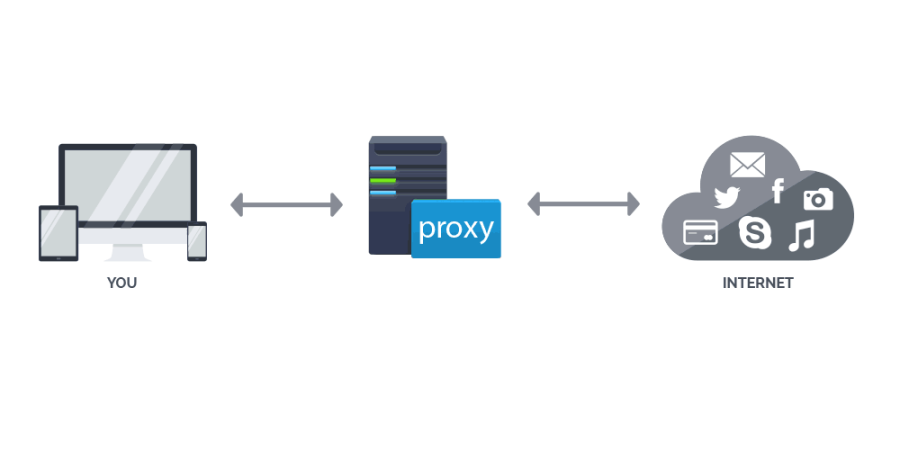
#### **Squid proxy trên pfSense**

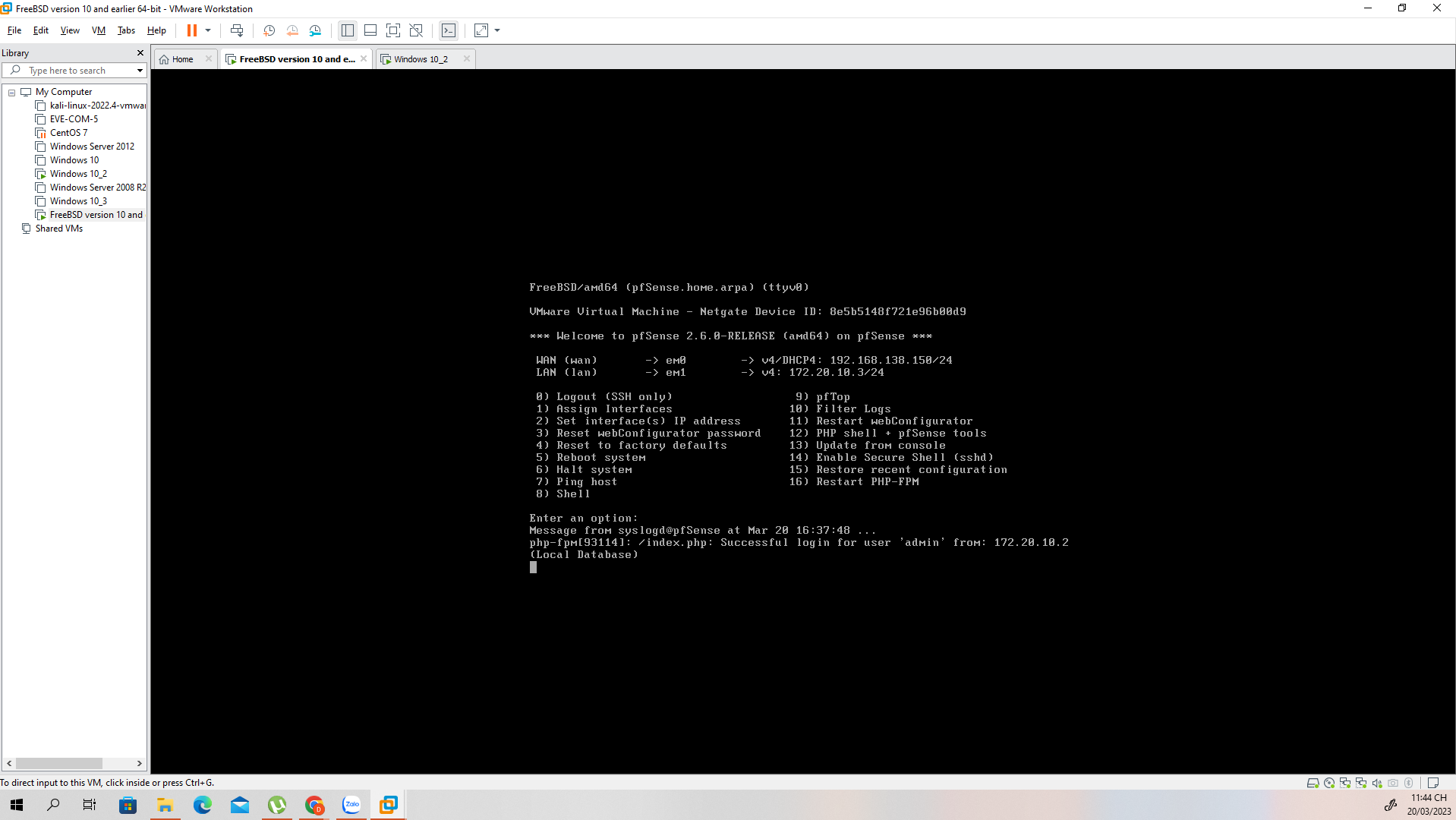
#### **Proxy là gì ?**

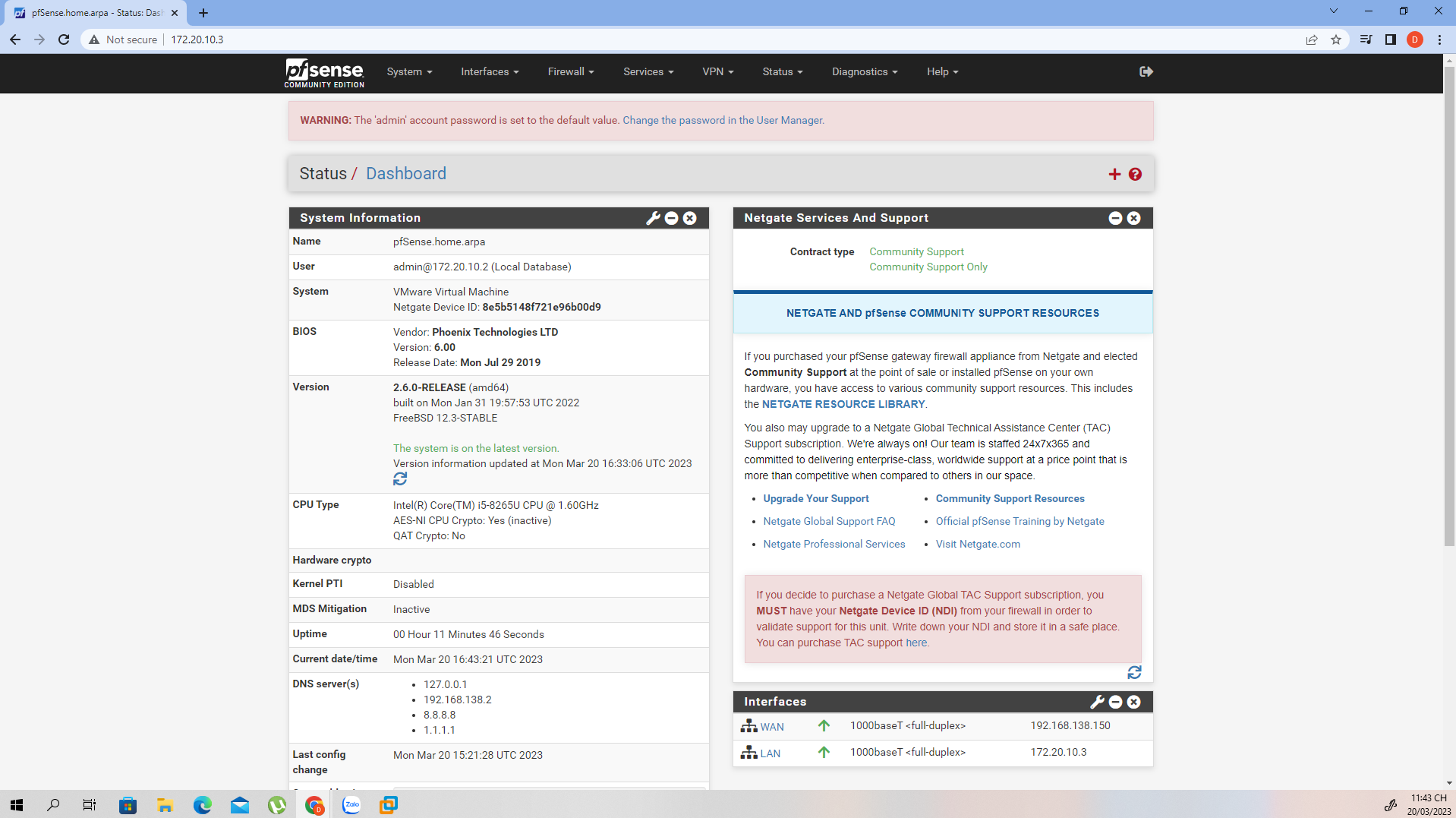
**Proxy, Server Proxy hay Proxy Server (cũng là 1), chúng ta có thể hiểu nôm na là 1 chiếc máy tính khác có nhiệm vụ xử lý dữ liệu, giống như 1 bộ chuyển đổi thông tin của tín hiệu Internet. Bằng việc kết nối qua 1 hoặc nhiều những chiếc server như trên, ban đầu máy tính của người dùng – bạn sẽ gửi đi những tín hiệu yêu cầu – request qua proxy server, tại đây những thông tin đó sẽ được xử lý và trả lại những gì bạn thấy mỗi khi truy cập vào Internet.**

**Theo cách hiểu này, thì Proxy đóng vai trò trung gian giữa chiếc máy tính bạn đang sử dụng với toàn bộ môi trường Internet bên ngoài. Bên cạnh đó, Proxy còn được dùng để lọc, ngăn chặn các website, hoặc chính xác hơn là những nội dung website tùy theo nhu cầu của chính phú, các nhà cung cấp dịch vụ…**

****

* **Đăng nhập vào Pfsense**

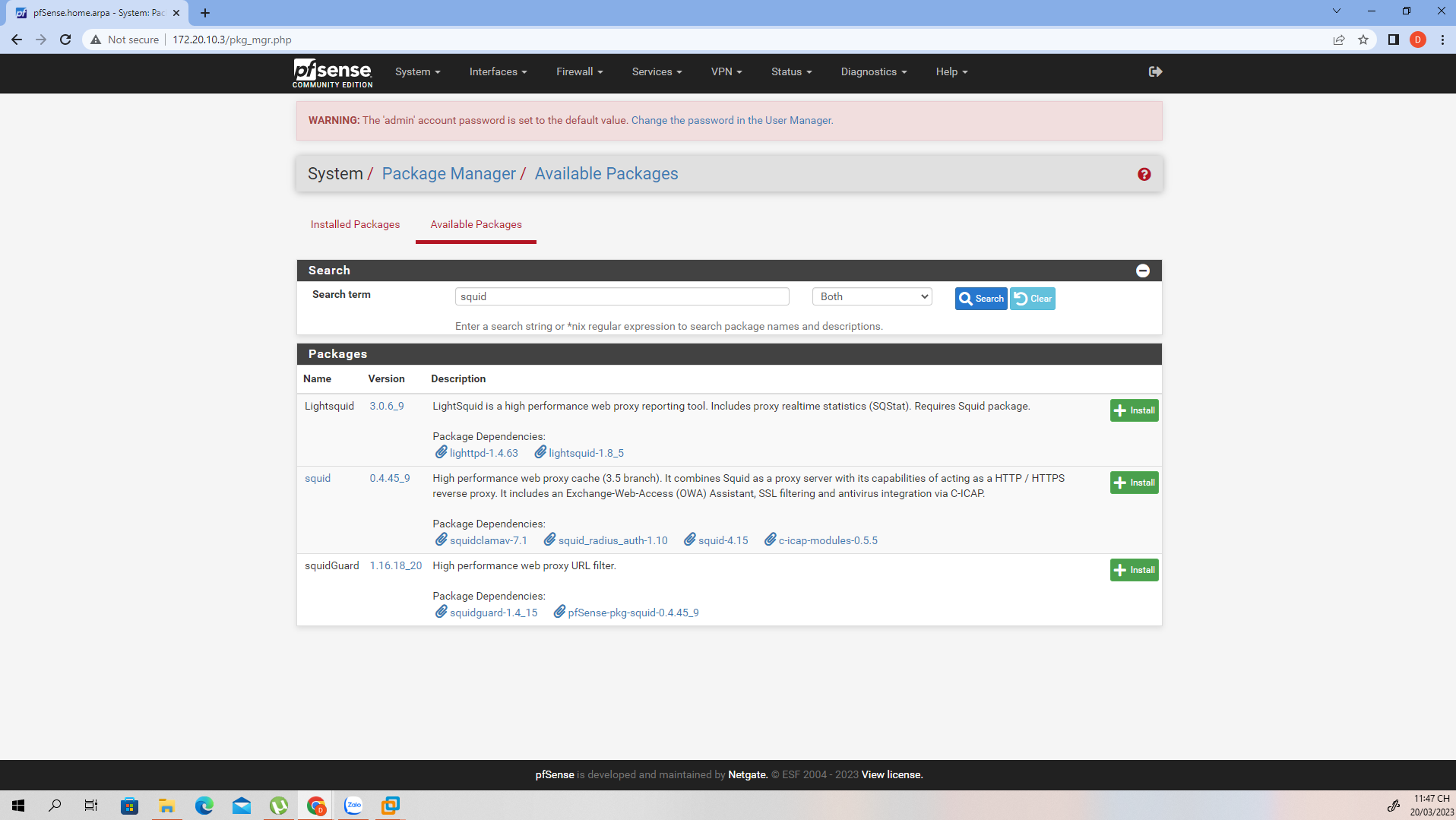


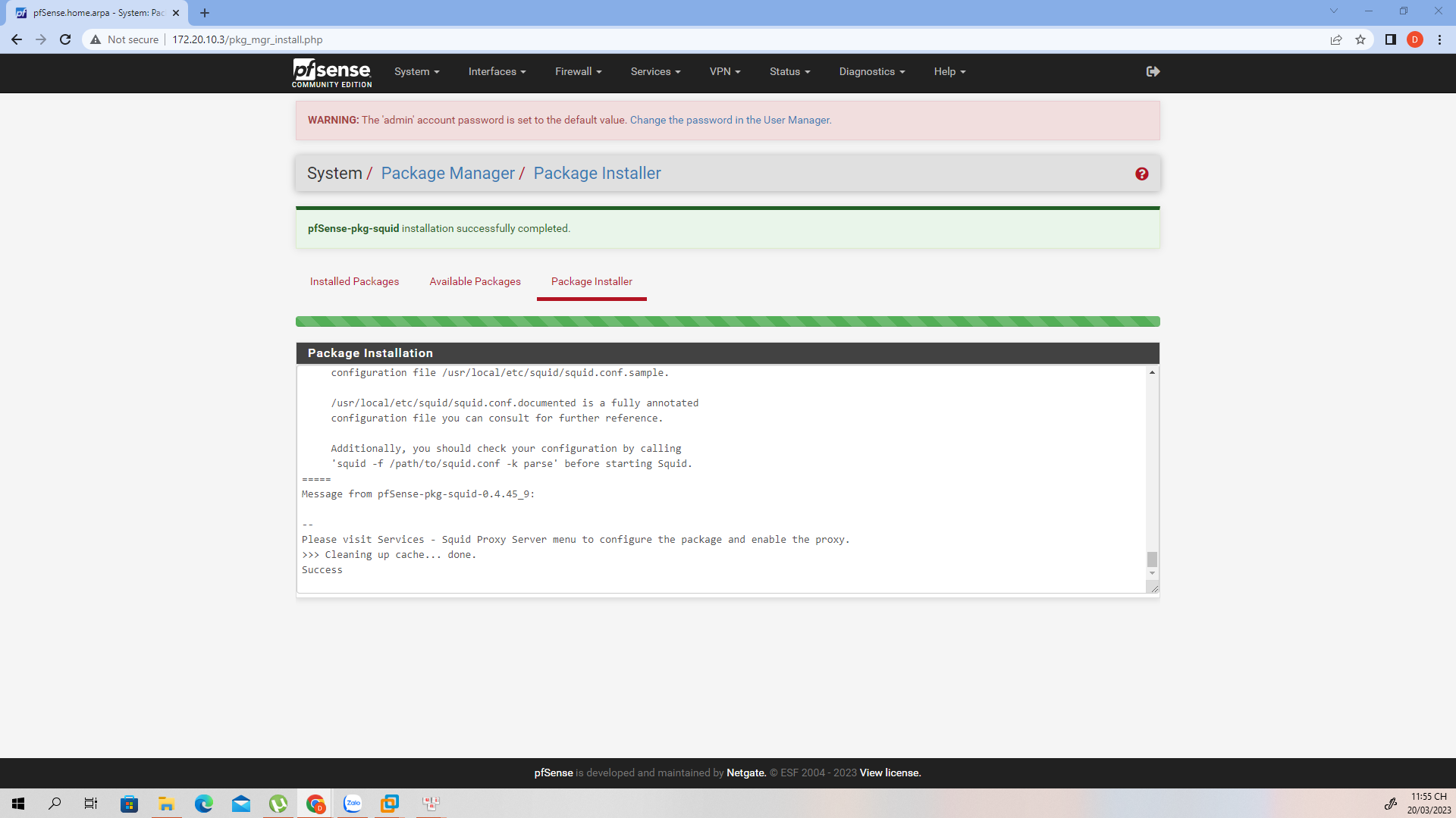


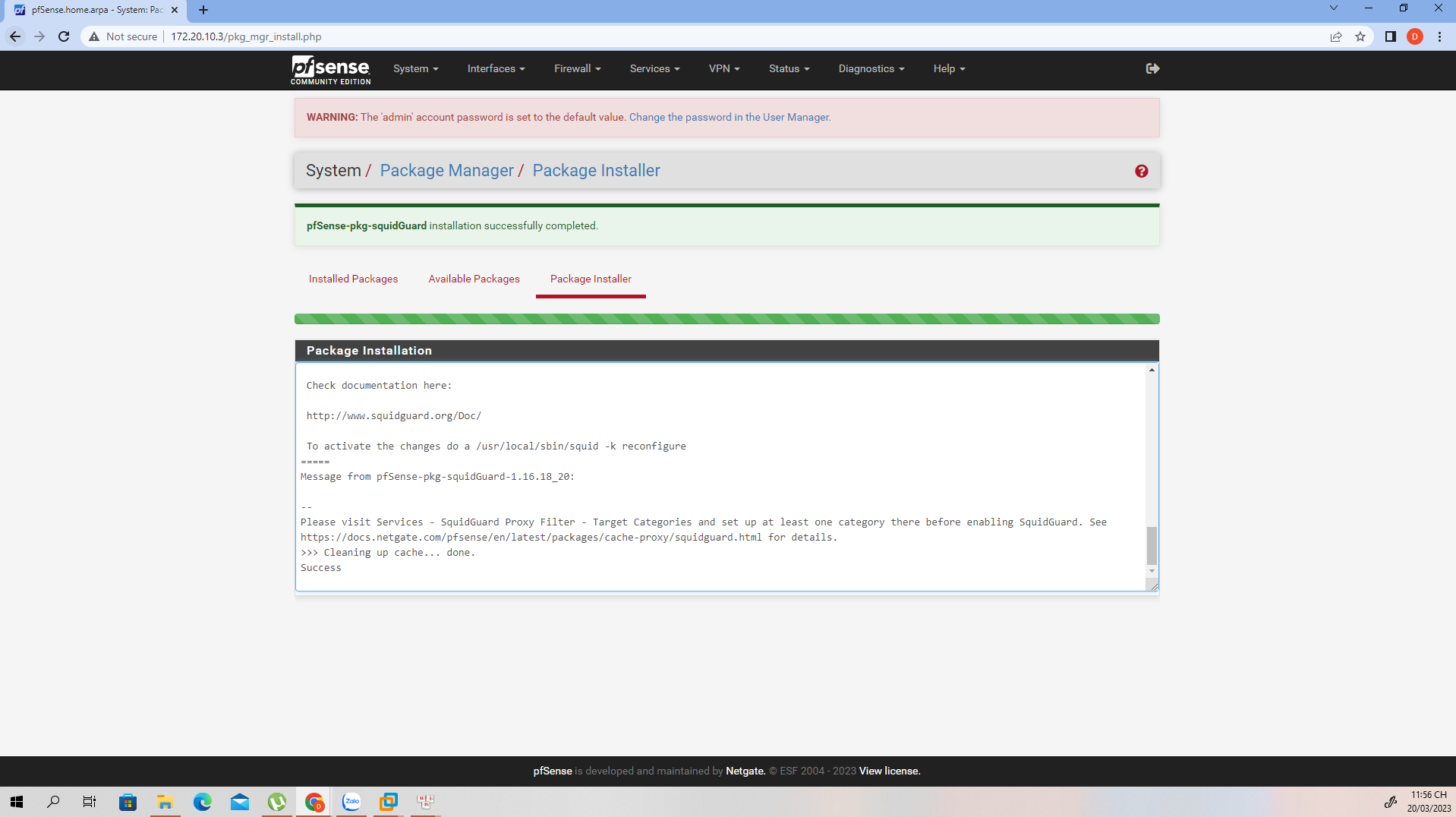
#### **1. Cấu hình squid proxy trên pfSense**

**Bước 1: Cài đặt squid package**.

– Chọn “**System** > **Package Manager** > chọn Tab **Available Packages**” , các bạn gõ “squid” vào ô tìm kiếm -> Nhấn “**Install**” để cài đặt “squid & squidGuard”





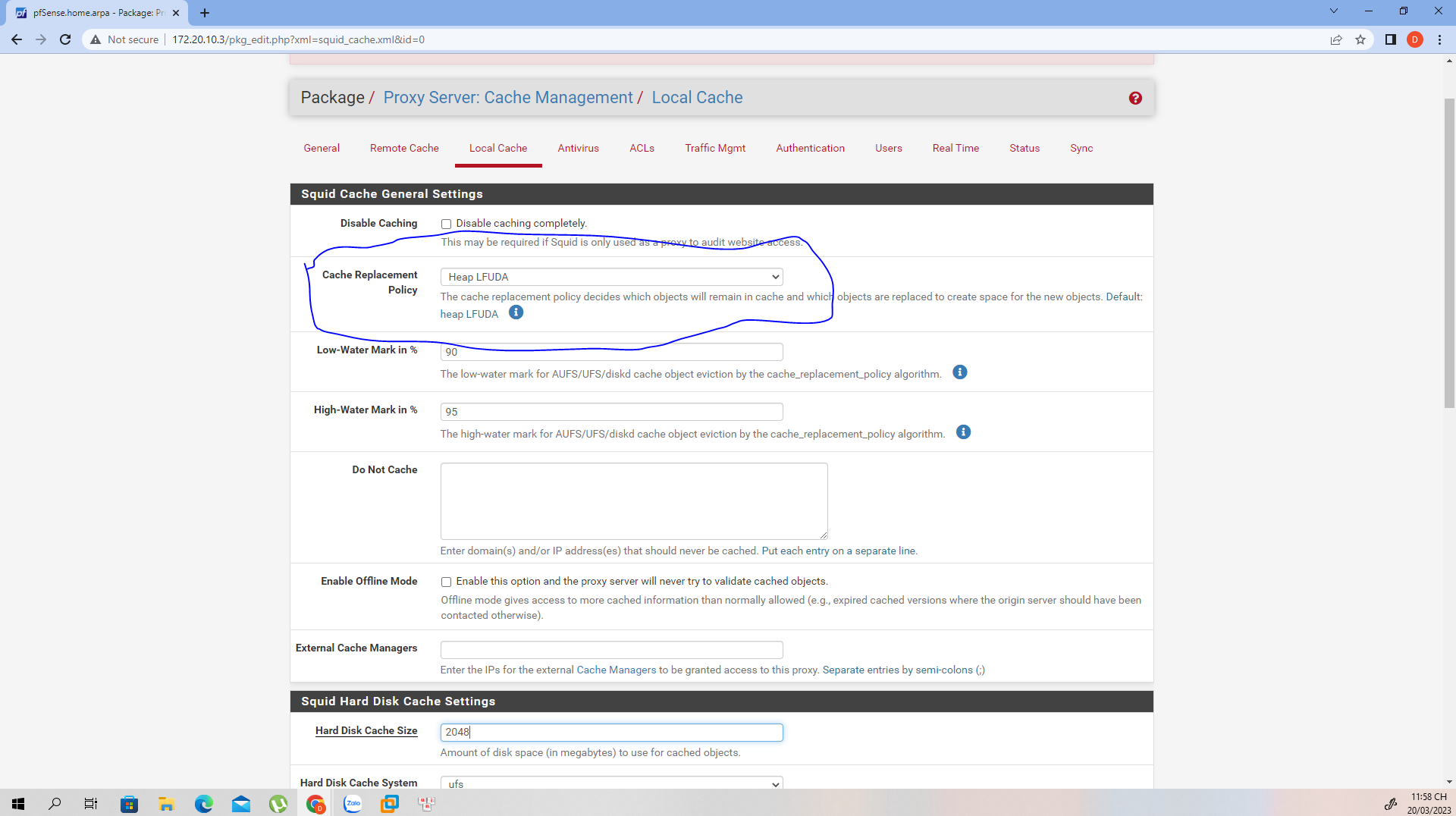


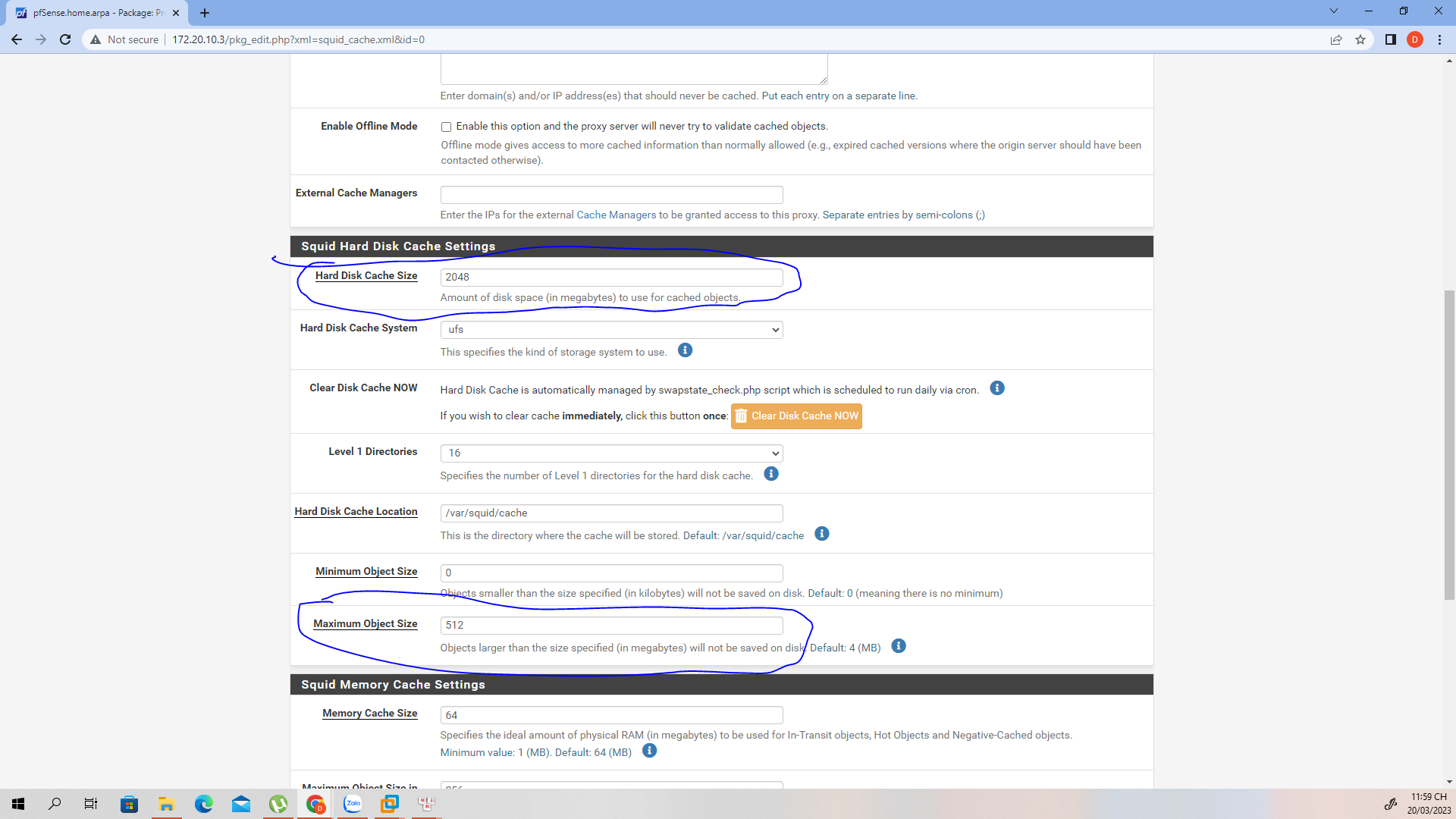
+ *Squid:* chức năng làm Proxy Server

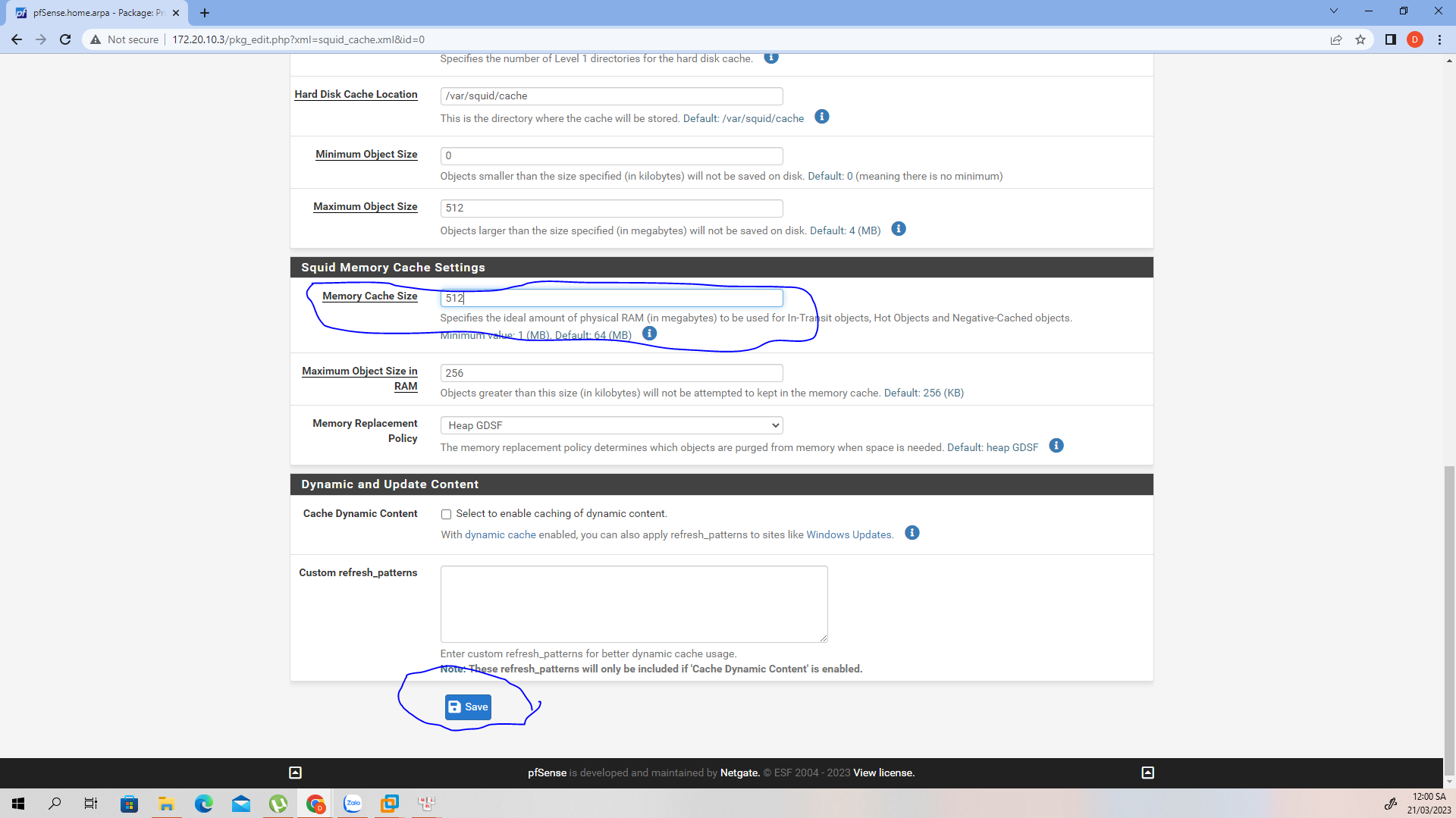
+ *SquidGuard:* cho phép ta cấu hình để lọc các đối tượng hay nói cách khác là tạo các Access List cho Proxy để cấm user truy cập vào website.

#### **Bước 2: Cấu hình squid proxy**

– **Cấu hình Local Cache** . Vào “**Services** > **Squid Proxy** **Server**> **Local Cache** Tab” .Mục **Cache Replacement: Heap LFUDA, Hard Disk Cache Size: 2048, Maximum Object Size: 512, Memory Cache size: 512** -> Click “**Save**” để lưu cấu hình







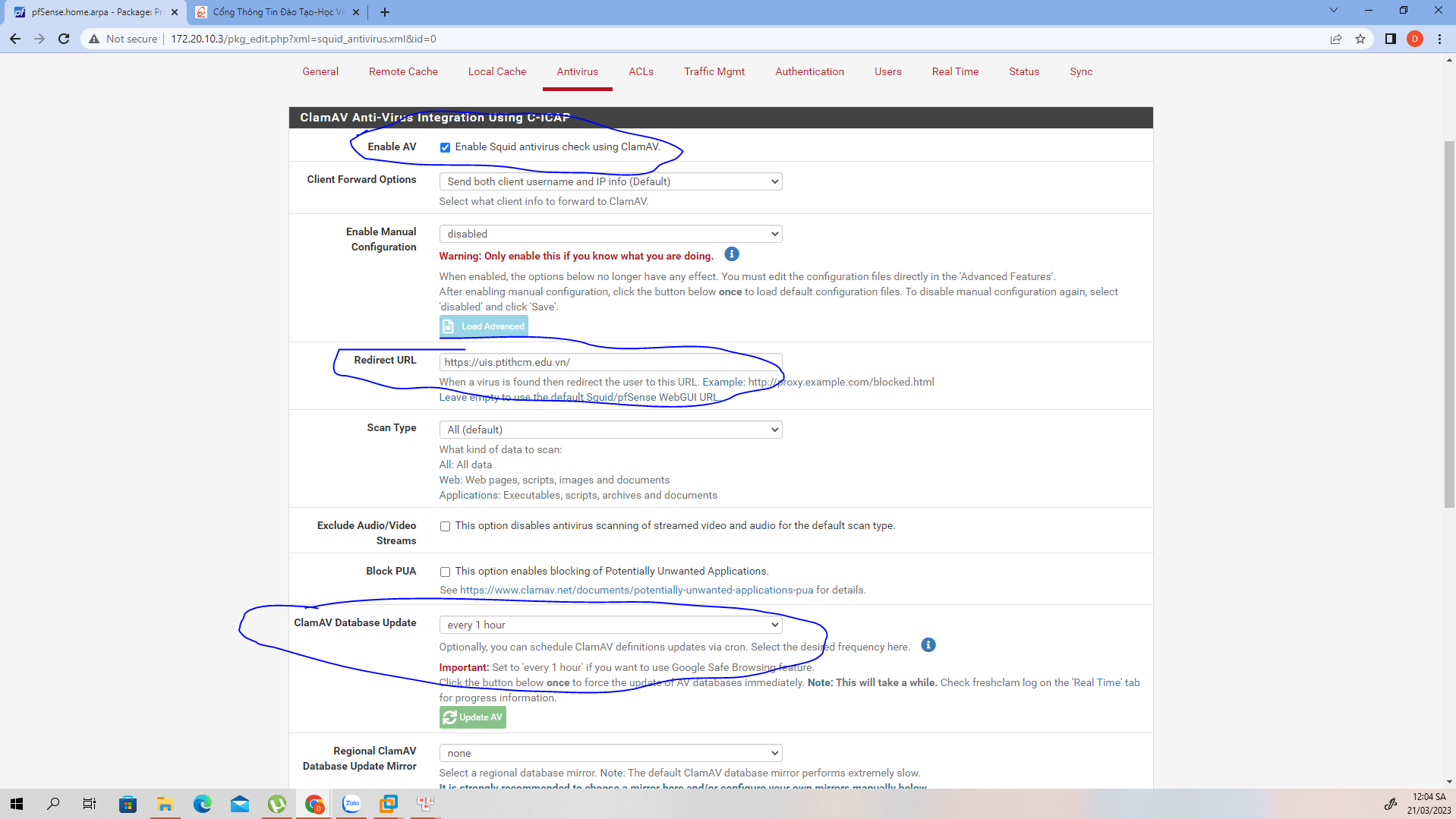
Mục Cache Replacement có 4 lựa chọn :

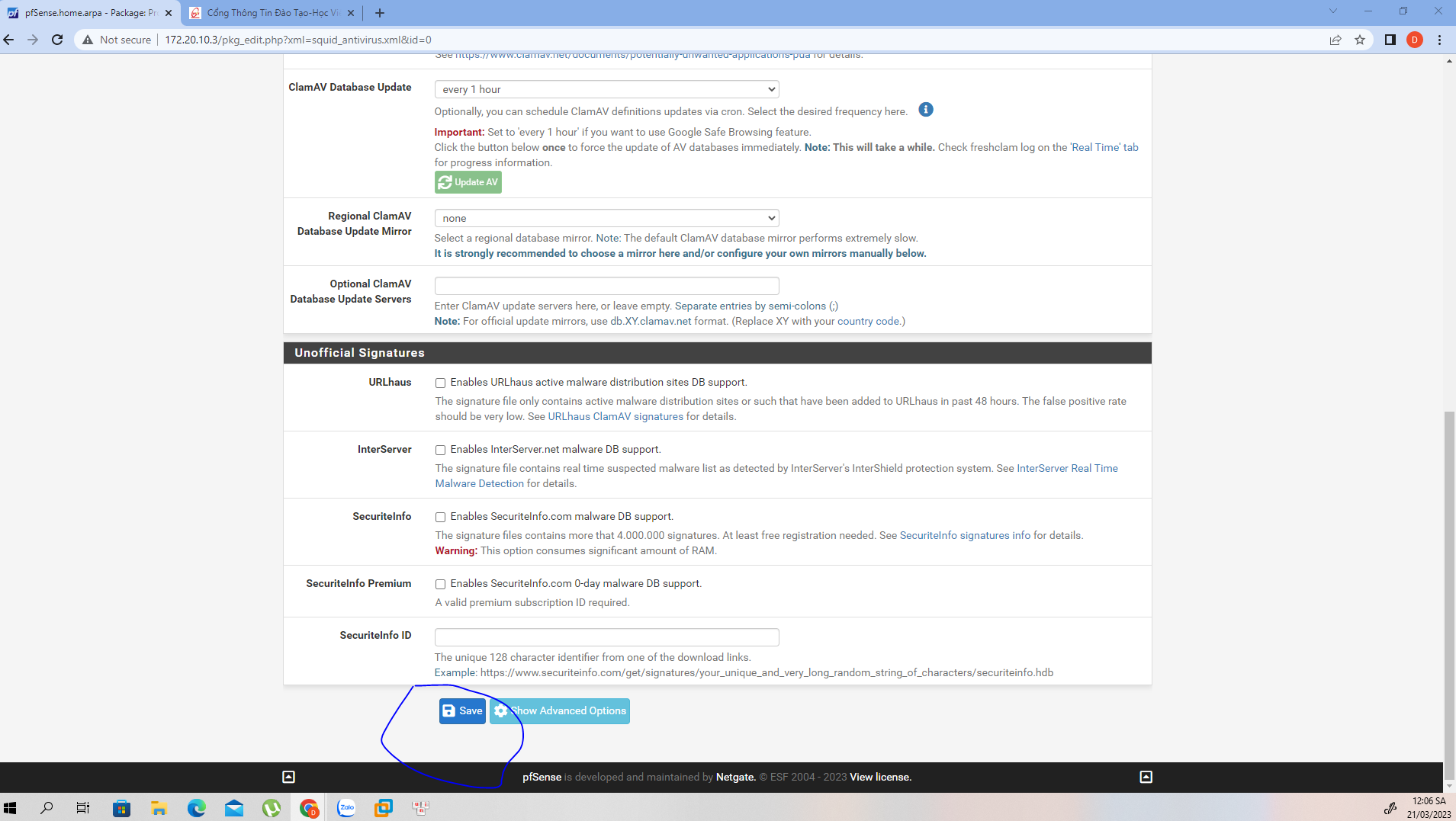
**Heap LFUDA :** Giữ các đối tượng phổ biến trong bộ nhớ cache bất kể kích thước của chúng nhờ đó tối ưu hóa tốc độ truy cập website của user

**Heal GDSF :** Tối ưu tốc độ truy cập website bằng cách lưu cache cho các đối tượng có dung lượng nhỏ hơn.

**LRU:** Giữ các đối tượng được truy cập gần nhất , các đối tượng có thời gian truy cập lâu nhất sẽ bị xóa bớt khỏi cache

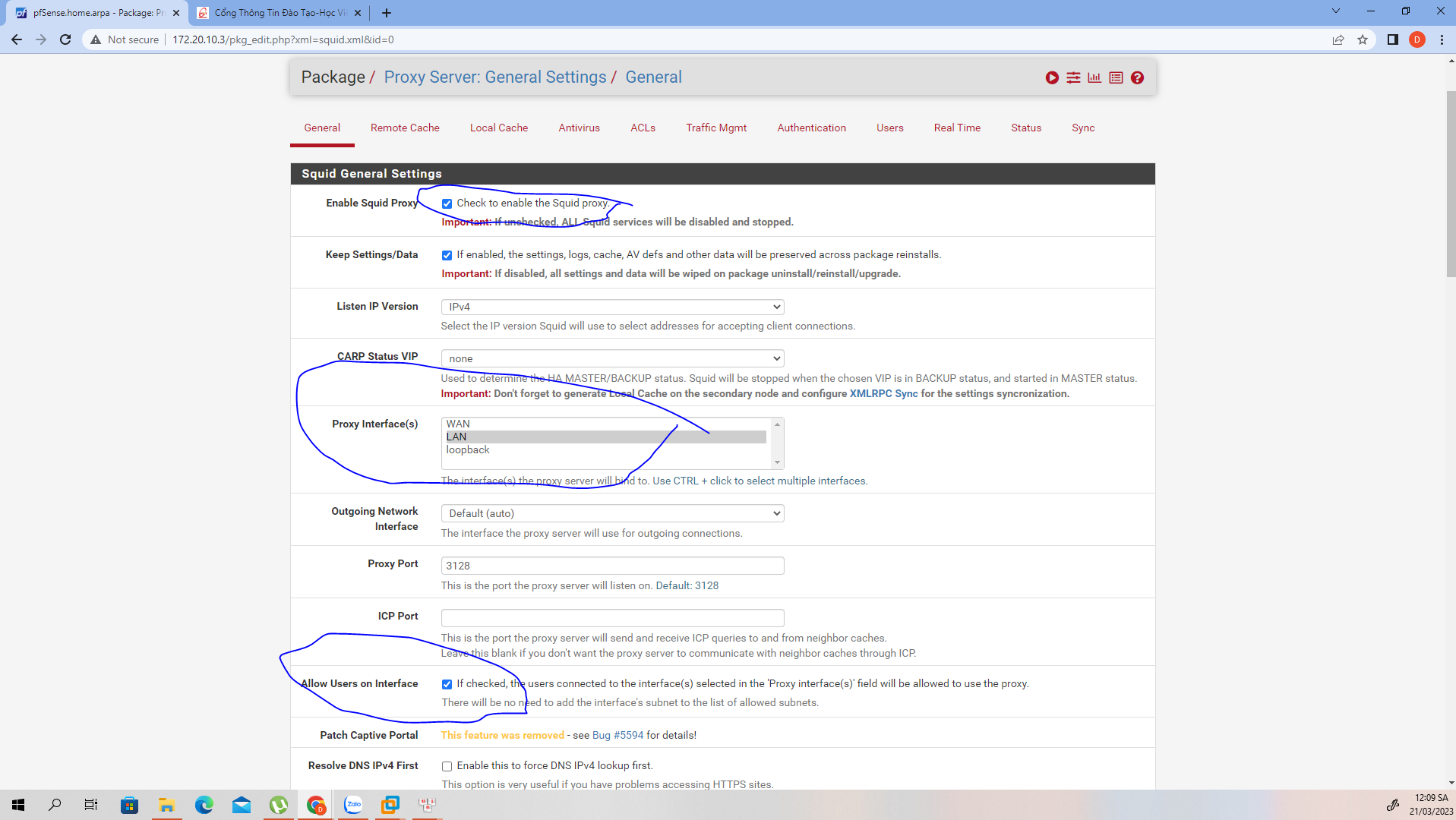
– **Tiếp theo cấu hình tích hợp antivirus**.Chọn “**Services** > **Squid Proxy** > **Antivirus** Tab” .Tích vào “**Enable Squid antivirus check using ClamAV**” , Chọn đường dẫn redirect URL nếu phát hiện virus, “**ClamAV Database Update : every 1 hour**” -> Click “**Save**” để lưu cấu hình

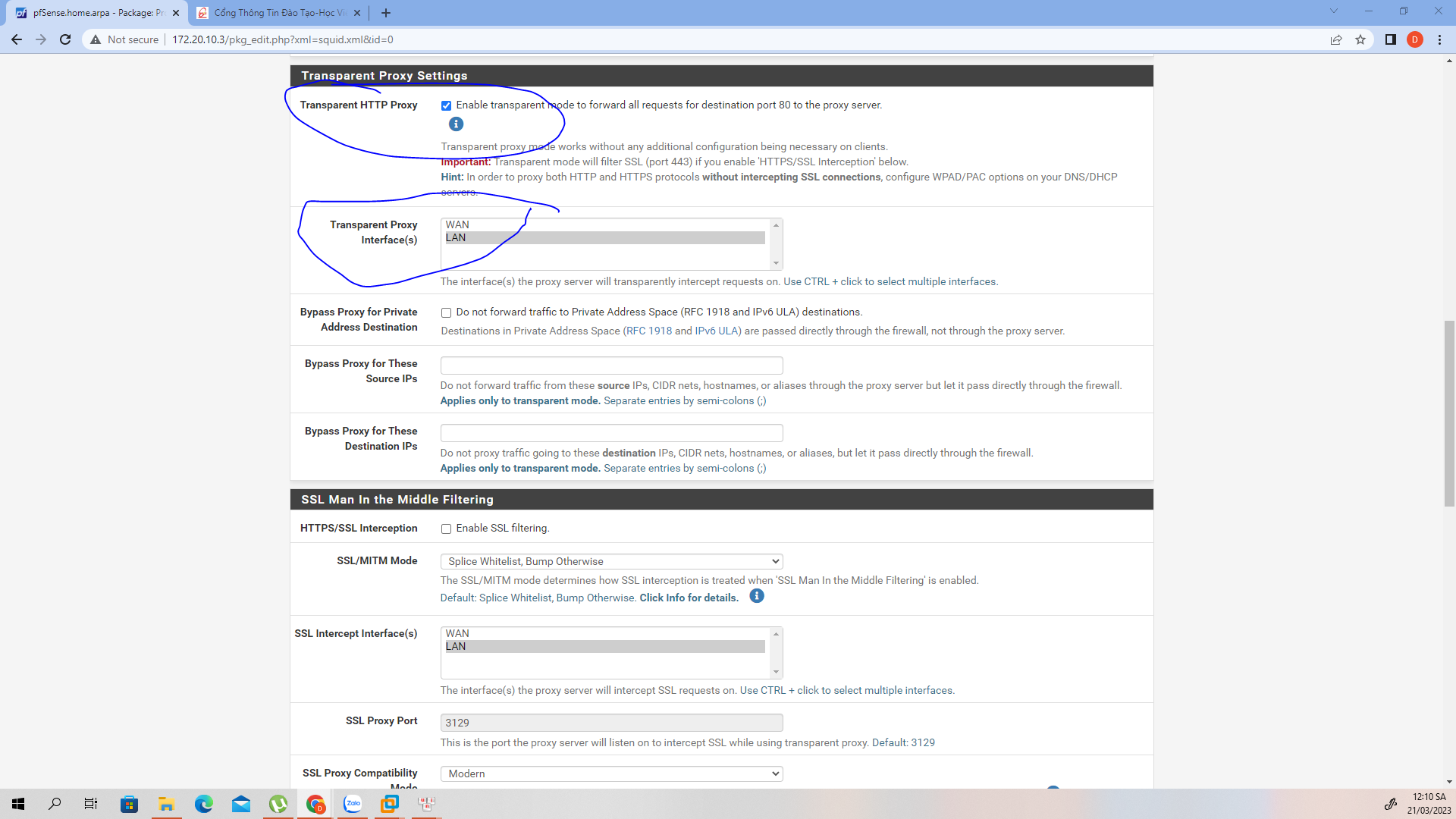


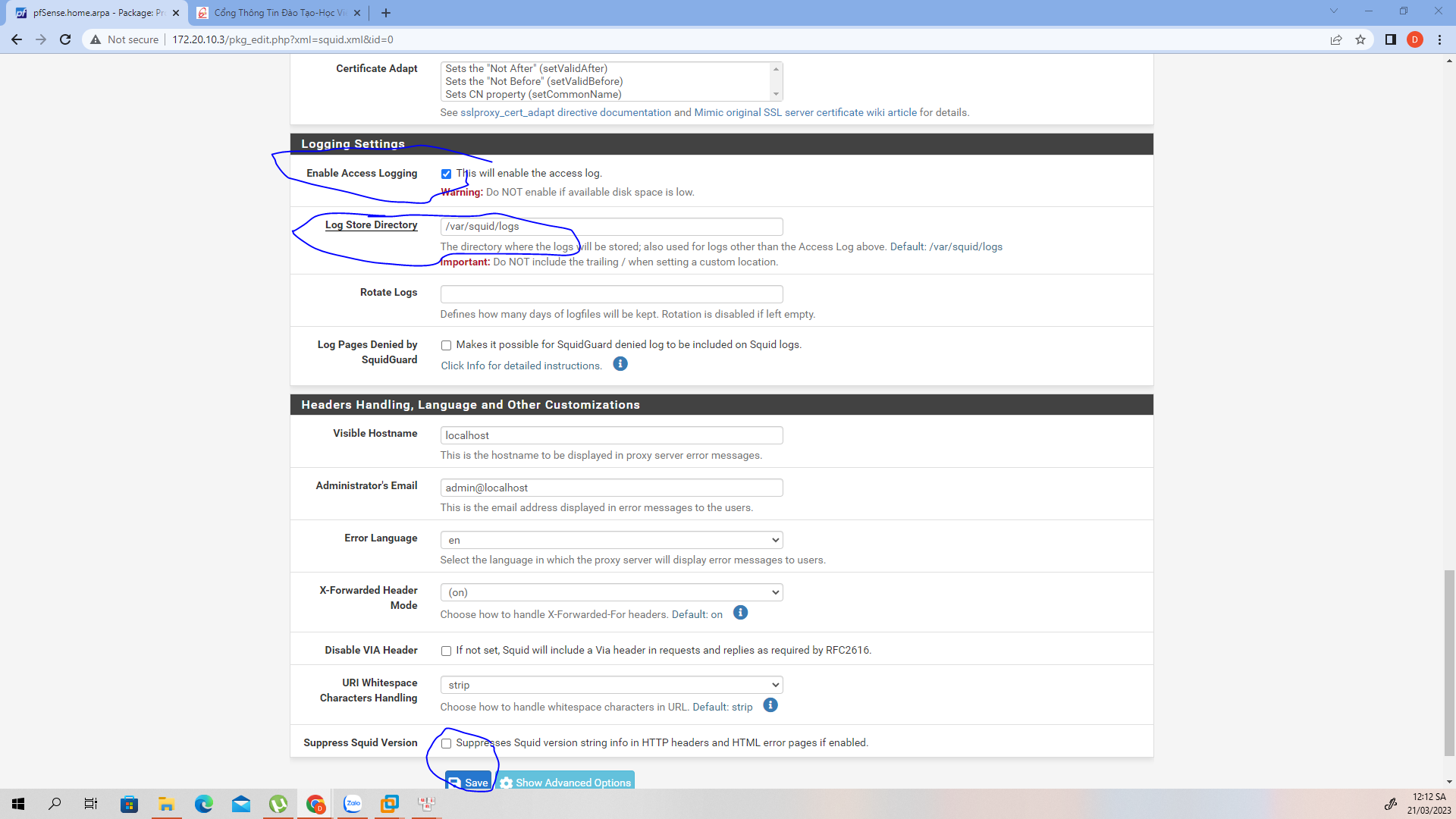


*ClamAV là một mã nguồn mở (GPL), bộ công cụ chống virus, đặc biệt là cho thư điện tử quét trên cổng email. Phát hiện hơn 750.000 virus, worms, trojan, bao gồm cả Microsoft Office virus macro, phần mềm độc hại di động và mối đe dọa khác.*

– Tiếp theo Enable Squid Proxy: Chọn “**Services** > **Squid Proxy** > **General** Tab” .Tích vào “**Check to enable the Squid Proxy**” , **Proxy interface(s): LAN**, Tích vào “**Allow Users on Interface**“, Tích vào “**Transparent HTTP Proxy**“, **Transparent Proxy Interface(s): LAN**, Tích “**Enable Access Logging**“, **Log Store Directory: /var/squid/logs** -> Click “**Save**” để lưu cấu hình

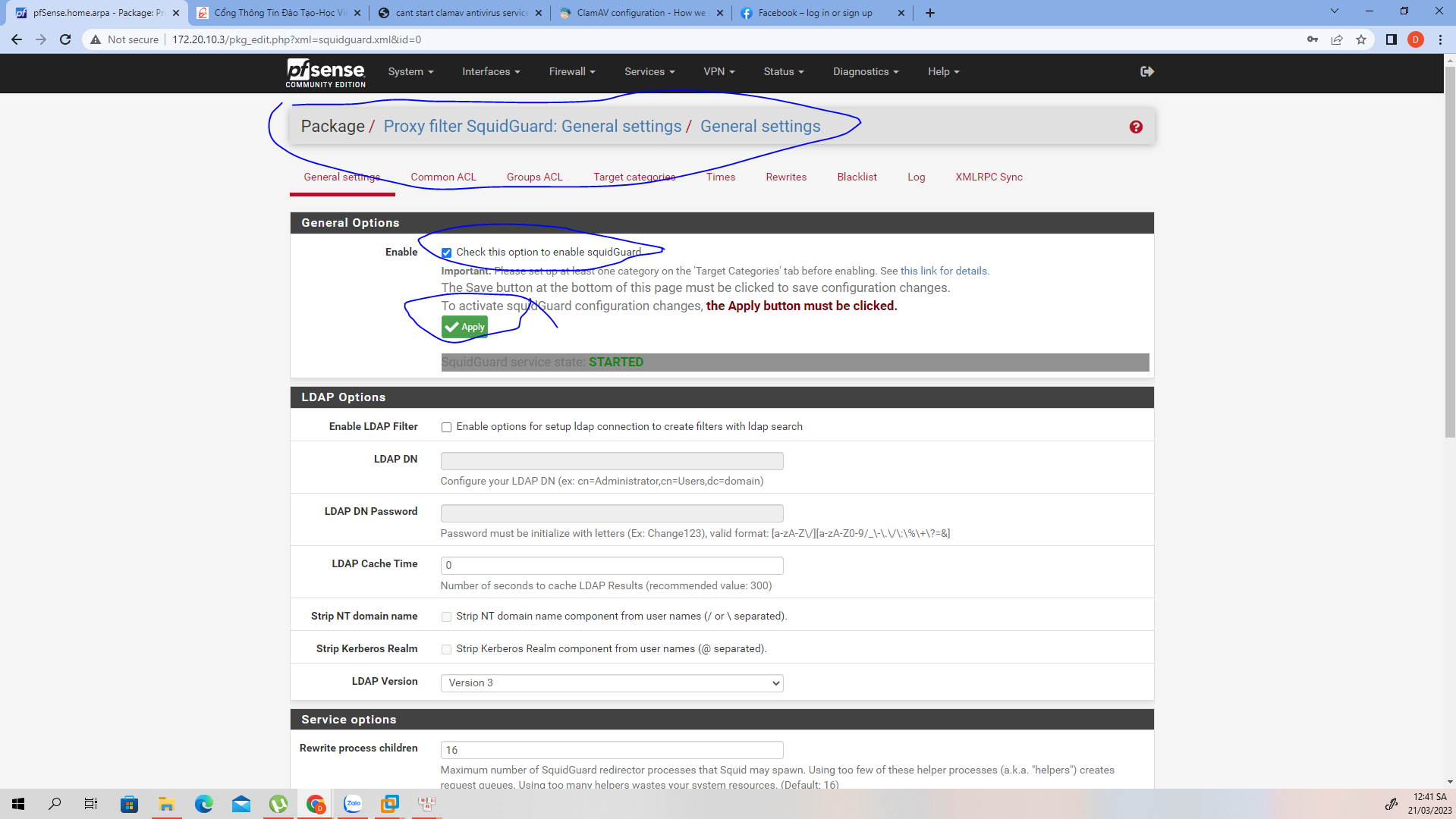




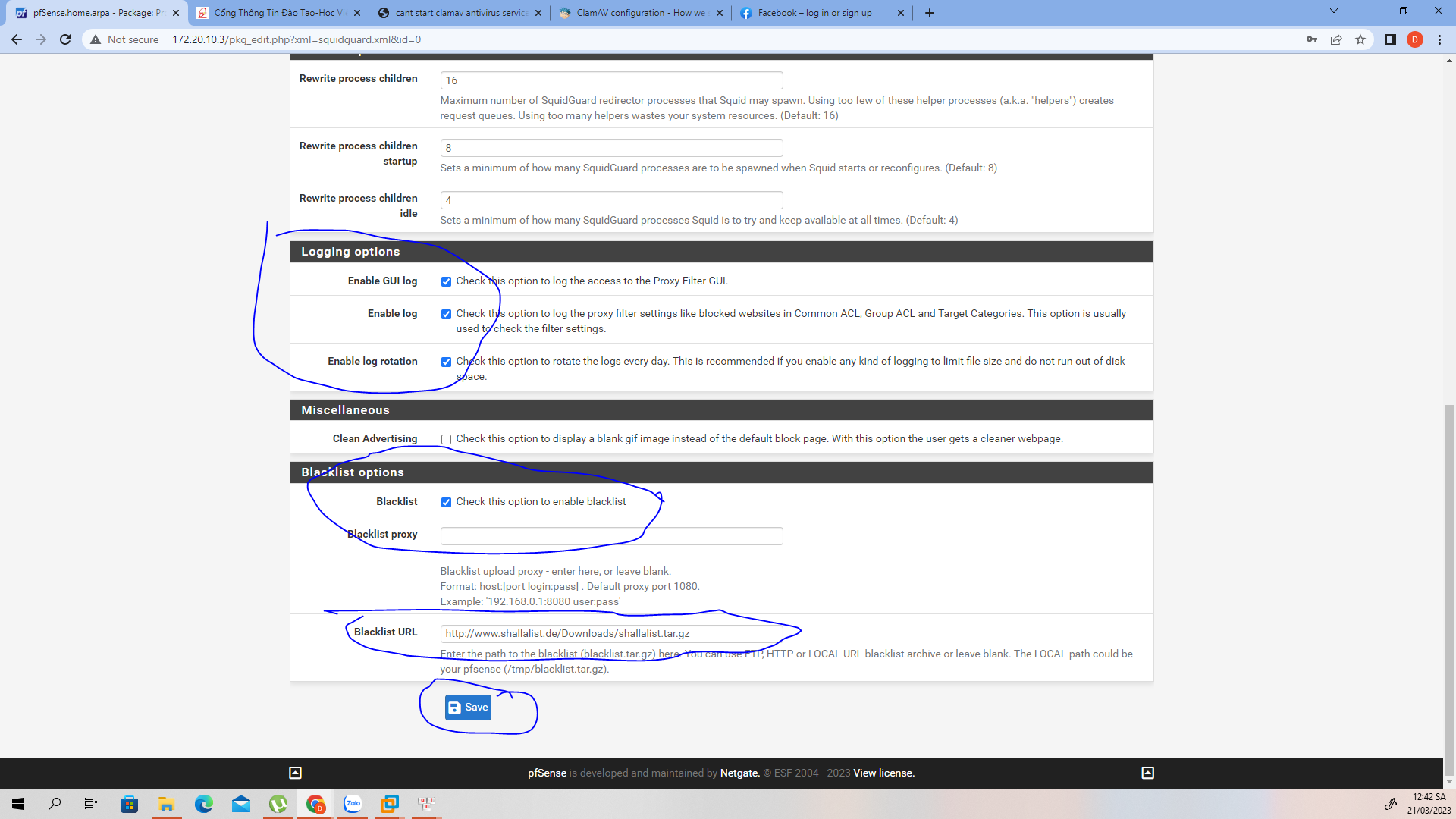


#### **2. Cấu hình squid Guard trên pfSense**

Squid Guard có tính năng chính để lọc web đen,web cấm, facebook…, để thực hiện việc này thì nó tạo ra access list rồi kết hợp với Squid Proxy để các user bên trong pfsense không truy cập được các website bị cấm.

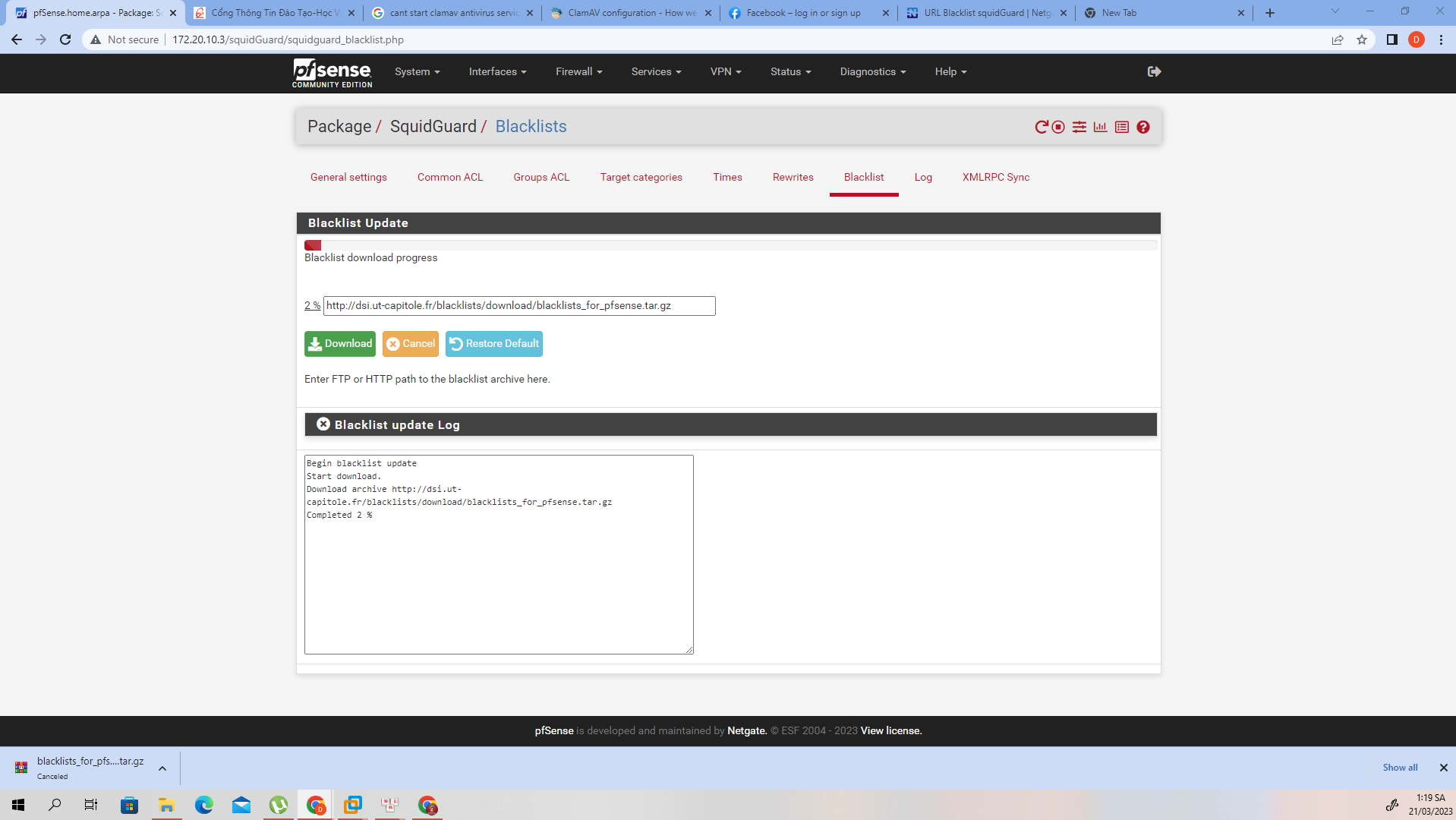


Phần **Logging** check cả 3 Options



Enable **BlackList** và nhập địa chỉ http://dsi.ut-capitole.fr/blacklists/download/blacklists\_for\_pfsense.tar.gz vào ô Blacklist URL , đây là địa chỉ update các list web đen , web bạo lực , web máu me … các thể loại web.

Tiếp theo **Services -> SquidGuard Proxy Filter -> Blacklist -> Download**



Tiếp theo **Services -> SquidGuard Proxy Filter -> Common ACL-> Target Rules List**  rồi chọn trang nào muốn deny/allow/whitelist

