ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC BÁCH KHOA  
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

Logo, company name

Description automatically generated

**Mật mã và an ninh mạng**

**Đề tài:**

**Thiết kế hệ thống tường lửa với pfSense**

Giảng viên hướng dẫn: Nguyễn Hữu Hiếu

Sinh viên thực hiện: Trần Trọng Nghĩa – 1813233

Nguyễn Văn Tĩnh – 1814356

Nguyễn Quốc Duy – 1811727

Võ Văn Toàn – 1814377

TP. Hồ Chí Minh, tháng 06 năm 2021

Mục lục

[**Chương I: Giới thiệu** 3](#_Toc74232992)

[**1.** **Đề tài** 3](#_Toc74232993)

[**2.** **Mục tiêu đề ra:** 3](#_Toc74232994)

[**Chương II: Phân tích và thiết kế hệ thống** 4](#_Toc74232995)

[**1.** **Tóm tắt** 4](#_Toc74232996)

[**2.** **Cơ sở lý thuyết** 4](#_Toc74232997)

[**2.1.** ***Firewall*** 4](#_Toc74232998)

[*2.1.1.* *Tổng quan Firewall* 4](#_Toc74232999)

[*2.1.2.* *Chức năng của Firewall* 5](#_Toc74233000)

[*2.1.3.* *Nguyên lý hoạt động của Firewall* 6](#_Toc74233001)

[*2.1.4.* *Phân loại* 7](#_Toc74233002)

[***2.2.*** ***pfSense*** 7](#_Toc74233003)

[*2.2.1.* *Giới thiệu về firewall PfSense* 7](#_Toc74233004)

*2.2.2. Các chức năng cơ bản của PfSense……………………………………………………….8*

[**Chương III: Hiện thực và đánh giá hệ thống** 9](#_Toc74233005)

[**1.** **Hiện thực** 9](#_Toc74233006)

[***1.1.*** ***Công cụ hiện thực*** 9](#_Toc74233007)

[***1.2.*** ***Các bước hiện thực*** 9](#_Toc74233008)

[*1.2.1.* *Cài đặt các gói bổ sung cho pfSense.* 9](#_Toc74233009)

[*1.2.2.* *Hiện thực các chức năng* 11](#_Toc74233010)

[a. Sử dụng ClamAV trong gói Squid để bảo vệ các máy Client khỏi virus, hỗ trợ HTTP/HTTPS. 11](#_Toc74233011)

[b. Sử dụng SquidGuard để chặn URL/Keyword/Prase 20](#_Toc74233012)

[c. Sử dụng Snort để phát hiện và ngăn chặn xâm nhập qua Java Applet, ActiveX. 25](#_Toc74233013)

[**2.** **Đánh giá hệ thống** 28](#_Toc74233014)

[**Chương IV: Kết luận** 29](#_Toc74233015)

[**Tài liệu tham khảo** 30](#_Toc74233016)

# **Chương I: Giới thiệu**

1. **Đề tài**

Triển khai một hệ thống bức tường lửa với nhiều chức năng bổ sung. Bạn có thể dùng các mã nguồn mở có trên web như pfSense Squid, SquidGuard, ClamAV,...

Hệ thống có các chức năng sau:

* Firewall: bộ lọc gói có trạng thái, không giới hạn số lượng giao tiếp mạng, nhiều giao tiếp mạng trên một zone và nhiều zone trên một giao tiếp, quản lý chỉ linh động (NAT, PAT).
* Lọc Web: chặn dựa trên URL/Keyword/Pharse, chặn Java Applet, Cookies, Active X.
* Antivirus: Hỗ trợ lọc trên các giao thức HTTP/HTTPS và cơ sở dữ liệu về virus được cập nhật tự động.
* Quản trị: Thông qua Web.

1. **Mục tiêu đề ra:**

Tìm hiểu các mối đe dọa đối với một hệ thống mạng máy tính.

* Tìm hiểu các khái niệm cơ bản của Firewall.
* Nghiên cứu về các công nghệ Firewall và cách làm việc của chúng.
* Mỗi thành viên trong nhóm tìm hiểu và hiện thực được ít nhất 1 trong các chức năng ở trên.
* Thực hiện demo thành công các chức năng sử dụng mã nguồn mở có trên web như pfSense Squid, SquidGuard, ClamAV,...

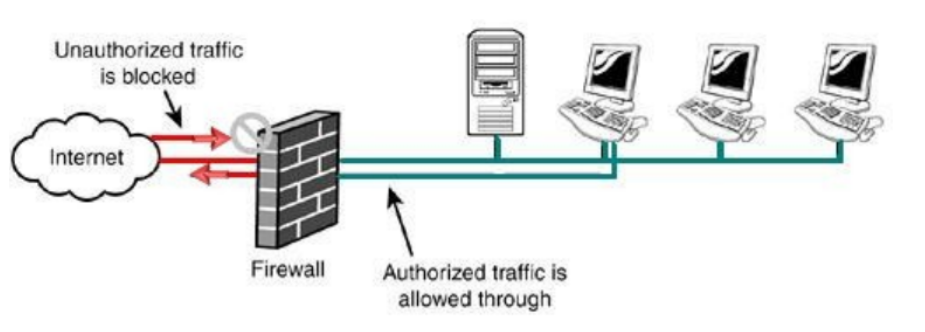
# **Chương II: Phân tích và thiết kế hệ thống**

1. **Tóm tắt**

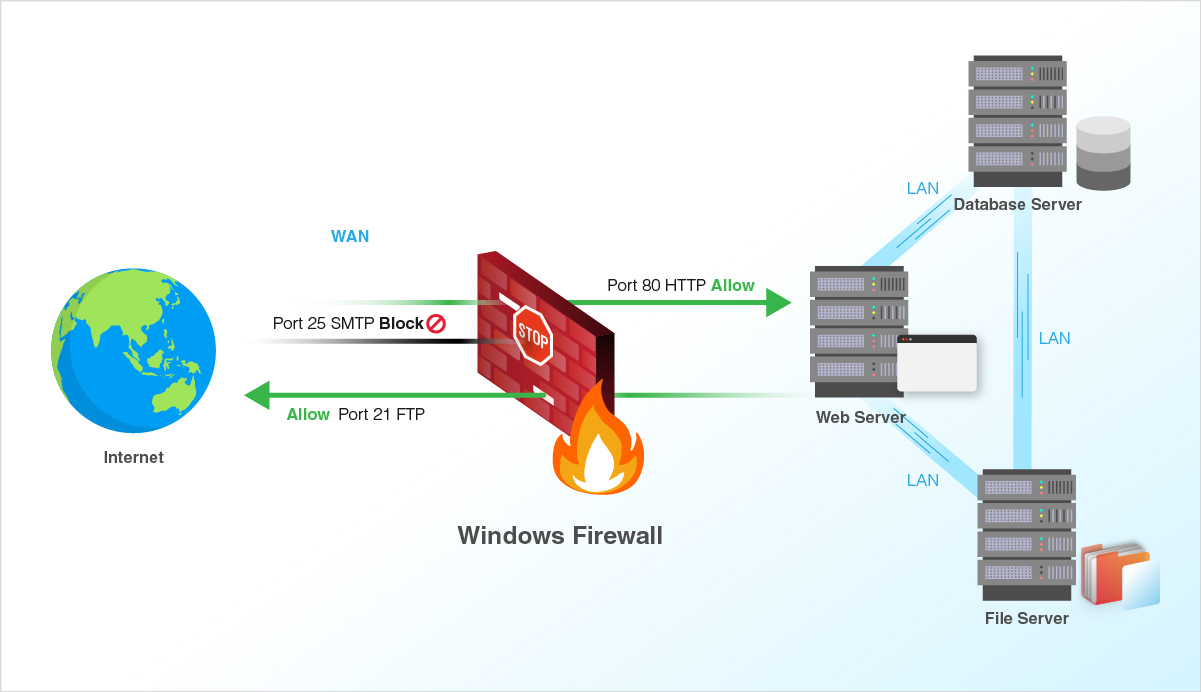
Triển khai hệ thống Firewall để bảo vệ mạng là vấn đề cấp thiết để việc sử dụng internet an toàn, hiệu quả và hạn chế những rủi ro, sự cố mất an toàn thông tin như: virus, bị xâm nhập, bị tấn công, mất dữ liệu hay bị mã hóa dữ liệu,…Xác định được tầm quan trọng trong việc bảo mật an toàn hệ thống mạng cũng như dữ liệu vì vậy việc triển khai hệ thống Firewall mã nguồn mở cho hệ thống mạng là hết sức cần thiết và áp dụng thực tiễn. Bài báo cáo này trình bày về cách hoạt động và quá trình triển khai các chức năng bảo vệ ứng dụng phần mềm mã nguồn mở PfSense.

1. **Cơ sở lý thuyết**
   1. ***Firewall***
      1. *Tổng quan Firewall*

Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết trong xây dựng để ngăn chặn, hạn chế hỏa hoạn. Trong công nghệ mạng thông tin, Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Firewall là hệ thống ngăn chặn việc truy cập trái phép từ bên ngoài vào mạng cũng như những kết nối không hợp lệ từ bên trong ra. Firewall thực hiện việc lọc bỏ những địa chỉ không hợp lệ dựa theo các quy tắc hay chỉ tiêu định trước.



Firewall là thiết bị hệ thống phần cứng hoặc phần mềm hoặc kết hợp cả 2. Tính chất chung của các Firewall là phân biệt địa chỉ IP dựa trên các gói tin hay từ chối việc truy cập bất hợp pháp căn cứ trên địa chỉ nguồn, việc này tương tự với hoạt động của các bức tường ngăn lửa trong các toà nhà. Firewall được miêu tả như hệ thống phòng thủ bao quanh với các “chốt” để kiểm soát tất cả các luồng lưu thông nhập xuất. Có thể theo dõi và khóa truy cập tại các chốt này.



* + 1. *Chức năng của Firewall*

Chức năng chính của Tường Lửa ( Firewall) là kiểm soát luồng thông tin giữa môi trường intranet và internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong và mạng internet.

* Cho phép hoặc cấm các dịch vụ truy cập ra ngoài.
* Cho phép hoặc cấm các dịch vụ từ ngoài truy cập vào trong.
* Theo dõi luồng dữ liệu giữ môi trường intranet và internet .
* Kiểm soát địa chỉ truy cập, cấm hoặc cho phép địa chỉ được truy nhập.
* Kiểm soát người dùng và việc truy cập của người dùng.
* Kiểm soát nội dung thông tin, gói tin lưu chuyển trên hệ thống mạng.
* Lọc các gói tin dựa vào địa chỉ nguồn, địa chỉ đích và số cổng ( port), giao thức
* Có thể sử dụng để ghi lại tất cả các sự cố gắng truy nhập vào mạng và báo cáo cho người quản trị

Một Firewall khảo sát tất cả các luồng lưu lượng giữa 2 mạng để xem nó có đạt chuẩn hay không. Nếu nó đạt, nó được định tuyến giữa các mạng, ngược lại nó bị hủy. Một bộ lọc Firewall lọc cả lưu lượng ra lẫn lưu lượng vào. Nó cũng có thể quản lý việc truy cập từ bên ngoài vào nguồn tài nguyên mạng của hệ thống và có thể truy cập xa hơn, các hoạt động của kẻ tấn công có thể được ghi lại và theo dõi.

Nếu có thể giữ kẻ phá hoại trong một thời gian, người quản trị có thể lần theo dấu vết của hộ. Ví dụ, có thể dùng lệnh finger để theo vết kẻ tấn công hoặc tạo ra tập tin “bẫy mồi” để họ phải mất thời gian truyền lâu, sau đó theo vết việc truyền tập tin về nơi của kẻ tấn công qua kết nối Internet.

* + 1. *Nguyên lý hoạt động của Firewall*

Firewall hoạt động chặt chẽ với giao thức TCP/IP, vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS,...) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các packet và những con số địa chỉ của chúng.

Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (header), dùng để cho phép truyền các packet đó ở trên mạng. Bao gồm:

Địa chỉ IP nơi xuất phát (Source)

Địa chỉ IP nơi nhận (Destination)

Những thủ tục truyền tin (TCP, UDP, ICMP, Ip tunnel,...)

Cổng TCP/UDP nơi xuất phát, nơi nhận

Dạng thông báo ICMP

Giao diện packet đến và đi

Nếu packet thỏa các luật lệ đã được thiết lập trước của Firewall thì packet đó được chuyển qua, nếu không thỏa thì sẽ bị loại bỏ. Việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định được phép mới vào được hệ thống mạng cục bộ. Cũng nên lưu ý là do việc kiểm tra dựa trên header của các packet nên bộ lọc không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu. Trong các phần sau chúng ta sẽ cùng tìm hiểu các kỹ thuật để vượt tường lửa.

* + 1. *Phân loại*

Firewall được chia làm 2 loại:

a. Firewall cứng:

Là những loại firewall được tích hợp trên Router. Các tổ chức lớn thì có thể sử dụng Router Cisco còn đối với mạng LAN trong gia đình thì thưởng sử dụng Router ADSL. Đặc điểm của Firewall cứng:

* Không linh hoạt như firewall mềm. Không thể thêm chức năng, thêm quy tắc như firewall mềm
  + Firewall cứng hoạt động ở tầng thấp hơn firewall mềm. Tầng Network và tầng Transport.
  + Firewall cứng không thể kiểm tra được nội dung của gói tin
  + Firewall cứng phổ biến nhất NAT (Network Address Translate)

b. Firewall mềm

Là những firewall được cài đặt trên Server. Đặc điểm của firewall mềm:

* Tính linh hoạt cao có thể thêm bớt các quy tắc, các chức năng.
* Firewall mềm hoạt động ở tầng cao hơn firewall cứng. Tầng ứng dụng (Application)
* Firewall mềm có thể kiểm tra được nội dung gói tin thông qua các từ khóa
* Các kiểu firewall mềm: Zone Alarm, Norton Firewall,...
  1. ***pfSense***
     1. *Giới thiệu về firewall PfSense*

Để bảo vệ cho hệ thống mạng bên trong thì chúng ta có nhiều giải pháp như sử dụng Router Cisco, dùng tường lửa của Microsoft ISA,... Tuy nhiên chi phí tương đối tốn kém. Nếu muốn có một tường lửa bảo vệ hệ thống mạng bên trong khi mà chúng ta giao tiếp với hệ thống mạng bên ngoài thì pfSense là một giải pháp tiết kiệm và hiệu quả tương đối tốt nhất đối với người dùng. PfSense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này sẽ cho phép mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. PfSense đã có hơn 1 triệu download và được sử dụng để bảo vệ các mạng ở tất cả kích cỡ, từ các mạng gia đình đến các mạng lớn của của các công ty. Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi phát hành nhằm cải thiện hơn nữa tính bảo mật, sự ổn định và khả năng linh hoạt của nó Pfsense bao gồm nhiều tính năng mà vẫn thấy trên các thiết bị tường lửa hoặc router thương mại, chẳng hạn như GUI trên nền Web tạo sự quản lý một cách dễ dàng, tích hợp tính năng phát hiện và phòng chống xâm nhập mạng Snort,…

Pfsense hỗ trợ lọc bởi địa chỉ nguồn và địa chỉ đích, cổng nguồn hoặc cổng đích hay địa chỉ IP. Nó cũng hỗ trợ chính sách định tuyến và có thể hoạt động trong các chế độ bridge hoặc transparent, cho phép bạn chỉ cần đặt pfSense ở giữa các thiết bị mạng mà không cần đòi hỏi việc cấu hình bổ sung. PfSense cung cấp NAT (Network Address Translation) và tính năng chuyển tiếp cổng, tuy nhiên ứng dụng này vẫn còn một số hạn chế với Point-to-Point Tunneling Protocol (PPTP), Generic Routing Encapsulation (GRE) và Session Initiation Protocol (SIP) khi sử dụng NAT. PfSense được dựa trên FreeBSD và giao thức Common Address Redundancy Protocol (CARP) của FreeBSD, cung cấp khả năng dự phòng bằng cách cho phép các quản trị viên nhóm hai hoặc nhiều tường lửa vào một nhóm tự động chuyển đổi dự phòng. Vì nó hỗ trợ nhiều kết nối mạng diện rộng (WAN) nên có thể thực hiện việc cân bằng tải và nhiều tính năng vượt trội. Tuy nhiên có một hạn chế với nó ở chỗ chỉ có thể thực hiện cân bằng lưu lượng phân phối giữa hai kết nối WAN và bạn không thể chỉ định được lưu lượng qua một kết nối.

* + 1. *Các chức năng cơ bản của Pfsense*

1. *Pfsense Aliases:*

Aliases có thể giúp ta tiết kiệm một lượng lớn thời gian nếu bạn sử dụng chúng một cách chính xác Một Aliases cho phép bạn sử dụng thay cho địa chỉ một host , hoặc một mạng có thể được sử dụng khi tạo các rules trong pfSense .Sử dụng Aliases sẽ giúp ta đại diện cho nhiều địa chỉ bằng 1 định danh duy nhất,có nghĩa là thay vì tạo nhiều rule thì ta chỉ gom lại trong 1 rule duy nhất từ đó việc quản lí các rules sẽ dễ dàng hơn.

1. *NAT (Network Address Translation):*

PfSense cung cấp NAT và tính năng chuyển tiếp cổng. Trong Firewall cũng có thể cấu hình các thiết lập NAT nếu cần sử dụng cổng chuyển tiếp cho các dịch vụ như Remote Desktop từ máy bên ngoài về máy Remote Server.

1. *Firewall Rules:*

Nơi lưu các Rules (Luật) của Firewall. Để vào Rules của pfsense vào Firewall → Rules. Mặc định PfSenSe cho phép mọi trafic ra/vào hệ thống. Chúng ta phải tạo ra các rules để quản lí mạng bên trong firewall.

1. *Snort:*

Snort là một chương trình mã nguồn mở, miễn phí, nó có khả năng phát hiện sự xâm nhập mạng và ngăn chặn sự xâm nhập trái phép theo rule được thu thập từ Snort và thực hiện ghi các gói và phân tích lưu lượng theo thời gian thực trên các mạng IP. Vào Tab System -> Packages -> Available Packages. Tìm đến packages Snort.

1. *Squid:*

Squid là một là một giải pháp proxy phần mềm mã nguồn mở được sử dụng nhiều nhất trong giải pháp Proxy của cộng đồng mạng. Squid proxy làm nhiệm vụ chuyển tiếp các yêu cầu từ phía client và đồng thời đóng vai trò kiểm soát tạo sự an toàn cho việc truy cập Internet của các client. Vào Tab System -> Packages -> Available Packages. Tìm đến packages Squid cài đặt gói tin này. Tab Antivirus để thêm chương trinh duyệt ClamAV Anti-Virus Integration Using C-ICAP là một proxy với một bộ lọc chống virus, malware… nhằm để bảo vệ máy client... khi truy cập vào các trang web nhiễm mã độc, virus…

1. *SquidGuard:*

SquidGuard là một là một giải pháp proxy phần mềm mã nguồn mở làm nhiệm vụ lọc các website, các file,…Vào Tab System -> Packages -> Available Packages. Tìm đến Packages SquidGuard. Sau đó qua tab Services -> Proxy filter SquidGuard. Tab Blacklist, click Download để tiến hành download Blacklist -> Click Save. Qua tab Common ACL, ở tab này sẽ hiện rất nhiều loại mà ta cần muốn cấm client ví dụ như các web nghe nhạc, music, video, các trang web tv, webradio, webmail, …Tab Target categories cho phép ta tùy biến thêm những website mà ta không cho truy cập vào.

1. *LightSquid:*

LightSquid là một phần mềm mã nguồn mở, nó là giao diện web based của Squid proxy dùng để phân tích lưu lượng truy cập, file log của mỗi user… Vào Tab System -> Packages -> Available Packages. Tìm đến packages LightSquid. Sau khi cài đặt xong ta vào Status -> Squid Proxy Reports ta được.

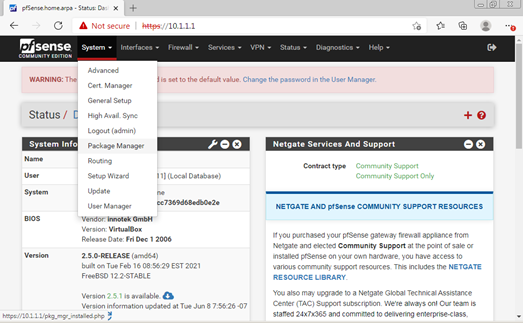
# **Chương III: Hiện thực và đánh giá hệ thống**

1. **Hiện thực**
   1. ***Công cụ hiện thực***

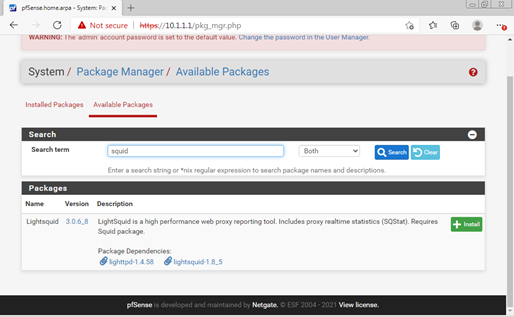
Trong bài báo cáo, nhóm em sử dụng các công cụ sau:

Phần mềm Virtual Box, file ISO pfSense, một đường mạng kết nối với internet để sử dụng các dịch vụ và để test các tính năng cũng như dịch vụ mà nhóm đã tạo trên Pfsense firewall, cùng với các phần mềm và công cụ hỗ trợ khác.

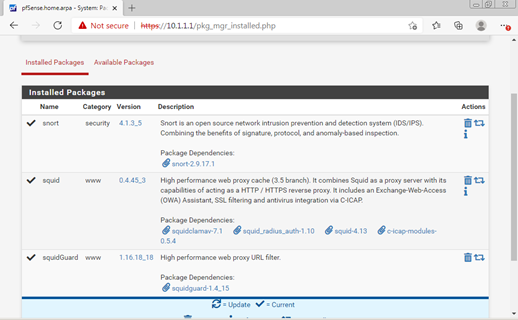
* 1. ***Các bước hiện thực***
     1. *Cài đặt các gói bổ sung cho pfSense.*
* Vào System. Chọn Package Manager



* Chọn tab Available Package, gõ ‘squid’ và bấm Search. Kết quả sẽ hiển thị tương tự như hình dưới. Do các gói squid và squidGuard đã được cài nên nó sẽ không hiển thị ở đây nữa. Chọn Install để cài đặt. Tương tự, cài đặt gói snort trên pfsense.



* Sau khi cài đặt hoàn tất, vào tab Installed Packages, ta sẽ thấy các gói bổ trợ đã được cài lên pfSense.



* + 1. *Hiện thực các chức năng*

1. Sử dụng ClamAV trong gói Squid để bảo vệ các máy Client khỏi virus, hỗ trợ HTTP/HTTPS.

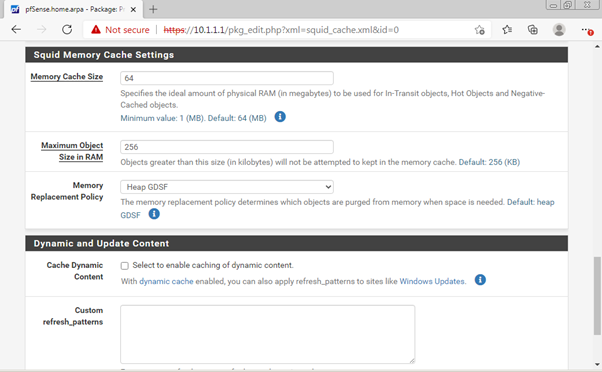
* Cấu hình Squid Proxy:
* Cấu hình Local Cache. Vào “Services > Squid Proxy Server> Local Cache Tab”. Mục Cache Replacement: Heap LFUDA, Hard Disk Cache Size: 2048, Maximum Object Size: 512, Memory Cache size: 512 -> Click “Save” để lưu cấu hình.

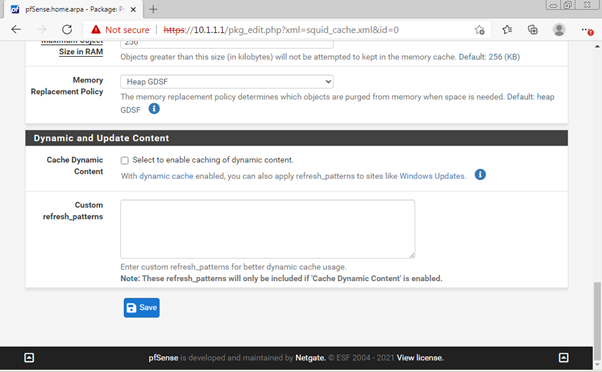
Graphical user interface, text, application, email

Description automatically generated

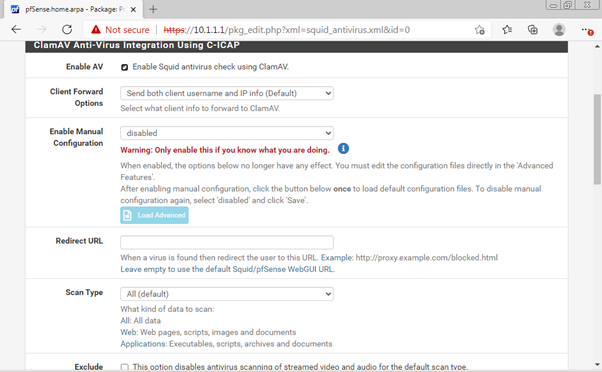
Graphical user interface

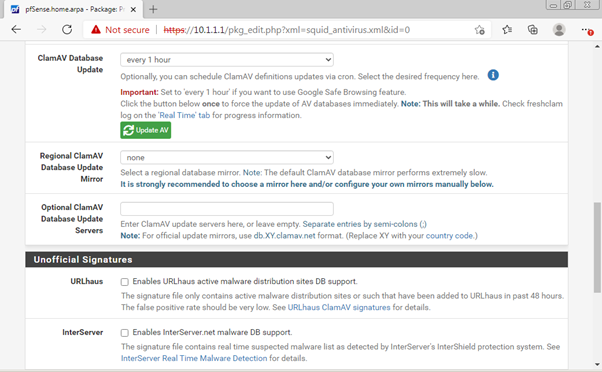
Description automatically generated

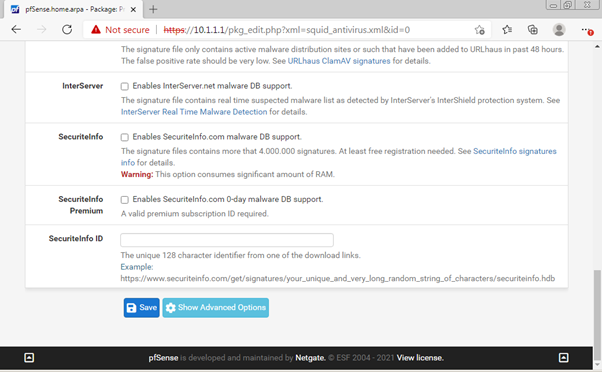




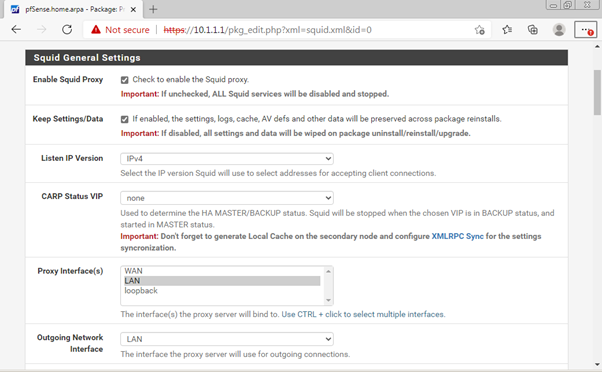
* Cấu hình ClamAV
* Tiếp theo cấu hình tích hợp antivirus. Chọn “Services > Squid Proxy Server > Antivirus Tab”. Tích vào “Enable Squid antivirus check using ClamAV”, “ClamAV Database Update: every 1 hour” > Click “Save” để lưu cấu hình.

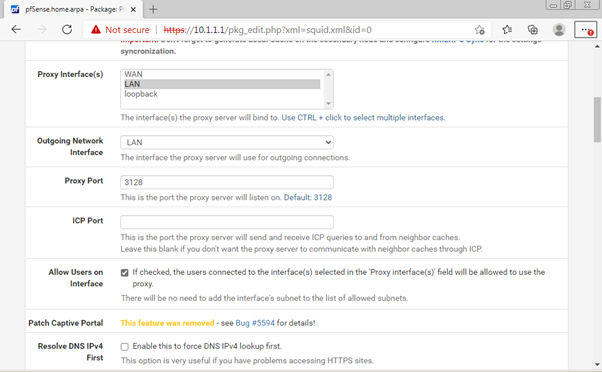
****

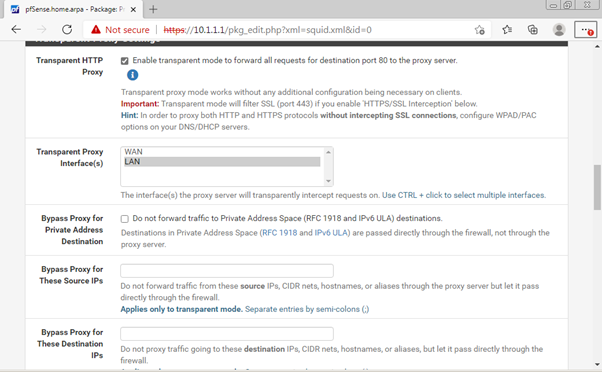
****

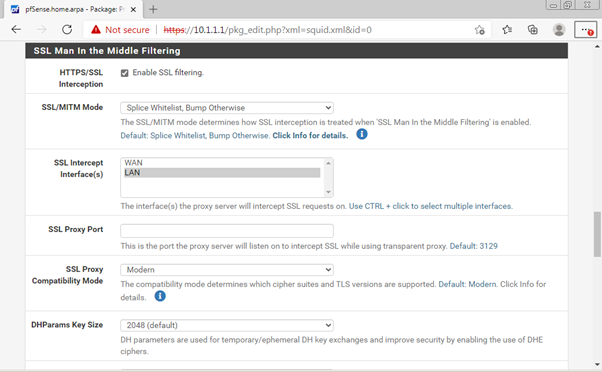
****

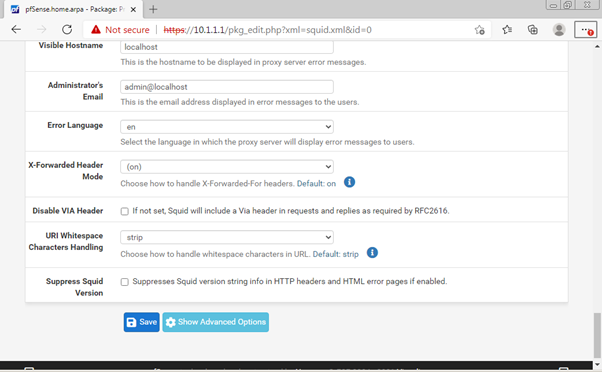
* Tiếp theo Enable Squid Proxy: Chọn “Services > Squid Proxy > General Tab”. Tích vào “Check to enable the Squid Proxy” , Proxy interface(s): LAN, Tích vào “Allow Users on Interface“, Tích vào “Transparent HTTP Proxy“, Transparent Proxy Interface(s): LAN, Tích “Enable Access Logging“, Log Store Directory: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

****

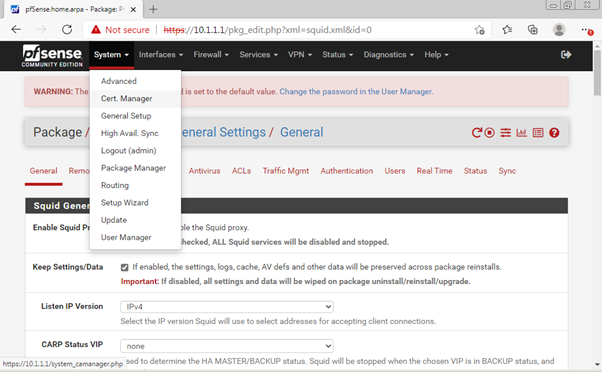
****

****

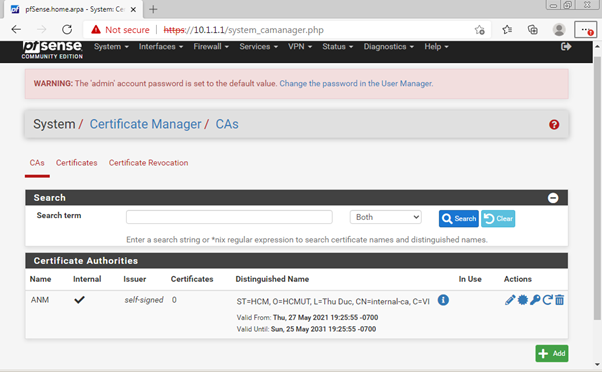
****

****

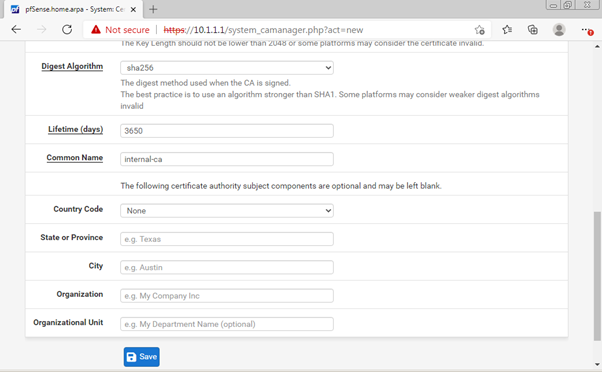
* Bật chức năng quét trên giao thức HTTPS
* Để hệ thống Proxy Server và Antivirus có thể quét trên giao thức HTTPS, ta cần tạo một CA và cài đặt nó lên các máy Client. Vào System > Cert. Manager.

****

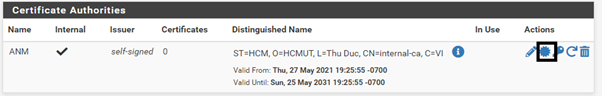
* Chọn Add để tạo CA mới.

****

* Điền tên và các thông tin cần thiết. Sau đó bấm Save để lưu.



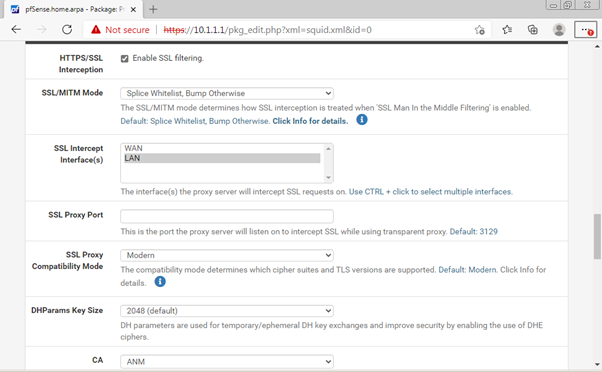
* Chọn icon để tải CA về máy client. Sau đó tiến hành cài như cài các Certificate.



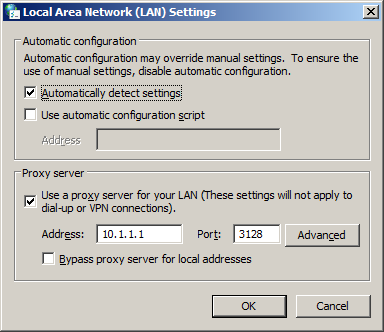
Graphical user interface, text, application

Description automatically generated

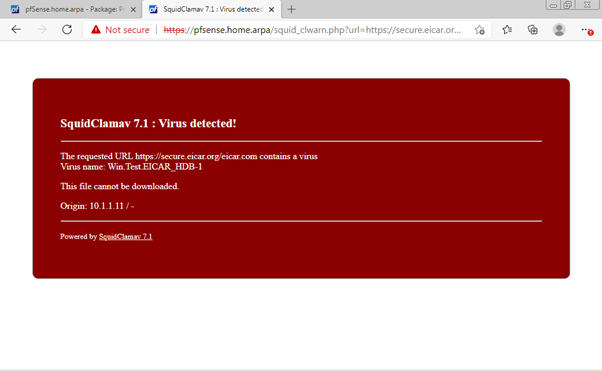
* Để quét được các trang web sử dụng giao thức HTTPS, ta vào Service > Squid Proxy Server > General > SSL Man in the Middle Filtering. Tích vào Enable SSL Filtering. SSL Interface: LAN. CA: ANM (đã tạo). Bấm Save để lưu lại.



* Thêm Proxy Server vào máy Client. Trong trường hợp này là thêm Proxy Server vào Windows 7. Start > Control Panel > Network and Internet > Internet Options > Connections > LAN Settings.



* Kết quả:
* Vào trang [Download Anti Malware Testfile – Eicar](https://www.eicar.org/?page_id=3950) để test chức năng quét Virus trên pfSense. Chọn một file test bất kì. Và hệ thống sẽ chặn không cho download file đó như ta mong muốn.

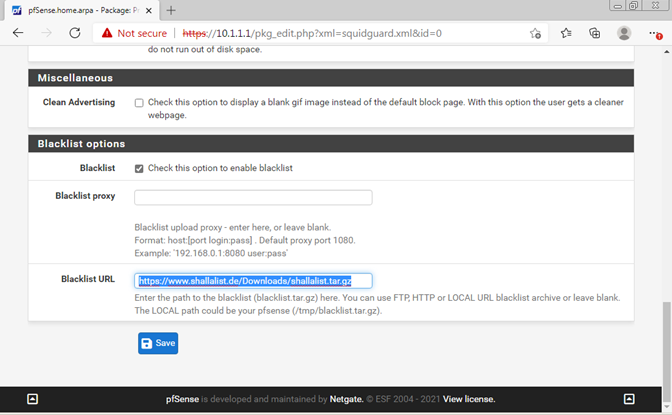
****

1. Sử dụng SquidGuard để chặn URL/Keyword/Prase

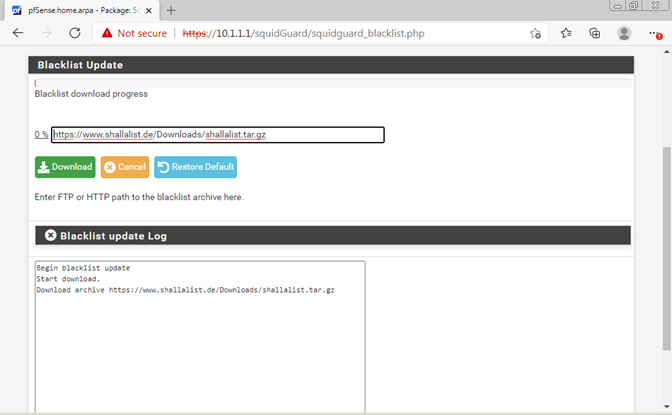
* Thiết lập chung
* Vào Service > SquidGuard Proxy Filter > General Setting.
* Tích vào Check this option to enable squidGuard. Ấn Apply.
* Sử dụng thiết lập mặc dịnh. Ấn Save để lưu.
* Tạo BlackList
* Vào Service > SquidGuard Proxy Filter > General Setting.
* Ở phần BlackList options, tích vào ô Check this option to enable blacklist.
* Ở phần BlackList URL, nhập vào đường dẫn

[**https://www.shallalist.de/Downloads/shallalist.tar.gz**](https://www.shallalist.de/Downloads/shallalist.tar.gz)

Đây là đường dẫn cho chúng ta tải về các blacklist để tích hợp vào hệ thống squidGuard trong pfSense.

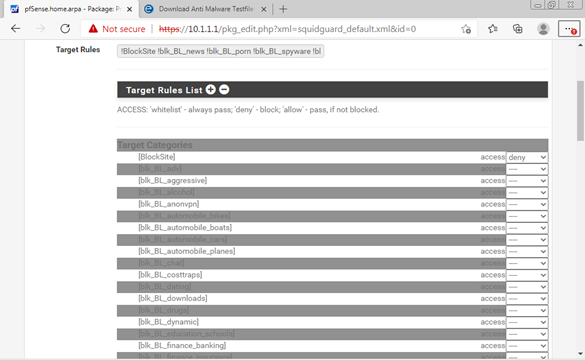
****

* Chuyển sang tab Blacklist. Ấn Download để tải về máy từ trang web ta đã nhập trước đó.

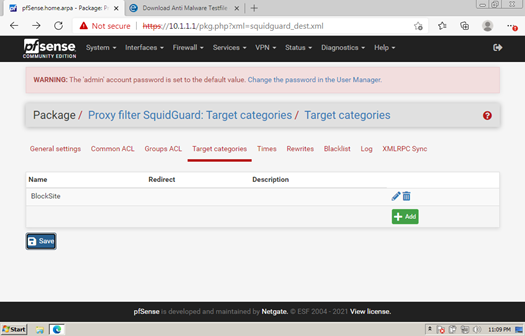
****

* Sau khi quá trình tải về và tích hợp vào hệ thống hoàn tất, để kiểm tra, chúng ta vào tab Common ACL > Target Rules List > +. Danh sách BlackList đã được tích hợp sẽ xuất hiện.

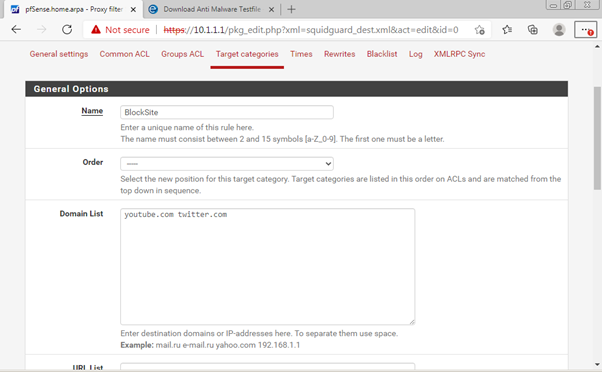
****

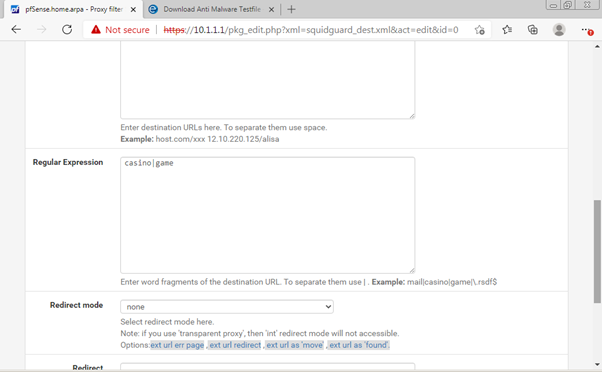
****

* Tạo danh sách cấm
* Chọn tab Target Categories. Chọn Add để tạo quy tắc cấm.



* Đặt tên cho quy tắc. Ở mục Domain List, nhập các tên miền mà bạn muốn chặn. Ở mục URL List, nhập các đường dẫn mà bạn muốn chặn. Ở mục Regular Expression, có thể nhập các từ khóa hoặc các biểu thức chính quy mà bạn muốn chặn. Ấn Save để lưu lại.

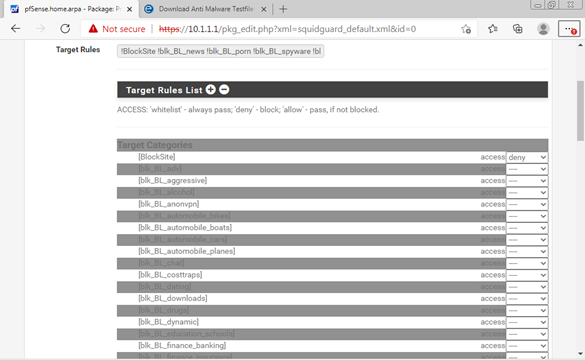




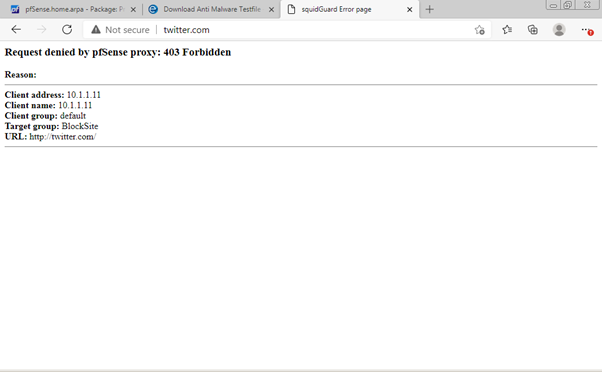
* Vào tab Common ACL, chọn dấu + trong Target Rule List.



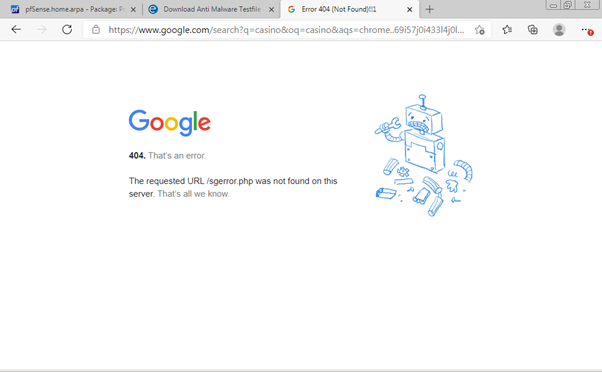
* Tìm quy tắc BlockSite đã tạo ở trên, chọn deny để chặn quy tắc đó. Ấn Save để lưu lại. Quay lại tab General Settings, ấn nút Apply để kích hoạt các thiết lập đã thực hiện.



* Kết quả:
* Do trong quy tắc BlockSite, chúng ta có cấm tên miền twitter.com, nên ta thử vào trang đó, trình duyệt sẽ hiển thị lỗi trang web bị chặn.



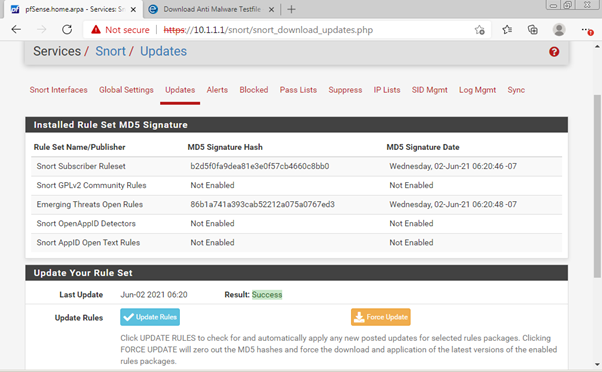
* Thử tìm kiếm trên Google với từ khóa casino, ta cũng nhận được thông báo lỗi do chúng ta đã chặn từ đó trong mục Regular Expressions.



Như vậy, việc chặn URL/Keyword/Phrase trên giao thức HTTPS đã thành công.

1. Sử dụng Snort để phát hiện và ngăn chặn xâm nhập qua Java Applet, ActiveX.

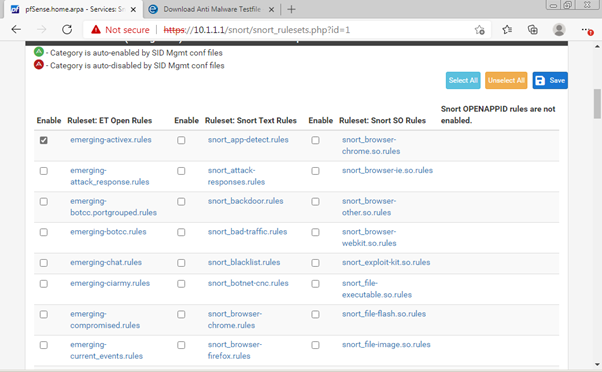
* Thiết lập chung
* Vào Service > Snort > Global Setting. Tích vào dòng Click to enable download of Snort free Registered User or paid Subscriber rules. Nhập Snort Oinkmaster Code (mã này sẽ được cấp khi bạn đăng kí tài khoản trên trang snort.org). Các thiết lập khác sử dụng mặc định. Ấn Save để lưu lại.
* Chuyển sang tab Updates. Ấn nút Update Rules để cập nhật các quy tắc mới nhất.



* Bật các quy tắc cho việc ngăn chặn xâm nhập qua Java Applet và ActiveX.
* Vào tab Snort Interfaces > Chọn nút để chỉnh sửa.

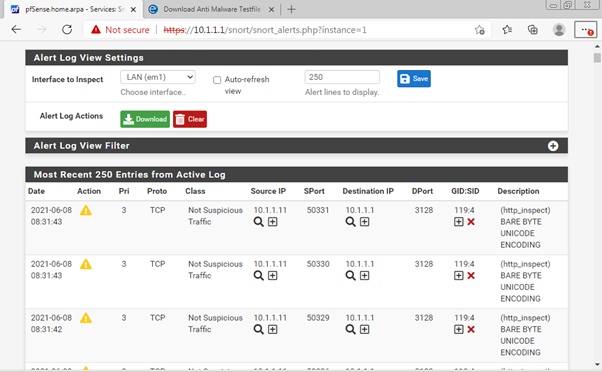


* Tích vào ô Enable Interface.
* Chuyển sang tab LAN Categories. Tích vào các quy tắcemerging activex.rules,snort\_browser-plugins.rules,snort\_file-java.rules, snort\_web-activex.rules, snort\_file-java-so.rules. Ấn Save để lưu lại.



* Kết quả

Sau khi bật các quy tắc, những hành động trên interface sẽ được ghi lại ở tab Alert. Nếu phát hiện có sự bất thường như tấn công xâm nhập mạng dựa trên Java Applet và ActiveX, Snort sẽ đưa ra cảnh báo và chặn các hành động đó.

****

1. **Đánh giá hệ thống**

Trong quá trình tìm hiểu và demo pfsense firewall nhóm chúng em đã thu được kết quả sau:

Biết cách xây dựng các mô hình ứng dụng Pfsense firewall trong thực tế và biết cách cấu hình để trở thành một firewall.

Nắm bắt và hiểu được quá trình hoạt động và các tính năng của pfsense. Triển khai được một số ứng dụng và dịch vụ của pfsense. Nắm được việc quản lý người dùng thông qua lịch làm việc và cấm truy cập một số trang web không được phép. Giúp chúng em hiểu sâu hơn về pfsense firewall

# **Chương IV: Kết luận**

Hệ thống Pfsense firewall được đề cập tới trong báo cáo tuy cơ bản nhưng khá đầy đủ, toàn diện và mang tính tổng quan. Báo cáo đã tìm hiểu những vấn đề cơ bản và đi sâu hơn ở nhiều khía cạnh và góc nhìn khác nhau để mọi người có thể hiểu hơn về pfsense. Sau khi hoàn thành báo cáo này, nhóm đã có cơ hội để mở mang kiến thức của mình và tìm hiểu sâu hơn về pfsense.

Qua việc tìm hiểu tổng quan về pfsense, nhóm chúng em nhận thấy được hướng phát triển trong tương lai của pfsense. Đặc điểm của pfsense cũng khá quan trọng là cấu hình để cài đặt và sử dụng phần mềm Pfsense không đòi hỏi phải cao như những phần mềm mới hiện nay. Pfsense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và ứng dụng này sẽ cho phép bạn mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Phần mềm được thiết kế nhỏ gọn, dễ dàng cấu hình thông qua giao diện web và đặc biệt là có khả năng cài đặt thêm gói dịch vụ để mở rộng các tính năng.

# **Tài liệu tham khảo**

* + 1. How To Install PfSense on VirtualBox?. Truy cập từ <https://getlabsdone.com/how-to-install-pfsense-on-virtualbox/>
    2. Hướng dẫn cấu hình squid proxy cho Pfsense Truy cập từ <https://mdungblog.wordpress.com/2018/07/27/cau-hinh-squid-proxy-cho-pfsense/>
    3. <https://www.snort.org/>
    4. Nội dung nghiên cứu Pfsense <https://issuu.com/namngan_nc/docs/noi_dung_nghi__n_c___u_pfsense>