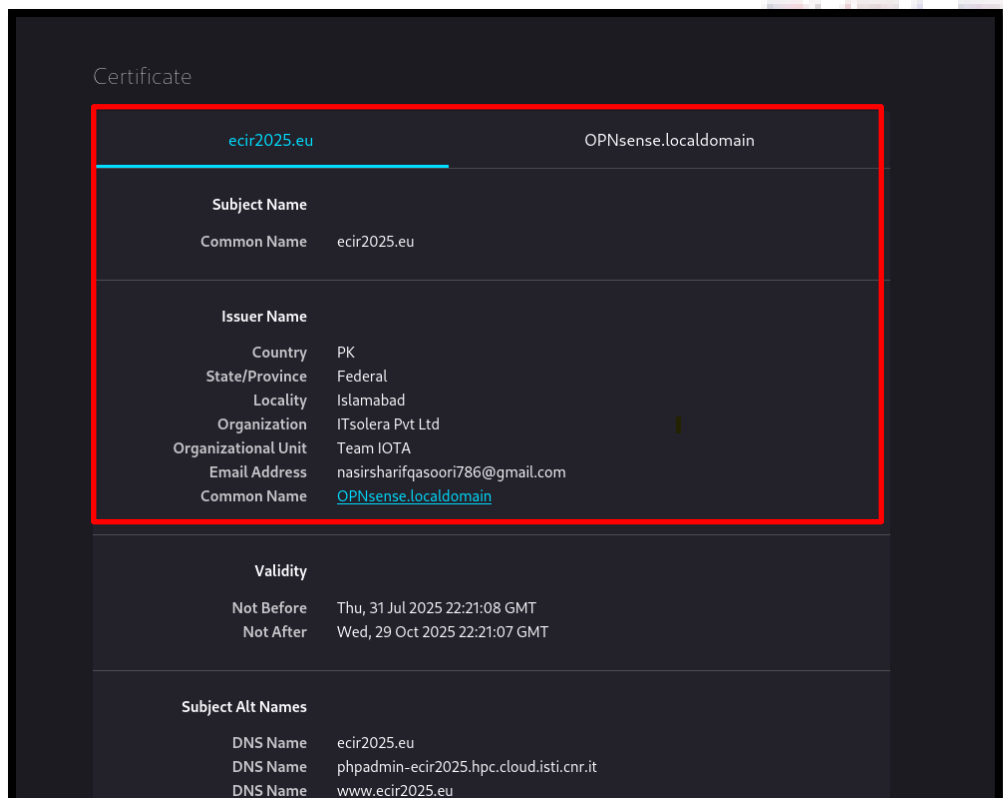
- Save it and restart Wazuh manager.

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:

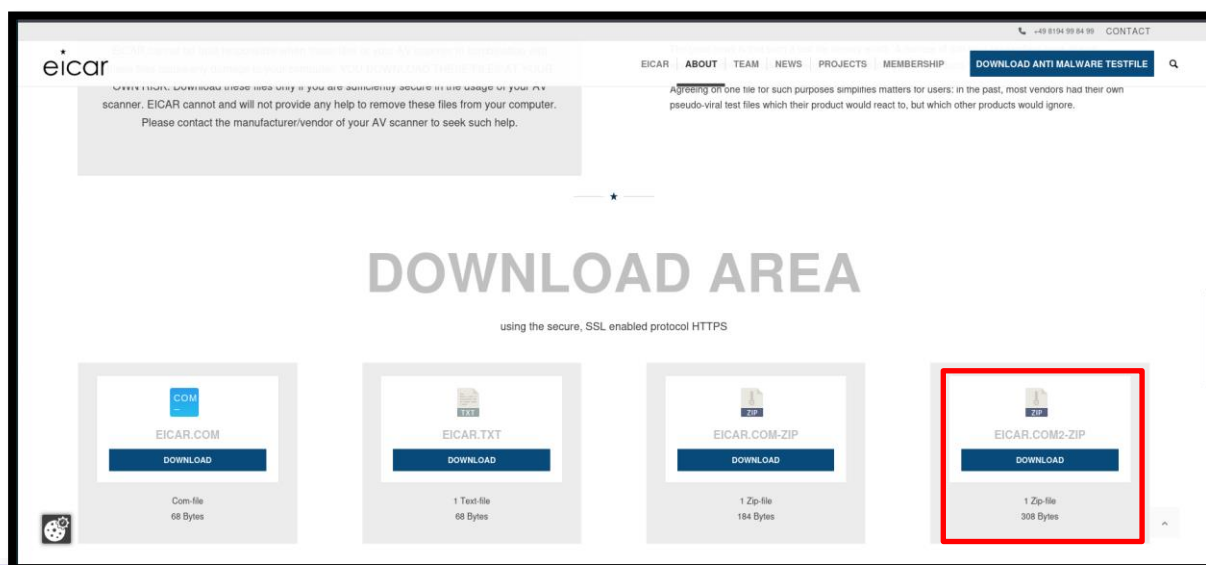


4.1 Downloading test malware and checking logs on firewall:

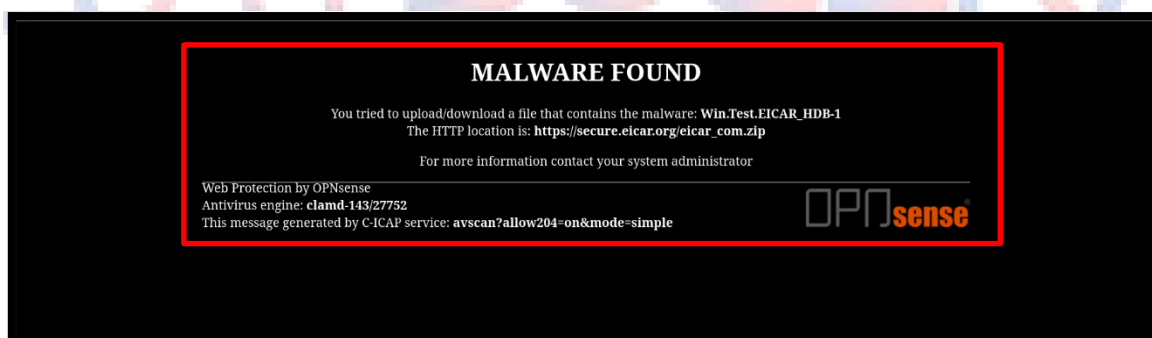
To download test malware, there are many sources on like EICAR, IKarussecurityetc.

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:

Services: C-ICAP: Log File

Time	Severity	Process	Line
2025-09-03T14:30:25	Critical	c-icap	17373/11103937953800, VIRUS DETECTED: Win.Test.EICAR_HDB-1, http client ip: 192.168.80.3, http user: -, http url: https://secure.eicar.org/eicar_com.zip
2025-09-03T14:29:33	Critical	c-icap	17373/11103937970184, Object size is 143093992. Bigger than max scannable file size (5242880). Allow it....
2025-09-03T14:29:30	Critical	c-icap	17373/11103937953800, Object size is 186184944. Bigger than max scannable file size (5242880). Allow it....
2025-09-03T14:29:23	Critical	c-icap	17373/11103937957896, Setting antivirus default engine: clamd
2025-09-03T19:23:22	Critical	c-icap	17395/11103937929224, recomputing istag ...
2025-09-03T19:23:22	Critical	c-icap	17373/11103937929224, recomputing istag ...
2025-09-03T19:23:22	Critical	c-icap	17431/11103937929224, recomputing istag ...
2025-09-03T19:23:21	Critical	c-icap	main proc, WARNING: Can not check the used c-icap release to build service clamd_mod.so
2025-09-03T19:23:21	Critical	c-icap	main proc, WARNING: Can not check the used c-icap release to build service virus_scan.so
2025-09-03T19:23:21	Critical	c-icap	main proc, Warning, alias is the same as service_name, not adding
2025-09-03T19:23:19	Critical	c-icap	main proc, Possibly a term signal received. Monitor process going to term all children
2025-09-03T19:22:31	Critical	c-icap	main proc, Registry 'virus_scan:engine' does not exist!
2025-09-03T19:22:31	Critical	c-icap	main proc, clamd_unit: Error while sending command to clamd server

Showing 1 to 20

Testing: The another File from Ikarussecurity.com

Test viruses for download
For IKARUS anti virus and IKARUS mobile security

Test viruses allow you to test the functionality of your [antivirus program](#) and reaction to malware without any risk. To download, please move the mouse pointer over the link, press the right mouse button and select "Save Link as ...". These are self-extracting archives, which have to be started and can be used after the download.

EICAR test virus

The EICAR test virus is not a real virus. It is a DOS program created by the European Institute for Computer Antivirus Research, which only displays the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE" on the screen and then terminates itself. The aim of test viruses is to test the functions of an anti-malware program or to see how the program behaves when a virus is detected.

Download the desired test file to your PC. If your network security does not already prevent the download of the file, the local antivirus program should start working when trying to save or execute the file. Since the Eicar test virus is the only standardized way to monitor antivirus programs "live" at work without endangering yourself, it is likely that all programs will recognize the file. However, it says nothing about the detection or other protection capabilities of the software. If the file is not detected by your virus scanner, it is advisable to investigate the reason for this, for example to detect possible malfunctions.

[Download EICAR-Testvirus](#)

Android-App „TestVirus“

To test your [Android security solution](#), we also offer a "TestVirus" app on Google Play. This is of course not "real" malware, but a harmless test file that should be recognized by all Android virus scanners.

This app can be used to test the functionality of security apps and to monitor the behavior of the app in case of a threat: The IKARUS TestVirus should be treated like a "real" pest and rendered harmless by warning the user of the infection and deleting the file.

[IKARUS TestVirus at Google Play](#)

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

MALWARE FOUND

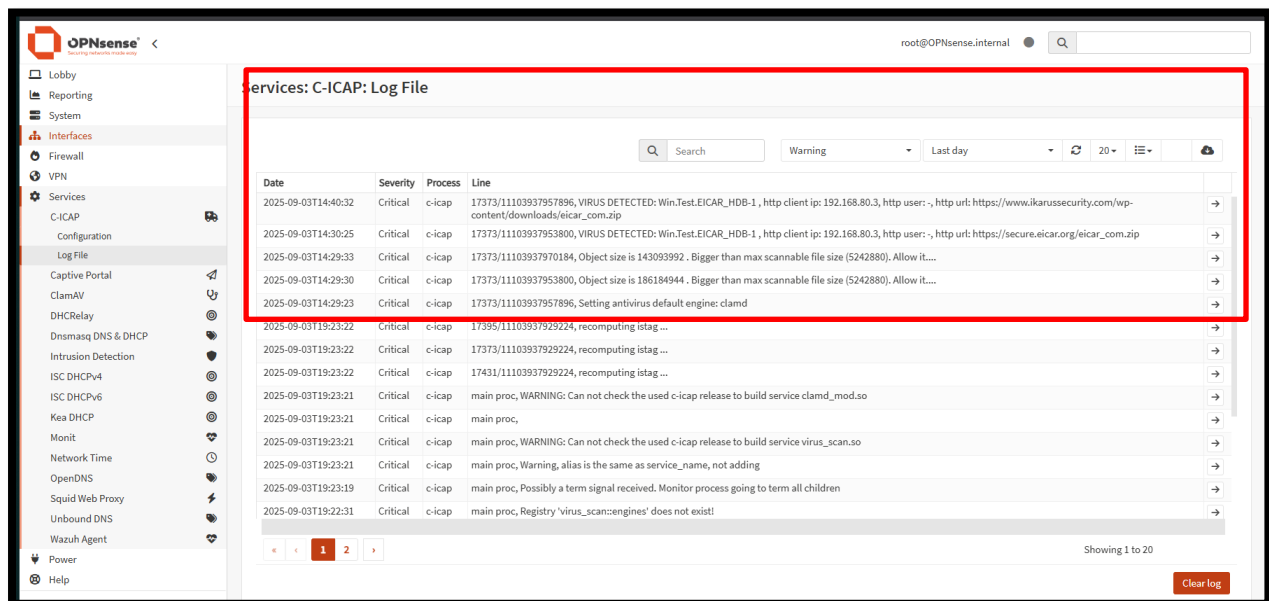
You tried to upload/download a file that contains the malware: Win.Test.EICAR_HDB-1
The HTTP location is: https://www.ikarussecurity.com/wp-content/downloads/eicar_com.zip

For more information contact your system administrator

Web Protection by OPNsense
Antivirus engine: clamd-143/27752
This message generated by C-ICAP service: avscan?allow204-on&mode=simple

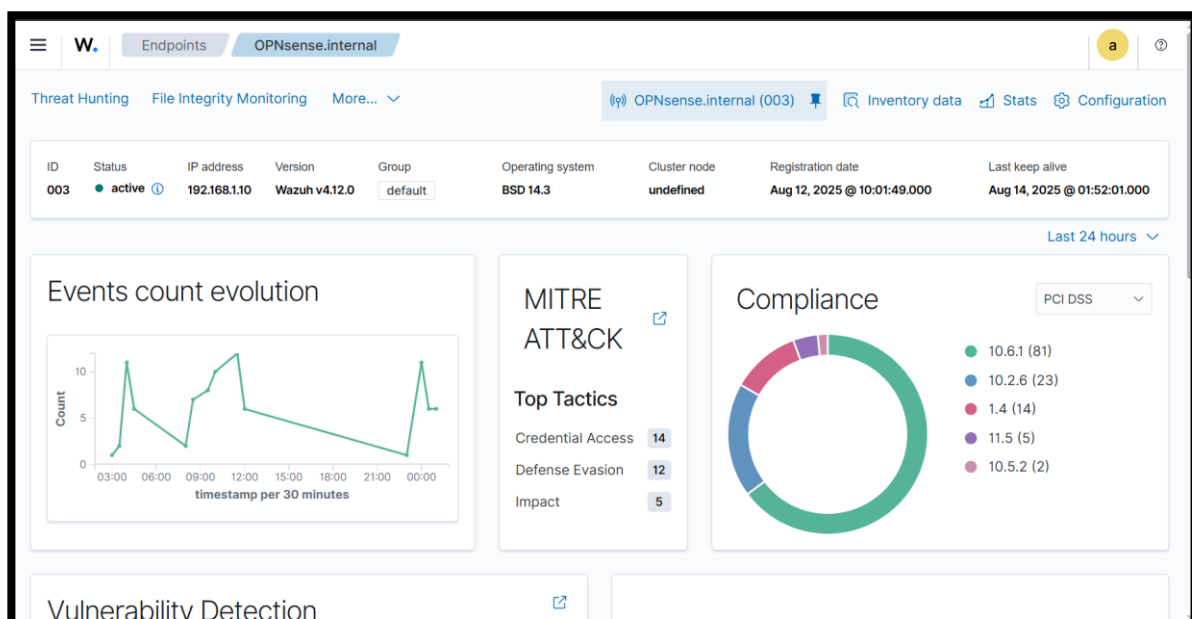
OPNsense

- 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.



data.status	VIRUS DETECTED
data.url	https://secure.eicar.org/eicarcom2.zip
data.virusname	Win.Test.EICAR_HDB-1
decoder.name	squid-proxy
full_log	<26>1 2025-07-25T05:08:39-05:00 OPNsense.localdomain c-icap 78643 - [meta sequenceId="203"] 78643/61327269781248, VIRUS DETECTED: Win.Test.EICAR_HDB-1, http client ip: 172.23.4.161, http user: -, http url: https://secure.eicar.org/eicarcom2.zip
id	1753438120.1164938
input.type	log
location	/var/log/cicap/latest.log
manager.name	kanz-VMware-Virtual-Platform
rule.description	Virus Found and Blocked by Squid Proxy.



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.

