

**BỘ CÔNG THƯƠNG**

**TRƯỜNG CAO ĐẲNG KỸ THUẬT CAO THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**…..** 🙦 🕮 🙤 **…..**



**ĐỒ ÁN MÔN HỌC**

***Đề tài***

**TÌM HIỂU VÀ TRIỂN KHAI HỆ THỐNG TƯỜNG LỬA PFSENSE.**

**Giáo viên: Nguyễn Võ Công Khanh**

**Sinh viên thực hiện:**

**1. PHẠM PHÚC BẢO 0306201515**

**2. NGUYỄN THÀNH ĐỨC 0306201526**

**3. TRƯƠNG ANH NGUYÊN 0306201559**

**LỚP: CĐ TH 20MMTF Môn: Cấu hình & quản trị thiết bị**

**KHÓA: 2020 – 2023 mạng Cisco**

**TP. HỒ CHÍ MINH, ngày 31 tháng 10 năm 2022**

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

**…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………**

**…………………………………………………………………………………………………………**

**………………………………………………………………………………………………………...**

TP.HCM, Ngày …….Tháng…….Năm 2020

Giáo viên hướng dẫn

MỤC LỤC

[CHƯƠNG 1: TỔNG QUAN VỀ TƯỞNG LỬA – FIREWALL PFSENSE 7](#_Toc121907538)

[1.1. Tổng quan về tường lửa 7](#_Toc121907539)

[1.2. Phân loại Firewall 7](#_Toc121907543)

[1.3. Nhiệm vụ của Firewall 9](#_Toc121907572)

[1.4. Chức năng của Firewall 9](#_Toc121907583)

[1.5. Những hạn chế của Firewall 10](#_Toc121907588)

[1.6. Tường lửa thế hệ mới (Next – generation Firewall (NGFW)) 10](#_Toc121907593)

[CHƯƠNG 2: GIỚI THIỆU MỘT SỐ CHỨC NĂNG VÀ DỊCH VỤ PFSENSE 11](#_Toc121907603)

[2.1. HA và CARP 11](#_Toc121907604)

[2.2. Hệ thống giám sát và phát hiện ngăn chặn xâm nhập (IDS/IPS) trên Firewall 13](#_Toc121907618)

[2.3. Open VPN 16](#_Toc121907634)

[2.4. Xác thực LDAP 17](#_Toc121907638)

[2.5. DHCP Server 19](#_Toc121907643)

[2.6. Captive Portal 19](#_Toc121907647)

[2.7. Network Load Balancer 20](#_Toc121907650)

[2.8. PPPoE Server 21](#_Toc121907655)

[2.9. Dynamic DNS 22](#_Toc121907659)

[2.10. Firewall Rules 23](#_Toc121907663)

[2.11. NAT 23](#_Toc121907667)

[2.12. Traffic Shaper 24](#_Toc121907671)

[2.13. Schedules 25](#_Toc121907675)

[2.14. Aliases 25](#_Toc121907677)

[2.15. Packages 25](#_Toc121907679)

[2.16. Virtual IPs 25](#_Toc121907681)

[CHƯƠNG 3: DEMO HỆ THỐNG TƯỜNG LỬA PFSENSE 27](#_Toc121907684)

[3.1. Cài đặt PFSense 27](#_Toc121907685)

[3.2. Setup PFSense 37](#_Toc121907726)

[3.3. Chặn nhân viên truy cập web 40](#_Toc121907729)

[3.4. Thiết lập không cho trưởng phòng truy cập facebook nhưng vẫn truy cập được web và nhưng trang khác. 44](#_Toc121907745)

[3.5. Thiết lập tốc độ upload và download. 45](#_Toc121907750)

[3.6. Thiết lập thời gian làm việc cho nhân viên 48](#_Toc121907764)

[CHƯƠNG 3: KẾT LUẬN 50](#_Toc121907770)

**DANH MỤC HÌNH ẢNH**

[Hình 1.1.1: Tổng quan về tường lửa 7](#_Toc121909108)

[Hình 1.2.1: Firewall cứng 8](#_Toc121909109)

[Hình 1.6.1: Tường lửa thế hệ mới 10](#_Toc121909110)

[Hình 2.1.1: High Availability Firewall 11](#_Toc121909111)

[Hình 2.1.2: Common Address Redundancy Protocol 12](#_Toc121909112)

[Hình 2.4.1: Lightweight Directory Access Protocol 18](#_Toc121909113)

[Hình 2.5.1: DHCP Server 19](#_Toc121909114)

[Hình 2.7.1: Network Load Balancer 21](#_Toc121909115)

[Hình 2.8.1: PPPoE Server 21](#_Toc121909116)

[Hình 2.9.1: Dynamic DNS 22](#_Toc121909117)

[Hình 2.10.1: Firewall Rules 23](#_Toc121909118)

[Hình 2.11.1: NAT 24](#_Toc121909119)

[Hình 2.12.1: Traffic Shaper 24](#_Toc121909120)

[Hình 2.16.1: Virtual IPs 26](#_Toc121909121)

[Hình 3.1.1: Cài đặt PFSense 29](#_Toc121909122)

[Hình 3.1.2: Đặt IPv4 32](#_Toc121909123)

[Hình 3.1.3: Tạo User 35](#_Toc121909124)

[Hình 3.2.1: Setup PFSense 39](#_Toc121909125)

[Hình 3.3.1: Tạo Rules chặn nhân viên 42](#_Toc121909126)

[Hình 3.4.1: Chặn trưởng phòng truy cập Facebook 44](#_Toc121909127)

[Hình 3.5.1: Thiết lập tốc độ Upload 46](#_Toc121909128)

[Hình 3.5.2: Thiết lập tốc độ Download 47](#_Toc121909129)

[Hình 3.6.1: Thiết lập thời gian làm việc 50](#_Toc121909130)

**LỜI CẢM ƠN**

Để hoàn thành đồ án này trước hết chúng em xin gửi đến quý thầy, cô giáo trong Khoa Công Nghệ Thông Tin, Trường Cao Đẳng Kỹ Thuật Cao Thắng lời cảm ơn chân thành.

Đặc biệt, chúng em xin gửi đến Thầy Nguyễn Võ Công Khanh, người đã giúp đỡ chúng em hoàn thành đề tài này lời cảm ơn sâu sắc nhất.

Trong quá trình làm đồ án, khó tránh khỏi sai sót, rất mong quý thầy cô bỏ qua. Đồng thời do trình độ lý luận cũng như kinh nghiệm thực tiễn còn hạn chế nên bài báo cáo đồ án không thể tránh khỏi những thiếu sót, chúng em rất mong nhận được ý kiến đóng góp của thầy cô để chúng em tích lũy và học thêm được nhiều kinh nghiệm.

Cuối cùng, chúng em xin chân thành cảm ơn gia đình và bạn bè, đã luôn tạo điều kiện, quan tâm, giúp đỡ, động viên chúng em trong suốt quá trình học tập và hoàn thành đồ án tốt nghiệp này.

***Chúng em xin chân thành cảm ơn****!*

*………., ngày…..tháng…..năm 2022*

***Sinh viên thực hiện***

**LỜI NÓI ĐẦU**

Tường lửa pfsense là phần không thể thiếu cho các công ty/ doanh nghiệp, chúng giúp kiểm soát truy cập, giám sát mạng, quản lý mạng…

Tường lửa pfsense là rào chắn mà một số cá nhân, tổ chức, doanh nghiệp thiết lập để ngăn chặn người dùng mạng internet truy cập các thông tin không mong muốn và ngăn chặn người dùng từ bên ngoài truy cập các thông tin bảo mật nằm trong mạng nội bộ.

Pfsense là một ứng dụng có chức năng định tuyến, tường lửa và miễn phí, ứng dụng này cho phép mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Bắt đầu vào năm 2004, pfsense đã có hơn 1 triệu lượt download và được sử dụng để bảo vệ các mạng có tất cả kích cở, từ mạng gia đình đến các mạng lớn của các doanh nghiệp.

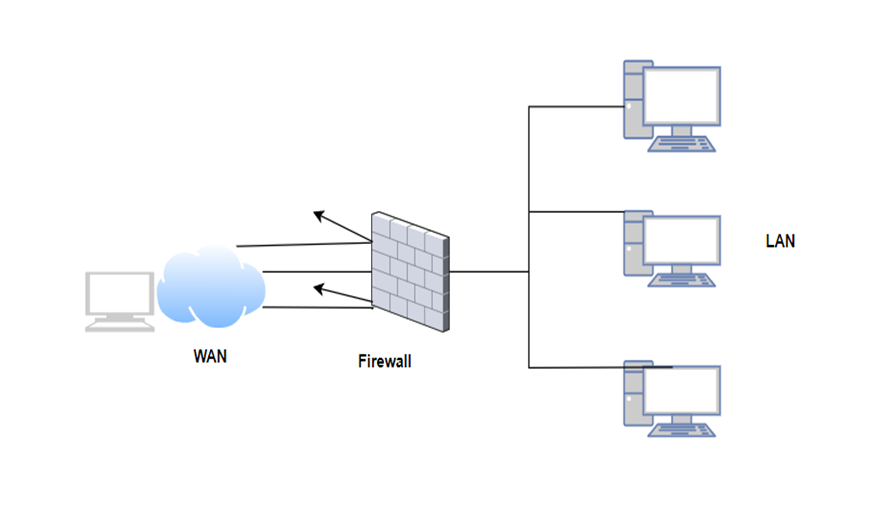
Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi lần phát hành, nhầm cải thiện tốt về tính năng bảo mật, sự ổn định và khả năng linh hoạt của nó.

Pfsense bao gồm nhiều tính năng đặc biệt là firewall trạng thái mà chúng ta vẩn thấy trên các thiết bị tường lửa hoặc router thương mại lớn.

# CHƯƠNG 1: TỔNG QUAN VỀ TƯỞNG LỬA – FIREWALL PFSENSE

## Tổng quan về tường lửa

Firewall hay còn gọi là tường lửa, được xem như một bức tường bảo vệ cơ bản giúp bảo vệ máy tính của bạn khỏi các cuộc tấn công. Lọc lưu lương vào và lưu lượng ra khỏi các chương trình khác nhau, đảm bảo chỉ có những lưu lượng truy cập được cấp phép mới được đi vào hệ thống.



Hình 1.1.1: Tổng quan về tường lửa

## Phân loại Firewall

Personal Firewall: Bảo vệ máy tính trước truy cập từ bên ngoài, theo dõi các phần mềm chống virus được tích hợp sẳn trong laptop hay PC.

Network Firewall: Bảo vệ các host trước sự truy cập từ bên ngoài. Bảo vệ số lượng lớn các host trong hệ thống mạng.

Có hai loại Firewall: Firewall cứng và Firewall mềm.

#### Firewall cứng:

Được đặt giữa mạng máy tính nằm trong cục bộ và Internet, kiểm tra dữ liệu đến từ bên ngoài internet cho phép dữ liệu an toàn đi qua và lọc các dữ liệu gây hại cho hệ thống.

Dùng cho doanh nghiệp có thể kiểm soát an ninh mạng giúp chặn mối đe dọa bằng cách lọc email và lưu lượng truy cập web.

Về mặt ưu điểm: Thời gian phản hồi lại nhanh hơn xử lý được các lượng truy cập nhanh.

Về bảo mật: Firewall cứng như điều hành riêng một hệ biệt ít bị tấn công, giảm được nguy cơ bảo mật. Quản lý tốt không làm chậm các ứng dụng.



Hình .: Firewall cứng

#### Firewall mềm:

Được cài đặt trên máy tính cá nhân, tách riêng biệt giữa các chương trình dùng trên máy tính. Lọc dữ liệu gửi đi các phản hồi yêu cầu từ xa gửi đi.

Yêu cầu cài đặt trên các máy chủ riêng lẻ.

Cung cấp quyền kiểm soát lưu lượng truy cập qua giao diện người dùng, dễ dàng sử dụng.

Hạn chế được ứng dụng cụ thể từ Internet linh hoạt hơn khi sử dụng.

#### So sánh giữa Firewall cứng và Firewall mềm:

|  |  |
| --- | --- |
| Firewall cứng | Firewall mềm |
| Dùng cho doanh nghiệp hiệu suất tốt | Dùng cho máy tính cá nhân |
| Hardware chuyên dụng | Hardware tùy chỉnh được theo nhu cầu sử dụng |
| Chi phí lắp đặt cao | Chi phí thấp |
| Đầu tư về mặt ban đầu cao | Đầu tư ban đầu thấp |
| Lọc kết nối chủ yếu sử dụng kết nối mạng lớn | Lập trình từ các quy tắc bộ lọc, kiểm soát lưu lượng mạng |
| Là sản phẩm dộc lập với máy tính hoặc hệ thống mạng để bảo vệ khỏi truy cập | Tích hợp trên máy tính cá nhân có sẳn |

Bảng 1.2.1: So sánh giữa Firewall cứng và Firewall mềm

## Nhiệm vụ của Firewall

* Quản lý truy cập
* Quản lý dữ liệu đi từ bên trong ra bên ngoài và ngược lại.
* Đảm nhiện vai trò như một proxy.
* Lọc các gói tin dựa theo địa chỉ nguồn và port
* Bảo vệ được tài nguyên của hệ thống.
* Cân bằng tải
* Kiểm soát được các địa chỉ truy cập
* Ngăn chặn được xâm nhập trái phép từ bên ngoài

- Ngoài ra Firewall còn có chức năng kiểm soát các dịch vụ cho phép người dùng sử dụng dịch vụ hoặc cấm sử dụng dịch vụ đó.

- Kiểm soát các file tệp khi tải về và loại bỏ các file tệp đó khi chứa nội dung độc hại cho máy tính.

## Chức năng của Firewall

Chức năng đầu tiên cơ bản của Firewall là quản lý kiểm soát nguồn dữ liệu: Kiểm soát tất cả các gói tin và lưu lượng mạng và các kết nối. Kiểm tra IP nguồn và IP đích, địa chỉ nguồn, địa chỉ đích, port nguồn và port đích. Để hai máy tính có thể giao tiếp với nhau giữa chúng cần thiết lập các kết nối. Phải xác định bản thân là host của nhau và nhiệm vụ của Firewall là kiểm tra kết nối này có được phép hay không, và giao thức sử dụng có hợp lệ hay không.

Xác nhận quyền truy cập: Khi người dùng muốn đăng nhập vào hệ thống Firewall có thể yêu cầu người dùng xác nhận danh tính, yêu cầu username và password xác nhận người dùng có phải là authentication hay người dùng truy cập từ xa. Có thể xác thực người dùng bằng public key hoặc Pre-share Keys để xác thực.

Là phần mềm trung gian: Việc người dùng truy cập ra ngoài Internet hay download dữ liệu từ bên ngoài vào máy tính có thể nhiều mối nguy hại tấn công như virus, các phần mềm độc hại. Firewall hoạt động như một proxy trung gian kiểm soát, giúp người dùng xác định đâu là phần mềm độc hại bị nhiễm mã độc đảm bảo sử dụng một cách an toàn.

Bảo vệ tài nguyên của hệ thống: Kiểm soát quyền truy cập, kiểm soát gói tin, bảo vệ khỏi những truy cập bất hợp pháp. Cũng là bước đầu để phòng chống các cuộc tấn công mạng.

## Những hạn chế của Firewall

* Firewall không tự phát hiện những lổ hỏng của hệ điều hành.
* Khi có lỗi cần phải nâng cấp Firewall để hệ thống hoạt động ổn định.
* Hiệu quả từ việc chống lại tấn công bỏ qua tường lừa hầu như bằng 0.
* Việc Attacker tấn công từ bên trong nội bộ có thể xảy ra và Firewall không thể chống lại.

## Tường lửa thế hệ mới (Next – generation Firewall (NGFW))

Tường lửa thế hệ mới NGFW có khả năng phân tích sâu vào gói tin (Deep-packet-Inspection) không bị gới hạn ở mức Protocol hay Port. Được xây dựng trên nhu cầu của doanh nghiệp.

Khả năng phân tích được những gói tin ở tầng Applicaton, có thể phát hiện và ngăn chặn xâm nhập.

Lọc các gói tin và địa chỉ mạng, kiểm tra mạng riêng ảo VPN. Ngăn chặn được nhũng cuộc tấn công tinh vi nhờ vào cơ chế phòng chống phát hiện ngăn chặn xâm nhập thực hiện các chính sách bảo mật ở lớp ứng dụng và giao thức ở các cổng để kiểm soát được toàn bộ hệ thống.

Bảo vệ chống lại những mối đe dọa TTL và người sử dụng ở tầng ứng dụng. Kiểm soát hiển thị chính sách của những hoạt động ứng dụng riêng lẻ.



Hình .: Tường lửa thế hệ mới

* **Lợi ích của NGFW:**

Ngăn chặn được các xâm nhập vào hệ thống mà Firewall truyền thống không thể làm được, giải quyết được nhũng mối đe dọa mới API. Giảm chi phí cho việc bảo vệ hệ thống, bằng việc tích hợp phần mềm diệt virus, bảo mật trong ứng dụng.

Thông qua cơ chế xác định ứng dụng, người dùng, nội dung và chính sách bảo mật.

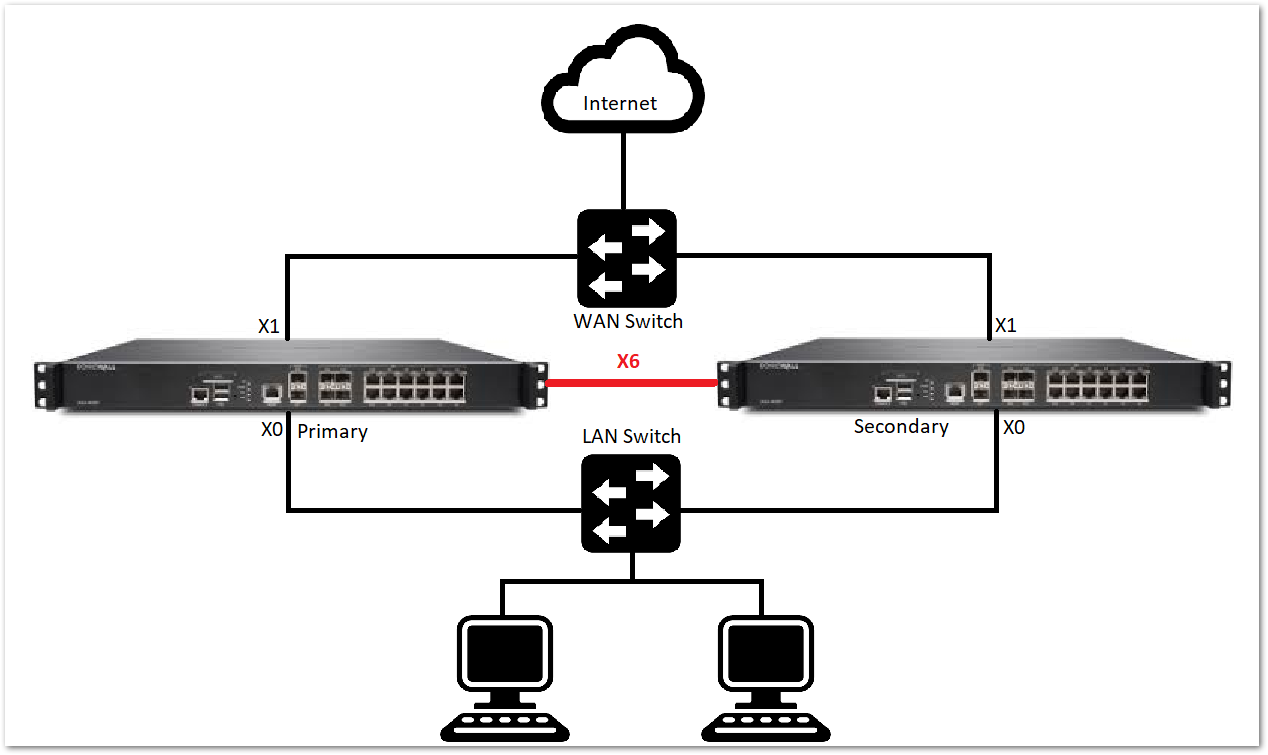
# CHƯƠNG 2: GIỚI THIỆU MỘT SỐ CHỨC NĂNG VÀ DỊCH VỤ PFSENSE

## HA và CARP

#### Giới thiệu về HA (High Availability)

High Availability (HA) có nghĩa là “ Độ sẵn sàng cao” những máy chủ loại này luôn sẵn sàng phục vụ bị sự cố trục trặc, hư hỏng sẽ gây gián đoạn công việc người sử dụng.

Để đảm bảo được điều đó, tối thiểu có một cặp máy, thiết bị chạy song song, liên tục liên lạc với nhau, khi máy chính hỏng hay gặp trục trặc, sự cố, máy phụ sẽ lập tức tự động thay thế máy chính hoạt động để không gây gián đoạn công việc của người dùng.



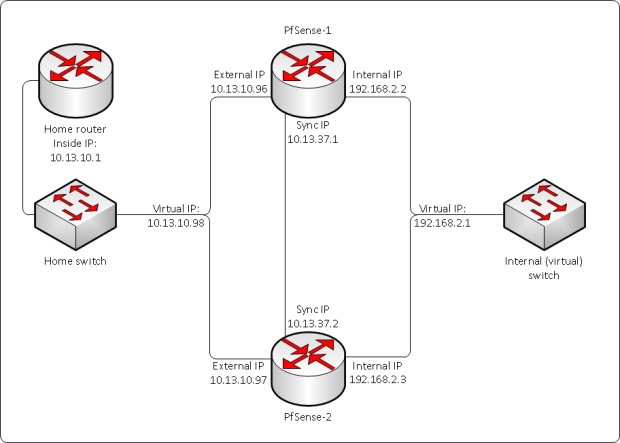
Hình .: High Availability Firewall

Thông thường các nhóm máy chủ được gọi là “CARP cluster” nhưng CARP chỉ là một phần. High Availability đạt được bằng cách sử dụng sự kết hợp của nhiều kỹ thuật có liên quan, bao gồm cả CARP, trạng thái đồng bộ (pfsync) và cấu hình đồng bộ (XMLRPC Sync).

#### Giới thiệu về CARP (Common Address Redundancy Protocol)

Common Address Redundancy Protocol (CARP): được sử dụng bởi các Node để chia sẻ một IP ảo (Virtual IP) giữa nhiều nút với nhau sao cho khi một Node Fail thì IP ảo đó vẫn hoạt động bởi các Node khác. CARP được bắt nguồn từ OpenBSD như một thay thế mã nguồn mở cho giao thức Route ảo VRRP (The Virtual Router Redundancy Protocol).

ARP sử dụng multicast vì vậy cần chú ý tới các switch trên hệ thống có hạn chế hoặc block, filter địa chỉ multicast hay không.



Hình .: Common Address Redundancy Protocol

#### State Synchronization (pfsync)

Trạng thái đồng bộ được xử lý bởi pfsync mà truyền thông tin trạng thái qua 1 bảng (nội dung, thêm, sửa, xóa …) tới các Node khác trên cổng mạng Private/Share mà bao gồm các trạng thái kết nối có giá trị.

Bằng cách này, nếu có một Node Fail thì các Node khác sẽ tiếp quản và người dùng có thể tiếp tục sử dụng mà không cần thiết phải Reconnect lại.

#### Configuration Synchronization (XMLRPC Sync)

Cấu hình đồng bộ được xử lý bởi XMLRPC Sync.

Cơ chế này cho phép Pfsense truyền thông tin cấu hình và các Command giữa các Node. Điển hình là các Node chính sẽ đồng bộ tới các Node phụ.

#### Cơ chế hoạt động

HA pfsense hoạt động theo Master – Slave khi có một thay đổi trên Master, Pfsense sẽ tạo một bản ghi XML và truyền tới tới Backup qua cổng 80 hoặc 443. Server Backup sẽ đồng bộ với Master theo những cấu hình đã được định sẵn.

#### Điều kiện cần để thực hiện được HA

* Có tối thiểu 3 IP mỗi subnet trên các cổng mạng của Pfsense (1 IP cho Master, 1 IP cho Backup và 1 Virtual IP chính dùng để giao tiếp với các thiết bị khác)
* Các thiết bị layer 2 phải cho phép multicast
* Upstream/ISP/các routers có liên quan phải có khả năng gọi được các Virtual IP được sử dụng bởi CARP

## Hệ thống giám sát và phát hiện ngăn chặn xâm nhập (IDS/IPS) trên Firewall

#### Hệ thống giám sát (IDS)

IDS được biết ngắn gọn của từ Intrusion detection System đây là một công nghệ phát hiện xâm nhập. Ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động xâm nhập không mong muốn đối với hệ thống máy tính.

Diagram

Description automatically generated

#### Hệ thống phát hiện ngăn chặn xâm nhập (IPS)

[IPS](https://en.wikipedia.org/wiki/IPS) được biết tắt bởi từ tiếng anh là Intrusion Prevention Systems (IPS) là một công nghệ phòng chống an ninh mạng. Mối đe dọa rằng giao thông kiểm tra mạng lưới luồng để phát hiện và ngăn chặn khai thác lỗ hổng. Khai thác lỗ hổng thường xuất hiện dưới dạng đầu vào độc hại cho ứng dụng hoặc dịch vụ mục tiêu mà kẻ tấn công sử dụng để làm gián đoạn và giành quyền kiểm soát ứng dụng hoặc máy.

Sau khi khai thác thành công, kẻ tấn công có thể vô hiệu hóa ứng dụng đích (dẫn đến trạng thái từ chối dịch vụ) hoặc có khả năng truy cập tất cả các quyền và quyền có sẵn cho ứng dụng bị xâm nhập.

Diagram

Description automatically generated

#### So sánh IDS và IPS

Cả IDS / IPS đều đọc các gói mạng và so sánh nội dung với cơ sở dữ liệu về các mối đe dọa đã biết. Sự khác biệt chính giữa chúng là những gì xảy ra tiếp theo. IDS là các công cụ phát hiện và giám sát không tự mình thực hiện. IPS là một hệ thống điều khiển chấp nhận hoặc từ chối một gói dựa trên bộ quy tắc.

IDS yêu cầu con người hoặc hệ thống khác xem xét kết quả và xác định hành động nào cần thực hiện tiếp theo, đây có thể là công việc toàn thời gian tùy thuộc vào lượng lưu lượng truy cập mạng được tạo ra mỗi ngày. IDS làm cho một công cụ pháp y sau khám nghiệm tử thi tốt hơn để CSIRT sử dụng như một phần của các cuộc điều tra sự cố an ninh của họ.

Mục đích của IPS, mặt khác, là để bắt các gói nguy hiểm và thả chúng trước khi chúng đến mục tiêu của chúng. Nó thụ động hơn IDS, chỉ cần yêu cầu cơ sở dữ liệu được cập nhật thường xuyên với dữ liệu mối đe dọa mới.

* Cách phòng ngừa và phát hiện xâm nhập:
* Phòng ngừa xâm nhập: IPS thường nằm ngay sau tường lửa và cung

cấp một lớp phân tích bổ sung, lựa chọn tiêu cực cho nội dung nguy hiểm. Không giống như người tiền nhiệm của nó. Hệ thống phát hiện xâm nhập (IDS) là một hệ thống thụ động quét lưu lượng và báo cáo lại các mối đe dọa. IPS được đặt nội tuyến (trong đường dẫn liên lạc trực tiếp giữa nguồn và đích), chủ động phân tích và thực hiện các hành động tự động trên tất cả luồng lưu lượng truy cập vào mạng.

* Cụ thể, những hành động này bao gồm: gửi một báo động cho quản trị

viên (như sẽ thấy trong IDS), bỏ các gói độc hại, chặn lưu lượng truy cập từ địa chỉ nguồn, đặt lại kết nối. Là một thành phần bảo mật nội tuyến, IPS phải hoạt động hiệu quả để tránh làm giảm hiệu suất mạng. Nó cũng phải hoạt động nhanh vì khai thác có thể xảy ra trong thời gian gần. IPS cũng phải phát hiện và phản hồi chính xác, để loại bỏ các mối đe dọa và dương tính giả (các gói hợp pháp bị đọc nhầm thành các mối đe dọa).

* Phát hiện xâm nhập: IPS có một số phương pháp phát hiện để tìm kiếm

khai thác, nhưng phát hiện dựa trên chữ ký và phát hiện dựa trên thống kê là hai cơ chế chi phối. Phát hiện dựa trên chữ ký được dựa trên một từ điển các mẫu (hoặc chữ ký) duy nhất trong mã của mỗi khai thác. Khi khai thác được phát hiện, chữ ký của nó được ghi lại và lưu trữ trong một từ điển chữ ký phát triển liên tục. Phát hiện bất thường thống kê lấy các mẫu lưu lượng mạng một cách ngẫu nhiên và so sánh chúng với mức hiệu suất cơ sở được tính toán trước. Khi mẫu hoạt động lưu lượng mạng nằm ngoài các tham số về hiệu suất cơ sở, IPS sẽ hành động để xử lý tình huống.

## Open VPN

#### Giới thiệu VPN

VPN (Virtual Private Network) là mạng riêng ảo, cho phép người dùng thiết lập mạng riêng ảo với một mạng khác trên Internet để kết nối các địa điểm hoặc người dùng từ xa với một mạng LAN ở trụ sở trung tâm. Thay vì dùng kết nối thật khá phức tạp như các đường dây thuê bao số.

Trước đây, để truy cập từ xa vào hệ thống mạng, người ta thường sừ dụng phương thức Remote Access quay số dựa trên mạng điện thoại. Phương thức này vừa tốn kém vừa không an toàn.

VPN cho phép các máy tính truyền thông với nhau thông qua một môi trường chia sẻ như mạng Internet nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu.

Giải pháp VPN (Virtual Private Network) được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa và địa bàn hoạt động rộng (trên toàn quốc hay toàn cầu). Tài nguyên ở trung tâm có thể kết nối đến từ nhiều nguồn nên tiết kiệm được được chi phí và thời gian.

#### Cơ chế hoạt động

Khi sử dụng VPN, thiết bị của cho dù đang ở bên ngoài công ty, vẫn có thể truy cập và ping được các máy trong hệ thống mạng nội bộ. VPN giúp tạo một đường hầm kết nối để thiết bị của chúng ta gia nhập vào mạng LAN này

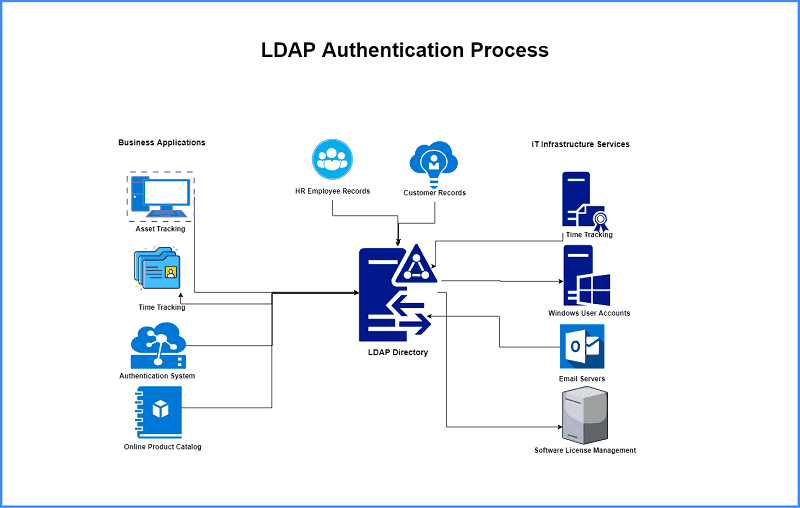
Một mạng VPN điển hình bao gồm mạng LAN chính tại trụ sở (Văn phòng chính), các mạng LAN khác tại những văn phòng từ xa, các điểm kết nối (như 'Văn phòng' tại gia) hoặc người sử dụng (Nhân viên di động) truy cập đến từ bên ngoài

Để cung cấp kết nối giữa các máy tính, các gói thông tin được bao bọc bằng một header có chứa những thông tin định tuyến, cho phép dữ liệu có thể gửi từ máy truyền qua môi trường mạng chia sẻ và đến được máy nhận, như truyền trên các đường ống riêng được gọi là tunnel. Để bảo đảm tính riêng tư và bảo mật trên môi trường chia sẻ này, các gói tin được mã hoá và chỉ có thể giải mã với những khóa thích hợp, ngăn ngừa trường hợp "trộm" gói tin trên đường truyền. PfSense hổ trợ VPN trong sử dụng Internet Protocol Security (IPSec), OpenVPN hoặc PPTP.

## Xác thực LDAP

#### Giới thiệu LDAP

LDAP là viết tắt của từ Lightweight Directory Access Protocol. Đây là một chuẩn cho dịch vụ thư mục (Directory Service – DS) chạy trên nền tảng OSI.



Hình .: Lightweight Directory Access Protocol

#### Cơ chế hoạt động

LDAP chỉ là một giao thức, không hỗ trợ xử lý như Database. Mà nó cần một nơi để lưu trữ Backend và xử lý các dữ liệu tại đó. Vì vậy mà LDAP Client sẽ kết nối tới LDAP server theo mô hình sau:

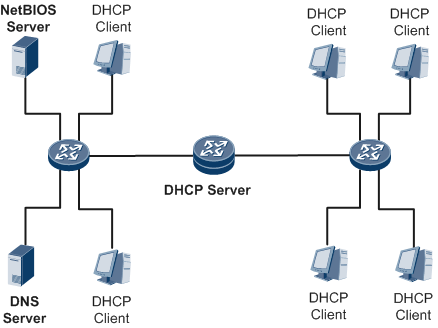
* LDAP là một giao thức truy cập vì vậy nó theo mô hình dạng cây (Directory Information Tree)

LDAP hoạt động theo mô hình là Client-Server. Một hay nhiều LDAP Server chứa các thông tin về cây thư mục (Directory Information Tree – DIT). Client kết nối đến Server và gửi đi yêu cầu. Server phản hồi lại bằng chính nó hoặc trỏ tới LDAP Server khác để Client lấy được thông tin. Trình tự khi có kết nối với LDAP.

* Connect (kết nối với LDAP): Client sẽ mở kết nối tới LDAP Server.
* Bind (kiểu kết nối: ẩn danh hoặc đăng nhập xác thực): Client gửi đi các thông tin xác thực.
* Search (tìm kiếm): Client gửi đi yêu cầu tìm kiếm.
* Interpret Search (xử lý tìm kiếm): Server thực hiện việc xử lý tìm kiếm.
* Result (kết quả): máy chủ trả lại kết quả cho Client.
* Unbind: client gửi đi yêu cầu đóng kết nối tới Server.
* Close Connection (đóng kết nối): đóng đi kết nối từ Server.

## DHCP Server

DHCP viết tắt của từ Dynamic Host Configuration Protocol - Giao thức cấu hình Host động. Giao thức cung cấp phương pháp thiết lập các thông số cần thiết cho hoạt động của mạng TCP/IP giúp giảm khối lượng công việc cho quản trị hệ thống mạng. DHCP server là một máy chủ có cài đặt dịch vụ DHCP. Nó có chức năng quản lý sự cấp phát địa chỉ IP động và các dữ liệu cấu hình TCP/IP. Pfsense và OPNSense cung cấp dịch vụ DHCP server dùng để tự động cấu hình cho mạng TCP/IP bằng cách tự động gán các địa chỉ IP cho các máy client khi nó tham gia vào mạng.

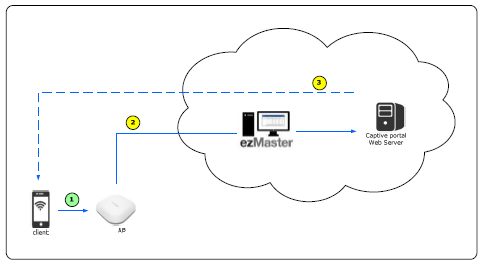


Hình .: DHCP Server

## Captive Portal

Captive Portal là một tính năng thuộc dạng Flexible, chỉ có trên các Firewall thương mại lớn. tính năng này giúp chuyển hướng trình duyệt của người dùng vào một trang Web định sẵn, từ đó giúp chúng ta có thể quản lý được người dùng (hoặc cấm không cho người khác dùng mạng của mình). Tính năng này tiên tiến hơn các kiểu đăng nhập như WPA, WPA2 ở chỗ người dùng sẽ thao tác trực tiếp với 1 trang web (http, https) chứ không phải là bảng đăng nhập khô khan như kiểu Authentication WPA, WPA2.

Captive Portal cho phép việc chứng thực có hiệu quả, hoặc chuyển hướng click chuột thông qua trang web để truy cập vào mạng. Điều này thường được dùng vào các vị trí mạng nóng, nhưng cũng được sử dụng rộng rãi trong các mạng doanh nghiệp thêm một lớp bảo mật truy cập mạng không dây hoặc Internet.



## Network Load Balancer

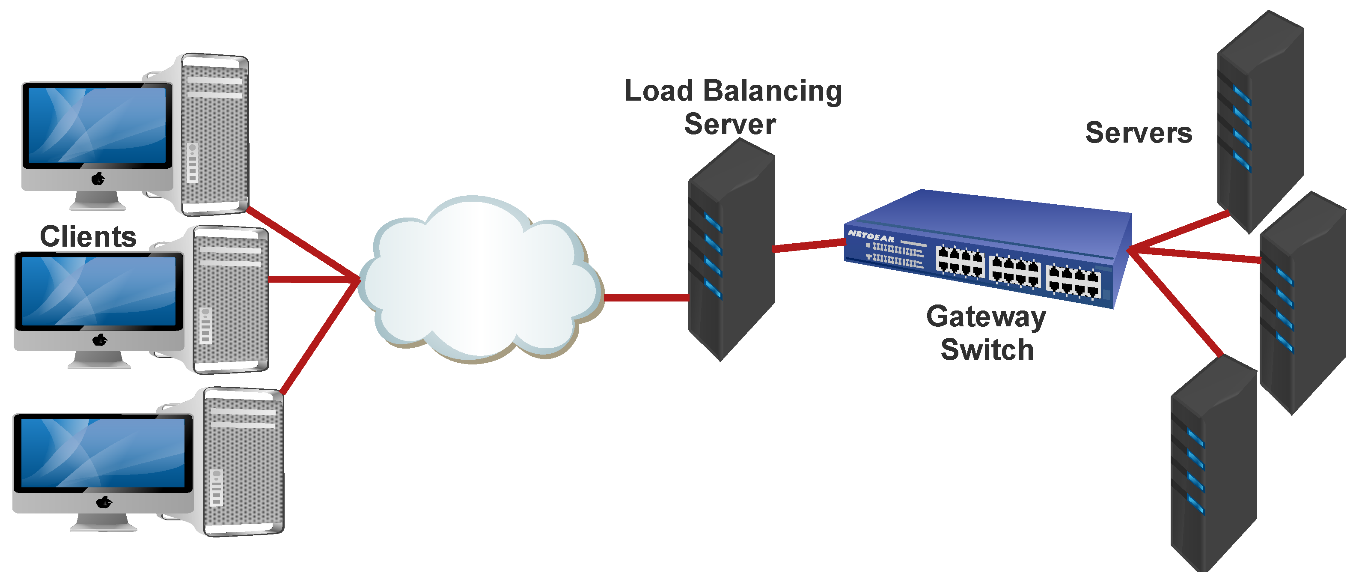
Networks Load Balancing hay còn gọi là cân bằng tải, đây là một dịch vụ tích hợp trong PfSense với nhiều tính năng hữu ích, nó có hai kiểu cân bằng tải, hỗ trợ khi một trong hai đường ADSL bị ngắt thì nó sẽ sử dụng đường còn lại hoặc nó có thể gom cả hai đường ADSL này thành một để tăng tốc độ tải xuống. Khả năng load balancing của PfSense rất tốt nó vẫn làm việc bình thường khi rút một trong hai đường ADSL nhưng khi cắm lại 2 đường thì tốc độ tải xuống được tăng tốc độ lên rất nhanh.

* Chức năng cân băng tải của pfsense có những đặc điểm
* Ưu điểm: miễn phí, có khả năng bổ sung thêm tính năng bằng gói dịch vụ

cộngthêm, dễ cài đặt, cấu hình.

* Hạn chế: phải trang bị thêm modem nếu không có sẵn, không được hỗ trợ

từ nhà sản xuất như các thiết bị cân bằng tải khác, vẫn chưa có tính năng lọc URL như các thiết bị thương mại, đòi hỏi người sử dụng phải có kiến thức cơ bản về mạng để cấu hình.

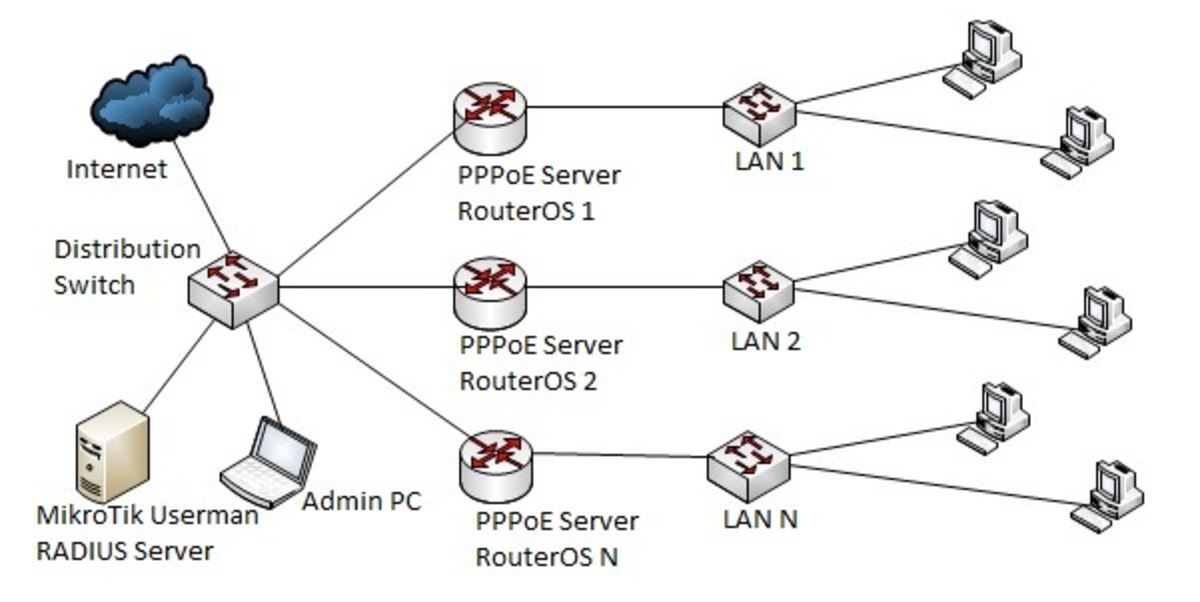


Hình .: Network Load Balancer

## PPPoE Server

Ponit-to-Point Protocol (hoặc PPP) là giao thức liên kết dữ liệu thường được dùng để thiết lập một kết nối trực tiếp giữa hai nút mạng. Nó có thể cung cấp kết nối xác thực, mã hóa việc truyền dữ liệu.

PfSense cung cấp một PPPoE Server. Một cơ sở dữ liệu người dùng cục bộ có thể được dùng để xác thực và RADIUS chứng thực với tùy chọn Accounting cũng được hỗ trợ.



Hình .: PPPoE Server

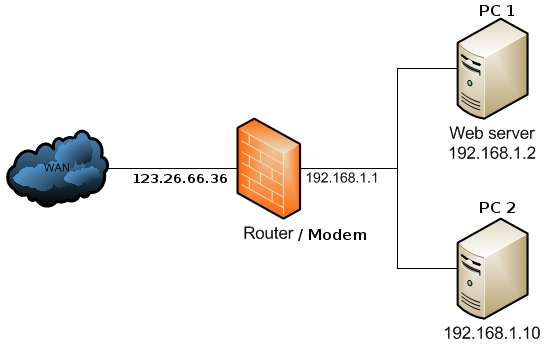
## Dynamic DNS

Dynamic DNS là một hệ thống cho phép tên miền internet được gán một địa chỉ bị thay đổi liên tục giá trị, điều này giúp cho các máy tính trên mạng có thể kết nối đến hệ thống mà không cần phải biết địa chỉ IP hiện tại của chúng.

Để thực hiện dịch vụ Dynamic DNS nhà cung cấp dịch vụ cần phải thiết lập thời gian truy cập địa chỉ IP sớm nhất (thông thường khoảng vài phút), đều này giúp cho các máy tính trên internet truy cập đến hệ thống khi có sự thay đổi địa chỉ IP xảy ra mà thời gian gián đoạn IP rất ít.

Dịch vụ Dynamic DNS được cung cấp trên một phạm vi rộng lớn bởi nhiều tổ chức khác nhau, các nhà cung cấp này sẽ duy trùy địa chỉ IP hiện tại trong cơ sở dữ liệu và cung cấp cơ chế cập nhật lại địa chỉ IP khi có yêu cầu.

Một Dynamic DNS client cho phép bạn đăng ký IP công cộng của bạn với số nhà cung cấp dịch vụ DNS động: DynDNS. DHS, DyNS, easyDNS, No-IP, ODS.org, ZoneEdit. Chỉ có thể cập nhật một tài khoản với một nhà cung cấp duy nhất. Nếu tôi có một modem, có được IP công cộng cho Pfsense một IP riêng thì các IP riêng sẽ được đăng ký với nhà cung cấp dịch vụ DNS.

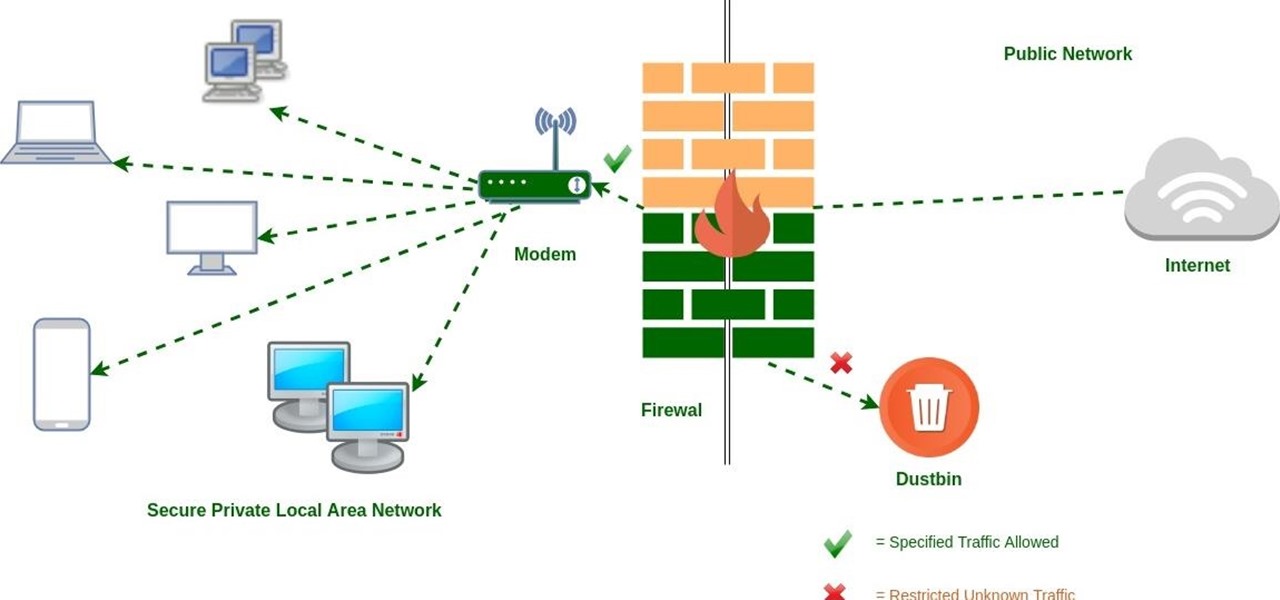


Hình .: Dynamic DNS

## Firewall Rules

Nơi lưu các rules (Luật) của Firewall. Lọc theo nguồn và đích IP, giao thức IP, cổng nguồn và đích cho TCP và UDP lưu lượng truy cập, có khả năng giới hạn kết nối đồng thời, cho phép các nhóm bí danh, tên mạng và các cổng. Điều này giúp giữ cho tường lửa của bạn sạch sẽ, đặc biệt là trong các môi trường với nhiều địa chỉ IP công cộng và các Server rất nhiều.

Mặc định Pfsense cho phép mọi traffic ra vào hệ thống. Bạn phải tạo ra các rules để quản lí mạng bên trong Firewall.

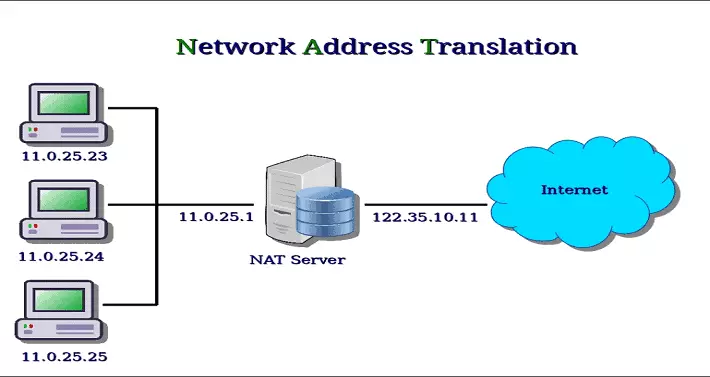


Hình .: Firewall Rules

## NAT

Pfsense cung cấp Network Address Translation (NAT) và tính năng chuyển tiếp cổng, tuy nhiên ứng dụng vẫn còn hạn chế với Point-to-Point Tunelling Protocol (PPTP) Generic Routing Encapsulation (GRE) và Session Intiation Protocol (SIP) khi sử dụng NAT.

Trong Firewall cũng có thể cấu hình các thiết lập NAT nếu cần sử dụng cổng chuyển tiếp cho các dịch vụ hoặc cấu hình NAT tĩnh (1:1) cho các Host cụ thể. Thiết lập mặc định của NAT cho các kết nối Outbound là automatic/dynamic .Tuy nhiên cũng có thể thay đổi kiểu manual nếu cần.

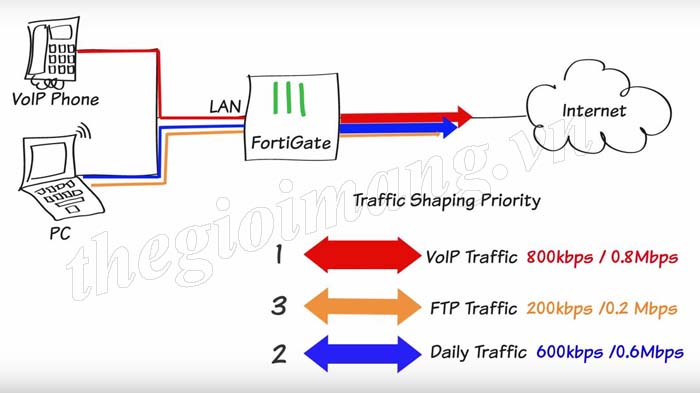


Hình .: NAT

## Traffic Shaper

Traffic Shape giúp theo dõi và quản băng thông mạng dễ dàng và hiệu quả hơn, điều khiển lưu lượng mạng máy tính để tối ưu hóa hiệu suất, độ trễ thấp hơn, hoặc tăng băng thông bằng cách trì hoãn, có thể sử dụng các gói dữ liệu đáp ứng theo tiêu chí nhất định.

Traffic Shaping là phương pháp tối ưu hóa kết nối Internet. Nó tăng tối đa tốc độ trong khi đảm bảo tối thiểu thời gian trễ. Khi sử dụng những gói dữ liệu ACK được sắp xếp thứ tự ưu tiên trong đường truyền tải lên, điều này cho phép tiến trình tải về được tiếp tục với tốc độ tối đa.



Hình .: Traffic Shaper

## Schedules

Các rules có thể được sắp xếp để nó có thể chỉ hoạt động vào các thời điểm nhất định cụ thể hoặc các ngày trong tuần. Đây là một tính năng giúp kiểm soát được thời gian làm việc ngoài ra schedule còn giúp ta có một lịch làm việc cụ thể và rõ ràng hơn.

## Aliases

Aliases có thể giúp bạn tiết kiệm một lượng lớn thời gian nếu bạn sử dụng chúng một cách chính xác

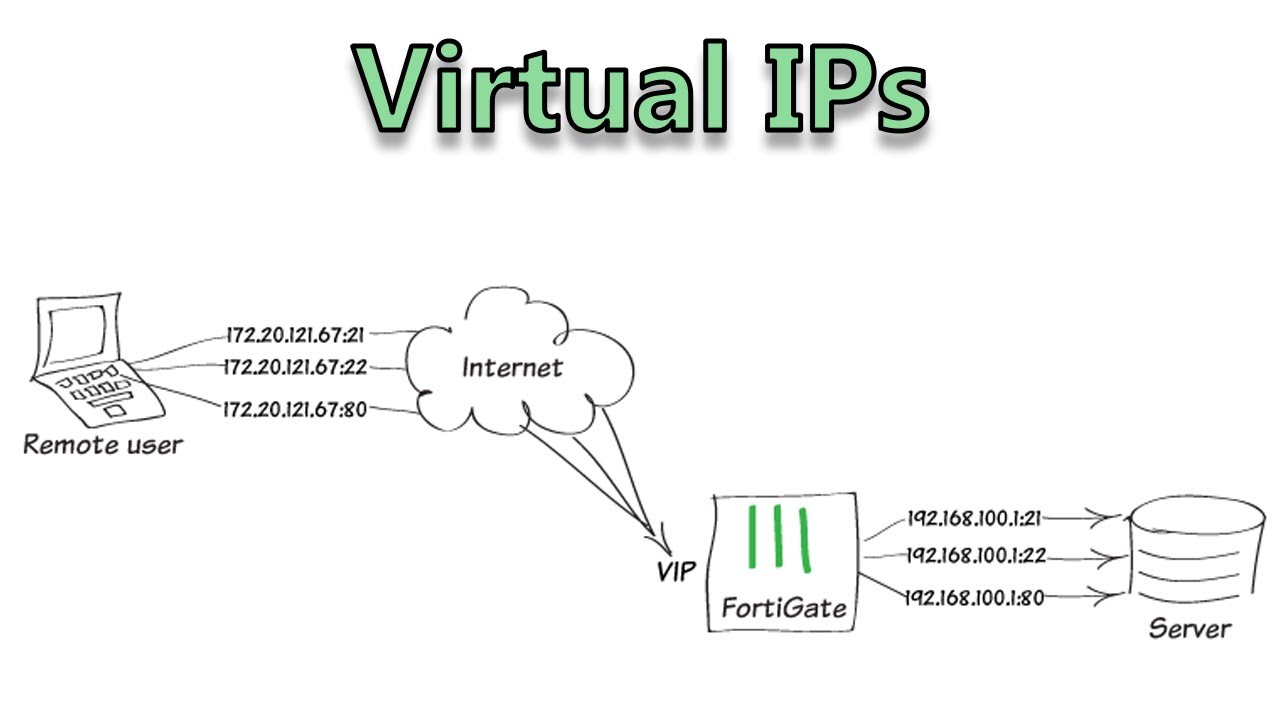
Một Aliases ngắn cho phép bạn sử dụng cho một host ,cổng hoặc mạng có thể được sử dụng khi tạo các rules trong pfSense .Sử dụng Aliases sẽ giúp bạn cho phép bạn lưu trữ nhiều mục trong một nơi duy nhất có nghĩa là bạn không cần tạo ra nhiều rules cho nhóm các máy hoặc cổng.

## Packages

Cung cấp thêm các chức năng mở rộng của pfsense, các gói có thể cài đặt bằng cách sử dụng Package Manager, nằm tại menu System,Packages Manager sẽ hiện thị tất cả các gói mở rộng,các gói mở rộng có miêu tả ngắn gọn về chức năng.

## Virtual IPs

Một Virtual IPs có thể sử dụng bất kỳ địa chỉ IP của pfSense, đó không phải là một địa chỉ IP chính. Trong các tình huống khác nhau, điều có các tính năng riêng của nó. Virtual IP được sử dụng để cho phép pfSense thực hiện đúng cách chuyển tiếp lưu lượng cho những cổng NAT, NAT Outbound, và NAT 1:1. Tính năng này cũng cho phép các tính năng như failover, và có thể cho phép các dịch vụ trên router để gắn kết với địa chỉ IP khác nhau.



Hình .: Virtual IPs

CARP: có thể sử dụng bởi các tường lửa của chính nó để chạy các dịch vụ hoặc được chuyển tiếp, tạo ra hai lớp traffic cho các VIP. Có thể được sử dụng cho clustering (tường lửa và tường lửa chủ failover chế độ chờ). Các VIP đã được đưa vào trong cùng một subnet IP của giao diện thực. Trả lời ICMP ping nếu được phép theo quy tắt tường lửa.

Proxy ARP: Không thể sử dụng được vì bị chặng bởi các tường lửa của chính nó, nhưng có thể được chuyển tiếp, tạo ra lớp hai traffic cho các VIP, Các VIP có thể được đưa vào trong một subnet khác với IP của giao diện thực, không trả lời gói tin ICMP ping.

# CHƯƠNG 3: DEMO HỆ THỐNG TƯỜNG LỬA PFSENSE

## Cài đặt PFSense

Đầu tiên, thêm đĩa pfsense vào máy ảo mới, sau đó sẽ vào được giao diện của pfsense.

Text

Description automatically generated

Chấp nhận quyền cho nó.

Graphical user interface, text

Description automatically generated

Sau đó **Install**.

Graphical user interface, application

Description automatically generated

Chọn **Continue with default keymap** và chọn **Auto (UFS) BIOS.**

Graphical user interface, text

Description automatically generated

Graphical user interface, application

Description automatically generated

Đợi sau khi cài đặt xong thì chọn No.

Graphical user interface, application, Teams

Description automatically generated

Hình .: Cài đặt PFSense

Graphical user interface, application

Description automatically generated

Sau đó Reboot lại máy.

Graphical user interface

Description automatically generated

Chọn card mạng cho phù hợp.

Graphical user interface, text, application

Description automatically generated

Sau đó chọn option là 2 và configure là 1. Chọn y cho DHCP và n cho DHCP6.

Text

Description automatically generated

Tại **revert to HTTP as the webConfigurator protocol** chọn **yes**.

Text

Description automatically generated

Chọn tiếp option 2. Đặt IPv4 là **192.168.1.10.**

Text

Description automatically generated

Hình .: Đặt IPv4

Chọn 24 subnet, no DHCP.

Text

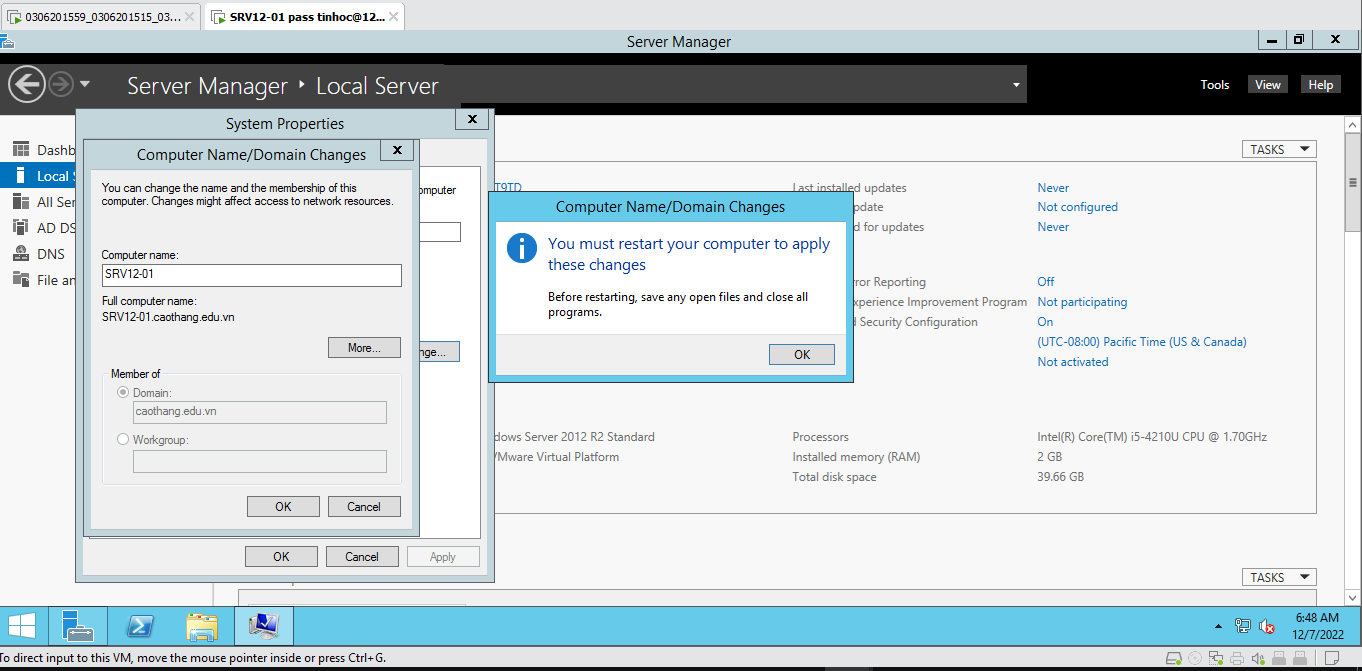
Description automatically generated

Sau đó ta sẽ vào được hệ thống pfsense.

Text

Description automatically generated

Join vào domain **caothang.edu.vn**.



Tiếp theo là đặt IP cho máy.

Graphical user interface, text, application

Description automatically generated

Sau đó tạo User Nhanvien với mật khẩu là 123456a@.

Graphical user interface, text, application, email

Description automatically generated

Hình .: Tạo User

Tương tự với user Truong Phong.

Graphical user interface, text, application

Description automatically generated

Tiếp theo, chỉnh card mạng máy win7 sau đó join domain caothang.edu.vn và login bằng user nv với mật khẩu 123456a@.

Graphical user interface, text

Description automatically generated

Làm tương tự với máy win7 (2) nhưng login bằng user tp.

Graphical user interface, text

Description automatically generated

Chuyển sang máy server, sau đó vào chrome, nhập **192.168.1.10** vào đường dẫn và login bằng tài khoản admin, mật khẩu là 123456a@.

Graphical user interface, website

Description automatically generated

## Setup PFSense

Tiến hành cài đặt pfsense theo hình.

Graphical user interface, application

Description automatically generated

A screenshot of a computer

Description automatically generated

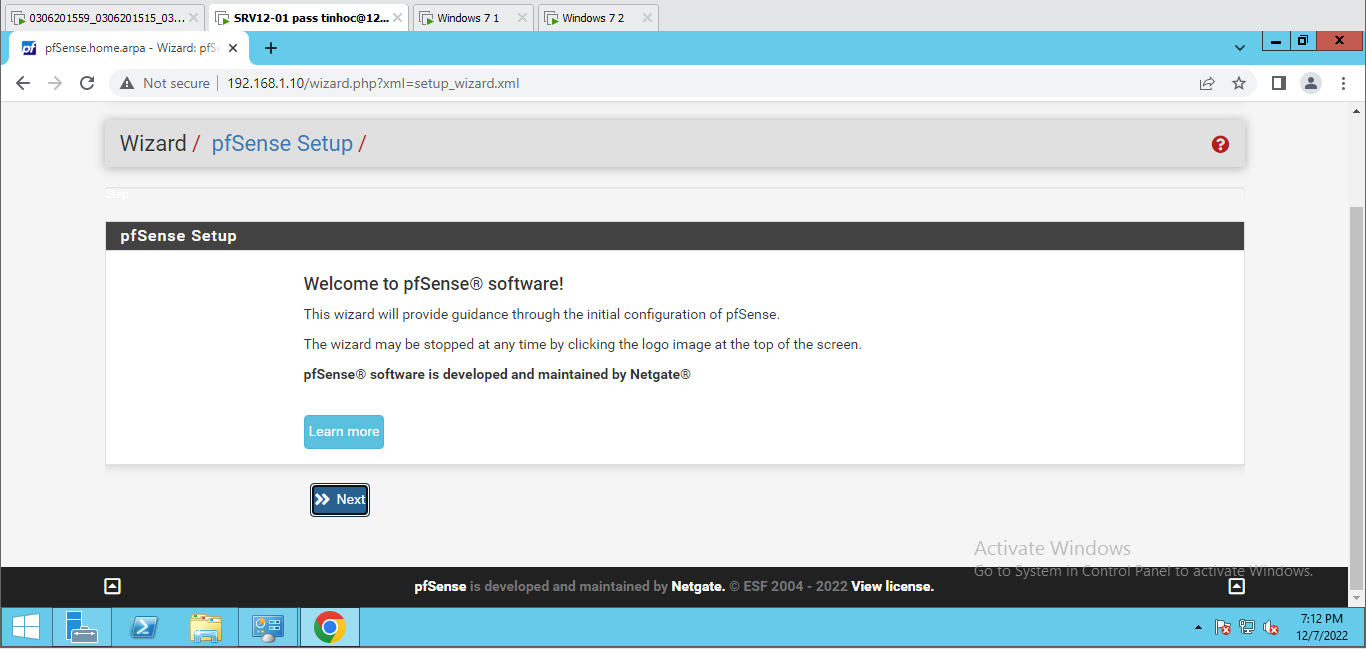
A screenshot of a computer

Description automatically generatedGraphical user interface, text, application

Description automatically generated

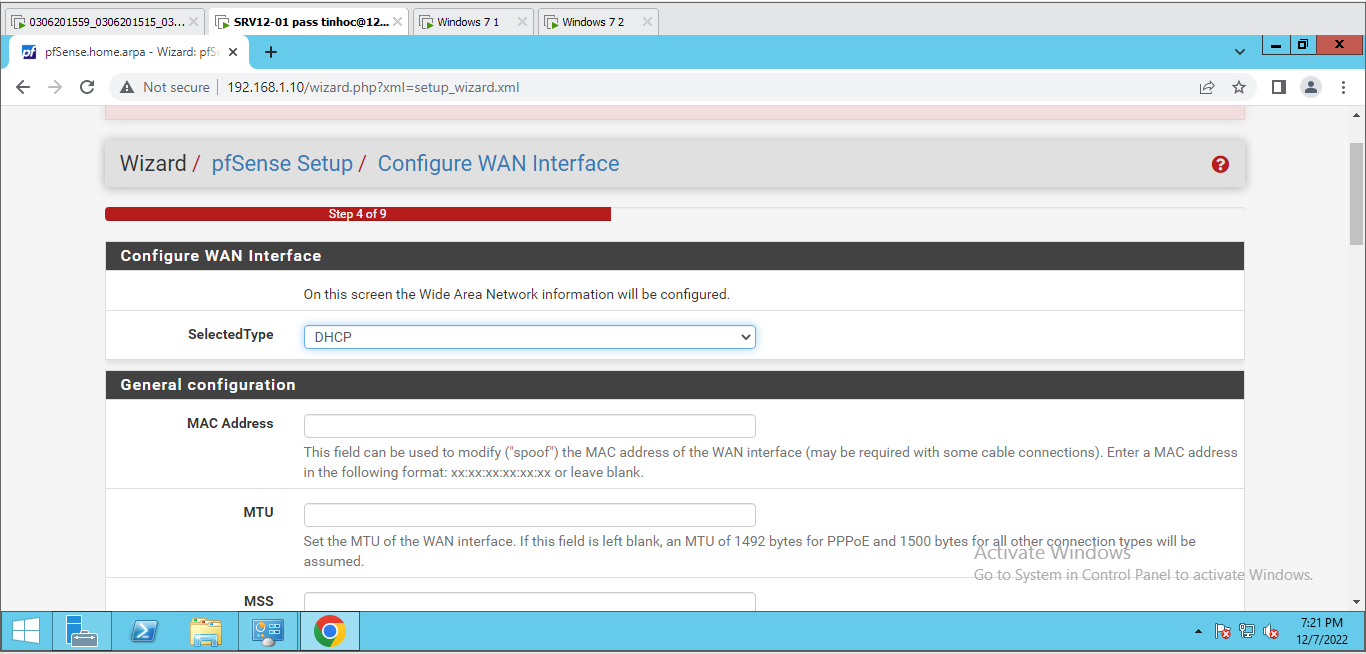
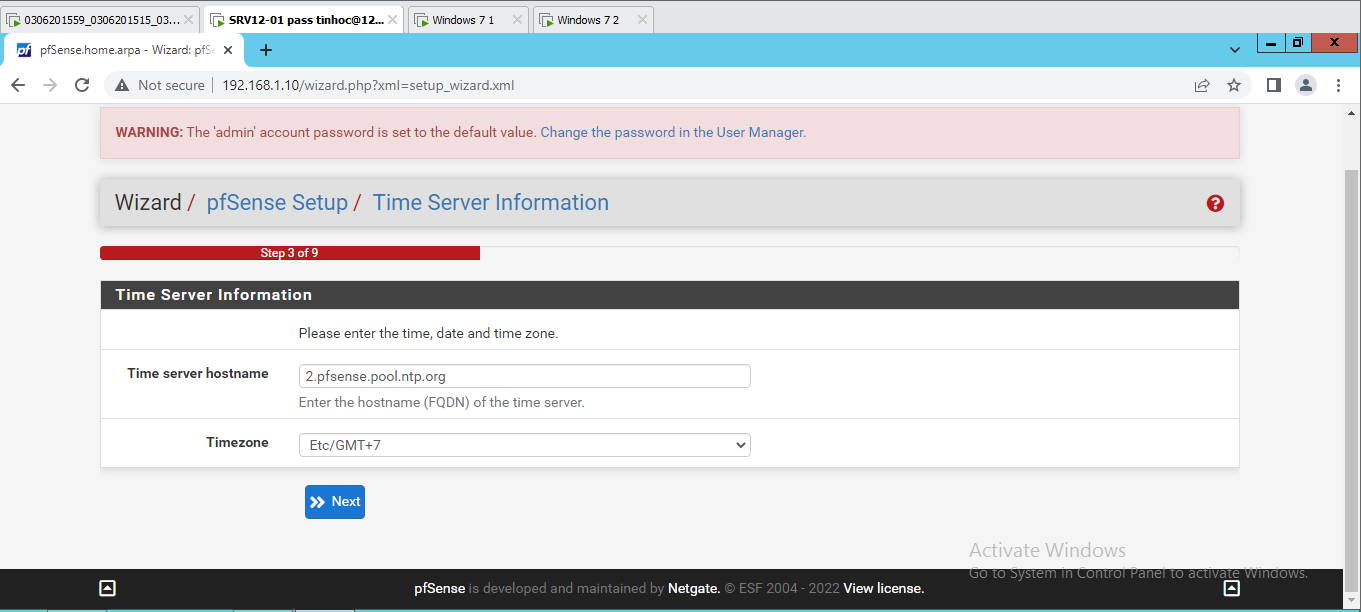
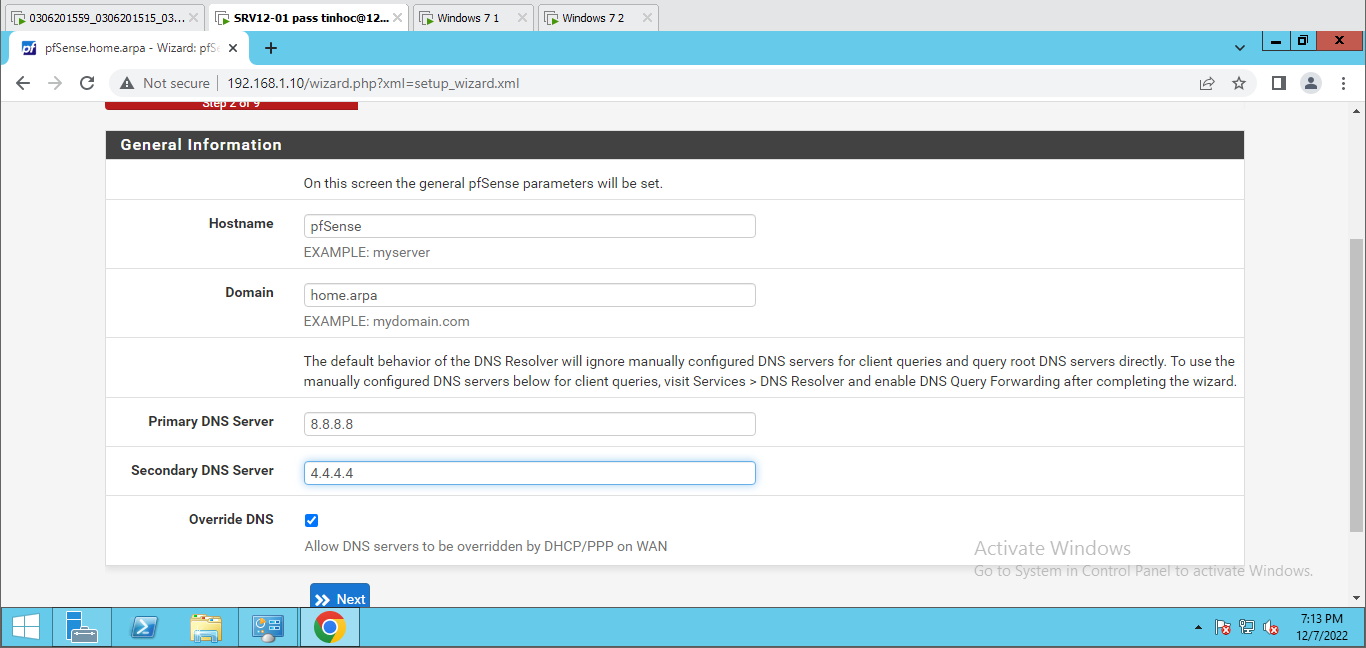
Graphical user interface, text, application, email

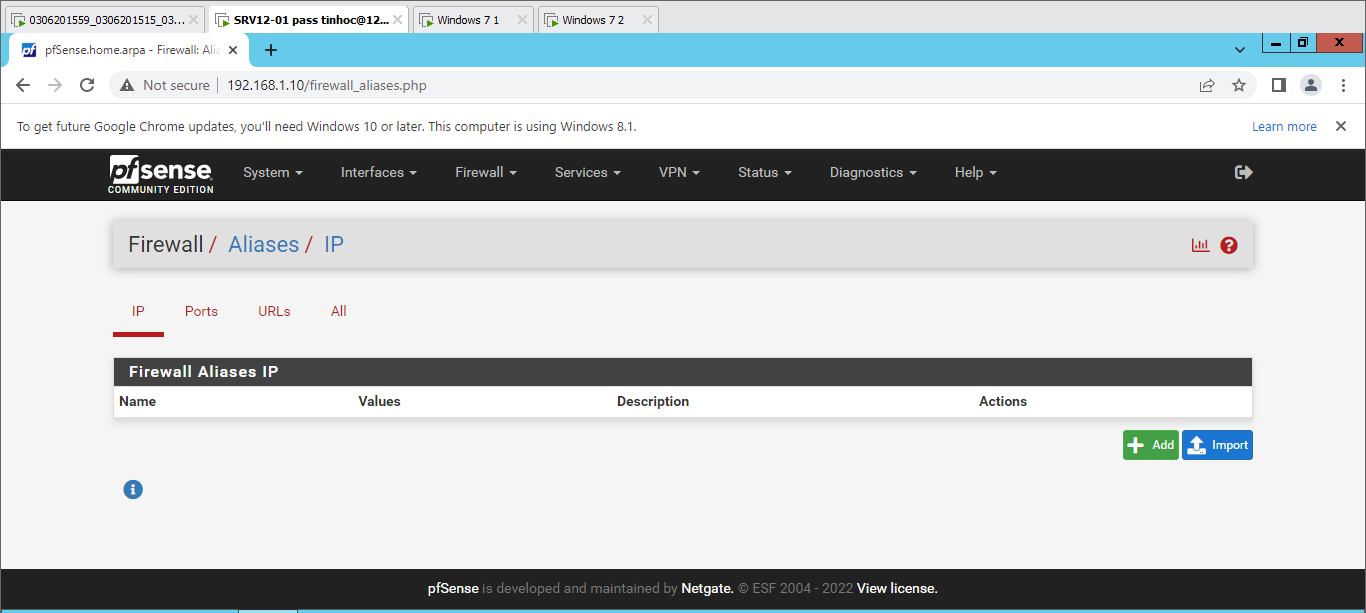
Description automatically generated



Hình .: Setup PFSense

## Chặn nhân viên truy cập web

Chọn **Firewall** trên menu sau đó chọn **Aliases**.



Chọn **add** và điền các thông số.

Graphical user interface, text, application, Word

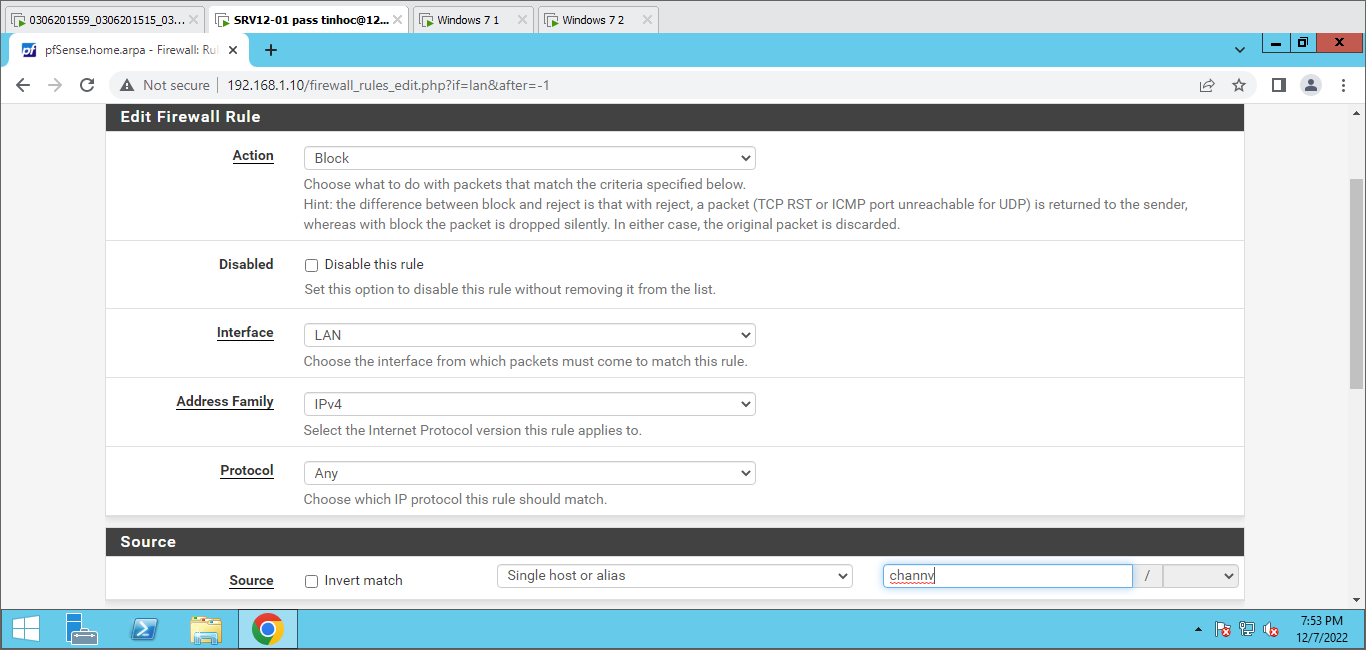
Description automatically generated

Tiếp theo, chọn **Rules** trong menu **Firewall**. Chọn **add** lên.

Graphical user interface, application

Description automatically generated

Chỉnh các thông số như sau.



Hình .: Tạo Rules chặn nhân viên

Như vậy sẽ chặn không cho nhân viên truy cập web được.

A screenshot of a computer

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Nhưng trưởng phòng vẫn truy cập web được.

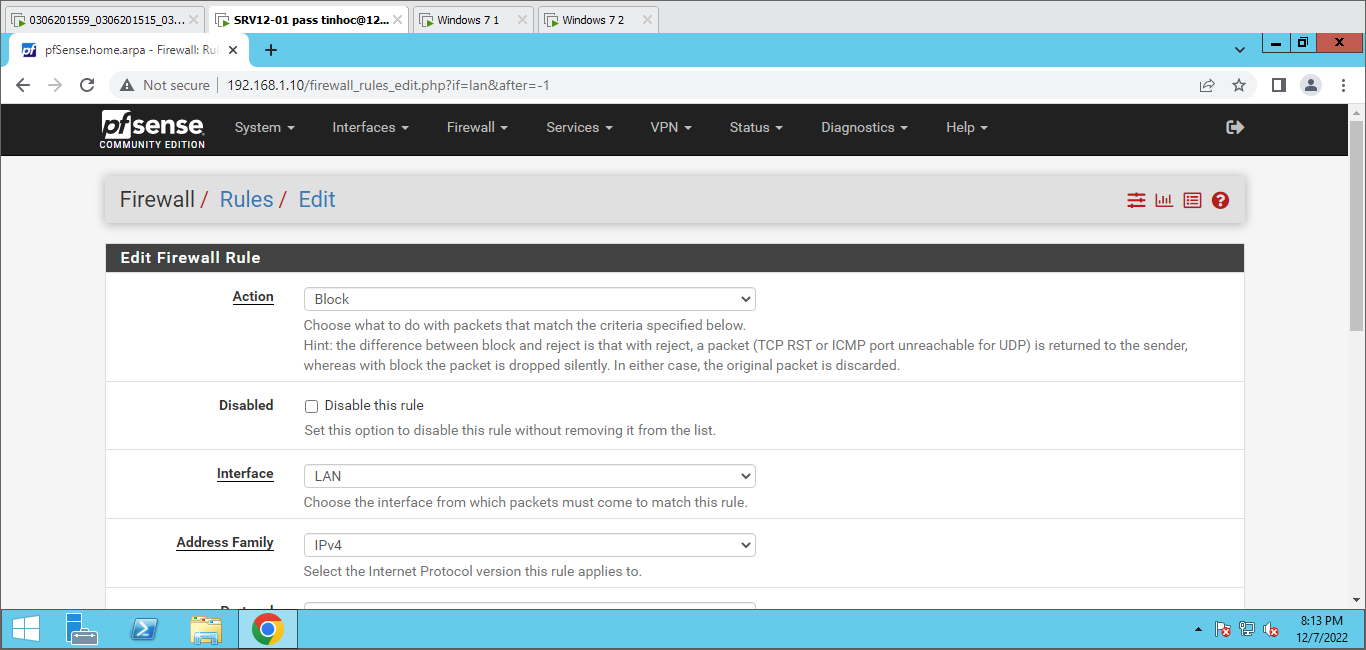
Text

Description automatically generated

A screenshot of a computer

Description automatically generated

## Thiết lập không cho trưởng phòng truy cập facebook nhưng vẫn truy cập được web và nhưng trang khác.



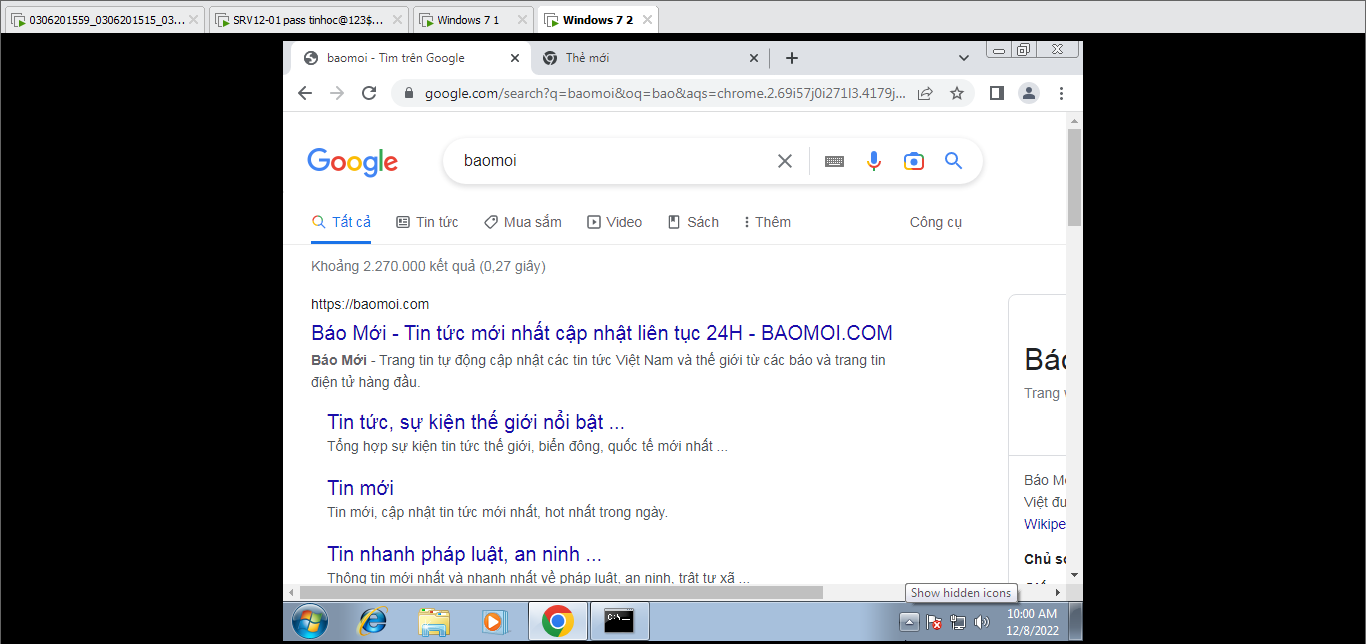
Graphical user interface, text, application, email

Description automatically generated

Hình .: Chặn trưởng phòng truy cập Facebook

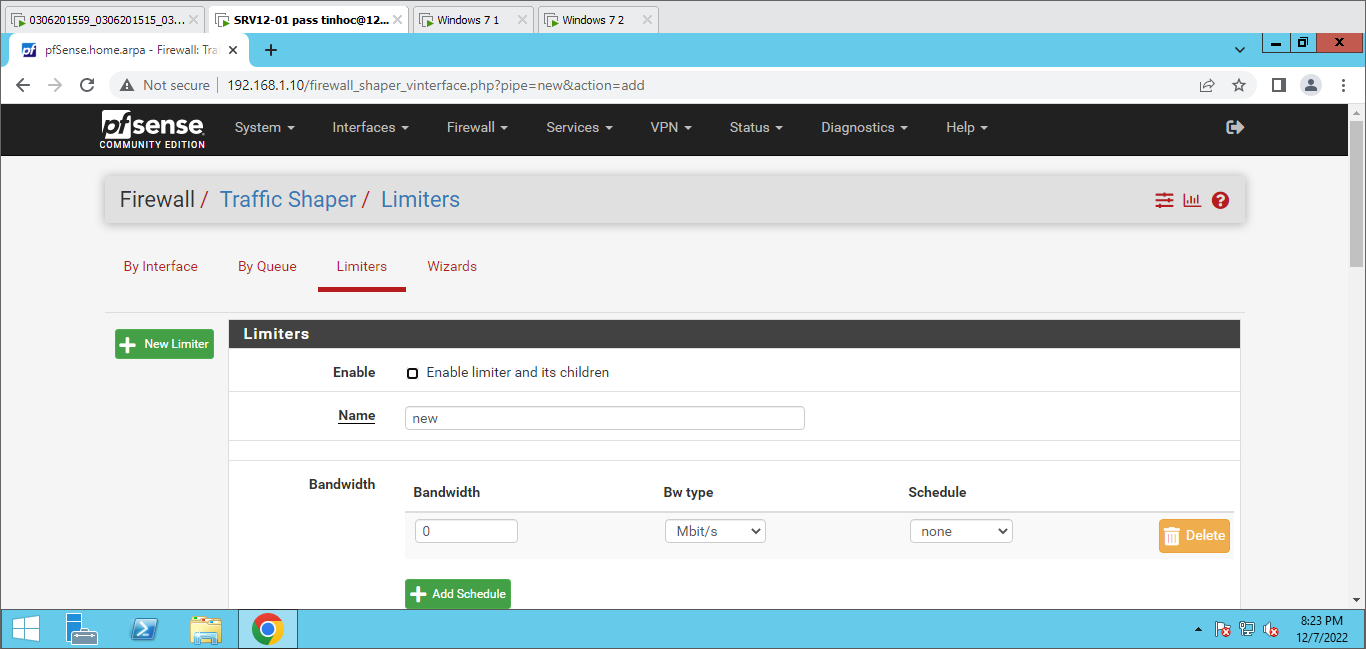
Graphical user interface, text

Description automatically generated



## Thiết lập tốc độ upload và download.

Chọn **Traffic Shaper** trên menu **Firewall**. Rồi chọn **New Limiter**



Nhập các dữ liệu.

Graphical user interface, application

Description automatically generated

Hình .: Thiết lập tốc độ Upload

Graphical user interface, text

Description automatically generated

Hình .: Thiết lập tốc độ Download

Sau đó vào **Rules** thêm Upload và Download cho máy nhân viên.

Graphical user interface, text, application, website

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Chọn **Display Advanced** để hiện thêm nhiều cài đặt hơn.

A screenshot of a computer

Description automatically generated

. Graphical user interface, text, application, email

Description automatically generated

Tiếp theo, tiến hành thử nghiệm đo tốc độ upload và download bằng trang web **speedtest.vn**.

A screenshot of a computer

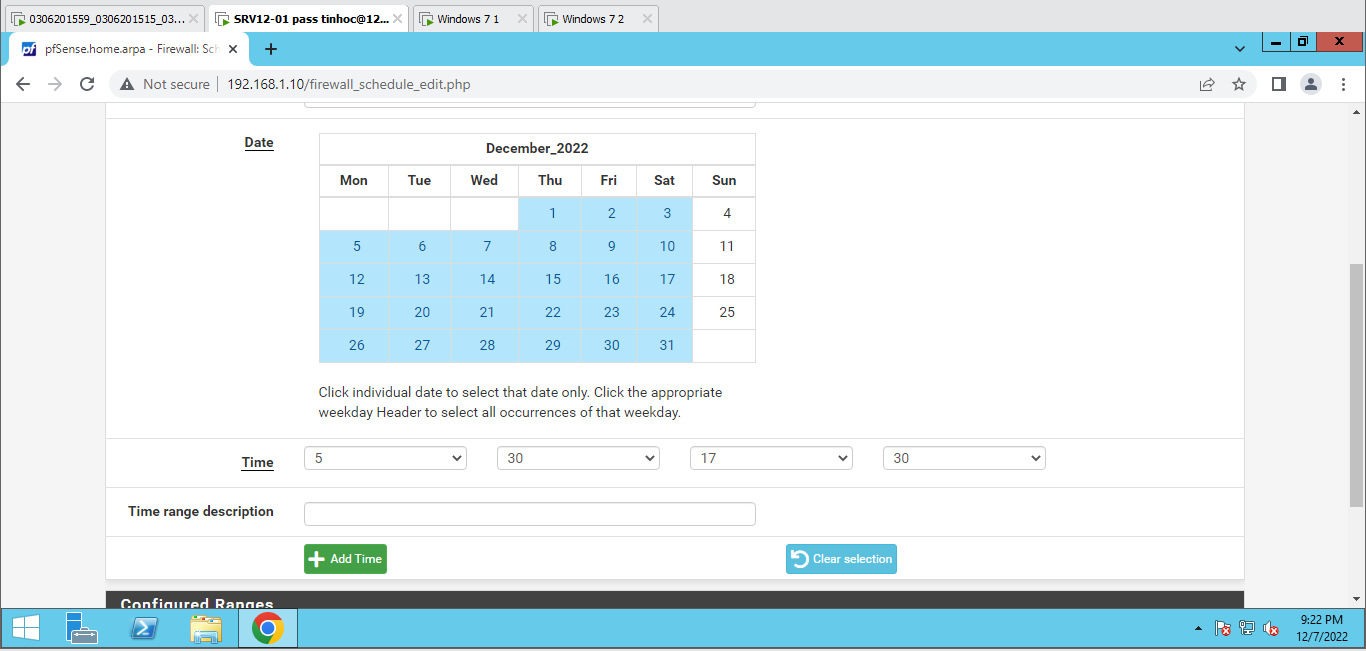
Description automatically generated

A computer screen with a blue background

Description automatically generated with low confidence

## Thiết lập thời gian làm việc cho nhân viên

Bắt đầu từ thứ 2 đến thứ 7 và từ 5:30 – 17:30.

. 

Hình .: Thiết lập thời gian làm việc

Sau đó thêm lịch làm việc cho nhân viên.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

# CHƯƠNG 3: KẾT LUẬN

Trong đồ án này chúng em đã tìm hiểu, triển khai hệ thống tường lửa PFSense.

Đã thực hiện :Tụi em đã áp dụng các kiến thức của môn học mình đã được học vào mô hình này và đã học hỏi thêm được nhiều kinh nghiệm về cách thức tổ chức, xây dựng, triển khai hệ thống tường lửa PFSense này.

Tuy nhiên, do thời gian và khả năng có hạn, nên chưa đi sâu tìm hiểu được thêm những vấn đề cần thiết của hệ thống. Mô hình tường lửa PFSense này chỉ là có những chức năng cơ bản chẳng hạn như: thiết lập thời gian làm việc, tốc độ upload và download cùng với chặn truy cập web, chặn truy cập mạng.

Ưu điểm là Người dùng máy server có thể thiết lập chặn hoặc cho phép người dùng máy client truy cập web hoặc có thể thiết lập thời gian hoạt động của máy client.

Nhược là phải cài một phần mềm được cung cấp bởi noip, dyndns lên một máy tính nào đó trong mạng nội bộ, để phần mềm đó cập nhật thường xuyên địa chỉ IP, rồi lại phải cấu hình tường lửa để cho phép phần mềm đó hoạt động.

Hướng phát triển: Trong tương lai sẽ phát triển và nghiên cứu sâu hơn thành hệ thống tường lửa dùng cho những doanh nghiệp lớn để cho phép hoặc chặn những nhân viên truy cập web và những chức năng nâng cao hơn.

|  |  |  |
| --- | --- | --- |
| MSSV | Họ Tên | Công Việc |
| 0306201526 | Nguyễn Thành Đức | Viết báo cáo slide word + hỗ trợ demo(30%) |
| 0306201515 | Phạm Phúc Bảo | Demo + video demo(40%) |
| 0306201559 | Trương Anh Nguyên | Demo + ảnh word(30%) |