**ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC BÁCH KHOA**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



**MÔN HỌC: MẬT MÃ & AN NINH MẠNG (C03069)**

**HỌC KÌ 202 - NĂM HỌC 2020-2021**

**Xây dựng hệ thống tường lửa sử dụng phần mềm mã nguồn mở pfSense**

**DANH SÁCH THÀNH VIÊN**

Phạm Đức Duy Anh 1810814

Lê Đỗ Thanh Bình 1811568

Trương Đình Đức 1811989

Hà Huy Long Hải 1812064

**Giảng viên:** Thầy Nguyễn Hữu Hiếu

**Tp. Hồ Chí Minh - 2021**

**MỤC LỤC**

1. GIỚI THIỆU 3
2. Đề tài 3
3. Yêu cầu 3
4. PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG 4
5. Xây dựng hệ thống firewall với phần mềm pfSense 4
6. Triển khai các chức năng của tường lửa trên pfSense 6
7. HIỆN THỰC VÀ ĐÁNH GIÁ HỆ THỐNG 7
8. Cài đặt pfSense trên VirtualBox và thiết lập Web GUI 7
9. Cài đặt và cấu hình Firewall trên pfSense 13
10. Cài đặt và cấu hình chức năng lọc Web 16
11. Cài đặt và cấu hình Antivirus 27
12. Đánh giá 28
13. KẾT LUẬN 32

TÀI LIỆU THAM KHẢO 33

PHỤ LỤC 34

# GIỚI THIỆU

## Đề tài

Ở trong bài tập lớn này, nhóm sẽ thực hiện triển khai một hệ thống tường lửa (firewall) sử dụng phần mềm mã nguồn mở pfSense. Phần mềm này sẽ được quản trị thông qua hệ thống Web được truy cập từ một máy nội bộ (local) với hệ thống tường lửa. Bên cạnh đó, nhóm cũng triển khai các công cụ tích hợp trên pfSense như Squid Proxy, Squidguard, ClamAV hay Snort để thực hiện thêm các tính năng cho firewall như lọc web, lọc virus, …

## Yêu cầu

Hệ thống tường lửa nhóm triển khai sẽ có những chức năng như sau:

- Firewall: có chức năng lọc gói (packet filtering) có trạng thái, không giới hạn số lượng giao tiếp mạng, nhiều giao thức mạng trên một zone và nhiều zone trên cùng một giao tiếp, quản lý địa chỉ linh động với 2 chế độ NAT (Netword Address Translation) và PAT (Packet Address Translation)

- Lọc Web: Hệ thống sẽ có khả năng chặn trên URL/Keyword/Pharse, chặn một vài tiện ích như Java Applet, Cookies, Actives X, …

- Antivirus: hỗ trợ lọc các gói tin hoặc các trang web có chứa virus, malware hay trojan trên các giao thức HTTP/HTTPS và cơ sở dữ liệu về virus được cập nhật tự động.

Ở chương 2 trong báo cáo, nhóm sẽ tiến hành phân tích và thiết kế hệ thống dựa trên những yêu cầu đã được đưa ra ở chương 1.

Ở chương 3 trong báo cáo, nhóm sẽ tiến hành hiện thực hệ thống đã mô tả ở chương 2, trình bày cách thức hoạt động cũng như đánh giá hệ thống đã xây dựng.

# Ở chương 4 trong báo cáo, nhóm sẽ tổng kết những yêu cầu đã đạt và chưa đạt với hệ thống đã triển khai, trình bày ưu nhược điểm cũng như hướng phát triển thêm cho hệ thống.

# PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG

# Xây dựng hệ thống firewall với phần mềm mã nguồn mở pfSense

# Tìm hiểu về tường lửa (firewall):

# Tường lửa là một công cụ phần cứng hoặc phần mềm hoặc là cả 2 được tích hợp vào hệ thống để chống lại sự truy cập trái phép, ngăn chặn virus… để đảm bảo nguồn thông tin nội bộ được an toàn, tránh bị kẻ gian đánh cắp thông tin.

# Tường lửa được chia làm 2 loại, đó là: Personal firewall và Network firewall

# Personal firewall: Loại này được thiết kế để bảo vệ một máy tính trước sự truy cập trái phép từ bên ngoài. Bên cạnh đó nó còn được tích hợp thêm các tính năng như theo dõi các phần chống virus, phần mềm chống xâm nhập để bảo vệ dữ liệu. Loại Firewall này thích hợp với cá nhân bởi vì thông thường chỉ cần bảo vệ máy tính của họ, thường được tích hợp sẵn trong máy tính laptop, máy tính cá nhân hoặc trong hệ điều hành.

# Network firewall: Được thiết kế ra để bảo vệ các host trong mạng trước sự tấn công từ bên ngoài, hay nói cách khác, network firewall dùng để bảo vệ cho một hệ thống mạng máy tính. Một hệ thống network firewall được cấu tạo bởi các thành phần chính như sau:

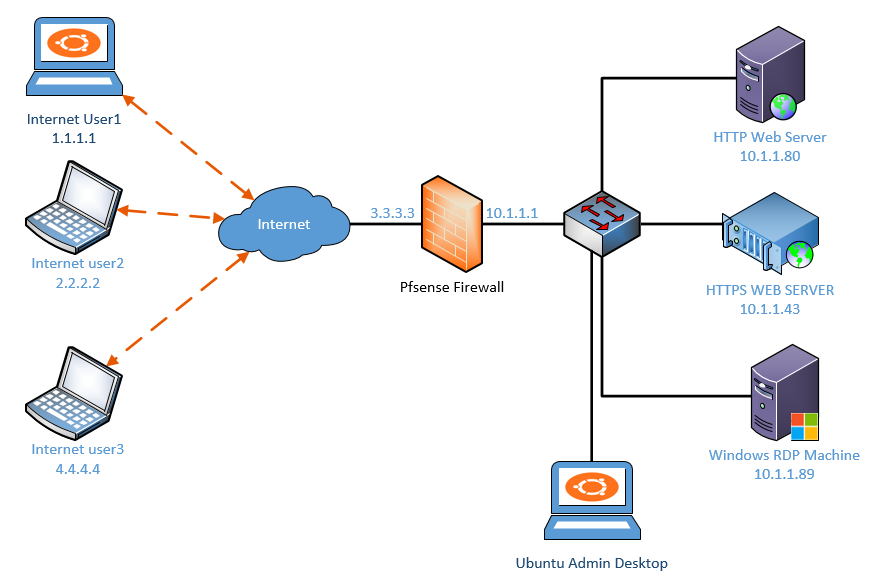
* Bộ lọc gói (Packet-Filtering Router): đóng vai trò như một Router cho phép hoặc không cho phép một packet được đi qua.
* Cổng mức ứng dụng (Application-level Gateway hay Proxy Gateway)
* Cổng mức mạch (Circuit-level Gateway)

1. **Tìm hiểu về phần mềm mã nguồn mở pfSense**

* pfSense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này sẽ cho phép bạn mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Pfsense có GUI trên nền Web tạo sự quản lý một cách dễ dàng
* 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.

1. **Thiết kế hệ thống tường lửa**

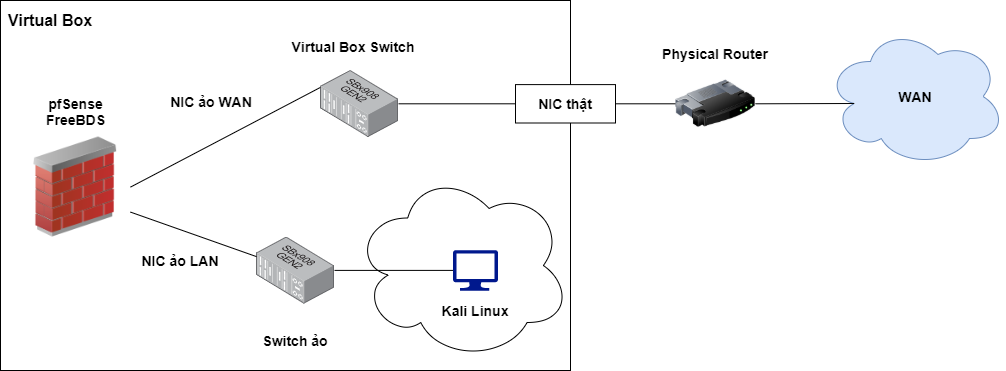
* Tường lửa giúp ngăn chặn các mối đe dọa từ bên ngoài, do đó tối thiểu ta phải có 2 NIC (Network Interface Card) lần lượt cho mạng LAN và WAN. Mạng LAN mô phỏng cho mạng nội bộ của chúng ta, còn mạng WAN mô phỏng cho nền tảng Internet kết nối với ISP bên ngoài. Như vậy ta sẽ có mô hình tường lửa như sau:



*Hình 1: Mô hình triển khai hệ thống với tường lửa*

1. **Xây dựng hệ thống tường lửa với pfSense**

* Để mô phỏng cho mô hình này, nhóm sẽ thực hiện cài đặt pfSense trên máy ảo Virtual Box với 2 adaptor: NAT cho WAN và Internal Network cho LAN. Việc sử dụng máy ảo cho pfSense giúp giảm thiểu sự hiện diện máy vật lý quản lý tường lửa, do pfSense có GUI trên nền Web giúp việc quản lý trở nên dễ dàng hơn. Bên cạnh đó ta cũng thiết lập thêm 1 máy Kali Linux trong LAN để kết nối đến tường lửa.



*Hình 2: Mô hình triển khai pfSense trên Virtual Box*

1. **Triển khai các chức năng của tường lửa trên pfSense**
2. **Chức năng lọc gói có trạng thái (dynamic packet filtering):**

* Lọc gói có trạng thái (dynamic packet filtering) là kĩ thuật dùng điểm kiểm soát việc truy cập network bằng cách giám sát trạng thái các gói tin được chuyển đến hay đưa đi và cho phép chúng thông qua hay bị chặn ở tường lửa dựa vào địa chỉ IP nguồn và IP đích, giao thức (protocol) của gói tin cũng như cổng (port) mà gói tin được chuyển đến. Việc lọc gói này thường được áp dụng cho việc đề phòng tấn công từ các máy tính bên ngoài mạng LAN
* Để thực hiện lọc gói không trạng thái trên pfSense, ta tiến hành định nghĩa tập các luật (rules) cho từng interface trong hệ thống.

1. **Quản lý địa chỉ linh động – NAT (Netword Address Translation)**

* **NAT** có nhiệm vụ truyền gói tin từ lớp mạng này sang lớp mạng khác trong cùng một hệ thống. **NAT** sẽ thực hiện thay đổi **địa chỉ IP** bên trong gói tin. Sau đó chuyển đi qua router và các thiết bị mạng.
* Trong giai đoạn gói tin được truyền từ mạng internet (public) quay trở lại **NAT**, **NAT** sẽ thực hiện nhiệm vụ thay đổi địa chỉ đích đến thành địa chỉ IP bên trong hệ thống mạng cục bộ và chuyển đi.
* Việc thực hiện NAT sẽ giúp tiết kiệm địa chỉ IPv4, cho phép lượng người truy cập vào mạng nội bộ nhiều hơn.
* Trong pfSense hỗ trợ 2 loại NAT, đó là: Inbound NAT và Outbound NAT.
* Inbound NAT giúp chuyển địa chỉ IP cục bộ (private) sang công cộng (public)
* Outbound NAT giúp chuyển địa chỉ IP công cộng (public) sang nội bộ (private)

1. **Lọc web (Web filtering)**

* Lọc web cho phép chúng ta chặn kết nối từ máy nội bộ đến một trong các URL đã được định nghĩa trên giao thức HTTP/HTTPS. Có rất nhiều package của pfSense hỗ trợ tính năng này, như pfBlockerNG, Squid Proxy có tích hợp SquidGuard, …
* pfBlockerNG là một công cụ lọc web dựa trên Domain. Với pfBlockerNG, chúng ta thiết lập tất cả các kết nối DNS từ máy nội bộ đến tường lửa và chặn tất cả các kết nối DNS không thông qua tường lửa (dựa vào tập rule của tường lửa). Khi đó pfBlockerNG sẽ dựa vào danh sách domain trong blacklist để tiến hành chuyển gói tin. Nếu như domain nằm trong blacklist, nó sẽ tiến hành gửi gói tin ta nhận được từ trang web chúng ta truy cập đến một địa chỉ IP ảo (virtual IP) mà ta đã khai báo. Và khi đó máy truy cập vào trang web sẽ không nhận được bất kì phản hồi nào.
* Squid Proxy là một proxy server hỗ trợ tính năng Squidguard lọc web dựa trên việc điều hướng URL. Với Squid Proxy, ta coi tường lửa như một Proxy Server – trung gian việc nhận và gửi gói tin. Trong SquidGuard chúng ta sẽ định nghĩa một blocklist các URL muốn chặn và khi Squid nhận ra chúng ta đang muốn truy cập vào các URL này, nó sẽ chặn kết nối.

1. **Antivirus**

* Antivirus là một tính năng giúp ta phát hiện và ngăn ngừa truy cập các trang web, tập tin có chứa virus, malware hay Trojan. Có rất nhiều package của pfSense hỗ trợ tính năng này như HTTP Antivirus (HAPV) hay ClamAV được tích hợp trên Squid Proxy.
* Các package này sẽ dựa vào một virus database để phát hiện tập tin hay trang web đó có chứa phần mềm độc hại hay không. Nếu như phát hiện ra tập tin hay trang web trong database, Squid sẽ chặn kết nối đến với trang web cũng như ngưng việc tải tập tin về máy.

# HIỆN THỰC VÀ ĐÁNH GIÁ HỆ THỐNG

## Cài đặt pfSense trên Virtual Box và thiết lập để quản trị thông qua Web GUI

## a. Cài đặt pfSense trên VirtualBox:

## Ta thiết lập một máy ảo với hệ điều hành FreeBSD (64-bit) để cài pfSense

## Cấu hình phần cứng cho pfSense, gồm: base memory (1024 MB), processor (1), …

## Tiến hành thiết lập network cho pfSense với 2 adaptor: adaptor 1 với mode là NAT đại diện cho mạng WAN và adaptor 2 với mode là Internal Network (intnet) đại diện cho mạng LAN. D:\BK\202\Mật mã & An ninh mạng\Assignment\2.PNGD:\BK\202\Mật mã & An ninh mạng\Assignment\1.PNG

## *Hình 3: Cài đặt Network cho pfSense trên Virtual Box*

## Đính kèm file ISO image (download tại [Download pfSense Community Edition](https://www.pfsense.org/download/)) trong mục Settings > Storage Device để cài pfSense

## 

## *Hình 4: Các thông số của máy ảo pfSense trên Virtual Box sau khi thiết lập*

## b. Cài đặt pfSense trên máy ảo

## - Khởi động máy ảo pfSense và bắt đầu quá trình cài đặt pfSense và thiết lập với các cài đặt mặc định.

## *Hình 5: Quá trình nạp file ISO trên máy ảo*

## 

## *Hình 6: Quá trình cấu hình disk cho pfSense*

## 

## *Hình 7: Quá trình cài đặt pfSense với các cấu hình đã chọn*

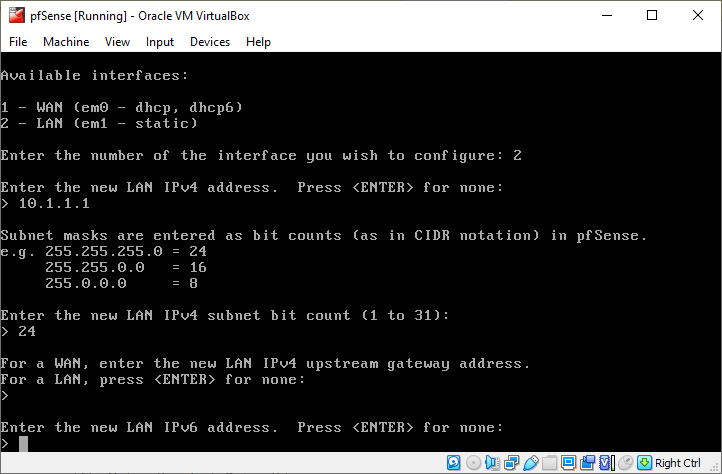
## Cấu hình pfSense theo mô hình thiết kế:

## Sau khi cài đặt pfSense trên máy ảo thành công, màn hình sẽ hiển thị giao diện:

## *Hình 8: Giao diện của pfSense sau khi cài đặt thành công trên Virtual Box*

## Khi cài đặt thành công, pfSense sẽ mặc dịnh WAN là card mạng có hỗ trợ DHCP. Ta cần cấu hình lại IP cho LAN tránh bị đụng IP với máy vật lý bên ngoài:

*Hình 9: Cấu hình lại IP cho mạng LAN*

*Hình 10: Cấu hình subnet mask cho IP LAN*

1. **Quản trị pfSense sử dụng WebGUI:**

## Truy cập pfSense Web GUI trên VirtualBox:

## Để có thể truy cập pfSense Web GUI, ta cần một máy có nằm chung LAN interface với pfSense, Với mục đích quản trị pfSense, ta sử dụng một máy ảo Kali Linux, việc sử dụng máy ảo này giúp giảm thiểu sự hiện diện của máy trong hệ thống máy vật lý. Ta cần cấu hình network cho máy ảo Kali Linux sử dụng cùng mạng LAN với pfSense bằng cách thay đổi adapter mode sang Internal Network (intnet).

*Hình 11: Cài đặt Network cho Kali Linux trên Virtual Box*

## Sử dụng trình duyệt (chẳng hạn như Firefox của Kali Linux) để truy cập pfSense Web GUI bằng cách nhập địa chỉ IP đã cấu hình cho pfSense trước đó (chẳng hạn như 10.1.1.1)

## *Hình 12: Web GUI của pfSense khi truy cập bằng Kali Linux*

## Hoàn tất thiết lập ban đầu (setup wizard)

## Đăng nhập vào pfSense bằng tài khoản mặc định cho tất cả người dùng: Username: admin, Password: pfSense

## Thực hiện các thiết lập ban đầu và chọn Finish để hoàn thành quá trình cài đặt pfSense, bỏ qua bước thiết lập WAN và LAN do ta đã cấu hình ở trên.

## *Hình 13: Thiết lập hostname và domain cho pfSense*

## 

## *Hình 14: Trang chủ của pfSense sau khi hoàn tất thiết lập ban đầu (setup wizard)*

## Cài đặt và cấu hình Firewall trên pfSense

## Graphical user interface, application, Word Description automatically generatedThiết lập bộ lọc gói cho mạng WAN: Vào Firewall > Rules > WAN

## *Hình 15: Tập các rule trên WAN interface*

## Thiết lập bộ lọc gói cho mạng LAN: Vào Firewall > Rules > LAN

## Graphical user interface, application, table Description automatically generated

## *Hình 16: Tập các rule trên LAN interface*

## Cấu hình NAT để chuyển đổi IP nội mạng thành IP public để truy cập ra ngoài internet (NAT Outbound):

## 

## *Hình 17: Cấu hình NAT Outbound*

## Cấu hình NAT chuyển hướng DNS:

## Text, email Description automatically generatedGraphical user interface, text, application Description automatically generated

## *Hình 18: Cấu hình NAT Port Forward*

## Các thông số cài đặt:

## Interface: LAN

## Protocol: TCP/UDP

## Destination port: DNS (53)

## Redirect target IP: Type: Single Host – Address: 127.0.0.1

## Redirect target port: DNS (53)

## Cài đặt và cấu hình chức năng lọc web trên pfSense

## Thiết lập các quy tắc lọc web dựa trên URL, keyword, phrase với Squid và SquidGuard trên pfSense

## Cài đặt Squid và SquidGuard trên pfSense

## Do Squid và SquidGuard là 2 công cụ được tích hợp trên pfSense nên để cài đặt, chọn System > Packet Manager, tìm các gói Squid và SquidGuard tương ứng:

## 

## *Hình 19: Tìm gói Squid và SquidGuard để cài đặt trên pfSense*

## Chọn “Install” để bắt đầu cài đặt squid

## 

## *Hình 20: File log thông báo Squid được cài đặt thành công*

## Thực hiện tương tự như trên để cài đặt SquidGuard

## Thiết lập các cấu hình cơ bản cho Squid Proxy

## Chọn Services > Squid proxy server:

## *Hình 21: Giao diện của Squid Proxy sau khi cài đặt trên pfSense*

## Để có thể kích hoạt được Squid Proxy ta phải thiết lập bộ đệm. Vào mục Servies > Squid Proxy Server > Local Cache để tiến hành thiết lập.

## *Hình 22: Thiết lập Local Cache cho Squid Proxy Server*

## Thiết lập các cấu hình cơ bản cho SquidGuard

## Chọn Services > SquidGuard proxy filter để cấu hình cho SquidGuard:

## 

## *Hình 23: Thiết lập cấu hình cho SquidGuard*

## SquidGuard sẽ có mục Blacklist – nơi ghi nhận các URL sẽ được chặn bởi Squid Proxy. Trong mục “Blacklist”, ta sử dụng các blacklist có sẵn trên <https://www.shallalist.de/Downloads/shallalist.tar.gz>. Trong mục Blacklist URL, ta nhập URL đến file gunzip trên để SquidGuard tải về.

## 

## *Hình 24: Thiết lập Blacklist URL cho SquidGuard*

## Tải blacklist cho SquidGuard

## Trong SquidGuard, vào mục “Blacklist”, chọn “Download” để bắt đầu cập nhật blacklist trong file gunzip mà ta đã chỉ đến URL cho SquidGuard. SquidGuard sẽ lần lượt đọc từng URL trong file và lưu vào local database của nó.

## *Hình 25: Blacklist update log hiển thị số lượng URL tìm thấy và trạng thái cập nhật*

## Lọc web dựa trên URL, keyword, phrase

## Graphical user interface, text, application, email Description automatically generatedTrong SquidGuard, chọn Target categories và chọn “Add” để thêm luật mới hoặc “Update” để cập nhật luật lọc:

## *Hình 26: Thêm một luật mới trong tab Target categories*

## Điền vào các mục “Domain List” (Chặn web dựa trên domain), “URL List” (Chặn web dựa trên URL) và “Regular Expression” (Chặn web dựa trên keyword, phrase) để hoàn thiện:

## Chọn “Save” để lưu luật lọc vừa tạo

## Vào “Common ACL” và chọn “Target Rules List”. Khi đó danh sách các target ta đã thêm sẽ hiện ra với luật lọc đi kèm. Mặc định các target sẽ có luật lọc là access. Do đó để chặn 1 target, ta tìm targer và chọn “deny” để kích hoạt luật lọc. Sau đó chọn “Save” để lưu.

## 

## *Hình 27: Thiết lập access mode với các target ta đã tạo*

## Vào “General Setting” và chọn “Apply” để cập nhật lại bộ lọc trên SquidGuard:

## 

## *Hình 28: Chọn Appy để cập nhật lại bộ lọc SquidGuard*

## Thiêt lập chức năng lọc web bằng domain với pfBlockerNG

## Cài đặt pfBlockerNG trên pfSense:

## Trên pfSense, chọn System > Packet Manager và tìm gói pfBlockerNG để cài đặt

## Chọn “Install” để tiến hành cài đặt pfBlockerNG

## 

## *Hình 29: Cài đặt pfBlockerNG trên pfSense*

## Thiết lập cấu hình cơ bản cho pfBlockerNG:

## Vào Firewall > pfBlockerNG > DNSBL để thiết lập Virtual IP (ví dụ: 20.16.16.16) điều hướng gói tin khi phát hiện domain bị chặn, port nhận và gửi gói tin của pfBlockerNG.

## *Hình 30: Thiết lập cho DNSBL*

## pfBlockerNG sẽ lưu thông tin các Domain bị chặn trong local database. Vào Firewall > pfBlockerNG > DNSBL Feeds, nhấn nút “Add” để thêm vào một tập các Domain mới. Giả sử ta thấy thông tin từ 2 file là: <https://someonewhocares.org/hosts/hosts> và <https://adaway.org/hosts.txt> và chọn update dữ liệu 1 tuần 1 lần và nhấn “Save”.

## *Hình 31: Thiết lập cho DNSBL Feeds*

## Vào pfBlockerNG > Update để cập nhật các Domain trên 2 URL trên:

## *Hình 32: pfBlockerNG log hiển thị cập nhật 2 tập domain thành công*

## Thiết lập chức năng chặn activeX, java applet, cookie với Snort trên pfSense

## Cài đặt snort trên pfSense

## Trên pfSense, chọn System >> Packet Manager và tìm gói snort để cài đặt:

## Chọn “Install” và tiến hành cài đặt snort:

## Thiết lập cấu hình cơ bản cho snort

## Tạo tài khoản snort tại <https://www.snort.org/> và lấy oinkcode:

## Trên pfSense, chọn Services >> Snort >> Global Settings để tiến hành cấu hình

## Chọn các rule set mong muốn thêm vào Snort. Ở đây ta sẽ dùng Snort VRT, Snort GPLV2, và ET Open rule:

## 

## *Hình 33: Thiết lập Snort*

## Cập nhật rule cho snort

## Tại Snort, chọn “Updates”:

## 

## *Hình 34: Cập nhật các rule trên Snort*

## Nhấn vào “Update” để tiến hành cập nhật rule cho snort:

## Tạo Snort interface mới cho mạng WAN:

## Trong Snort, chọn Snort Interfaces và “Add” để thêm interface mới cho Snort:

## 

## *Hình 35: Tạo interface mới cho WAN*

## Chặn activeX, java applet, cookie

## Trong Snort interface vừa tạo, chọn WAN categories

## 

## *Hình 36: Giao diện của WAN categories trong Snort*

## Chọn các luật “emerging\_activex.rules” (Chặn Active X), “emerging\_malware.rules” (Chặn một số lỗ hổng như java applet), “emerging\_web\_server.rules” và “emerging\_web\_client.rules” (Chặn một số lỗ hổng web sử dụng cookie) và một số luật chặn malware, trojan, worm khác:

## 

## *Hình 37: Chọn các luật muốn chặn*

## Ngăn chặn các tấn công quét mạng và từ chối dịch vụ

## Trong Snort interface vừa tạo, chọn WAN categories

## Chọn các luật “emerging\_dos.rules”, “emerging\_exploit.rules” và “emerging\_scan.rules” để ngăn chặn các tấn công quét mạng và từ chối dịch vụ

## Nhấn “Save” để lưu thiết lập

## Kích hoạt các rule trên Snort interface:

## Trong Snort Interface, chọn “WAN Rules” đẻ quản lý hoạt động của các rule trên interface:

## *Hình 38: Quản lý các rule trên WAN interface*

## Cài đặt và cấu hình Antivirus trên pfSense

## Kích hoạt ClamAV trên Squid Proxy

## Trong Squid Proxy, chọn mục “Antivirus” và kích hoạt ClamAV cho Squid proxy, lựa chọn Database server lưu trữ dữ liệu về virus và thiết lập tự động cập nhật cơ sở dữ liệu virus mỗi ngày:

## 

## 

## *Hình 39: Kích hoạt clamAV*

## Đánh giá chức năng của hệ thống

## Firewall

## Lọc web

## Với Snort, ta chặn được tấn công quét mạng và từ chối dịch vụ

*Hình 40: Kiểm tra IP của máy tấn công*

## 

## *Hình 41: Mô phỏng tấn công quét mạng bằng nmap trên kali linux*

## 

## 

## *Hình 42: Firewall đã phát hiện và tiến hành chặn IP tấn công*

## Graphical user interface, text, application, email Description automatically generatedSau khi thiết lập các luật lọc web trên SquidGuard, ta không thể truy cập một số trang web bị chặn nữa:

## *Hình 43: Không thể truy cập được trang web do SquidGuard*

## Sau khi thiết lập các domain bị chặn trên pfBlockerNG, ta vẫn có thể truy cập các trang web nhưng không nhận về gói tin nào. Do pfBlockerNG phát hiện ra Domain ta truy cập bị chặn, nên nó đã chuyển gói tin trang web trả về cho Virtual IP 20.16.16.16

## *Hình 44: Không nhận được thông tin gói tin trang web bleachbit.com trả về*

## *Hình 45: Trang web bleachbit.com khi truy cập bình thường*

## Antivirus

## Sau khi Antivirus được kích hoạt, pfSense có thể phát hiện và ngăn chặn những trang web có nguy cơ nhiễm virus

## *Hình 46: Thông báo trang web có nguy cơ nhiễm virus bị chặn*

* Ta có thể xem lịch sử (log) các trang web và virus đã bị chặn

Text

Description automatically generated with low confidence

Hình 47: File log các trang web là file tải về bị chặn bởi Antivirus

1. **KẾT LUẬN**

* Hệ thống được triển khai tương đối đầy đủ các chức năng đã đặt ra:
* 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 địa 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.
* Hướng phát triển trong tương lai:
* Mở rộng hệ thống mô phỏng phức tạp hơn với phân vùng DMZ và tường lửa nội bộ để bảo vệ các máy tính chưa dữ liệu quan trong trong LAN
* Bổ sung thêm các tính năng cho firewall như kiểm soát lưu lương kết nối, hỗ trợ cân bằng tải, …

**TÀI LIỆU THAM KHẢO**

1. [How To Install PfSense on VirtualBox? - GetLabsDone](https://getlabsdone.com/how-to-install-pfsense-on-virtualbox/)
2. [pfSense Documentation | pfSense Documentation (netgate.com)](https://docs.netgate.com/pfsense/en/latest/)

**PHỤ LỤC**

## pfSense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này sẽ cho phép bạn mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. pfSense 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.

* pfSense bao gồm nhiều tính năng đặc biệt là firewall trạng thái mà bạn vẫn thấy trên các thiết bị tường lửa hoặc router thương mại lớn, chẳng hạn như giao diện người dùng (GUI) trên nền Web tạo sự quản lý một cách dễ dàng. Trong khi đó phần mềm miễn phí này còn có nhiều tính năng ấn tượng đối với firewall/router miễn phí, tuy nhiên cũng có một số hạn chế.
* 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 cơ chế hoạt động trong chế độ brigde 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 cơ chế NAT 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

Vì nó hỗ trợ nhiều kết nối mạng diện rộng (WAN) nên có thể thực hiện việc cân bằng tải. 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 không thể chỉ định được lưu lượng cho qua một kết nối.