**Các bước triển khai Squid SSL Proxy trên OPNsense**

Dưới đây là hướng dẫn **từ đầu tới cuối** để cấu hình **Squid Proxy** trên **OPNsense 25.1**, tích hợp với **c‑icap** và **ClamAV** nhằm thực hiện **SSL Inspection** (Transparent HTTPS proxy + quét virus).

**Tóm tắt nhanh**

1. Cài 3 plugin: **os‑squid**, **os‑c‑icap**, **os‑clamav** [docs.opnsense.org](https://docs.opnsense.org/plugins.html?utm_source=chatgpt.com)
2. Tạo **Certificate Authority** nội bộ dùng cho SSL bump [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)
3. Bật **Transparent HTTP/HTTPS** proxy (SSL bump) trong Squid [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)
4. Tạo luật **NAT** để redirect port 80 → 3128, 443 → 3129 [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)
5. Cấu hình **ICAP** để chuyển nội dung qua c‑icap [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/c-icap.html?utm_source=chatgpt.com)
6. Bật **ClamAV** và cập nhật signatures [docs.opnsense.org](https://docs.opnsense.org/manual/antivirus.html?utm_source=chatgpt.com)
7. Kiểm tra bằng **EICAR** và giám sát log

**Mục tiêu:**

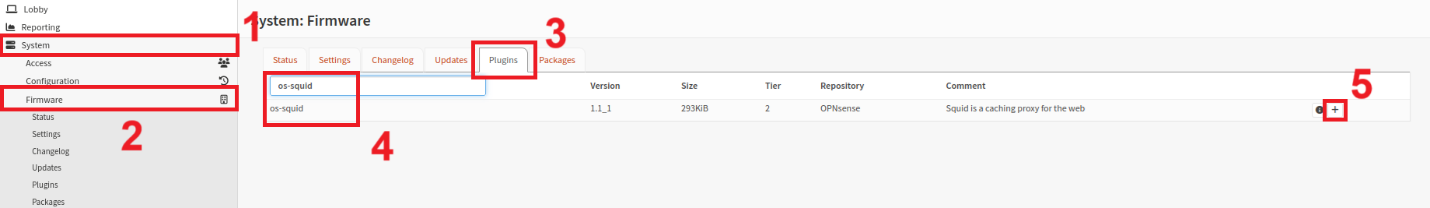
1. Dùng Squid để intercept HTTPS traffic (SSL bump)
2. Gửi nội dung đến ICAP server (c-icap + ClamAV) để quét mã độc
3. Không cần máy chủ phụ – tất cả trên cùng một OPNsense

## **Cài đặt các plugin**

Vào **System > Firmware > Plugins**, cài 3 plugin sau (nếu chưa):

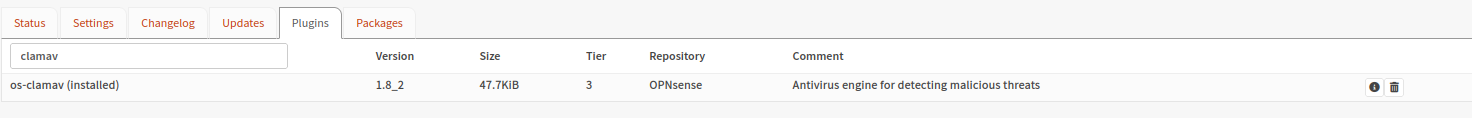
Trước tiên, bạn cần cài Squid trên OPNsense:

* **Bước 1**: Đăng nhập vào **OPNsense** qua web UI (ví dụ: https://192.168.1.20).
* **Bước 2**: Vào **System > Firmware > Plugins**.
* **Bước 3**: Tìm plugin os-squid và nhấn **+ Install**.

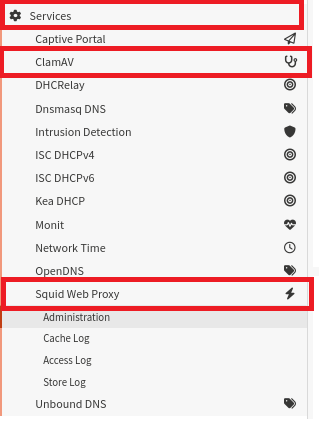


* **Bước 4:** Tìm plugin os-c-icap; os-clamav và nhấn **+ Install**. (gồm Squid + c-icap + ClamAV + giao diện cấu hình ICAP)





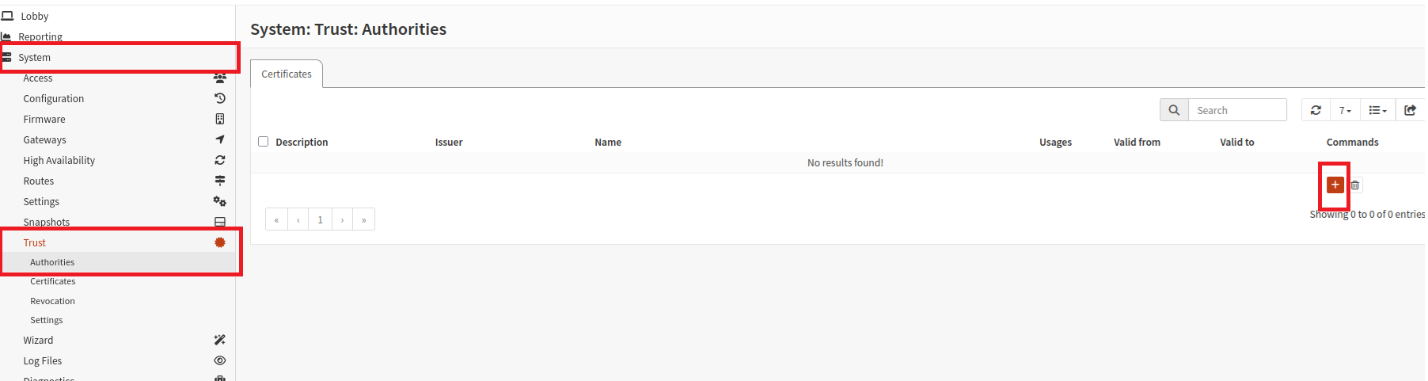
Sau khi cài xong, bạn sẽ thấy Squid và clamAV xuất hiện trong **Services**.



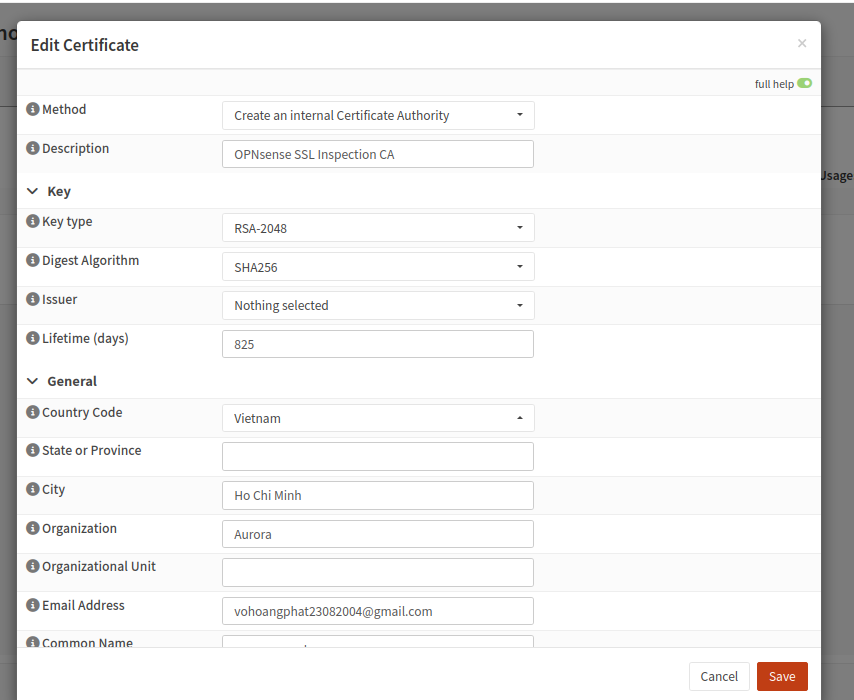
**Lưu ý:** Plugin os-squidclamav *không còn được duy trì riêng*, vì chức năng đã tích hợp vào os-c-icap + os-clamav.

## **Tạo Certificate Authority (CA) cho SSL Bump**

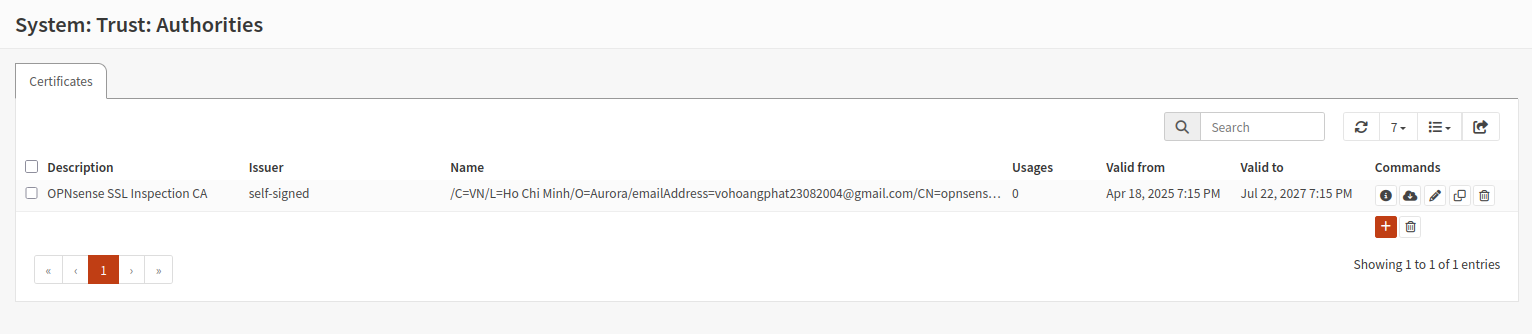
1. Vào **System → Trust → Authorities → Add** [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)



1. Điền:
   * **Descriptive name**: OPNsense SSL Inspection CA
   * **Method**: *Create internal Certificate Authority*
   * **Distinguished name** (Country, State, Org, Common Name…)
   * **Lifetime**: 3650 ngày



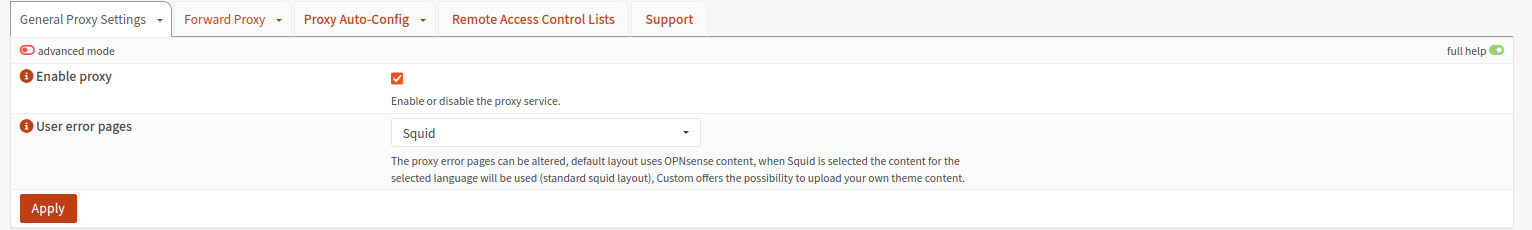
1. Nhấn **Save** để lưu CA. Đây là CA mà Squid sẽ dùng để ký các chứng chỉ “bumped” [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)



## **Cấu hình Squid làm Transparent Proxy và SSL Bump**

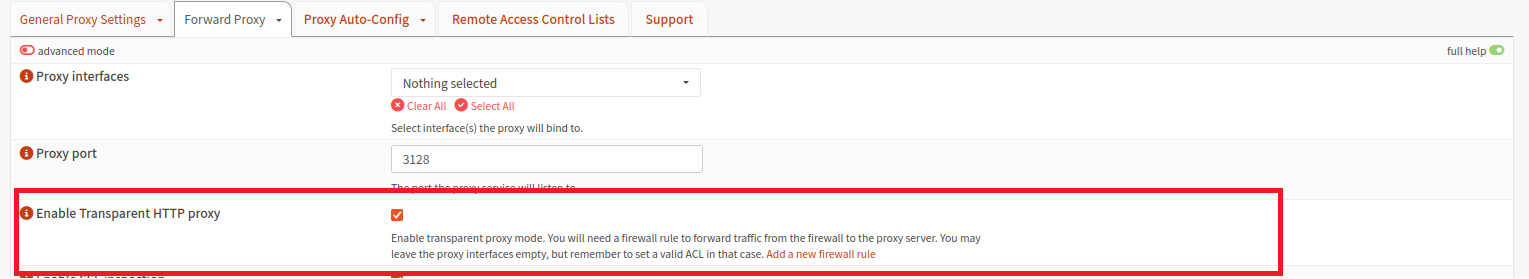
**3.1. Thiết lập cơ bản (Basic Proxy)**

1. Vào **Services → Web Proxy → Administration → General Proxy Settings**
2. ☑ **Enable proxy** → **Apply** [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)



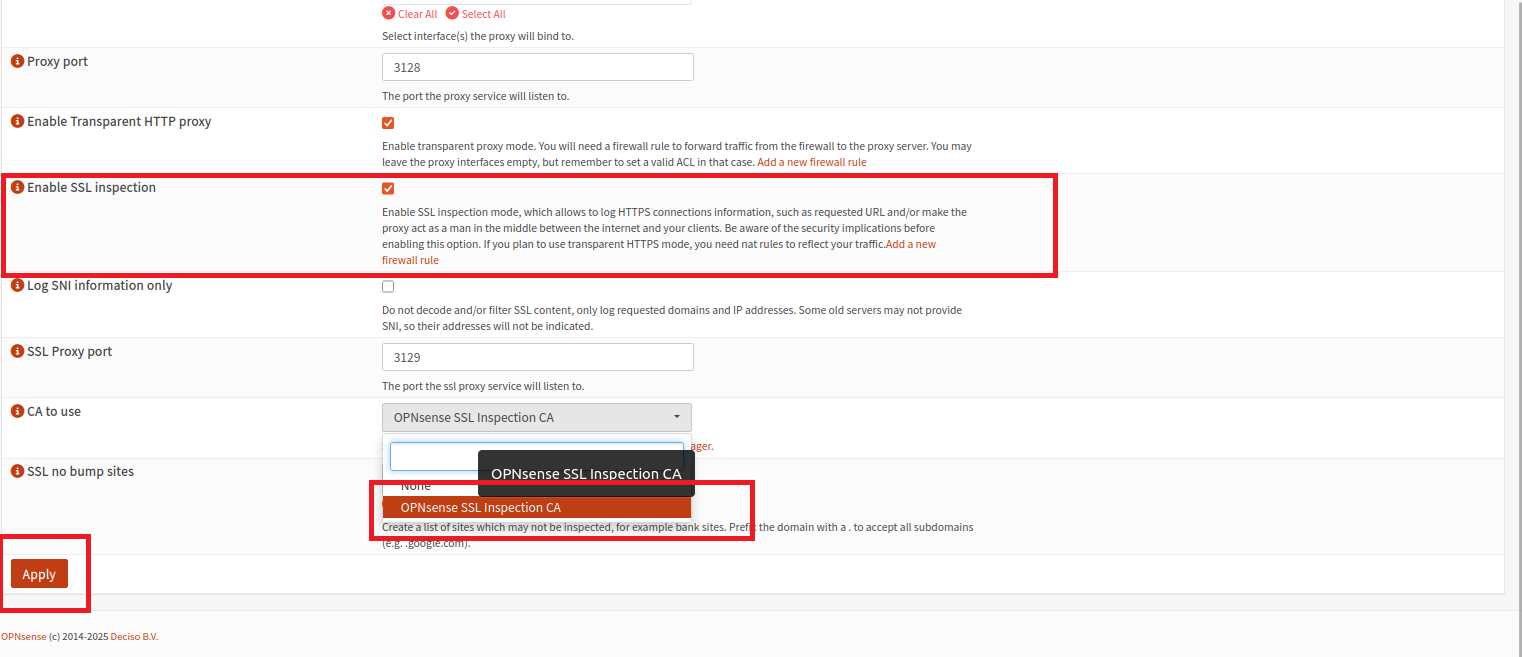
**3.2. Bật Transparent HTTP Proxy**

1. Chuyển sang tab **Forward Proxy** → **General Forward Settings**
2. ☑ **Enable Transparent HTTP proxy** → **Apply** [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)



**3.3. Bật SSL Inspection (HTTPS / SSL Bump)**

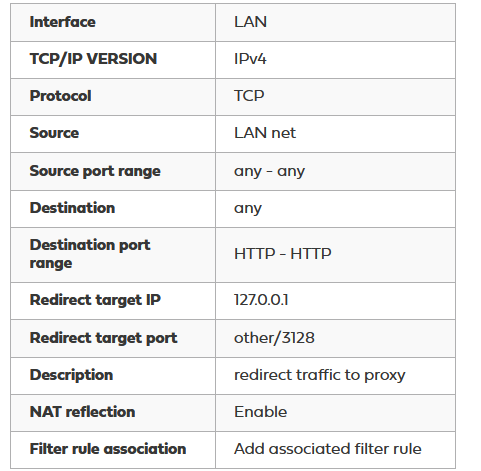
1. Vẫn trong **General Forward Settings**:
   * ☑ **Enable SSL mode**
   * **CA to use**: chọn OPNsense SSL Inspection CA
2. Nhấn **Apply** [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)



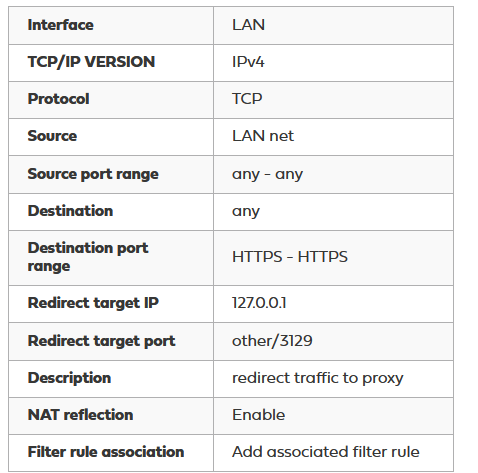
**3.4. Tạo luật NAT chuyển traffic HTTP/HTTPS về Squid**

Nếu OPNsense chưa tự tạo, vào **Firewall → NAT → Port Forward** và thêm:

* **Rule HTTP**:
  + Interface: LAN
  + Protocol: TCP
  + Destination port: 80 → Redirect to 127.0.0.1:3128

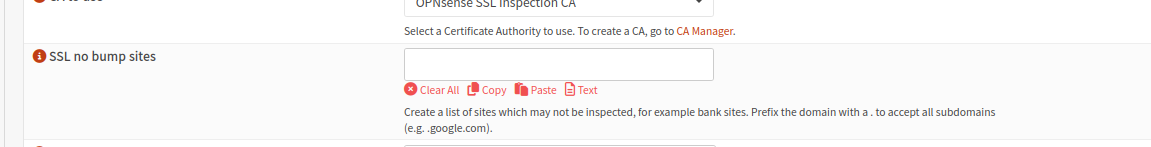


* **Rule HTTPS**:
  + Interface: LAN
  + Protocol: TCP
  + Destination port: 443 → Redirect to 127.0.0.1:3129
* Source: LAN net, Destination: Any → Save & Apply [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)



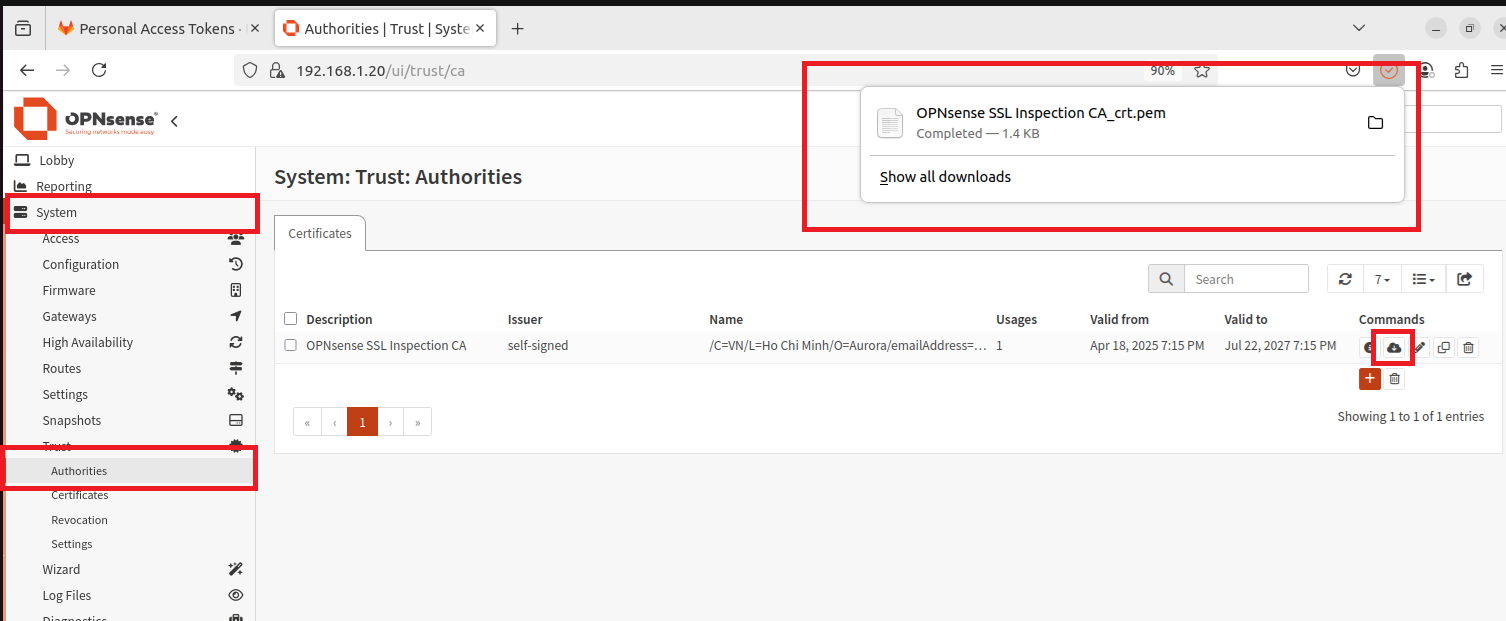
**3.5. Cấu hình danh sách “No SSL Bump” (không giải mã)**

1. Trong **Forward Proxy → General Forward Settings**, bật **Advanced Mode**
2. Thêm các host/nội dung không muốn bump (ví dụ: .paypal.com) vào **SSL no bump sites** [docs.opnsense.org](https://docs.opnsense.org/manual/how-tos/proxytransparent.html)



**3.6. Cài đặt chứng chỉ CA lên client**

1. Vào **System → Trust → Authorities**, nhấn **Export** CA vừa tạo



1. Trên máy client, import vào **Trusted Root Certificate Authorities** để trình duyệt chấp nhận SSL Proxy

## **Cấu hình ICAP (c‑icap)**

**4.1. Bật ICAP trong Squid**

Vào **Services → Web Proxy → ICAP Settings**, bật **Enable ICAP** citeturn0search1

**4.2. Thiết lập URL cho REQMOD/RESPMOD**

* **Request Modify URL**:
* icap://127.0.0.1:1344/reqmod
* **Response Modify URL**:
* icap://127.0.0.1:1344/respmod

Nhấn **Apply** citeturn0search1

## **Cấu hình ClamAV**

**5.1. Bật dịch vụ clamd và freshclam**

Vào **Services → ClamAV**:

* ☑ **Enable clamd service**
* ☑ **Enable freshclam (signature updates)**
* ☑ **Enable TCP Port** (mặc định port 3310)
* Nhấn **Save** citeturn0search4

**5.2. Tích hợp ClamAV với c‑icap**

Plugin **os-c-icap** mặc định đã cấu hình để dùng ClamAV tại /usr/local/etc/c-icap/c-icap.conf citeturn0search6

* Kiểm tra service tên srv\_clamav trong file để chắc ClamAV được gọi đúng

## **6. Khởi động và kiểm tra**

**6.1. Khởi động dịch vụ**

Truy cập **Dashboard → Services**, đảm bảo:

* Web Proxy đang chạy
* c-icap đang chạy
* clamd đang chạy citeturn0search15

**6.2. Kiểm tra thực tế**

* **HTTP**: truy cập http://example.com → hiển thị bình thường qua proxy
* **HTTPS**: truy cập https://eicar.org/download/eicar.com.txt → Squid bump → ICAP gửi tới ClamAV → chặn file EICAR citeturn0search19

**6.3. Xem log**

* **Squid Access Log**: **Services → Web Proxy → Access Log**
* **c-icap log**: /var/log/c-icap/server.log
* **ClamAV log**: /var/log/clamav/clamd.log

## **Lưu ý & Tối ưu**

* **Bảo mật CA**: giữ khóa riêng an toàn, bổ sung cuối list “No SSL Bump” cho e‑banking citeturn2view0
* **Theo dõi tài nguyên**: SSL bump tốn CPU/RAM, nên giám sát hiệu năng OPNsense
* **Kết hợp Suricata**: nếu cần IDS/IPS trên traffic đã decrypt, cài os-suricata, chọn interface LAN, bật rules TLS/HTTP citeturn0search6

Chúc bạn thành công triển khai **Squid + c‑icap + ClamAV** trên OPNsense 25.1 để có giải pháp SSL Inspection và quét virus toàn diện! Nếu cần thêm mẫu cấu hình squid.conf hay snippet Jinja2, cứ báo mình nhé.