**BỘ CÔNG THƯƠNG**

**TRƯỜNG CAO ĐẲNG KỸ THUẬT CAO THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**…..** 🙦 🕮 🙤 **…..**



**ĐỒ ÁN TỐT NGHIỆP**

***ĐỀ TÀI***

**Tìm hiểu và triển khai hệ thống**

**tường lửa PfSense**

**Gíáo viên hướng dẫn : Tô Vũ Song Phương**

**Sinh viên thực hiện :**

1. **PHẠM PHÚC BẢO 0306201515**
2. **TRƯƠNG ANH NGUYÊN 0306201559**

**LỚP: CĐTH20 MMTF**

**KHÓA : 2020 - 2023**

**TP.HỒ CHÍ MINH, ngày …tháng 06 năm 2023**

**BỘ CÔNG THƯƠNG**

**TRƯỜNG CAO ĐẲNG KỸ THUẬT CAO THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**….. 🙦 🕮 🙤 …..**



**ĐỒ ÁN TỐT NGHIỆP**

***ĐỀ TÀI***

**Tìm hiểu và triển khai hệ thống**

**tường lửa PfSense**

**Gíáo viên hướng dẫn : Tô Vũ Song Phương**

**Sinh viên thực hiện :**

1. **PHẠM PHÚC BẢO 0306201515**
2. **TRƯƠNG ANH NGUYÊN 0306201559**

**LỚP: CĐTH20MMTF**

**KHÓA : 2020 - 2023**

**TP.HỒ CHÍ MINH, ngày …tháng 06 năm 2023**

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

………………………………………………………………………………………

**TP. Hồ Chí Minh, ngày … tháng … năm 2023**

**Giáo viên hướng dẫn ký tên**

**NHẬN XÉT CỦA GIÁO VIÊN PHẢN BIỆN**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

………………………………………………………………………………………

**TP. Hồ Chí Minh, ngày … tháng … năm 2023**

**Giáo viên nhận xét ký tên**

**NHẬN XÉT CỦA HỘI ĐỒNG**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

………………………………………………………………………………………

**TP. Hồ Chí Minh, ngày … tháng … năm 2023**

**Giáo viên nhận xét ký tên**

**MỤC LỤC**

[DANH MỤC KÝ TỰ VIẾT TẮT I](#_Toc139556935)

[DANH MỤC BẢNG II](#_Toc139556936)

[MỤC LỤC HÌNH ẢNH III](#_Toc139556937)

[LỜI CẢM ƠN VI](#_Toc139556938)

[LỜI MỞ ĐẦU VII](#_Toc139556939)

[CHƯƠNG 1: GIỚI THIỆU ĐỀ TÀI 1](#_Toc139556940)

[1.1. Lý do chọn đề tài 1](#_Toc139556941)

[1.2. Giới thiệu đề tài 1](#_Toc139556942)

[1.2.1. Đối tượng 1](#_Toc139556943)

[1.2.2. Mục đích 1](#_Toc139556944)

[1.2.3. Sơ lược về PfSense 2](#_Toc139556945)

[1.3. Cấu trúc đồ án 3](#_Toc139556946)

[CHƯƠNG 2: TÌM HIỂU VỀ PFSENSE 5](#_Toc139556947)

[2.1. Tổng quan về PfSense 5](#_Toc139556948)

[2.1.1. Khái niệm 5](#_Toc139556949)

[2.1.2. Một số chức năng chính 5](#_Toc139556950)

[2.1.3. Một số dịch vụ của pfSense 9](#_Toc139556951)

[2.1.4. Một số chức năng khác 10](#_Toc139556952)

[2.1.5. Một số hạn chế của pfSense 10](#_Toc139556953)

[2.2. Firewall redundancy/ High Availability 11](#_Toc139556954)

[2.2.1. Cơ chế cân bằng tải 11](#_Toc139556955)

[2.2.2. Common Address Redundancy Protocol (CARP) 11](#_Toc139556956)

[2.2.3. Điều kiện để thực hiện Firewall redundancy/ high availability 12](#_Toc139556957)

[2.3. OpenVPN trên PfSense 13](#_Toc139556958)

[2.3.1. VPN (Virtual Private Network) 13](#_Toc139556959)

[2.3.2. Các giao thức thường dùng trong VPN 13](#_Toc139556960)

[2.3.3. Các loại VPN 14](#_Toc139556961)

[CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG 16](#_Toc139556962)

[3.1. Mô hình triển khai. 16](#_Toc139556963)

[3.1.1. Mô hình. 16](#_Toc139556964)

[3.1.2. Bảng địa chỉ ip. 16](#_Toc139556965)

[3.2. Các tính năng triển khai trong mô hình. 17](#_Toc139556966)

[3.3. Cấu hình cơ bản. 17](#_Toc139556967)

[3.3.1. Cấu hình máy pfsense. 17](#_Toc139556968)

[3.3.2. Cấu hình pfsense 21](#_Toc139556969)

[3.3.3. Gia nhập miền cho các client. 29](#_Toc139556970)

[3.4. Triển khai các chính sách. 30](#_Toc139556971)

[3.4.1. Hệ thống 2 firewall – failover đáp ứng máy trong mạng LAN luôn truy cập được Internet. 30](#_Toc139556972)

[3.4.2. Chặn truy cập Internet thông qua host IP. 37](#_Toc139556973)

[3.4.3. Chặn truy cập website thông qua network IP. (chặn truy cập website Facebook) 41](#_Toc139556974)

[3.4.4. Thiết lập thời gian quản lý (Schedule). 46](#_Toc139556975)

[3.4.5. Thiết lập giới hạn tốc độ upload và download. 49](#_Toc139556976)

[CHƯƠNG 4: KẾT LUẬN 53](#_Toc139556977)

[4.1. Đánh giá chung về Pfsense. 53](#_Toc139556978)

[4.2. Ưu điểm và nhược điểm. 53](#_Toc139556979)

[4.3. Kết luận. 54](#_Toc139556980)

[TÀI LIỆU KHAM THẢO 55](#_Toc139556981)

# DANH MỤC KÝ TỰ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Ý nghĩa** |
| 1 | SOHO | Small Office Home Office |
| 2 | IP | Internet Protocol |
| 3 | GUI | Graphical User Interface |
| 4 | NAT | Network Address Translation |
| 5 | VPN | Virtual Private Network |
| 6 | ISA | Industry Standard Architecture |
| 7 | DHCP | Dynamic Host Configuration Protocol |
| 8 | DNS | Domain Name System |
| 9 | URL | Uniform Resource Locator |
| 10 | MAC | Media Access Control |
| 11 | HTTP | Hyper Text Transfer Protocol |
| 12 | CARP | Common Address Redundancy Protocol |
| 13 | ARP | Address Resolution Protocol |
| 14 | TCP | Transmission Control Protocol -  Giao thức truyền tin cậy |
| 15 | UTP | User Datagram Protocol – Giao thức truyền không tin cậy |

# DANH MỤC BẢNG

[Bảng 3‑1: Bảng địa chỉ ip. 16](#_Toc139557421)

[Bảng 4‑1: Ưu điểm và nhược điểm. 53](#_Toc139557422)

# MỤC LỤC HÌNH ẢNH

[Hình 2‑1 : Firewall PfSense 5](#_Toc139556833)

[Hình 2‑4 : Mô hình Firewall redundancy 13](#_Toc139556834)

[Hình 3‑1: Mô hình triển khai. 16](#_Toc139556835)

[Hình 3‑2: Cấu hình card WAN máy Pfsense Master. 18](#_Toc139556836)

[Hình 3‑3: Cấu hình card LAN máy Pfsense Master. 19](#_Toc139556837)

[Hình 3‑4: Cấu hình card LAN máy Pfsense Master. 19](#_Toc139556838)

[Hình 3‑5: Cấu hình card WAN máy Pfsense Backup. 20](#_Toc139556839)

[Hình 3‑6: Cấu hình card LAN máy Pfsense Backup. 21](#_Toc139556840)

[Hình 3‑7: Giao diện đăng nhập. 21](#_Toc139556841)

[Hình 3‑8: Giới thiệu về Pfsense. 22](#_Toc139556842)

[Hình 3‑9: Các chính sách hỗ trợ. 22](#_Toc139556843)

[Hình 3‑10: Đặt hostname. 23](#_Toc139556844)

[Hình 3‑11: Chọn múi giờ. 23](#_Toc139556845)

[Hình 3‑12: Cấu hình card WAN. 24](#_Toc139556846)

[Hình 3‑13: Đặt lại mật khẩu. 24](#_Toc139556847)

[Hình 3‑14: Reload lại các thiếp lập đã cấu hình. 25](#_Toc139556848)

[Hình 3‑15: Kết thúc quá trình. 25](#_Toc139556849)

[Hình 3‑16: Giao diện hiển thị thông tin. 26](#_Toc139556850)

[Hình 3‑17: Giao diện đăng nhập. 26](#_Toc139556851)

[Hình 3‑18: Giới thiệu về Pfsense. 27](#_Toc139556852)

[Hình 3‑19: Đặt hostname. 27](#_Toc139556853)

[Hình 3‑20: Chọn múi giờ. 28](#_Toc139556854)

[Hình 3‑21: Cấu hình card WAN. 28](#_Toc139556855)

[Hình 3‑22: Đặt password. 28](#_Toc139556856)

[Hình 3‑23: Giao diện hiển thị thông tin. 29](#_Toc139556857)

[Hình 3‑24: Gia nhập Domain máy client. 30](#_Toc139556858)

[Hình 3‑25: Cấu hình High Availability Sync. 31](#_Toc139556859)

[Hình 3‑26: Cấu hình High Availability Sync. 32](#_Toc139556860)

[Hình 3‑27: Cấu hình High Availability Sync. 32](#_Toc139556861)

[Hình 3‑28: Cấu hình Virtual Ips. 33](#_Toc139556862)

[Hình 3‑29: Cấu hình Virtual Ips. 34](#_Toc139556863)

[Hình 3‑30: Cấu hình Virtual Ips. 34](#_Toc139556864)

[Hình 3‑31: Cấu hình CARP ở pfsense Master. 35](#_Toc139556865)

[Hình 3‑32: Cấu hình CARP ở pfsense Backup. 35](#_Toc139556866)

[Hình 3‑33: Địa chỉ Ip của máy DC. 36](#_Toc139556867)

[Hình 3‑34: Địa chỉ Ip của máy P1. 36](#_Toc139556868)

[Hình 3‑35: Địa chỉ Ip của máy P2. 37](#_Toc139556869)

[Hình 3‑36: Thông tin máy P1. 37](#_Toc139556870)

[Hình 3‑37: Nhập thông tin máy P1. 38](#_Toc139556871)

[Hình 3‑38: Cấu hình IP Aliases. 38](#_Toc139556872)

[Hình 3‑39: Thêm rules mới. 39](#_Toc139556873)

[Hình 3‑40: Cấu hình chặn internet. 39](#_Toc139556874)

[Hình 3‑41: Cấu hình chặn internet. 40](#_Toc139556875)

[Hình 3‑42: Trước khi áp dụng rules. 40](#_Toc139556876)

[Hình 3‑43: Sau khi áp dụng rules. 41](#_Toc139556877)

[Hình 3‑44: Thông tin của máy P2. 41](#_Toc139556878)

[Hình 3‑45: Địa chỉ ip của facebook. 42](#_Toc139556879)

[Hình 3‑46: Nhập thông tin ip của máy P2. 42](#_Toc139556880)

[Hình 3‑47 : Nhập thông tin địa chỉ Facebook. 43](#_Toc139556881)

[Hình 3‑48: Cấu hình chặn trang Facebook. 44](#_Toc139556882)

[Hình 3‑49: Cấu hình chặn trang Facebook. 44](#_Toc139556883)

[Hình 3‑50: Trước khi áp dụng rules. 45](#_Toc139556884)

[Hình 3‑51: Sau khi áp dụng rules. 45](#_Toc139556885)

[Hình 3‑52: Thiết lập thời gian quản lý. 46](#_Toc139556886)

[Hình 3‑53: Thiết lập thời gian quản lý. 46](#_Toc139556887)

[Hình 3‑54: Cấu hình thời gian quản lý. 47](#_Toc139556888)

[Hình 3‑55: Cấu hình thời gian quản lý. 48](#_Toc139556889)

[Hình 3‑56: Thời gian firewall. 48](#_Toc139556890)

[Hình 3‑57: Trong thời gian áp dụng. 49](#_Toc139556891)

[Hình 3‑58: Sau thời gian áp dụng. 49](#_Toc139556892)

[Hình 3‑59: Giới hạn Upload. 50](#_Toc139556893)

[Hình 3‑60: Giới hạn Download. 50](#_Toc139556894)

[Hình 3‑61: Cấu hình rules upload và download. 51](#_Toc139556895)

[Hình 3‑62: Cấu hình rules upload và download. 51](#_Toc139556896)

[Hình 3‑63: Trước khi giới hạn băng thông. 52](#_Toc139556897)

[Hình 3‑64: Sau khi giới hạn băng thông. 52](#_Toc139556898)

# **LỜI CẢM ƠN**

Trong suốt quá trình học tập ở Trường Cao Đẳng Kỹ Thuật Cao Thắng, chúng em đã nhận được rất nhiều sự quan tâm, tận tình, giúp đỡ của quý Thầy Cô và bạn bè. Chúng em xin gửi lòng biết ơn chân thành nhất đến quý Thầy Cô ở Khoa Công Nghệ Thông Tin – Trường Cao Đẳng Kỹ Thuật Cao Thắng. Chúng em cũng xin cảm ơn gia đình, bạn bè và tập thể lớp CĐTH20 MMTF đã giúp đỡ chúng em trong thời gian qua.

Chúng em xin cảm ơn đến trường Cao Đẳng Kỹ Thuật Cao Thắng và Khoa Công Nghệ Thông Tin đã tạo điều kiện cho nhóm chúng em hoàn thành tốt đồ án tốt nghiệp. Đặc biệt chúng em vô cùng biết ơn  thầy Tô Vũ Song Phương đã tận tình hướng dẫn nhóm chúng em trong thời gian thực hiện đề tài của đồ án tốt nghiệp, thông qua những buổi nói chuyện, thảo luận, những nhận xét và góp ý của thầy.

Mặc dù chúng em đã cố gắng hoàn thành tốt đề tài của đồ án tốt nghiệp với tất cả nổ lực của bản thân, nhưng do kiến thức, hiểu biết và kinh nghiệm còn hạn chế, chắc chắn sẽ không tránh khỏi những thiếu sót nhất định, nhóm chúng em rất mong nhận được sự cảm thông, chia sẻ và tận tình góp ý, đóng góp của quý Thầy Cô để chúng em rút ra được những kinh nghiệm, kiến thức quý báu từ đề tài của đồ án tốt nghiệp, để chúng em hoàn thiện bản thân và hoàn thành tốt hơn cho các dự án tương lai sau này.

Chúng em xin chân thành cảm ơn.

# LỜI MỞ ĐẦU

Ngày nay, Internet đã trở thành một nguồn tài nguyên cô cùng quan trọng và không thể thiếu trong cuộc sống của chúng ta. Nó mang lại nhiều lợi ích to lớn, mở ra một cửa sổ thông tin vô tận và tạo điều kiện thuận lợi cho giao tiếp và trao đổi thông tin trên mạng. Tuy nhiên, cùng với sự phát triển của Internet, ngày càng xuất hiện nhiều mối đe dọa và rủi ro phức tạp, nguy hiểm hơn.

Mạng Internet không chỉ là một nguồn thông tin vô tận mà còn là một môi trường tiềm ẩn những mối nguy hiểm đối với các thiết bị và hệ thống mạng. Kẻ xấu luôn tìm cách tấn công và xâm nhập vào các thiết bị, hệ thống mạng thông qua các phương thức lây nhiễm virus, sâu mạng, trojan, phần mền nghe lén, tấn công từ chối dịch vụ và nhiều hình thức khác.

Để đảm bảo an ninh và bảo mật cho các thiết bị và hệ thống mạng hoạt động ổn định, chúng ta cần đảm bảo rằng chúng luôn được bảo vệ khỏi những nguy cơ và mối đe dọa đến sự an toàn của toàn bộ hệ thống. Đây là lúc tường lửa (firewall) trở nên cực kỳ quan trọng.

Tường lửa, hay còn gọi là hệ thống tường lửa, là một công cụ bảo mật được tích hợp vào hệ thống mạng như một rào cản hoặc lá chắn. Nhiệm vụ chính của tường lửa là bảo vệ hệ thống mạng bên trong bằng cách ngăn chặn truy cập trái phép, giới hạn và kiểm soát lưu lượng mạng, và phát hiện các hoạt động xâm nhập không mong muốn từ bên ngoài. Đồng thời, tường lửa cũng giúp bảo vệ tính toàn vẹn và bảo mật của dữ liệu nội bộ.

Mục đích cuối cùng là cung cấp kết nối có kiểm soát an toàn giữa các vùng với độ tin cậy khác nhau thông qua việc áp dụng một chính sách an ninh và mô hình kết nối dựa trên nguyên tắc các quyền tối thiểu và các chức năng cơ bản trên tường lửa cần thiết cho một hệ thống mạng hoạt động.

# GIỚI THIỆU ĐỀ TÀI

## Lý do chọn đề tài

Ngày nay, máy tính và mạng máy tính đã được phổ biến rộng rãi, các tổ chức, cá nhân đều có nhu cầu sử dụng máy tính và mạng máy tính để tính toán, lưu trữ, quảng bá thông tin hay sử dụng các giao dịch trực tuyến trên mạng. Nhưng đồng thời với những cơ hội được mở ra lại có những nguy cơ khi mạng máy tính không được quản lý sẽ dễ dàng bị tấn công, gây hậu quả nghiêm trọng.

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 như ISA,...

Tuy nhiên những thành phần kể trên tương đối tốn kém. Vì vậy đối với người dùng không muốn tốn tiền nhưng lại muốn có một tường lửa bảo vệ hệ thống mạng bên trong (mạng nội bộ) khi mà chúng ta giao tiếp với hệ thống mạng bên ngoài (Internet) thì PFSENSE là một giải pháp tiết kiệm và hiệu quả tương đối tốt nhất đối với người dùng.

## Giới thiệu đề tài

### **Đối tượng**

PfSense là một ứng dụng có chức năng định tuyến, tường lửa và miễn phí, được sử dụng để bảo vệ các mạng có tất cả kích thước, từ mạng gia đình đến các mạng lớn của các công ty hay doanh nghiệp.

### **Mục đích**

Ứng dụng mã nguồn mở miễn phí, cho phép mở rộng hệ thống mạng dễ dàng

Khả năng định tuyến vào tường lửa chặn quảng cáo, chặn các Website, và ưu tiên Website nào cần thiết

Kết nối VPN nhanh và ít băng thông đảm bảo được tính bảo mật IPSec và VPN.

Chuẩn đoán mạng bên trong như packet sniffer cải thiện sự cố và khắc phục hiệu quả.

PfSense không cần phần mạnh về phần cứng hoạt động như thiết bị mạng tổng hợp đầy đủ các tính năng  NAT, Forward, IPSec, VPN, … và sẵn sàng bất cứ lúc nào.

Cấm hoặc cho phép các truy cập từ bên ngoài hoặc bên trong nội bộ

Cấm được truy cập theo thời gian như lập lịch cấm vào thời gian buổi sáng và cho phép truy cập vào thời gian buổi tối. Có thể xây dựng cấm chat/ xem phim sử dụng các ứng dụng cho phép.

Cho phép truy cập máy chủ nội bộ từ internet, thông qua cơ chế đó các doanh nghiệp có thể đưa các dịch vụ muốn sử dụng như Web, chia sẻ file ra bên ngoài đối tác hoặc nhà cung cấp. Giải quyết các nhu cầu phổ biến đơn giản cho người dùng.

Người dùng có thể dùng tài khoản riêng lẻ truy cập vào Wireless riêng dành cho user, chức năng này tối ưu cho các doanh nghiệp muốn khách hàng của họ có một mạng wireless riêng để truy cập đến Công Ty. Giới hạn được băng thông điều này không làm ảnh hưởng đến công việc của người khác.

Kết nối mạng nội bộ từ các vùng khác nhau, nhiều doanh nghiệp có nhiều chi nhánh việc thiết lập VPN cho các chi nhánh khác nhau chi phi sẽ cao và khó kiểm soát. Sử dụng pfSense các doanh nghiệp có thể kết nối mạng cục bộ các chi nhánh với nhau dễ dàng và tin cậy.

### **Sơ lược về PfSense**

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 địa chỉ 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.

## Cấu trúc đồ án

Chương 1: Giới thiệu đề tài

* Giới thiệu tổng quan về vấn đề nghiên cứu và lý do chọn đề tài.
* Đối tượng và mục đích của đề tài.
* Trình bày cấu trúc của đồ án.

Chương 2: Tìm hiểu về PfSense

* Giới thiệu tổng quan các khái niệm và các tính năng có trên PfSense.

Chương 3: Triển khai hệ thống

* Mô hình hệ thống.
* Các bước cài đặt pfSense.
* Triển khai tính năng.

Chương 4: Kết luận

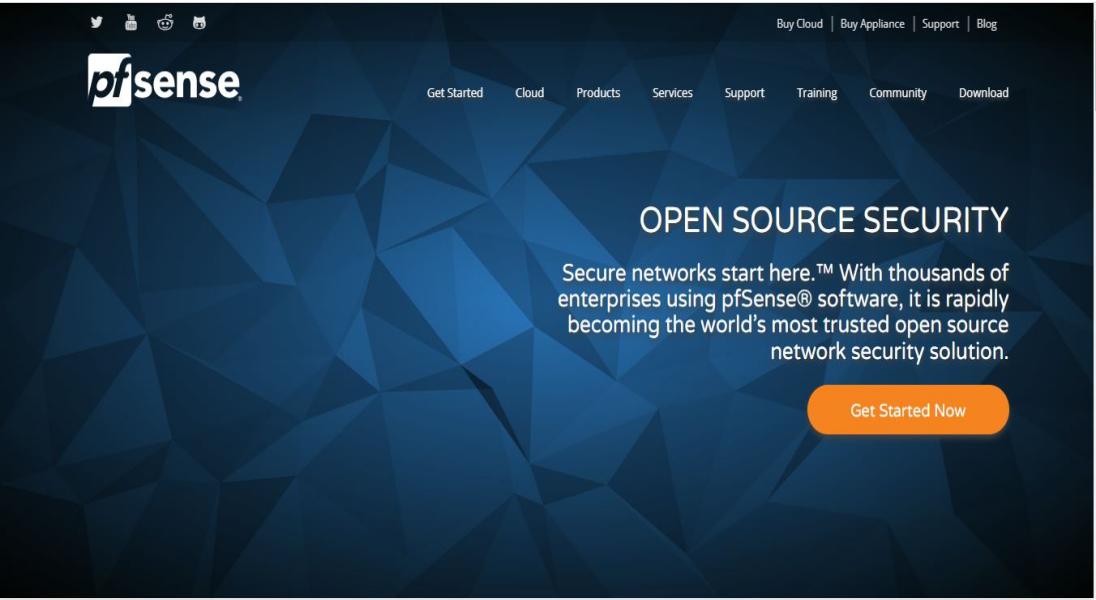
* Tổng kết lại những kết quả đã đạt được và chưa được trong quá trình thực hiện sau đó đề ra hướng phát triển cho tương lai.

# TÌM HIỂU VỀ PFSENSE

## Tổng quan về PfSense

### **Khái niệm**

PfSense là tường lửa cung cấp các giải pháp an ninh mạng cho doanh nghiệp, lớn và các giải pháp SOHO và giúp bảo vệ hệ thống dễ dàng. PfSense có tính năng giống như trên tường lửa hoặc router hỗ trợ định tuyến, NAT và chuyển tiếp, WAN, cân bằng tải.



Hình 2‑1 : Firewall PfSense

### **Một số chức năng chính**

**Aliases**

Với tính năng này chúng ta có thể gom nhóm các ports, host hoặc Network(s) khác nhau và đặt cho chúng một cái tên chung để thiết lập những quy tắc được dễ dàng và nhanh chóng hơn.

Các thành phần trong Aliases:

* Host: Tạo các nhóm địa chỉ IP.
* Network: Tạo các nhóm mạng.
* Port: cho phép gom nhóm các port nhưng không cho phép tạo nhóm các protocol. Các protocol được sử dụng trong các rules.

**Rules**

Nơi lưu các rules (luật) của firewall.

Mặc định PfSense cho phép mọi lưu thông ra/vào hệ thống. Bạn phải tạo các rules để quản lý mạng bên trong firewall.

Một số lựa chọn trong Destination và Source.

* Any: Tất cả.
* Single host or alias: Một địa chỉ ip hoặc là một bí danh.
* Lan subnet: Đường mạng Lan.
* Network: Địa chỉ mạng.
* Lan address: Tất cả địa chỉ mạng nội bộ.
* Wan address: Tất cả địa chỉ mạng bên ngoài.
* PPTP clients: Các clients thực hiện kết nối VPN sử dụng giao thức PPT.
* PPPoE clients: Các clients thực hiện kết nối VPN sử dụng giao thức PPPoE.

**NAT**

Trong firewall bạn 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 mặt định của NAT cho các kết nối outbound là Automatic outbound NAT,...tuy nhiên bạn có thể thay đổi kiểu Manual outbound NAT nếu cần.

**Virtual IPs**

PfSense cho phép sử dụng nhiều địa chỉ IP công cộng kết hợp với cơ chế NAT thông qua IP ảo. Có ba loại IP ảo có sẵn trên pfSense: Proxy ARP, CARP và một loại khác. Mỗi loại đều rất hữu ích trong các tình huống khác nhau. Trong hầu hết các trường hợp, pfSense sẽ cũng cấp ARP trên IPs, do đó cần phải sử dụng Proxy ARP hoặc CARP. Trong tình huống mà ARP không cần thiết, chẳng hạn như khi các IP công cộng bổ sung được định tuyến bởi nhà cung cấp dịch vụ mạng, sẽ sử dụng IP ảo loại khác nhau.

Virtual IP được sử dụng để cho phép pfSense đúng cách chuyển tiếp lưu lượng cho những việc như chuyển tiếp cổng NAT, NAT Outbound và NAT 1:1. Họ cũng cho phép các tính năng như failover, và có thể cho phép dịch vụ trên router để gắn kết nối với địa chỉ IP khác nhau.

**Traffic shaper**

Traffic shaper giúp bạn theo dõi và quản lí băng thông mạng dễ dàng và hiệu quả hơn.

Traffic shaper 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 một 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.

**Server Load Balancing**

Với chức năng này bạn có thể điều phối mạng hay còn gọi là cân bằng tải.

Có 2 loại load balancing trên pfSense:

* Gateway load balancing: được dùng khi có nhiều kết nối WAN. Client bên trong LAN khi muốn kết nối ra ngoài Internet thì pfSense lựa chọn card WAN để chuyển packet ra card đó giúp cho việc cân bằng tải cho đường truyền.
* Server load balancing: cho phép cân bằng tải cho các server của mình. Được dùng phổ biến cho các web server, mail server và server không hoạt động nữa thì sẽ bị xóa.

**Captive Portal**

Captive portal cho phép admin có thể chuyển hướng client tới một trang web khác, từ trang web này client có thể phải chứng thực trước khi kết nối tới internet

Captive portal: các chức năng của Captive Portal

* Enable captive portal: Đánh dấu chọn nếu muốn sử dụng captive portal.
* Maximum concurrent connections: Giới hạn các connection trên mỗi ip/user/mac.
* Idle timeout: Nếu mỗi ip không còn truy cập mạng trong 1 thời gian xác định thì sẽ ngắt kết nối của ip/user/mac.
* Hard timeout: Giới hạn thời gian kết nối của mỗi ip/users/mac.
* Logout popup windows: Xuất hiện 1 popup thông báo cho ip / user / mac.
* Redirect URL: Địa chỉ URL mà người dùng sẽ được direct tới sau khi đăng nhập
* Pass-through MAC: Các MAC address được cấu hình trong mục này sẽ được bỏ qua không authentication.
* Allowed IP address: Các IP address được cấu hình sẽ không authentication
* Users: Tạo local user để dùng kiểu authentication: local user
* File Manager: Upload trang quản lý của Captive portal lên pfSense.

Có 3 kiểu chứng thực client:

* No authentication: pfSense sẽ điều hướng người dùng tới 1 trang nhất định mà không chứng thực.
* Local user manager: pfSense hỗ trợ tạo user để chứng thực.
* Radius authentication: Chứng thực bằng radius server (Cần chỉ ra địa chỉ IP của radius, port, …)

### **Một số dịch vụ của pfSense**

**DHCP Server**

Dịch vụ này cho phép pfSense cấp địa chỉ IP và các thông tin cấu hình cho client trong mạng LAN.

**DHCP Relay**

Dịch vụ này cho phép pfSense forward yêu cầu cấp IP của client nằm trong một subnet nào đó tới một DHCP server cho trước.

Chỉ được phép chạy một trong hai dịch vụ DHCP server và DHCP relay.

**Dynamic DNS**

PfSense cho phép đăng ký địa chỉ IP của WAN interface của nhiều nhà cung cấp DNS động. Nó rất hữu ích khi muốn điều khiển từ xa.

**SNMP (Simple Network Management Protocol)**

Chức năng SNMP của pfSense sẽ cho phép giám sát từ xa các thông số hệ thống pfSense. Tùy thuộc vào các tùy chọn cho phép mà có thể theo dõi như: lưu lượng mạng, hàng đợi, thông tin chung hệ thống (CPU, bộ nhớ,...).

**PPPoE Server**

PfSense có thể hoạt động như một máy chủ PPPoE, chấp nhận hoặc xác thực kết nối từ client PPPoE trên interface cục bộ. Nó được dùng để bắt buộc người dùng xác thực trước khi được quyền truy cập mạng hoặc kiểm soát hoạt động đăng nhập của họ.

### **Một số chức năng khác**

**System log**: theo dõi hoạt động của hệ thống pfSense và các dịch vụ mà pfSense cung cấp. Mọi hoạt động của hệ thống và dịch vụ đều được ghi lại.

**System Status:** Liệt kê các thông tin và tình trạng của hệ thống.

**Service Status:** Hiển thị trạng thái của tất cả các service có trong hệ thống. Mỗi service có hai trạng thái là: running, stopped.

**Interface Status:** Hiển thị thông tin của tất cả card mạng.

**RRD Graph:** Hiển thị các thông tin dưới dạng đồ thị. Các thông tin mà RRD Graph sẽ thể hiện là: System, Traffic, Packet, Quality, Queues.

Pfsense khá linh hoạt với các hệ thống khác để hỗ trợ tốt hơn cho việc vận hành của pfSense như: kết hợp chứng thực người dùng thông qua hệ thống RADIUS…

### **Một số hạn chế của pfSense**

Thiếu tính năng tối ưu hóa mạng WAN của hệ thống mặc dù nó cung cấp tính năng Tối ưu hóa WAN, nhưng không thể tải chương trình của mình trên "máy ảo" vì kết nối mạng yêu cầu địa chỉ IP trực tiếp.

Nếu có nhiều thiết bị đầu cuối hỗ trợ Tối ưu hóa WAN được kết nối với cùng một tường lửa, chúng sẽ gây nhiễu cho nhau. Tính năng tối ưu hóa WAN bị vô hiệu hóa, các ứng dụng Internet của như e-mail, trò chuyện và các hoạt động sử dụng nhiều băng thông khác sẽ bị ảnh hưởng tiêu cực.

## Firewall redundancy/ High Availability

### **Cơ chế cân bằng tải**

Firewall redundancy cung cấp cơ chế dự phòng trong hạ tầng mạng, đảm bảo các host luôn truy cập được đến các server quan trọng trong mạng hoặc Internet ở bất cứ thời điểm nào. Hầu hết các hạ tầng mạng doanh nghiệp hiện nay đều được triển khai tính năng đó.

Đảm bảo hệ thống luôn hoạt động ổn định khi thiết lập cần tối thiểu một cặp máy chạy song song với nhau. Khi có sự cố 1 trong 2 cặp máy bị down máy còn lại vẫn còn hoạt động tự động luồng dữ liệu sẽ chạy qua bên máy thứ 2 đảm bảo hệ thống luôn hoạt động xuyên suốt không gián đoạn.

Khi thiết kế cấu trúc liên kết mạng, cần tính khả năng xảy ra sự cố và nên thiết kế dự phòng ở những nơi cần thiết:

* Dự phòng các tuyến từ Workstation đến router ở lớp building access.
* Máy chủ dự phòng trong các server farm module.
* Tuyến đường dự phòng bên trong và giữa các thành phần mạng.
* Liên kết phương tiện truyền thông dự phòng ở lớp truy cập.

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).

### **Common Address Redundancy Protocol (CARP)**

CARP là một failover và dự phòng tự động, được thiết kế để chia sẻ một địa chỉ IP phổ biến nhiều trong host. Cung cấp khả năng dự phòng đến nhiều máy chủ, đây là một thay thế cho các giao thức Internet Engineering Task Force(IETF) , Virtual Router Redundancy Protocol (VRRP) và Host Standby Redundancy Protocol (HSRP) của Cisco.

**Hoạt động của CARP :**

* Cho phép một nhóm các host trên cùng 1 mạng chia sẻ 1 địa chỉ IP.
* Phổ biến một ID máy chủ ảo.
* Cho phép các thành viên trong nhóm để xác định khả năng dự phòng.

CARP được sử dụng bởi các node để chia sẻ IP ảo giữa nhiều nút với nhau khi 1 node bị fail ( nghĩa là không hoạt động được ) thì IP ảo đó vẫn hoạt động bởi các node khác.

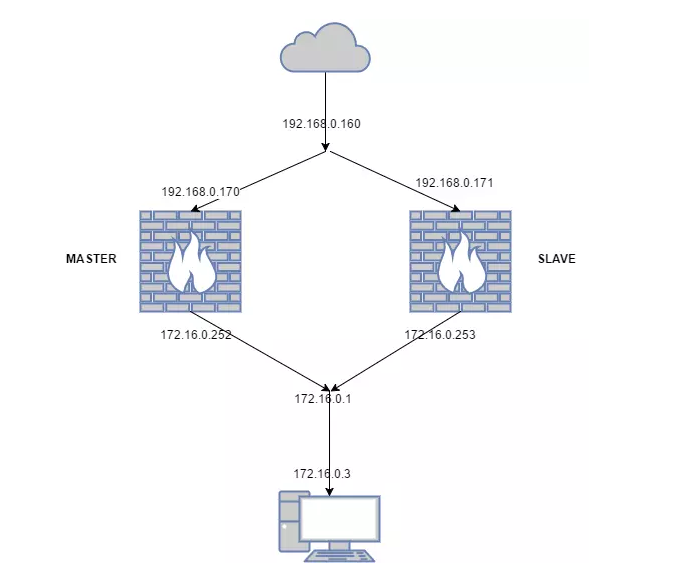
### **Điều kiện để thực hiện Firewall redundancy/ high availability**

Tối thiểu 3 IP mỗi subnet trên một Pfesense:

* 1 IP cho Master.
* 1 IP cho Slave ( máy dự phòng Backup ).
* Và một Virtual IP dùng để giao tiếp với các thiết bị khác.

Các thiết bị ở tầng Layer2 phải cho phép tính năng multicast.

Upstream/ISP các routers có liên quan có khả năng gọi được các Virtual IP.



Hình 2‑4 : Mô hình Firewall redundancy

## OpenVPN trên PfSense

### **VPN (Virtual Private Network)**

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

### **Các giao thức thường dùng trong VPN**

Hầu hết các VPN đều dựa trên Tunneling để hình thành mạng riêng ảo trên internet.

Tunneling (kỹ thuật truyền dữ liệu qua nhiều mạng có giao thức khác nhau).

Chức năng cơ bản của VPN là phân phối các gói (packet) từ điểm này đến điểm khác mà không để lộ chúng cho bất kỳ ai trên đường truyền. Để làm điều này, VPN đóng gói tất cả dữ liệu theo định dạng mà cả máy khách và máy chủ đều hiểu được. Bên gửi dữ liệu đặt nó vào định dạng tunneling và bên nhận trích xuất để có được thông tin.

Mã hóa: Tunneling không cung cấp tính năng bảo vệ. Bất cứ ai cũng có thể trích xuất dữ liệu. Dữ liệu cũng cần phải được mã hóa trên đường truyền. Bên nhận sẽ biết cách giải mã dữ liệu từ một người gửi nhất định.

Xác thực: Để bảo mật, VPN phải xác nhận danh tính của bất kỳ client nào cố gắng “giao tiếp” với nó. Client cần xác nhận rằng nó đã đến đúng máy chủ dự định.

Quản lý phiên: Một khi người dùng được xác thực, VPN cần duy trì phiên để client có thể tiếp tục “giao tiếp” với nó trong một khoảng thời gian.

### **Các loại VPN**

VPN Site to Site: Site to Site VPN còn có tên gọi khác là Router to Router VPN. Nó thường được dùng trong các công ty và tổ chức đoàn thể. Ngày nay, nhiều công ty có văn phòng đặt ở cả trong và ngoài nước; do đó, họ dùng mạng Site to Site VPN để kết nối mạng lưới của văn phòng chính với các văn phòng.

 PPTP VPN: PPTP là từ viết tắt của Point-to-Point Tunneling Protocol (giao thức tạo đường hầm điểm nối điểm). Giống như tên gọi của mình, mạng riêng ảo PPTP tạo một đường hầm cho dữ liệu đi qua. Quả là một cái tên khá dài cho mạng VPN được sử dụng nhiều nhất

 L2TP VPN: L2TP, Layer 2 Tunneling Protocol (giao thức đường hầm lớp 2), là mạng riêng ảo được phát triển bởi Microsoft và Cisco. L2TP là mạng VPN thường được kết hợp với một giao thức VPN khác để thiết lập một kết nối an toàn hơn. Mạng L2TP hình thành một đường hầm giữa 2 điểm kết nối L2TP, đồng thời một mạng VPN khác.

 IPSec: IPSec là từ viết tắt của thuật ngữ Internet Protocol Security (Giao thức bảo mật Internet). IPSec là một giao thức VPN được dùng để đảm bảo an toàn cho việc truyền dữ liệu qua mạng IP. Một đường hầm thiết lập từ xa cho phép người dùng truy cập đến vị trí trung tâm

 SSL TLS: SSL là từ viết tắt của Secure Socket Layer (Tẩng ổ bảo mật), và TLS là từ viết tắt của Transport Layer Security (Bảo mật lớp vận chuyển). Cả 2 được kết hợp lại thành một giao thức dùng để xây dựng kết nối VPN. Đây là một mạng VPN trong đó trình duyệt web đóng vai trò máy khách và người dùng chỉ được truy cập một số ứng dụng nhất định, thay vì toàn bộ mạng lưới.

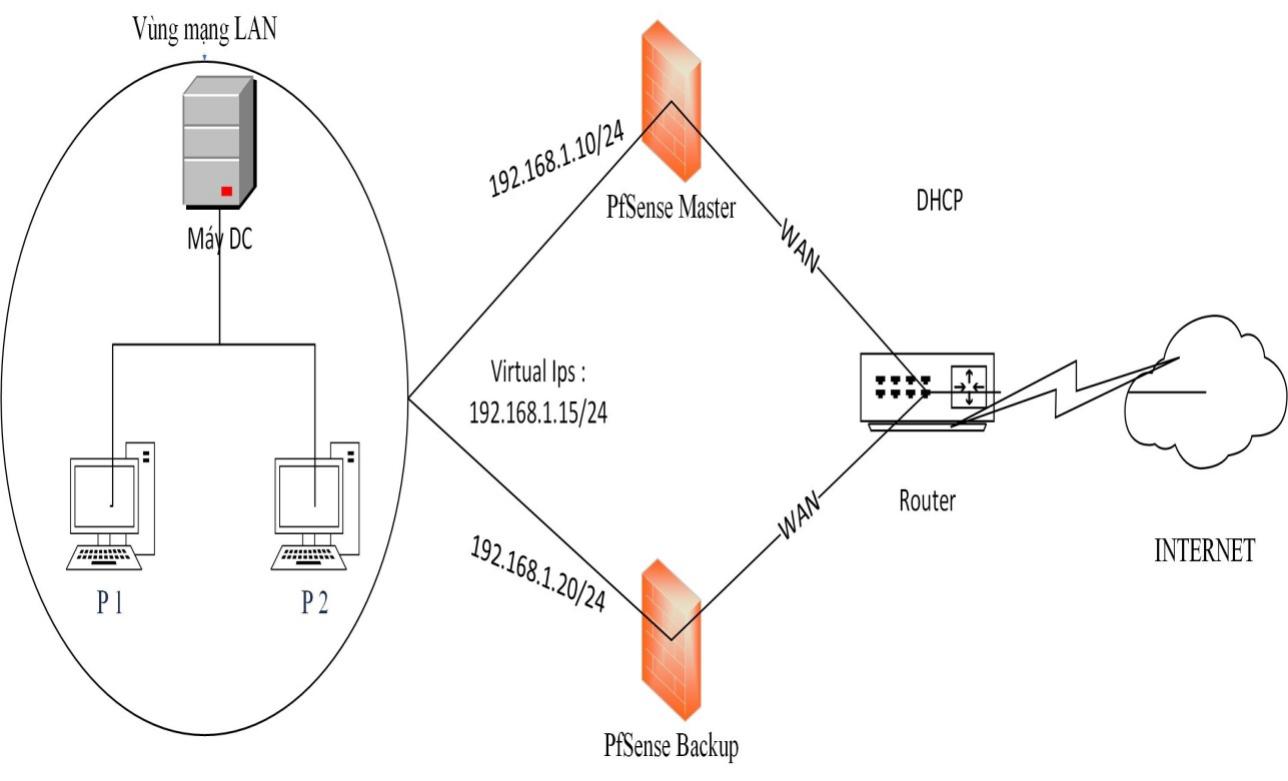
 MPLS VPN: Chuyển mạch nhãn đa giao thức (MPLS) là một công nghệ được dùng nhiều nhất cho kết nối Site to Site. Nguyên nhân là vì MPLS là lựa chọn có tính linh hoạt và khả năng thích nghi cao nhất. MPLS là một nguồn dựa trên các tiêu chuẩn được dùng để tăng tốc độ phân chia các gói mạng lưới thông qua nhiều giao thức khác nhau.

 Hypird VPN: VPN lai là sự kết hợp giữa MPLS VPN và IPSec VPN. Dù 2 loại mạng riêng ảo này thường được sử dụng cho các mục đích khác nhau, nhưng chúng ta vẫn có thể kết hợp chúng lại với nhau. Mục đích là dùng IPSec VPN làm phương án dự phòng cho MPLS.

# TRIỂN KHAI HỆ THỐNG

## Mô hình triển khai.

### **Mô hình**.



Hình 3‑1: Mô hình triển khai.

### **Bảng địa chỉ ip**.

Bảng 3‑1: Bảng địa chỉ ip.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tên máy | Card mạng | Địa chỉ IP | Default gateway | DNS |
| pfSense Master | VMnet0 (WAN) | DHCP | | |
| VMnet1 (LAN) | 192.168.1.10/24 |  |  |
| pfSense Backup | VMnet0 (WAN) | DHCP | | |
| VMnet1 (LAN) | 192.168.1.20/24 |  |  |
| Domain  Controller | VMnet1 (LAN) | 192.168.1.2/24 | 192.168.1.15 | 8.8.8.8 |
| P1 | VMnet1 (LAN) | 192.168.1.40/24 |  | 192.168.1.2 |
| P2 | VMnet1 (LAN) | 192.168.1.60/24 |  | 192.168.1.2 |
|  | Virtual Ips: 192.168.1.15 | | | |

## Các tính năng triển khai trong mô hình.

* Hệ thống 2 firewall – failover đáp ứng máy trong mạng LAN luôn truy cập được internet.
* Chặn truy cập internet thông qua host IP.
* Chặn truy cập website thông qua network IP (chặn truy cập website facebook).
* Thiết lập thời gian quản lý.
* Thiết lập giới hạn tốc độ upload và download.

## Cấu hình cơ bản.

### **Cấu hình máy pfsense.**

* **Cấu hình trên máy pfsense master.**
* Cấu hình card mạng WAN nhận địa chỉ DHCP:

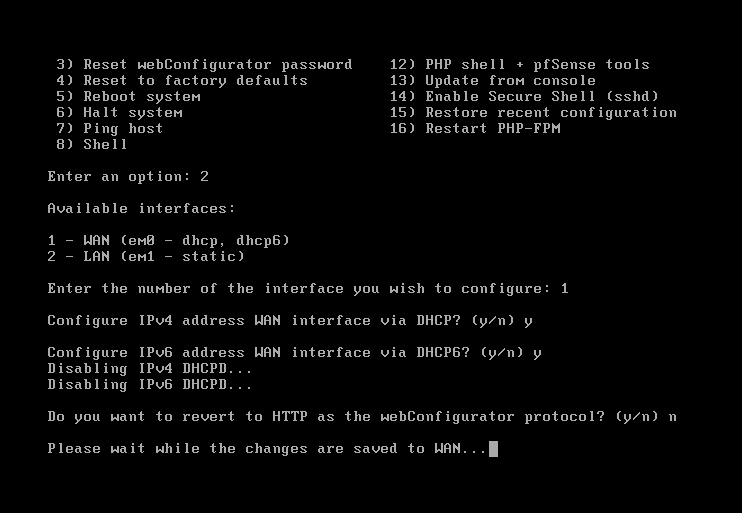
Nhấn số **2** để chọn vào mục ***Set interface(s) IP address***.

Sau đó ***Enter the number of the interface you wish to configure:*** ta chọn số **1**.

Ở phần ***Configure Ipv4 address WAN interface via DHCP ? (y/n)***: ta chọn **y**.

***Configure Ipv6 address WAN interface via DHCP6 ? (y/n)***: ta chọn **y.**

***Do you want to revert to HTTP as the webConfigurator protocol? (y/n)***: ta chọn **n.**

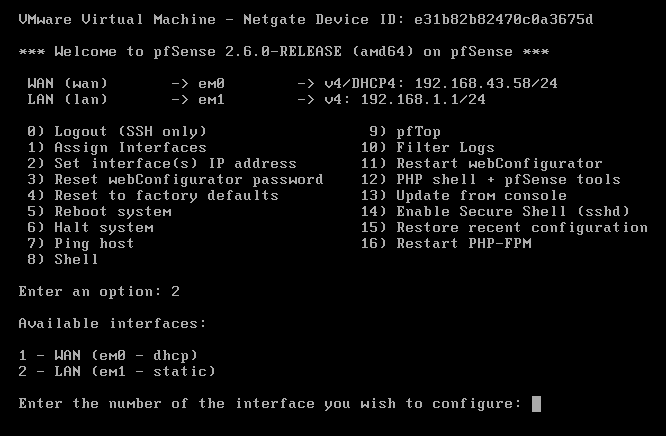


Hình 3‑2: Cấu hình card WAN máy Pfsense Master.

* Cấu hình card mạng LAN:

Ở dòng Enter an option ta chọn 2 để vào Set interface(s) IP address.

Sau đó chọn 2 để đặt IP cho card LAN.



Hình 3‑3: Cấu hình card LAN máy Pfsense Master.

**Enter the new LAN IPv4 address. Press <Enter> for none:**

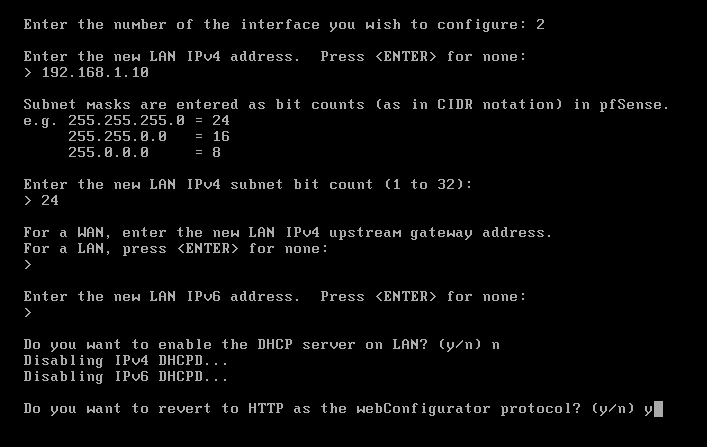
> 192.168.1.10

**Enter the new LAN IPv4 subnet bit count (1 to 32):**

> 24

Nhấn Enter khi đến dòng **Do you want to enable the DHCP server on LAN? (y/n)** ta chọn **n.**

Ở dòng **Do you want to revert to HTTP as the web Configurator protocol? (y/n):** ta chọn **y**.



Hình 3‑4: Cấu hình card LAN máy Pfsense Master.

* **Cấu hình trên máy pfsense backup.** (tương tự như trên máy pfsense master)
* Cấu hình card mạng WAN nhận địa chỉ DHCP.

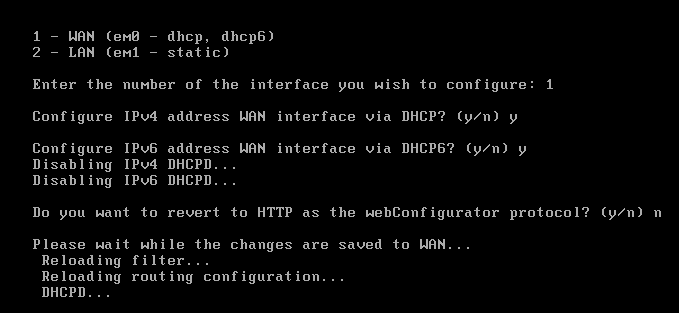
Enter an option : 2.

Enter the number of the interface you wish to configure : 1.

Configure Ipv4 address WAN interface via DHCP ? (y/n) : y.

Configure Ipv6 address WAN interface via DHCP6 ? (y/n) : y.

Do you want to revert to HTTP as the webConfigurator protocol? (y/n): n.



Hình 3‑5: Cấu hình card WAN máy Pfsense Backup.

Enter an option : 2.

Enter the number of the interface you wish to configure : 1.

Enter the new LAN IPv4 address. Press <Enter> for none:

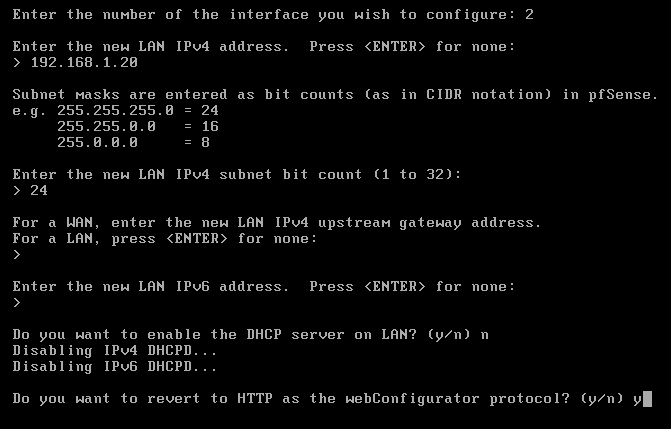
> 192.168.1.20

Enter the new LAN IPv4 subnet bit count (1 to 32):

> 24

Do you want to enable the DHCP server on LAN? (y/n): n.

Do you want to revert to HTTP as the web Configurator protocol? (y/n): y.

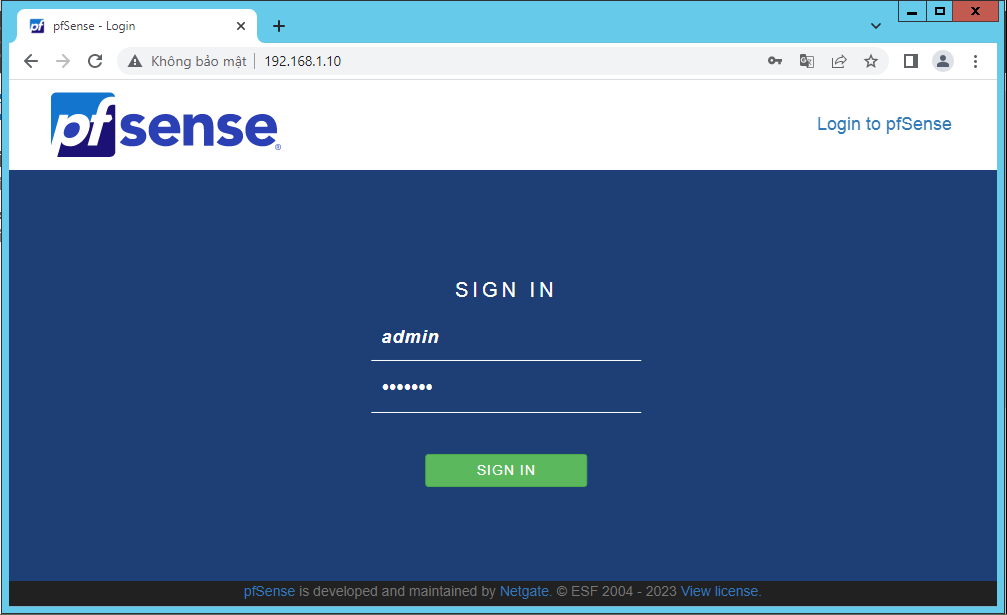


Hình 3‑6: Cấu hình card LAN máy Pfsense Backup.

### **Cấu hình pfsense**

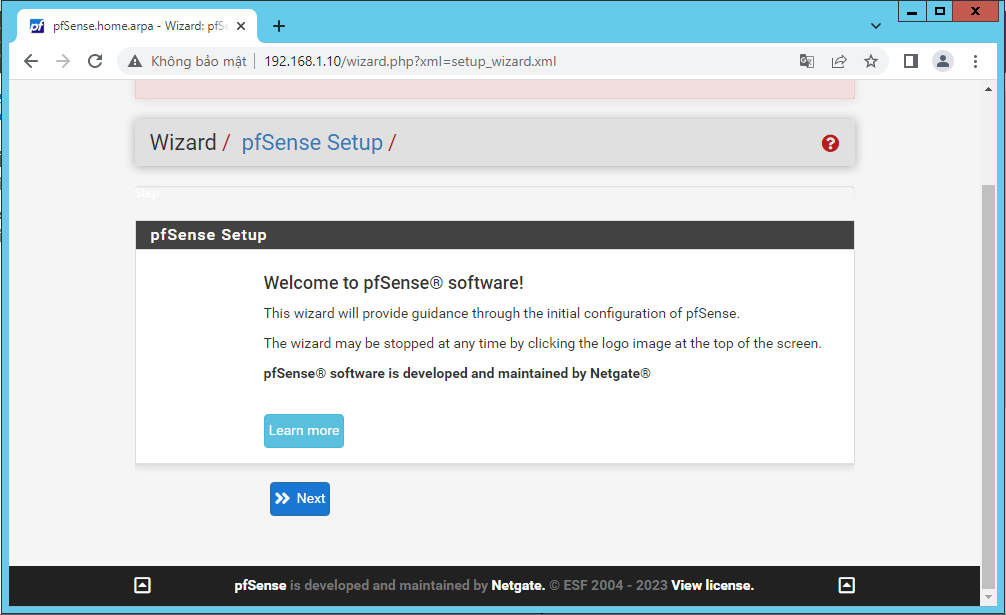
**Pfsense Master.**

Đăng nhập vào pfsense Master trên máy DC với thông tin tài khoản là **admin/pfsense**.

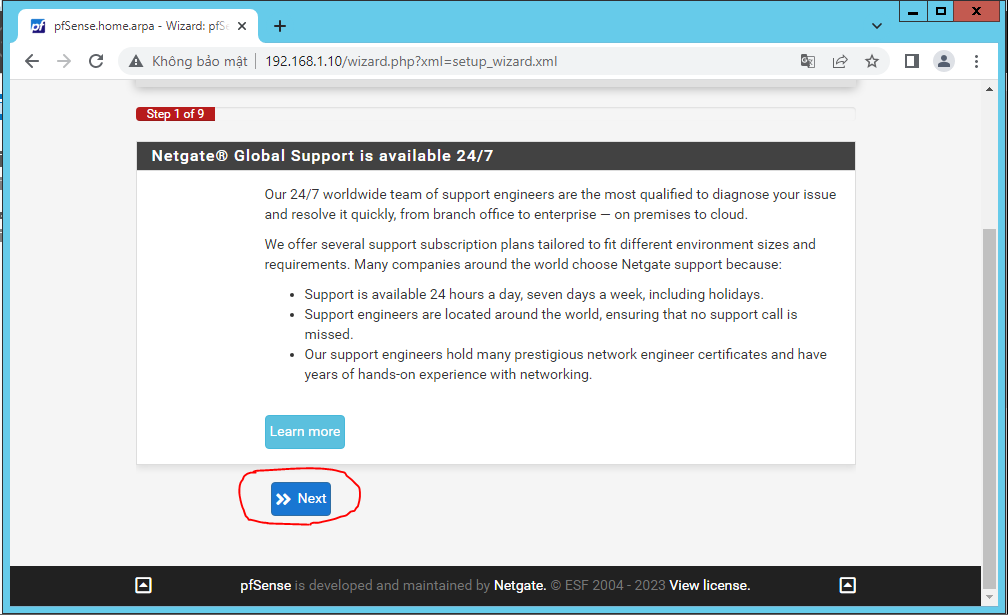


Hình 3‑7: Giao diện đăng nhập.

Sau đó nhấn **Next**.

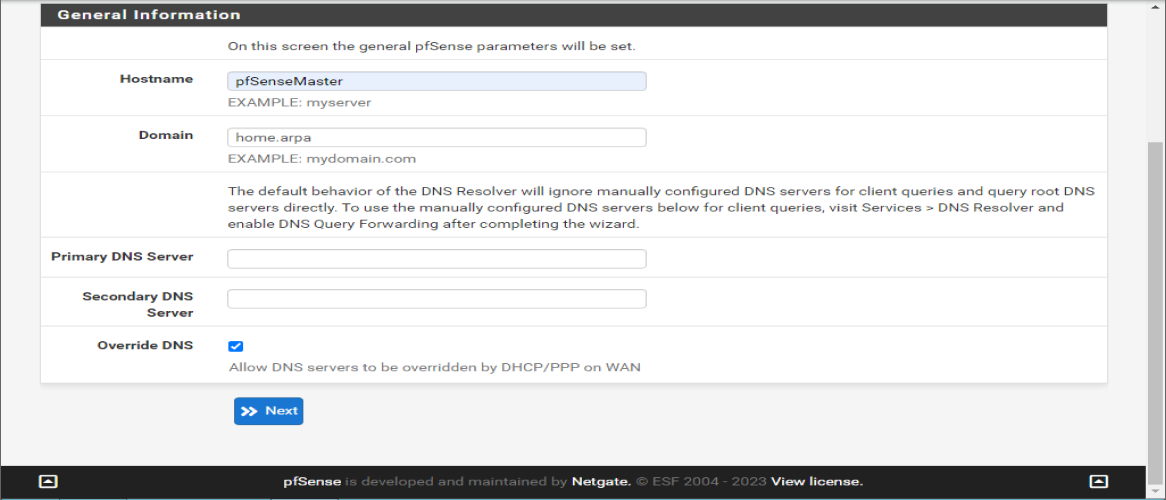


Hình 3‑8: Giới thiệu về Pfsense.



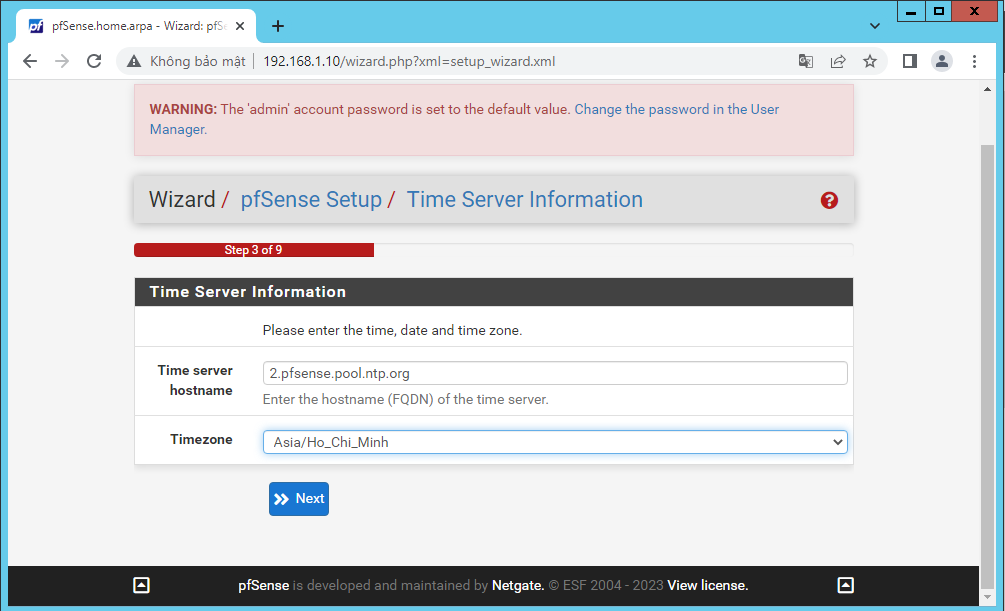
Hình 3‑9: Các chính sách hỗ trợ.

Ở đây ta nhập **Hostname** là pfSenseMaster, chọn **Next** để tiếp tục.



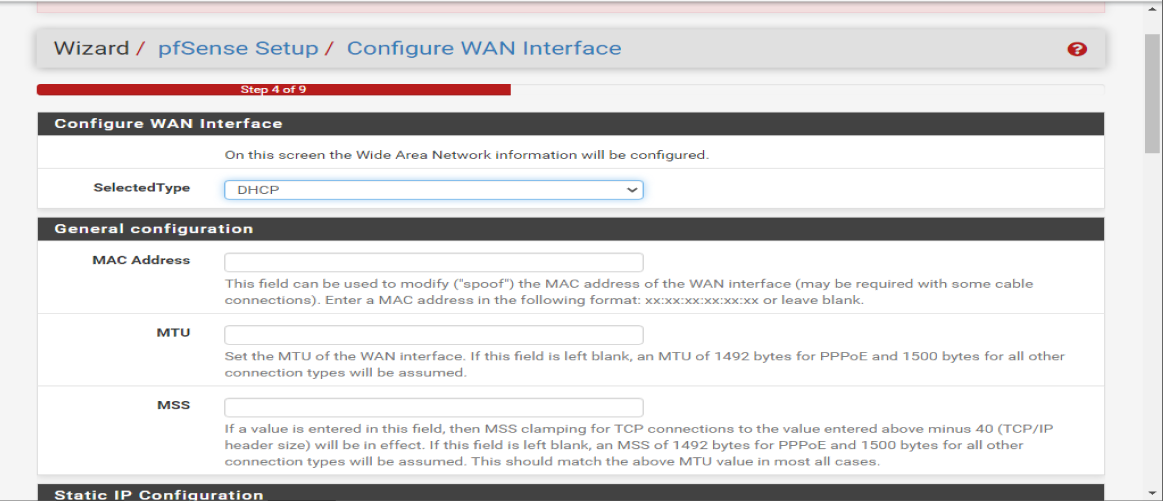
Hình 3‑10: Đặt hostname.

**Timezone** ta chọn Asia/Ho\_Chi\_Minh, chọn **Next** để tiếp tục.



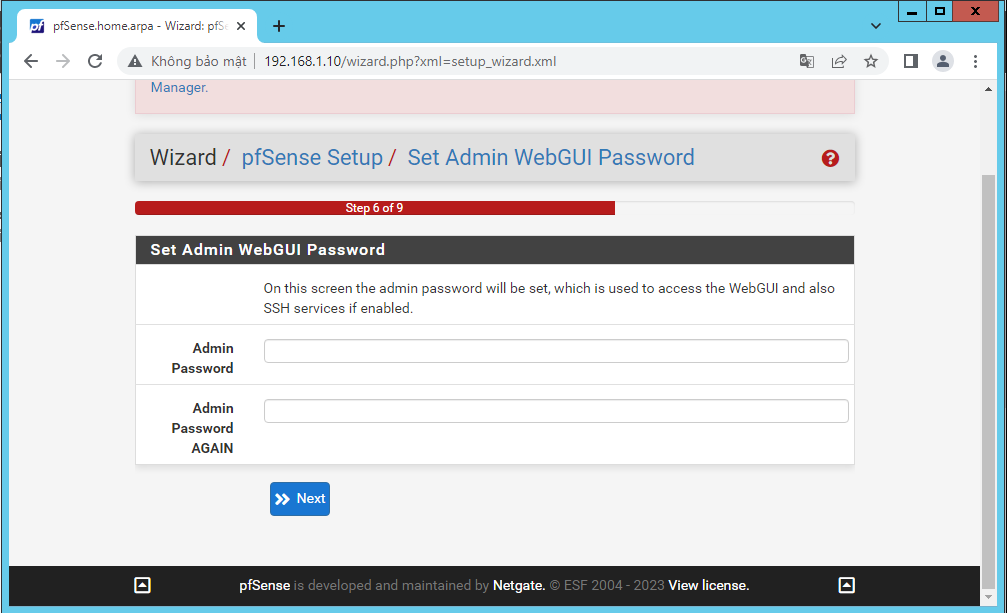
Hình 3‑11: Chọn múi giờ.

Ở interface WAN ta chọn DHCP ở mục **SelectedType**, 🡪 chọn **Next**, 🡪 chọn **Next**.



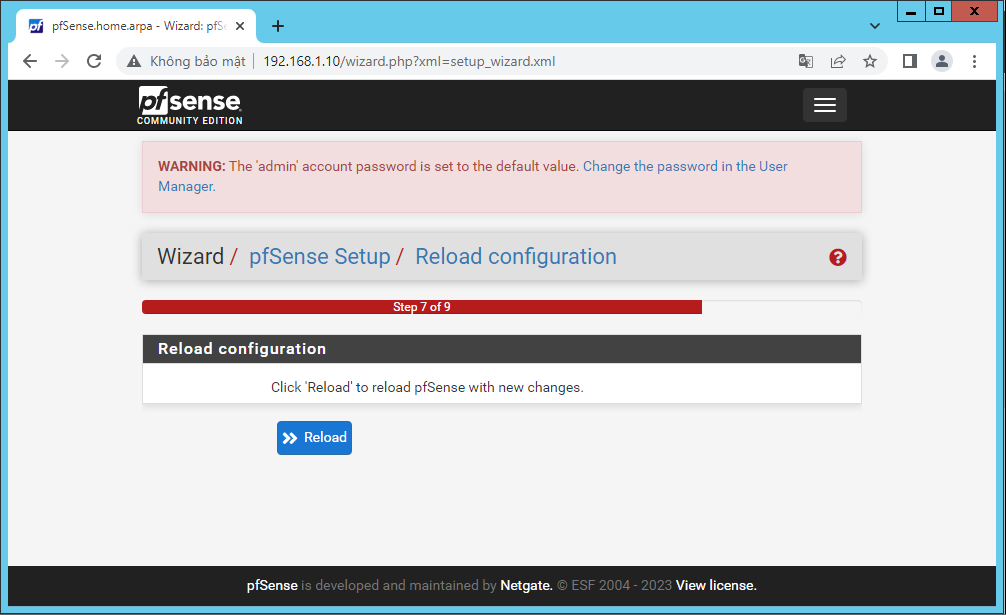
Hình 3‑12: Cấu hình card WAN.

Đặt lại password ( có thể nhấn **Next** để tiếp tục và mật khẩu sẽ là mật khẩu mặt định), sau đó chọn **Next** 🡪 chọn **Reload** 🡪 chọn **Finish** để hoàn thành thiết lập.



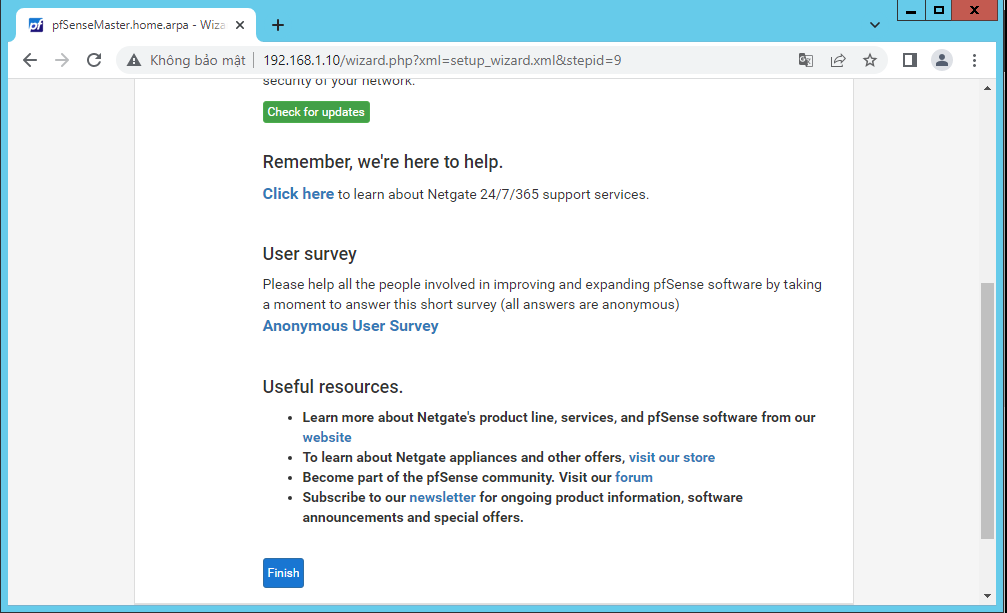
Hình 3‑13: Đặt lại mật khẩu.

Chọn **reload** để lưu lại các thiết lập đã cấu hình.



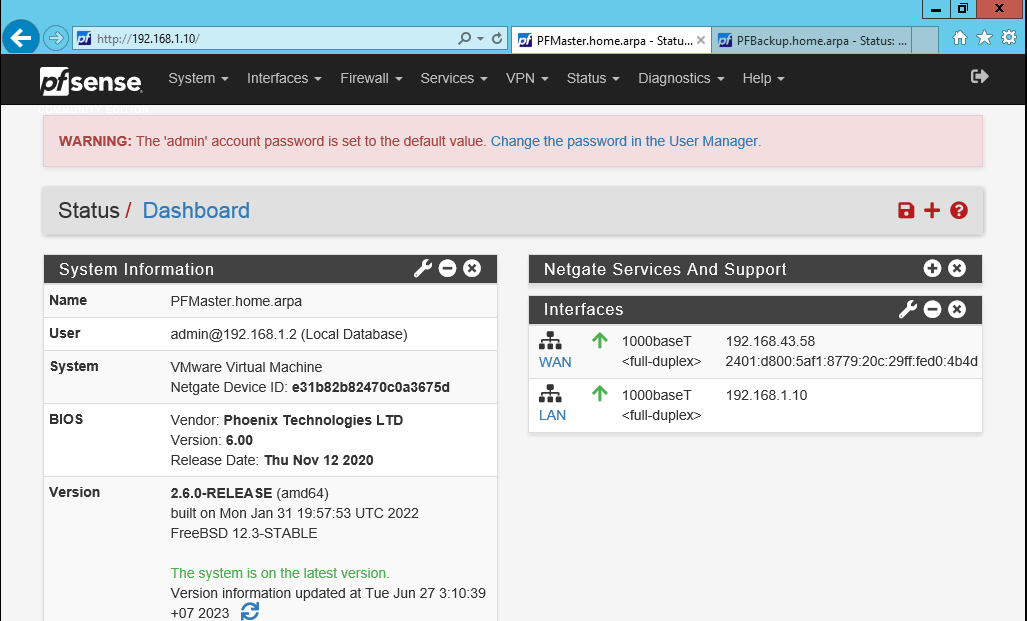
Hình 3‑14: Reload lại các thiếp lập đã cấu hình.

Chọn **Finish** để kết thúc quá trình thiết lập.



Hình 3‑15: Kết thúc quá trình.

Sau đó hệ thống sẽ trở về giao diện hiển thị các thông tin về user đăng nhập, hệ thống, cấu hình máy, DNS Server, trạng thái RAM CPU Disk, interface, ...



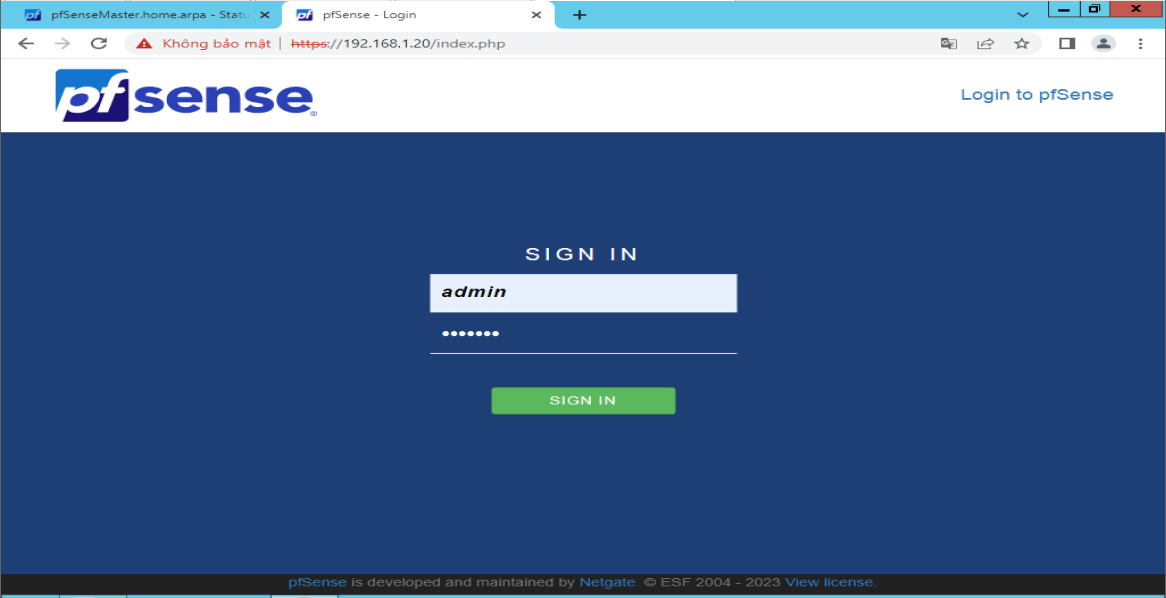
Hình 3‑16: Giao diện hiển thị thông tin.

**Pfsense Backup**.

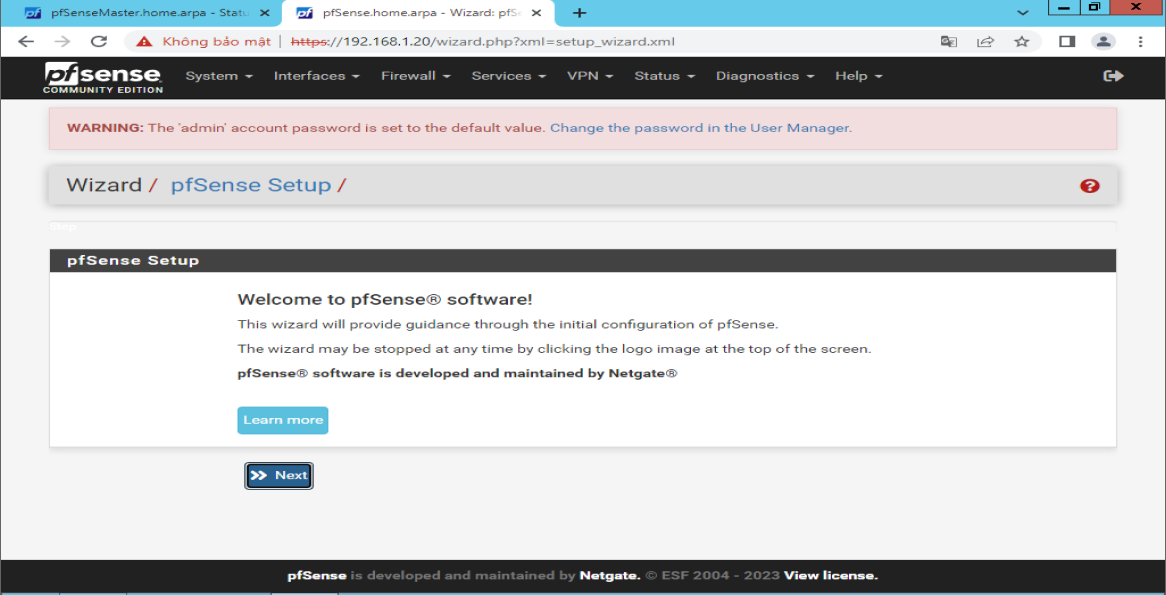
Tạo tab nhập địa chỉ 192.168.1.20 để vào pfsense Backup.

Cấu hình tương tự như pfsense Master trên pfsense Backup.

Tài khoản **admin/pfsense**.



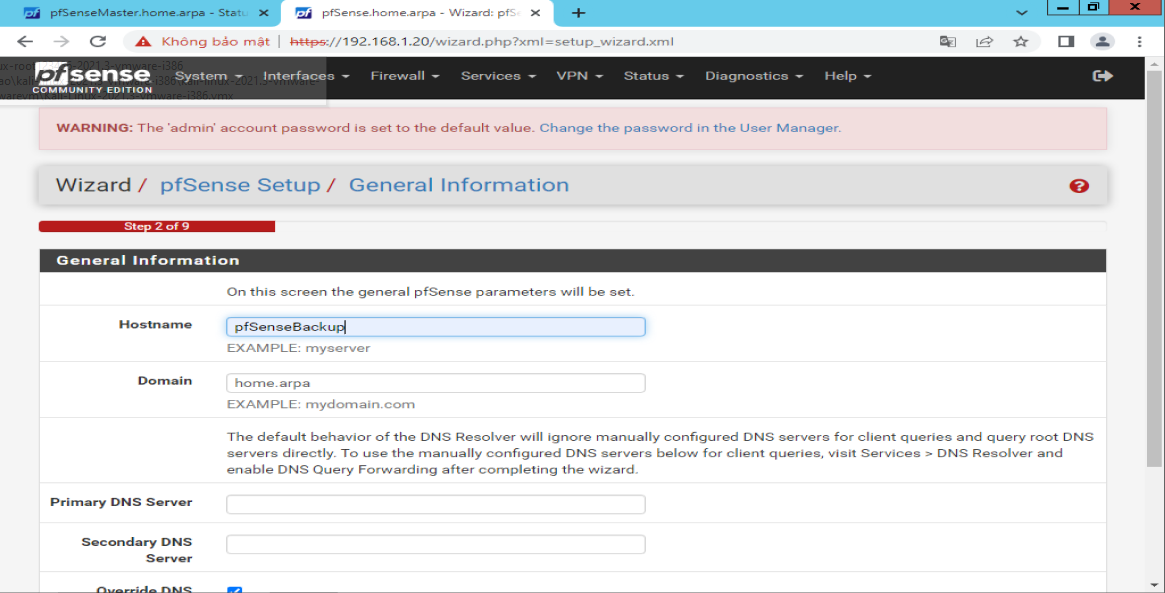
Hình 3‑17: Giao diện đăng nhập.



Hình 3‑18: Giới thiệu về Pfsense.

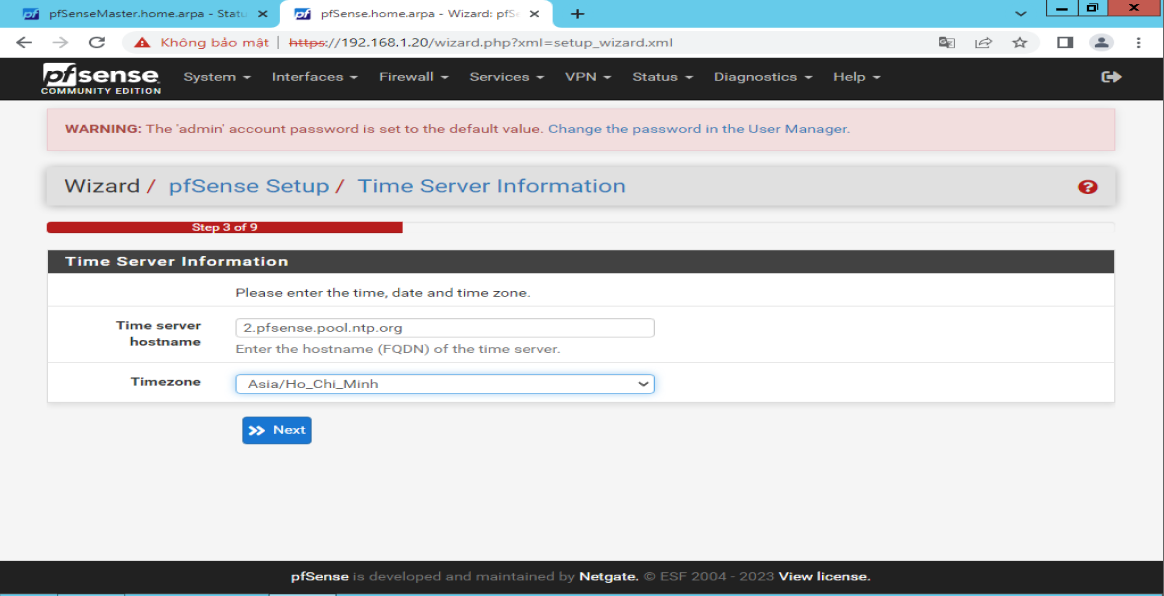
Nhấn chọn **Next**, sau đó 🡪 chọn **Next**.

Đặt **Hostname** là pfSenseBackup. 🡪 chọn **Next**.

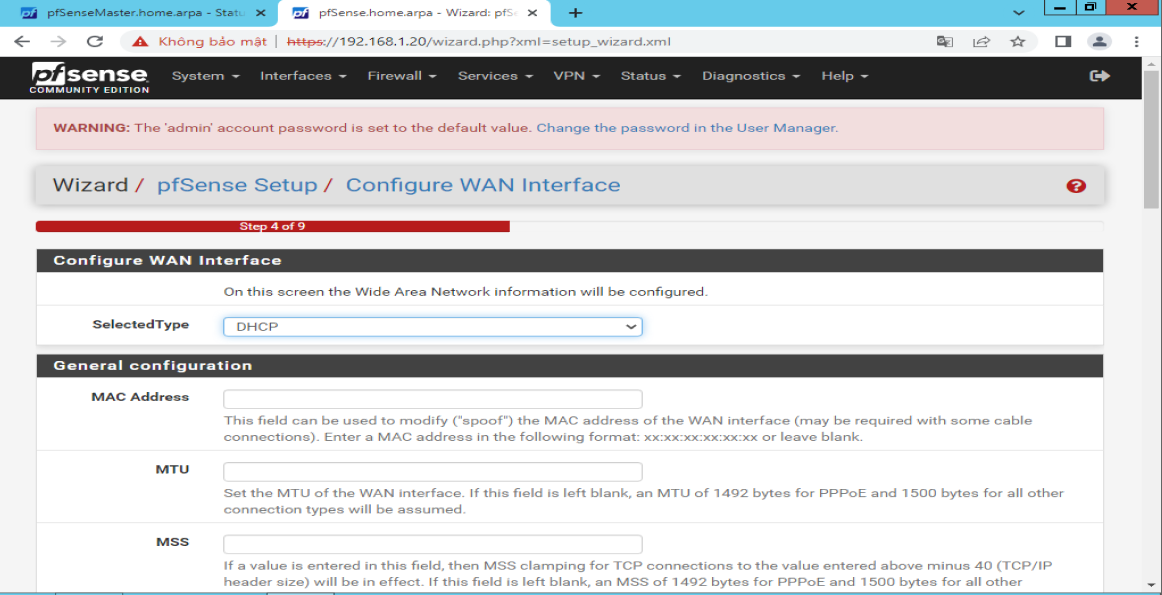


Hình 3‑19: Đặt hostname.

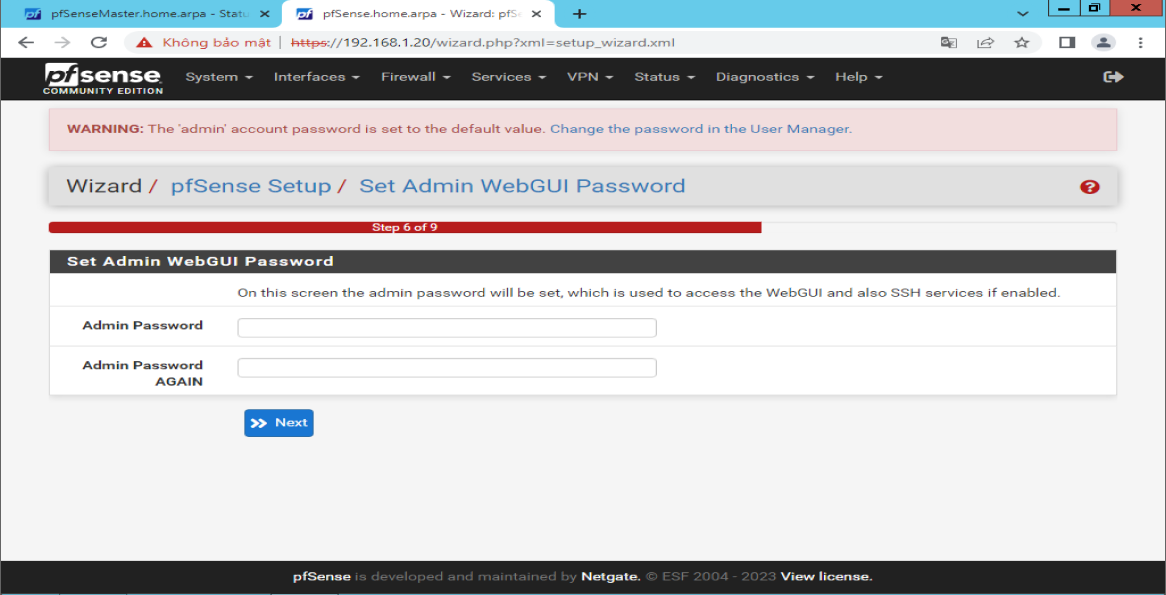
Sau đó chỉnh **Timezone** về Asia/Ho\_Chi\_Minh.



Hình 3‑20: Chọn múi giờ.

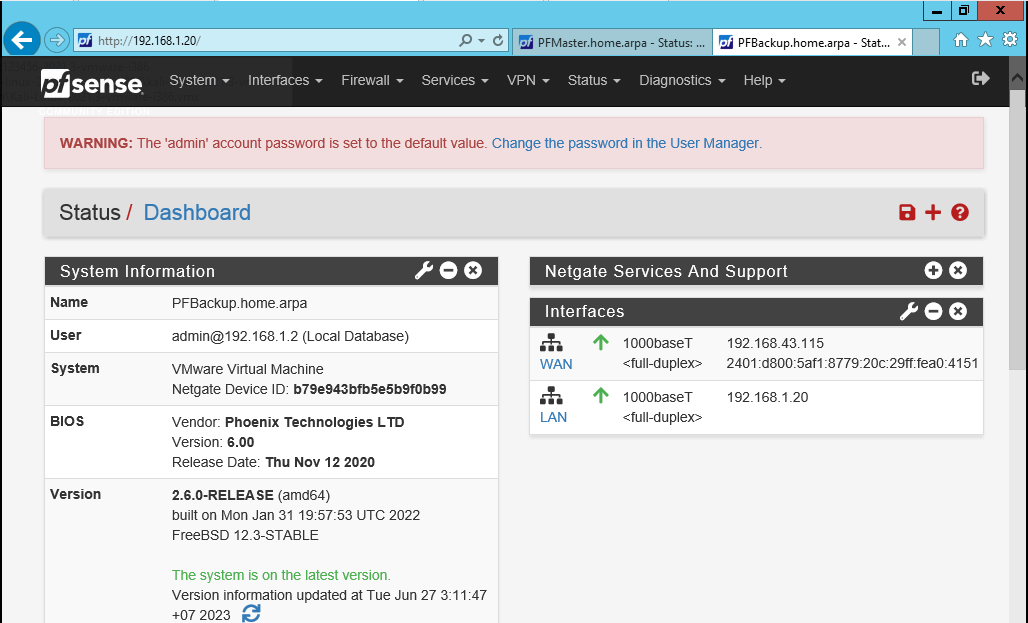


Hình 3‑21: Cấu hình card WAN.



Hình 3‑22: Đặt password.

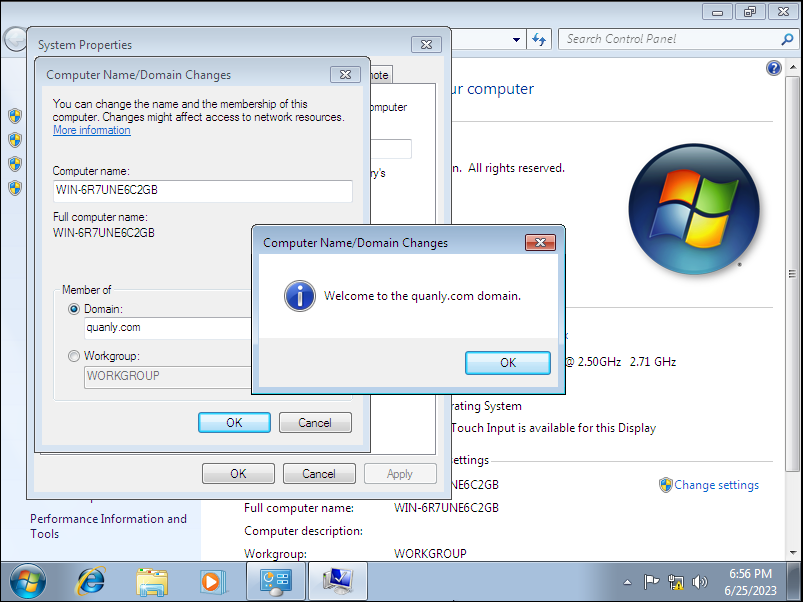
Nhấn chọn **Reload**, 🡪 chọn **Finish**. Sau đó hệ thống sẽ trở về giao diện hiển thị thông tin.



Hình 3‑23: Giao diện hiển thị thông tin.

### **Gia nhập miền cho các client**.

Ta click chuột phải vào **Computer** 🡪 **Properties** 🡪 **Change settings** 🡪 click vào **Domain** và nhập **quanly.com**.



Hình 3‑24: Gia nhập Domain máy client.

Sau khi nhấn **Ok** sẽ hiện ra bảng thông báo đăng nhập tài khoản Domain Controller để xác thực. Nhập tài khoản: **administrator** và mật khẩu: **123456a@** để xác thực gia nhập miền cho máy client.

Sau khi gia nhập miền thành công máy tính sẽ khởi động lại và chúng ta sẽ dùng tài khoản đã tạo ở máy Domain Controller để đăng nhập vào.

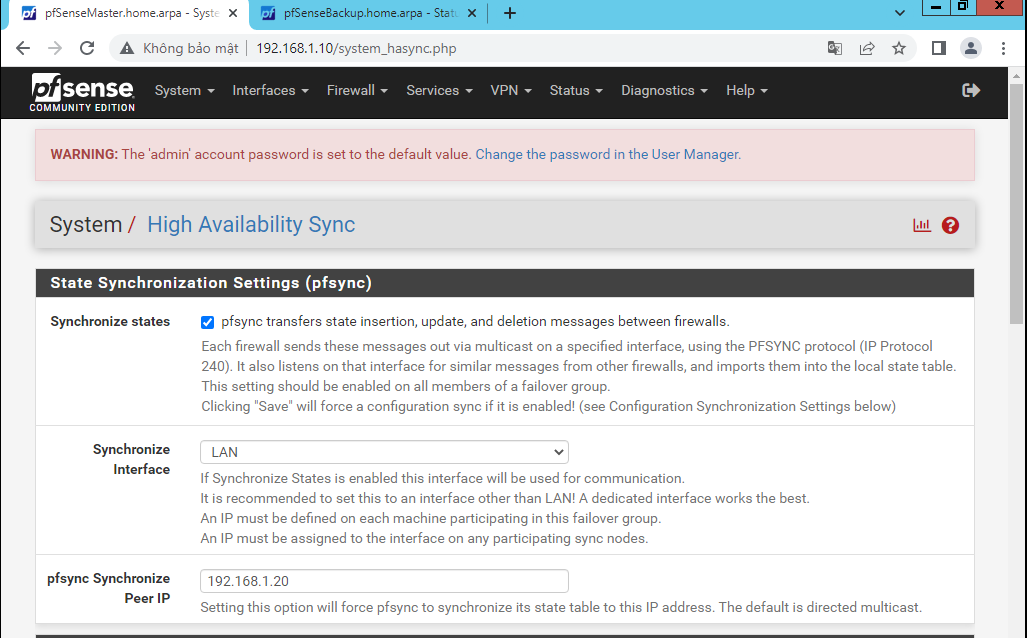
## Triển khai các chính sách.

### **Hệ thống 2 firewall – failover đáp ứng máy trong mạng LAN luôn truy cập được Internet.**

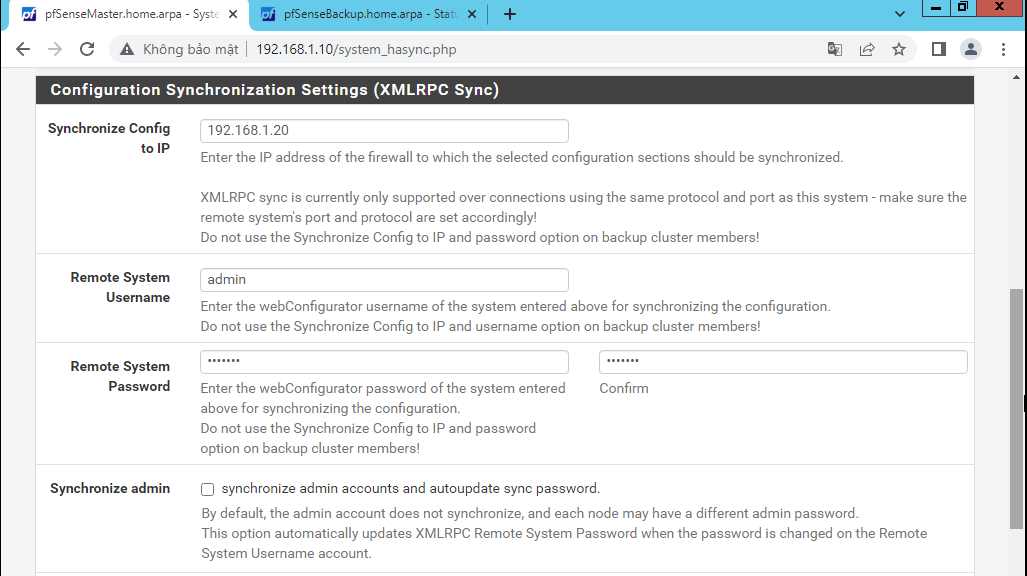
Trên máy pfsense Master ta vào **System** 🡪 **High Availability Sync** và cấu hình các thông số như sau:

* **Synchronize states**: check chọn vào ô **pfsync transfers state insertion, update, and deletion messages between firewalls**.
* **Synchronize Interface**: Chọn port LAN.
* **Pfsync Synchronize Peer IP**: 192.168.1.20 (IP của port LAN phía pfsense Backup).
* **Synchronize Config to IP**: 192.168.1.20 (IP của port LAN phía pfsense Backup).
* **Remote System Username**: admin (Sử dụng user bên phía pfsense Backup).
* **Remote System Password**: pfsense (nhập 2 lần mật khẩu của user phía bên pfsense Backup).
* **Select options to sync**: Ta check chọn những thông tin ta muốn đồng bộ từ pfsense Master sang pfsense Backup.

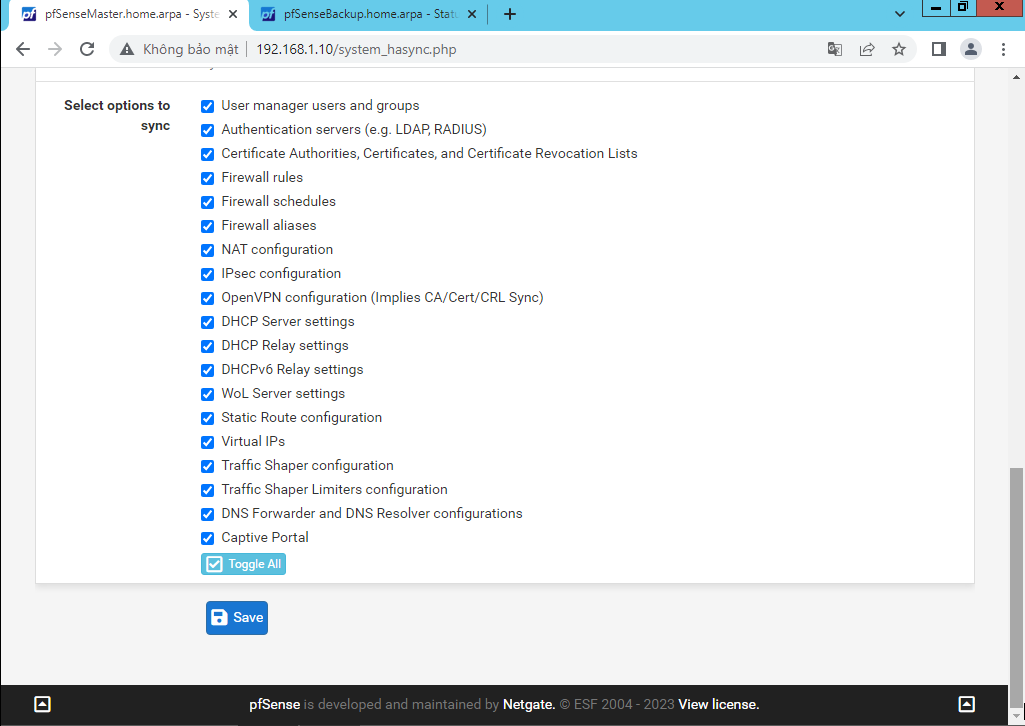
🡪 Chọn **Save** để lưu cài đặt.



Hình 3‑25: Cấu hình High Availability Sync.



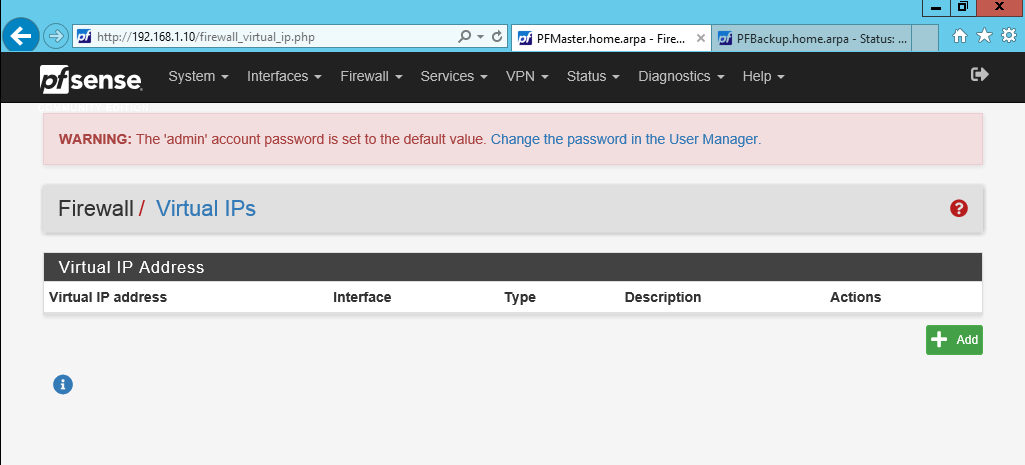
Hình 3‑26: Cấu hình High Availability Sync.



Hình 3‑27: Cấu hình High Availability Sync.

Lưu ý: High Availability (HA) trên pfsense không đồng bộ cấu hình cổng interface và các packages cài đặt thêm vào pfsense.

Tạo Virtual IP LAN. Việc thực hiện chỉ cần trên pfSense Master. Vì lúc này, quá trình đồng bộ đã bắt đầu xảy ra. Trên pfsense Master ta vào **Firewall** 🡪 **Virtual IPs** 🡪 **+Add** để tạo mới Virtual IP.

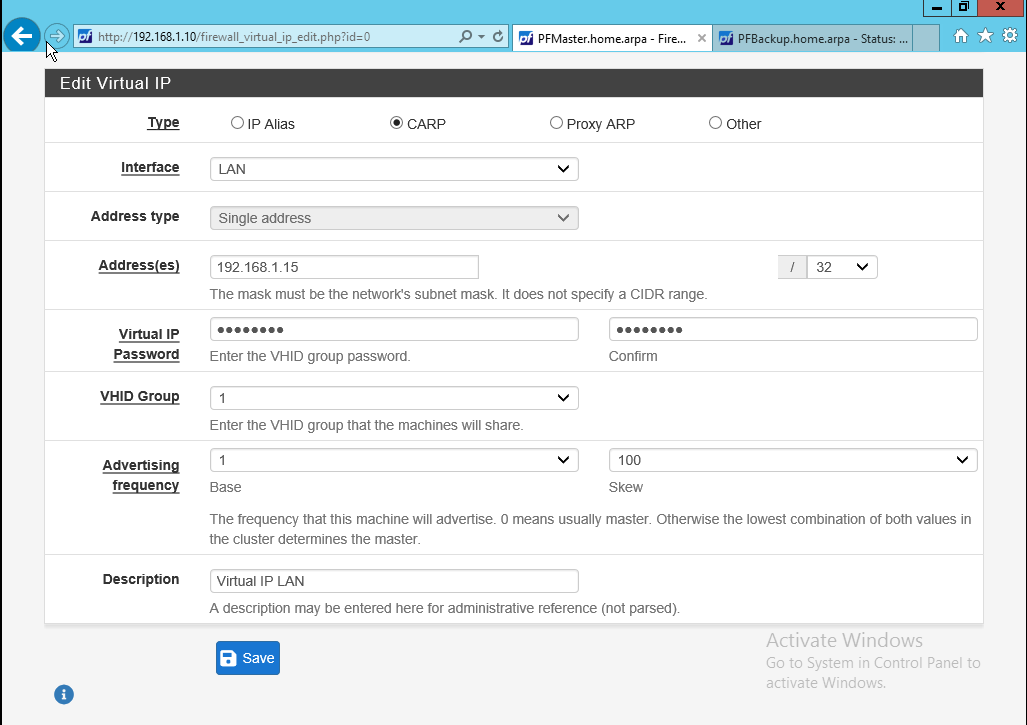


Hình 3‑28: Cấu hình Virtual Ips.

Ta cấu hình các thông số Virtual IP như sau:

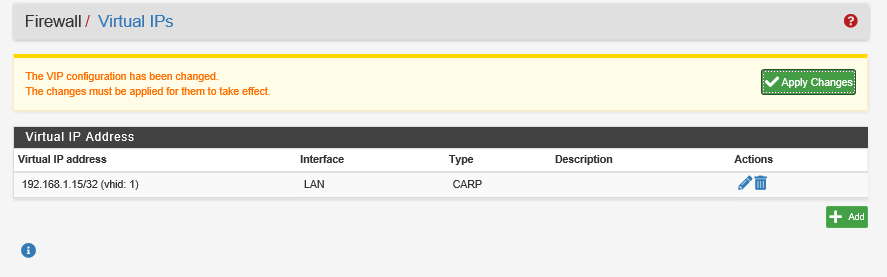
* **Type**: CARP.
* **Interface**: LAN.
* **Address type**: Single address.
* **Address(es)**: 192.168.1.15 (lấy IP này làm IP LAN ảo).
* **Virtual IP Password**: \*\*\* \*\*\* (nhập 2 lần mật khẩu bất kỳ, mật khẩu này cũng sử dụng bên pfsense Master).
* **VHID Group**: chọn 1 (nếu sử dụng nhiều Virtual IP thì cài VHID Group giá trị khác nhau).
* **Advertising frequency**: Base=1, Skew=100.
* **Description**: Virtual IP LAN.

🡪 Chọn **Save** để lưu cài đặt.



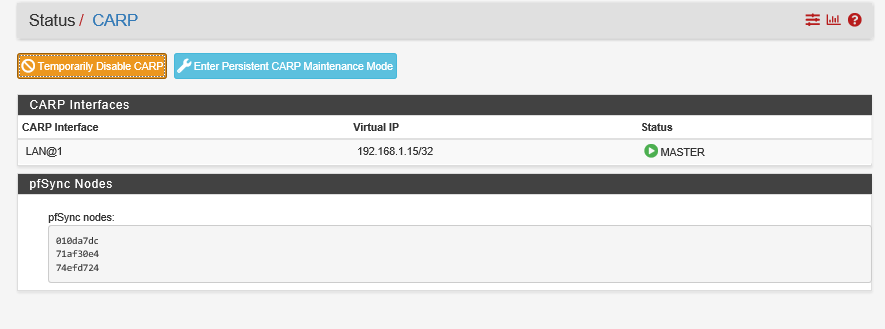
Hình 3‑29: Cấu hình Virtual Ips.

Tiếp theo nhấn chọn **Apply Changes**.



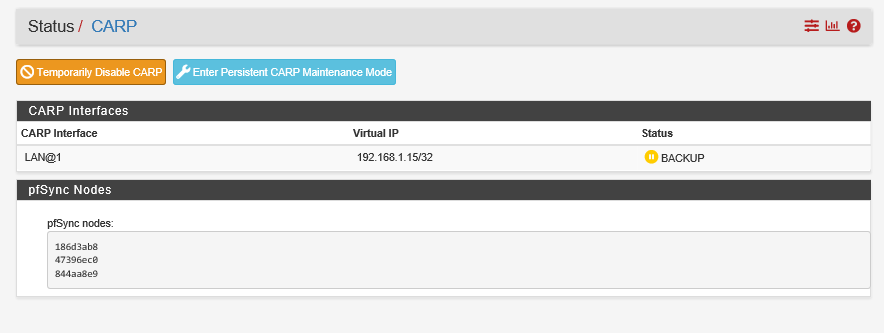
Hình 3‑30: Cấu hình Virtual Ips.

Trên 2 firwall pfsense ta vào mục **Status** 🡪 **CARP**, chúng ta thấy pfsense Master được bầu làm **Master**



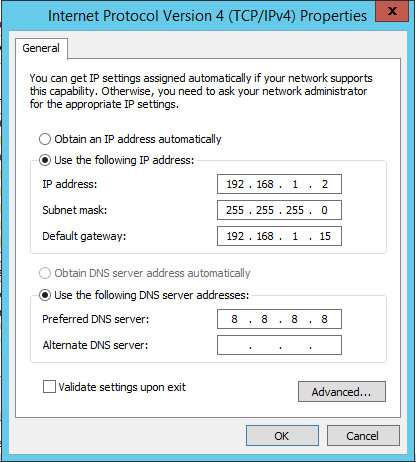
Hình 3‑31: Cấu hình CARP ở pfsense Master.

Và pfsense Backup được bầu làm **Backup**.

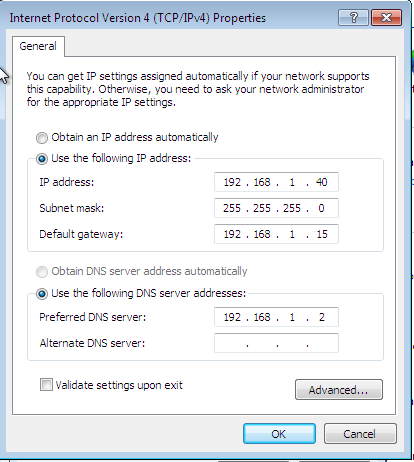


Hình 3‑32: Cấu hình CARP ở pfsense Backup.

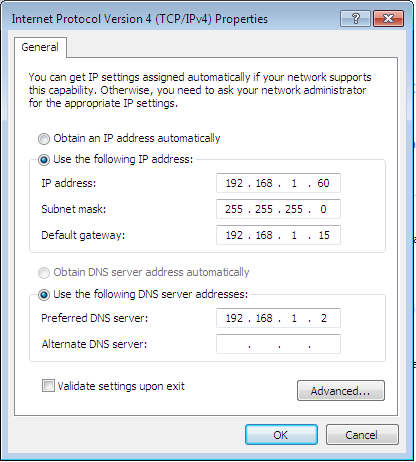
Bây giờ các thiết bị user trỏ **Default Gateway** về IP 192.168.1.15 (IP LAN ảo) là có thể truy cập internet. Trong trường hợp firewall pfsense Master gặp sự cố thì hệ thống tự động bầu pfsense Backup làm Master và hệ thống vẫn hoạt động bình thường, không làm ảnh hưởng đến User.



Hình 3‑33: Địa chỉ Ip của máy DC.



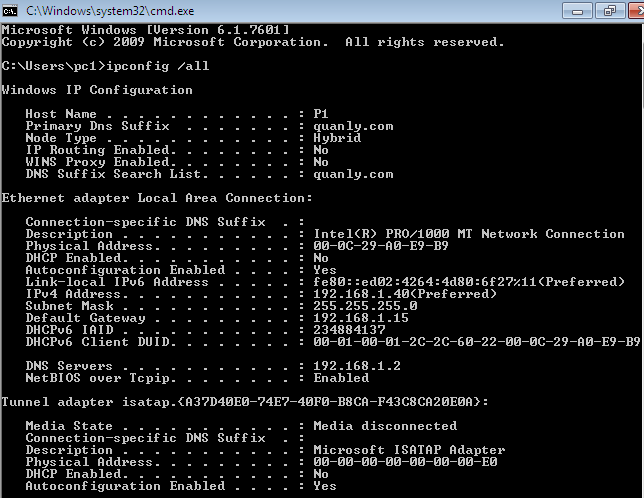
Hình 3‑34: Địa chỉ Ip của máy P1.



Hình 3‑35: Địa chỉ Ip của máy P2.

### **Chặn truy cập Internet thông qua host IP.**

Trên máy P1, mở cmd để xem thông tin máy P1 🡪 máy P1 có IP là **192.168.1.40**.



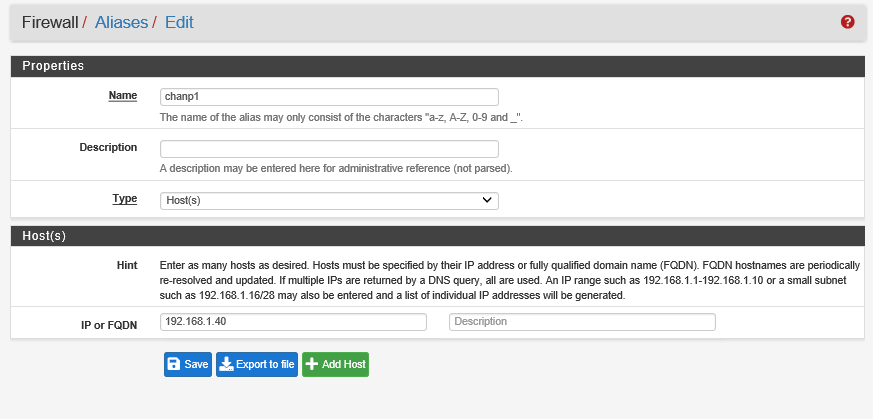
Hình 3‑36: Thông tin máy P1.

Thực hiện trên máy DC.

Ta vào **Firewall** 🡪 **Aliases** 🡪 **+Add** nhập vào các thông tin như tên, địa chỉ ip:

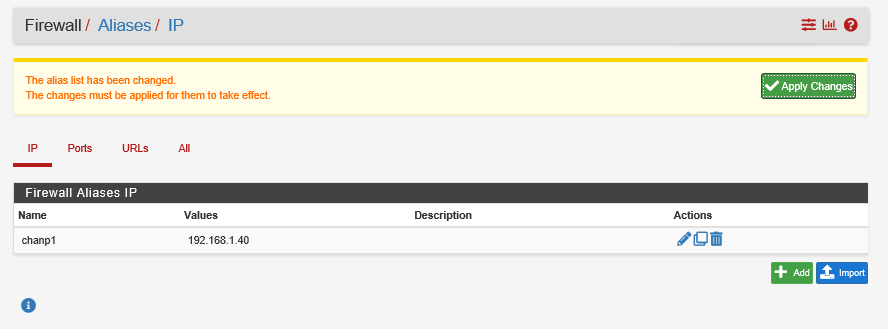
* **Name**: chanp1.
* **Type**: Host(s).
* **IP or FQDN**: 192.168.1.40.(địa chỉ ip của P1)

🡪 chọn **Save** để lưu lại cấu hình.



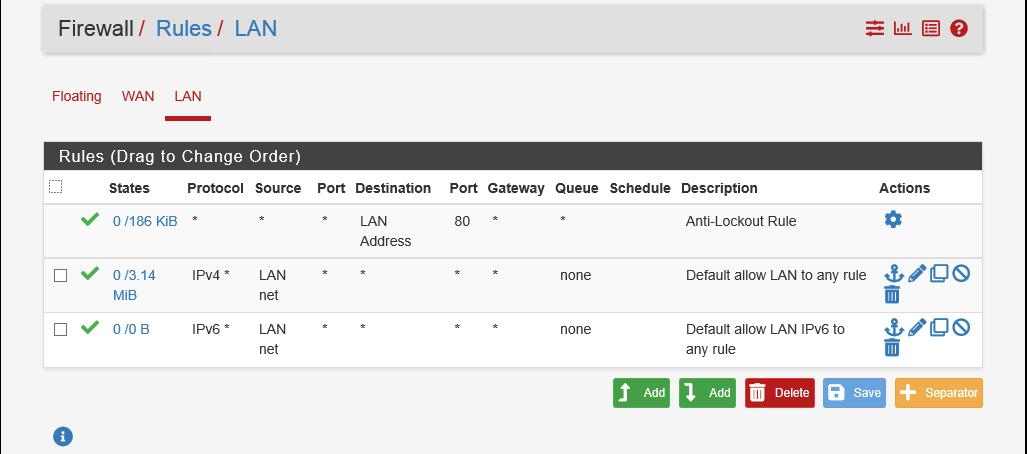
Hình 3‑37: Nhập thông tin máy P1.

Sau đó nhấn chọn **Apply Changes**.



Hình 3‑38: Cấu hình IP Aliases.

Tiếp theo đó ta vào **Firewall** 🡪 **Rules** chọn mạng **LAN**, tiếp theo chọn **Add** để thêm mới rules.

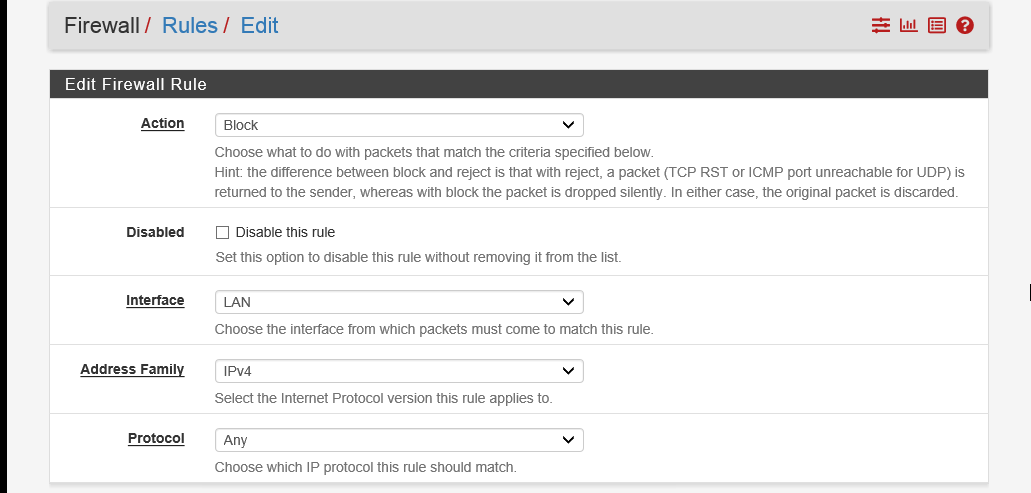


Hình 3‑39: Thêm rules mới.

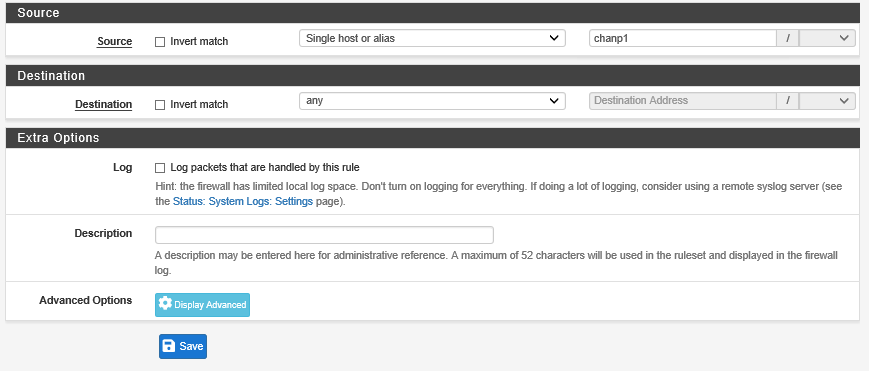
Cấu hình như sau:

* **Action**: Block.
* **Interface**: LAN.
* **Address Family**: IPv4.
* **Protocol**: Any.
* **Source**: chọn Single host or alias và nhập name chanp1.
* **Description**: Block IP P1.

🡪 chọn **Save** để lưu lại cấu hình. Sau đó nhấn chọn **Apply Changes**.

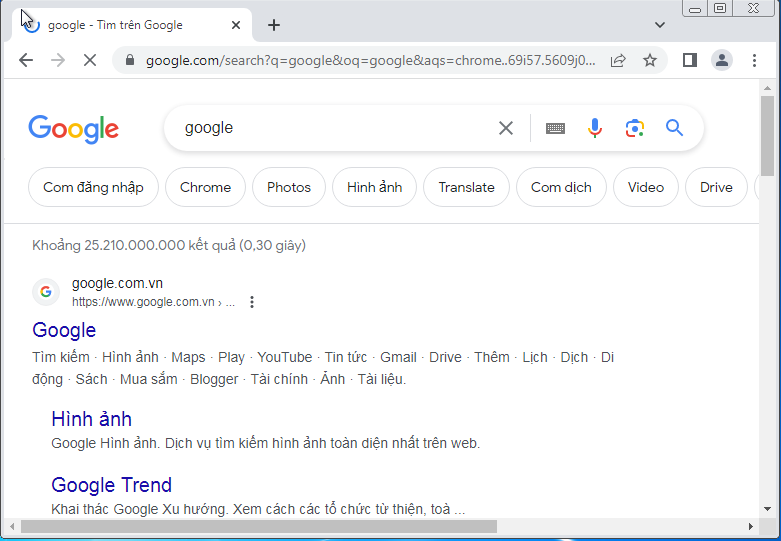


Hình 3‑40: Cấu hình chặn internet.

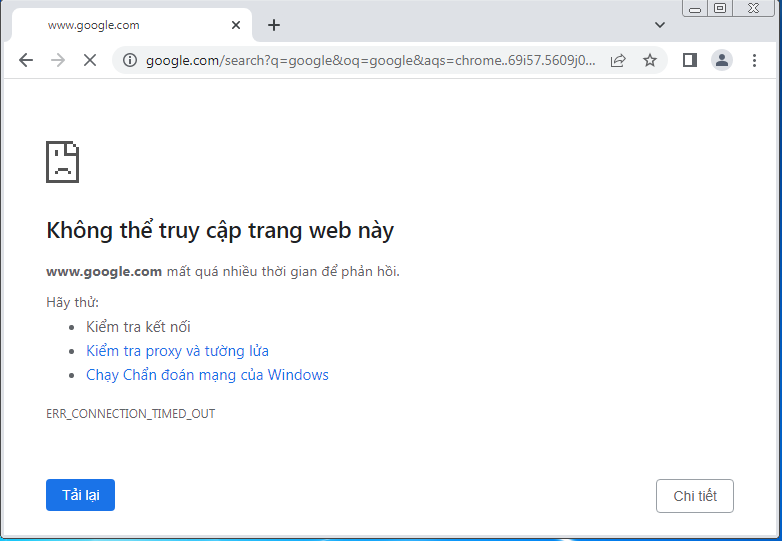


Hình 3‑41: Cấu hình chặn internet.

Trên máy P1, ta thử truy cập internet. Kết quả đã bị chặn.



Hình 3‑42: Trước khi áp dụng rules.

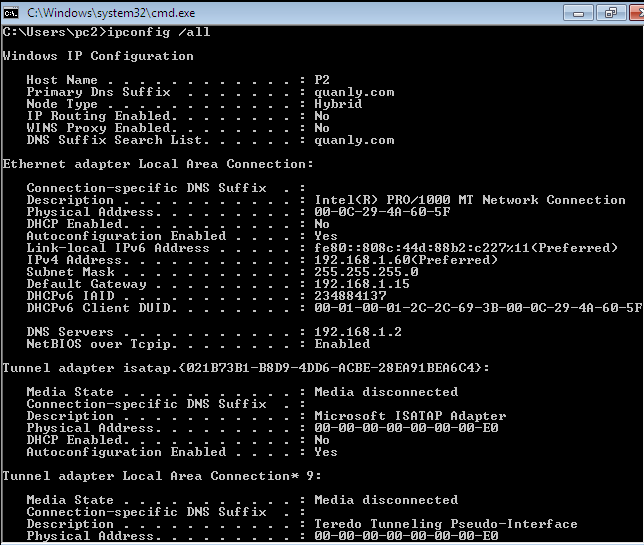


Hình 3‑43: Sau khi áp dụng rules.

Trên máy P2, truy cập mạng bình thường.

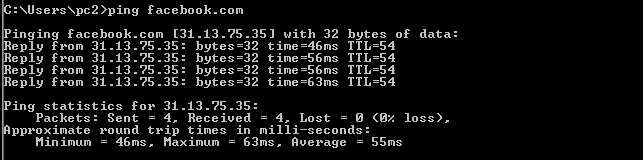
### **Chặn truy cập website thông qua network IP. (chặn truy cập website Facebook)**

Trên máy P2, kiểm tra ip máy bằng cách vào cmd nhập câu lệnh **ipconfig /all.**



Hình 3‑44: Thông tin của máy P2.

Ping đến trang facebook.com để lấy IP của facebook.(ở đây ip của facebook là 31.13.75.35)



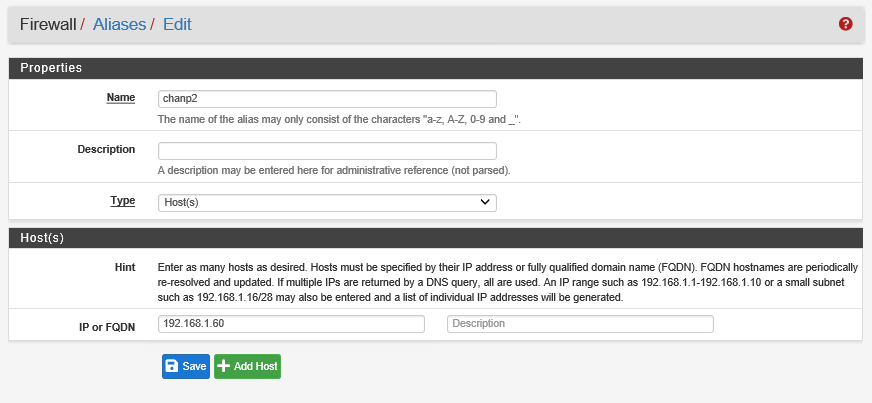
Hình 3‑45: Địa chỉ ip của facebook.

Thực hiện trên máy DC.

Tạo Alias cho địa chỉ ip muốn chặn ( tại đây Ip bị chặn là **192.168.1.60** của P2 ). Chọn **Firewall** 🡪 **Aliases** 🡪 **+Add** nhập vào các thông tin sau:

* **Name**: chanp2.
* **Type**: Host(s).
* **IP or FQDN**: 192.168.1.60.(địa chỉ ip của P2).

🡪 chọn **Save** để lưu lại cấu hình. Sau đó nhấn chọn **Apply Changes**.

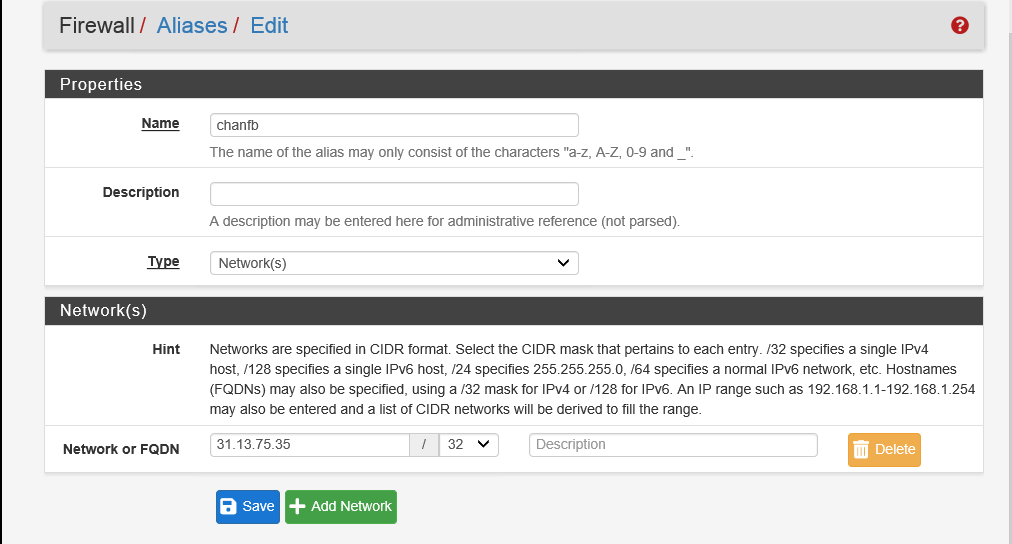


Hình 3‑46: Nhập thông tin ip của máy P2.

Ta tiếp tục tạo Alias cho địa chỉ website muốn chặn (ở đây website muốn chặn là facebook với địa chỉ là 31.13.75.35). Các thông tin như sau:

* **Name**: chanfb.
* **Type**: Network(s).
* **IP or FQDN**: nhập địa chỉ ip của facebook (ở đây địa chỉ ip facebook là 31.13.75.35).

🡪 chọn **Save** để lưu lại cấu hình. Sau đó nhấn chọn **Apply Changes**.

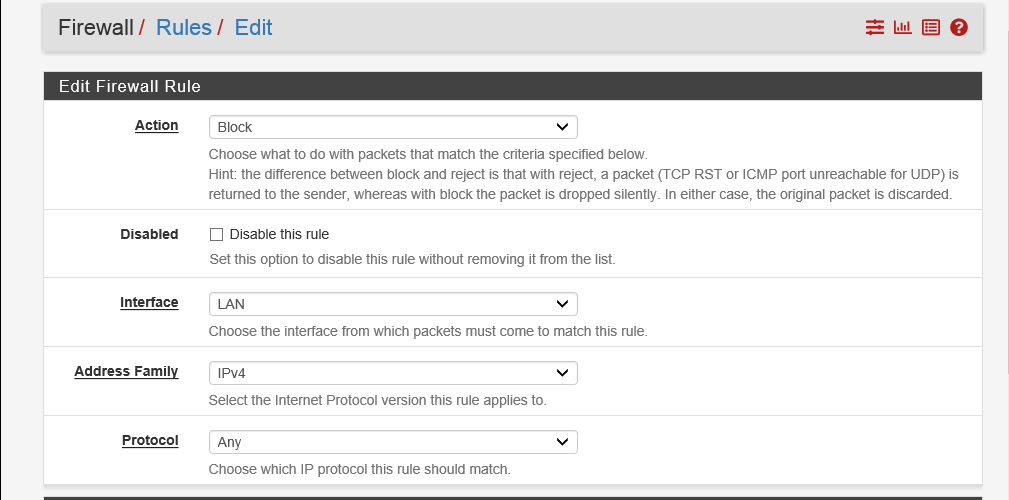


Hình 3‑47 : Nhập thông tin địa chỉ Facebook.

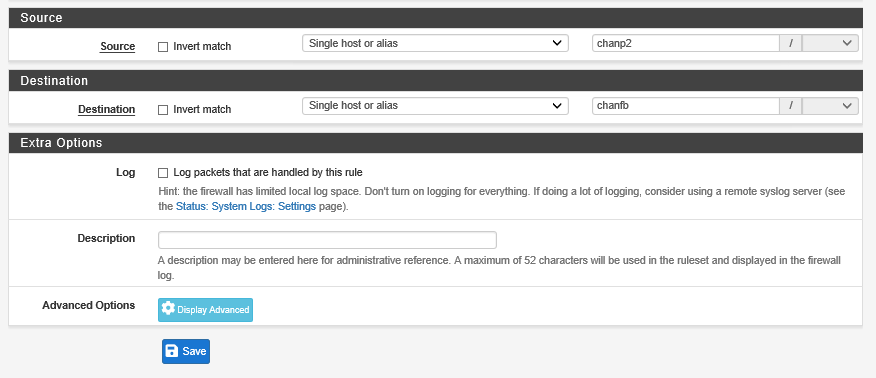
Tiếp theo đó ta vào **Firewall** 🡪 **Rules** chọn mạng **LAN**, ta **Add** thêm rules mới vào.

* **Action**: Block.
* **Interface**: LAN.
* **Address** **Family**: Ipv4.
* **Protocol**: Any.
* **Source**: ta chọn Single host or alias và nhập name chanp2.
* **Destination**: ta chọn Single host or alias và nhập name chanfb.

🡪 chọn **Save** để lưu lại cài đặt. Sau đó nhấn chọn **Apply Changes**.

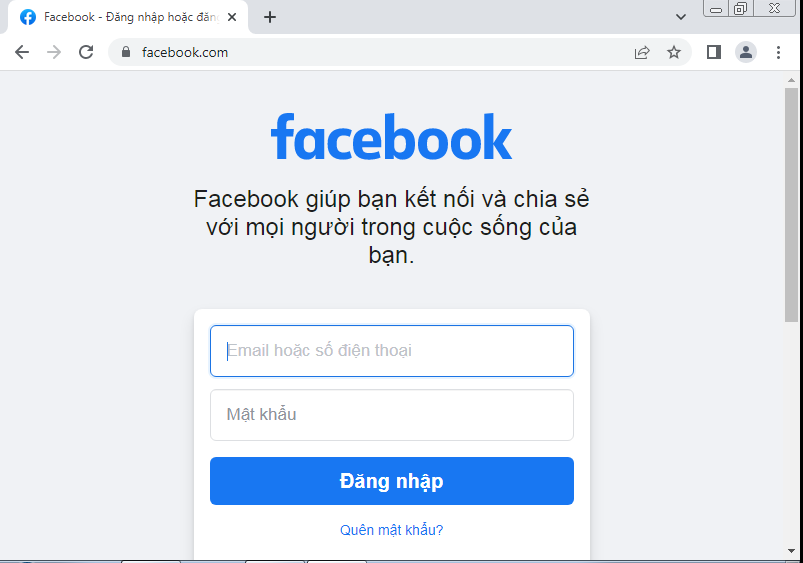


Hình 3‑48: Cấu hình chặn trang Facebook.

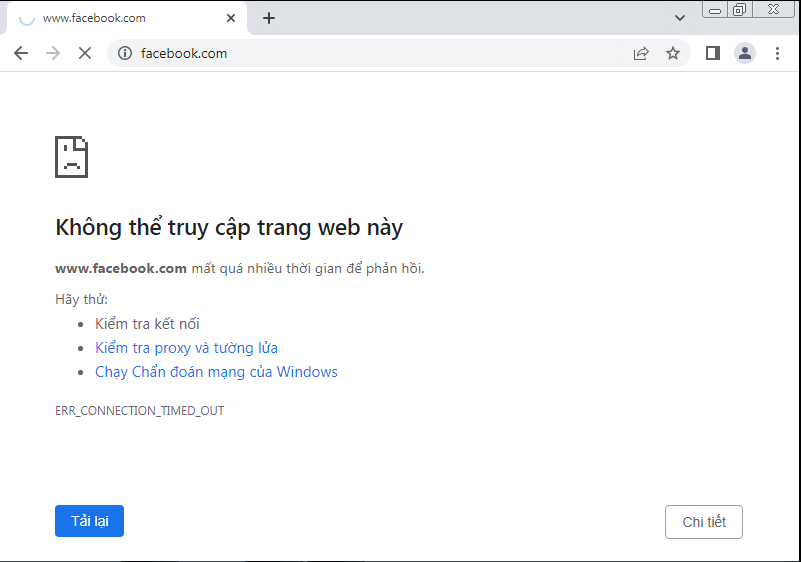


Hình 3‑49: Cấu hình chặn trang Facebook.

Trên máy P2, ta kiểm tra kết quả.



Hình 3‑50: Trước khi áp dụng rules.



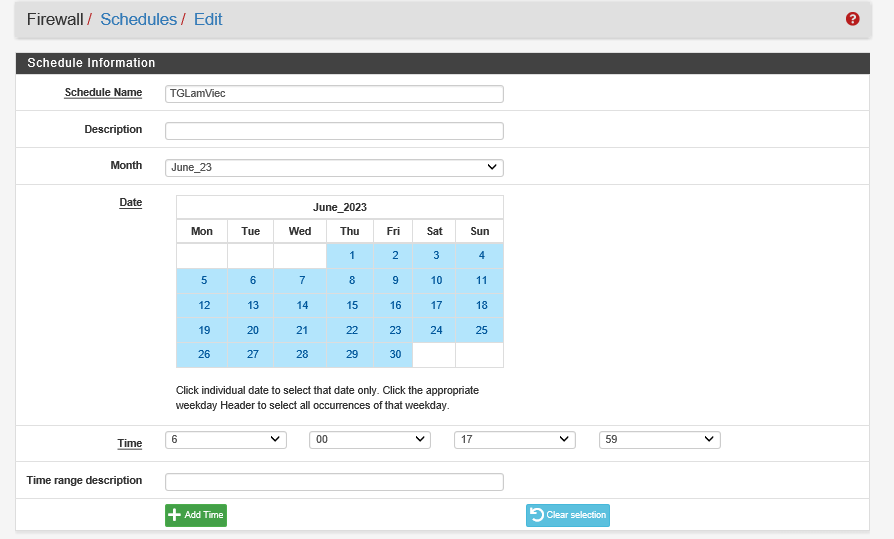
Hình 3‑51: Sau khi áp dụng rules.

### **Thiết lập thời gian quản lý (Schedule).**

Thực hiện trên máy DC. Ta vào **Firewall** 🡪 **Schedules** để cấu hình thời gian quản lý.

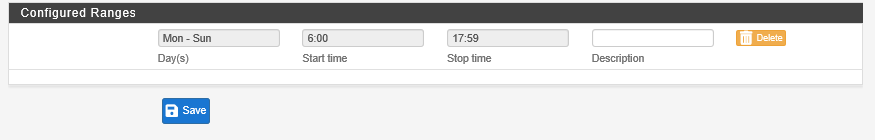
* **Schedule Name**: TGLamViec.
* **Month**: ta chọn tháng năm hiện tại.
* **Date**: ta chọn hết tất cả các ngày trong tháng.
* **Time**: ta chọn mốc thời gian mà ta muốn lập( ở đây thời gian từ 6:00 – 17:59).

Sau đó ta nhấn chọn **+Add Time** để lưu lại mốc thời gian.



Hình 3‑52: Thiết lập thời gian quản lý.

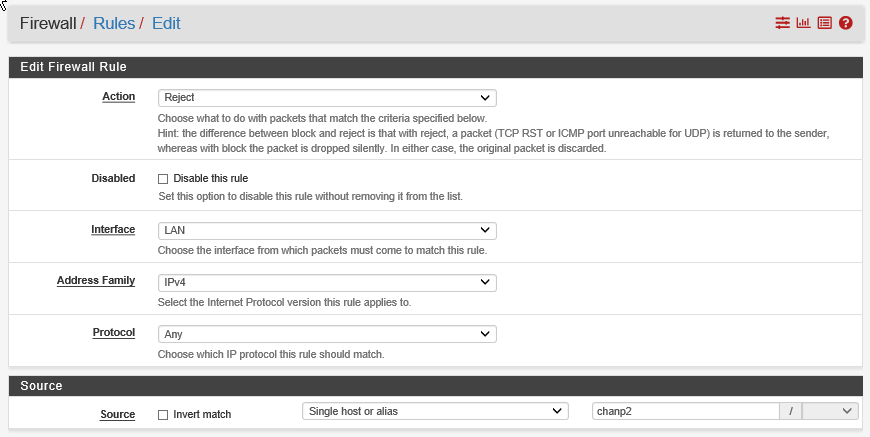
Tiếp theo chọn **Save** để lưu lại.



Hình 3‑53: Thiết lập thời gian quản lý.

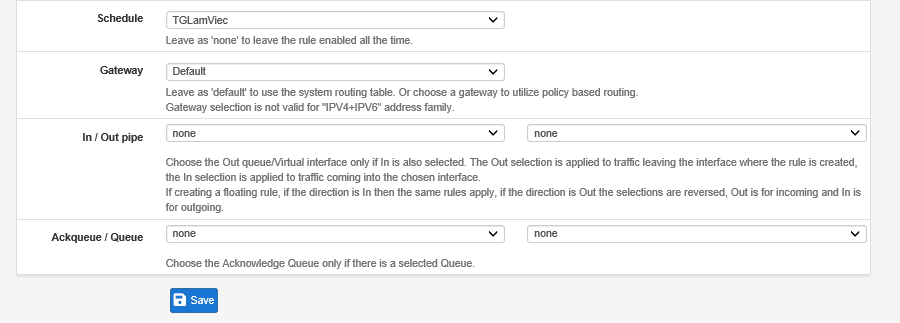
Ta sẽ áp dụng Schedule lên máy P2. Vào **Firewall** 🡪 **Rules** chọn mạng **LAN**, nhấn **+Add** để tạo rules mới.

* **Action**: Reject.
* **Interface**: LAN.
* **Address Family**: Ipv4.
* **Protocol**: Any.
* **Source**: ta chọn Single host or alias và nhập name chanp2.



Hình 3‑54: Cấu hình thời gian quản lý.

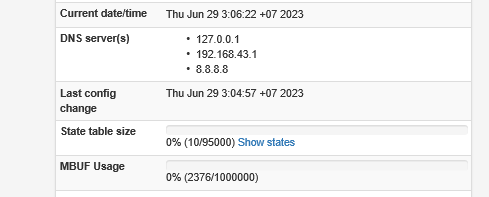
Ở dòng **Advanced Options** ta nhấn vào **Display Advanced** để hiển thị toàn bộ phần Advanced Options. Sau đó ta tìm đến dòng **Schedule** chọn tên schedule ta đã tạo là **TGLamViec**.



Hình 3‑55: Cấu hình thời gian quản lý.

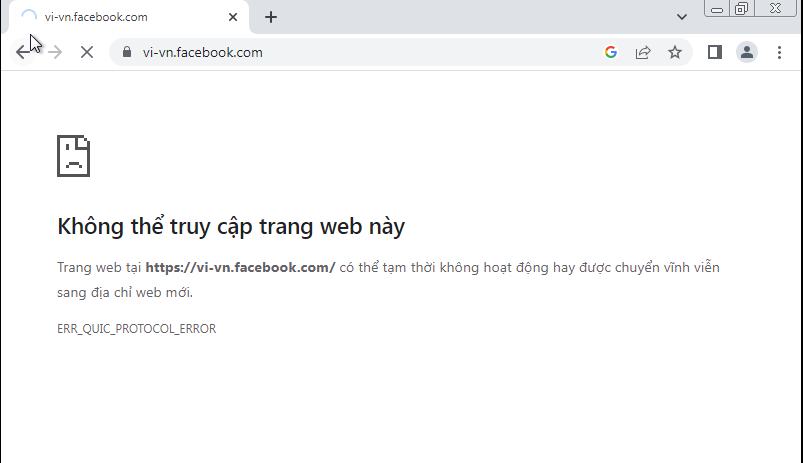
Chọn **Save** để lưu lại cài đặt. Tiếp theo nhấn **Apply Changes**.

Thời gian được thực hiện theo giờ được thiết lập trên firewall.

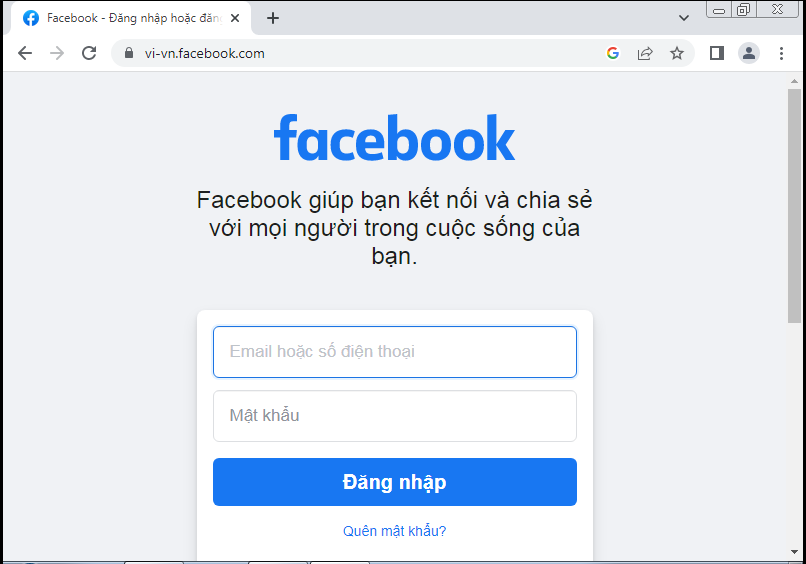


Hình 3‑56: Thời gian firewall.

Khi áp dụng các chính sách được thực hiện theo giờ trên firewall.



Hình 3‑57: Trong thời gian áp dụng.



Hình 3‑58: Sau thời gian áp dụng.

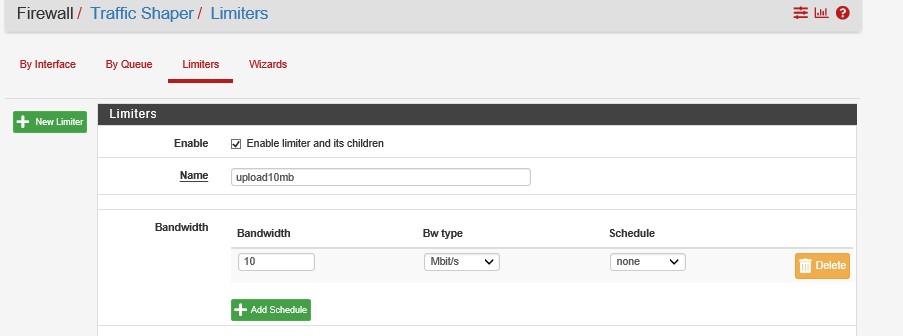
### **Thiết lập giới hạn tốc độ upload và download.**

Thực hiện trên máy DC.

Ta vào **Firewall** 🡪 **Traffic** **Shaper** 🡪 chọn đến mục **Limiters** 🡪 chọn **New** **Limiters** để tạo limiter Upload.

* **Enable**: ta check chọn vào ô Enable limiter and its children.
* **Name**: upload10mb.
* **Bandwidth**: ta nhập Bandwidth là 10, Bw type : Mbit/s.

🡪 Chọn **Save** để lưu lại cài đặt. Chọn **Apply Changes**.

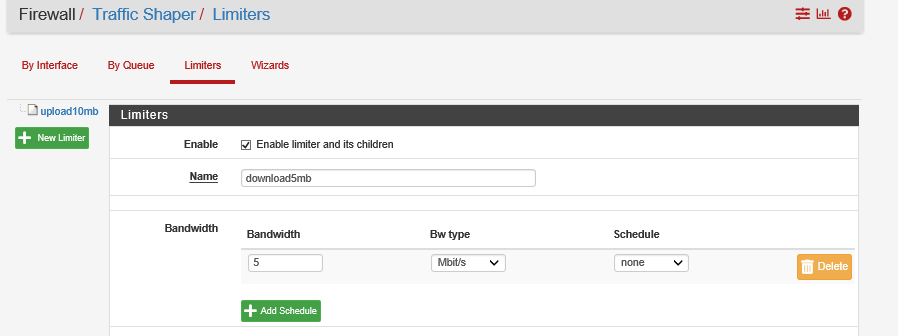


Hình 3‑59: Giới hạn Upload.

Tiếp theo ta tiếp tục chọn **New** **Limiters** để tạo limiter Download.

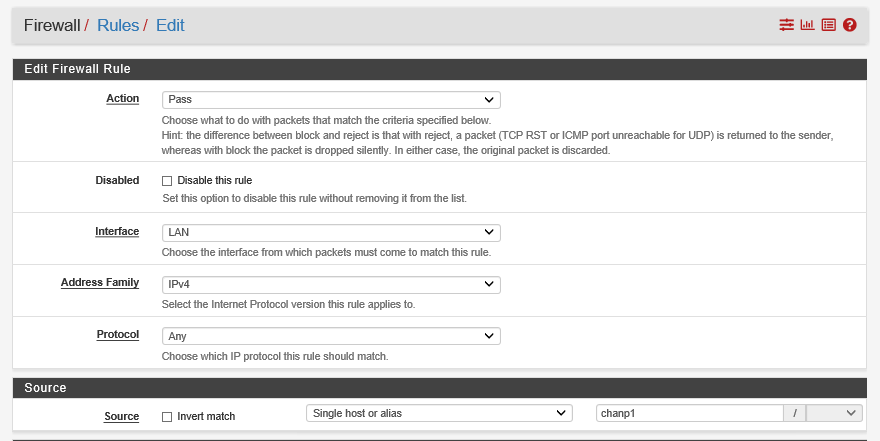
* **Enable**: ta check chọn ô Enable limiter and its children.
* **Name**: download5mb.
* **Bandwidth**: ta nhập Bandwidth là 5, Bw type : Mbit/s.

🡪 Chọn **Save** để lưu lại cài đặt. Chọn **Apply Changes**.



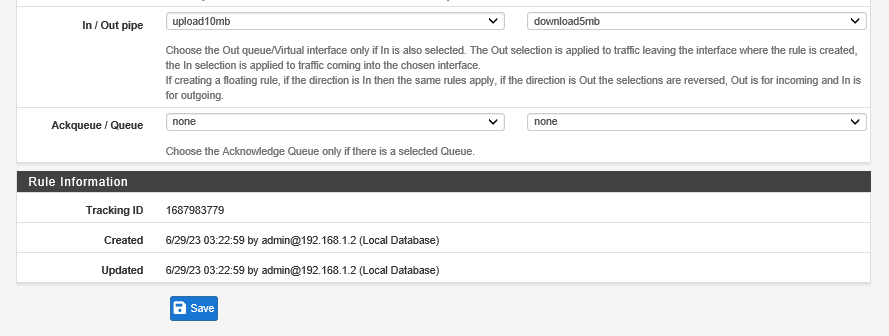
Hình 3‑60: Giới hạn Download.

Tiếp theo ta vào **Firewall** 🡪 **Rules** 🡪 chọn mạng **LAN**, ta **+Add** thêm rules mới vào.



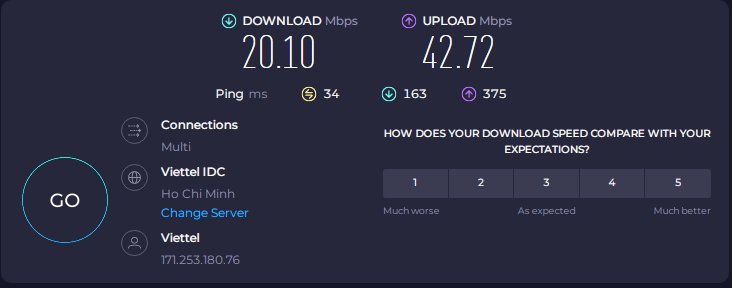
Hình 3‑61: Cấu hình rules upload và download.

Tại dòng **In/Out pipe** của **Advanced Options** ta chọn 2 giới hạn đã cấu hình vào. Sau đó chọn **Save** để lưu lại.

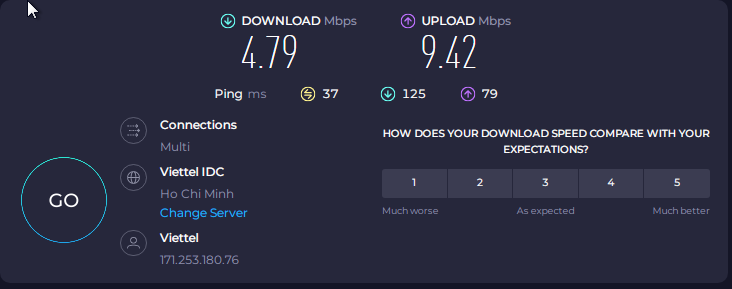


Hình 3‑62: Cấu hình rules upload và download.

Sử dụng website speedtest.net để kiểm tra kết quả. Kết quả trước và sau khi giới hạn băng thông.



Hình 3‑63: Trước khi giới hạn băng thông.



Hình 3‑64: Sau khi giới hạn băng thông.

# KẾT LUẬN

## Đánh giá chung về Pfsense.

* Ứng dụng mã nguồn mở miễn phí, cho phép mở rộng hệ thống mạng dễ dàng.
* Thiết lập ban đầu rất dễ dàng .
* Các chính sách thiết lập và quản lý rất tốt.
* Các tính năng phù hợp với nhu cầu sử dụng của người dùng.
* Tính năng bảo mật web cũng như khả năng tường lửa web rất tốt

## Ưu điểm và nhược điểm.

Bảng 4‑1: Ưu điểm và nhược điểm.

|  |  |
| --- | --- |
| **Ưu điểm** | **Nhược điểm** |
| * Thiết lập ban đầu rất dễ dàng, khả năng mở rộng tuyệt vời của nền tảng. * Các tính năng tường lửa cơ bản tốt, giải pháp là rất mạnh mẽ. * Sao lưu và khôi phục trong vài phút. DHCP luôn hoạt động mà không gặp bất kỳ sự cố nào. * Kiểm soát tốt các Access List. * Giải pháp OpenVPN: đơn giản và rất dễ  quản lý, dễ dàng để thiết lập máy khách thông qua trình hướng dẫn xuất OpenVPN. * Gói và tính năng bổ sung có thể được cài đặt nhanh chóng, bao gồm những thứ như OpenBGPD, Freeradius3 và Lightsquid. * Cân bằng tải và proxy kết nối được tích hợp và khả năng HAProxy dễ dàng. * Giải pháp này đã tăng mức độ bảo mật, cho phép chúng ta kiểm soát nhiều hơn, cung cấp cái nhìn sâu sắc về lưu lượng mạng và là một giải pháp VPN tuyệt vời. * Khả năng tương thích phần cứng tốt. | * Giao diện người dùng còn một chút vụng về. * Bảo mật: bản phát hành không thường xuyên dựa trên FreeBSD (trung lập) * Các tính năng tường lửa nâng cao lớp 7 không được bao gồm trong giải pháp. * Giải pháp đòi hỏi rất nhiều quản trị. * Nếu người dùng không có nhiều kinh nghiệm trong hệ thống Linux, họ sẽ gặp vấn đề khi sử dụng giải pháp này. * Người dùng cần có kỹ năng cao trong khả năng xử lý sự cố. Người dùng không có kỹ năng cao sẽ thấy sản phẩm khó sử dụng. * ClamAV AntiVirus có thể gây ra một số lỗi. * Người dùng phải nhớ được số hiệu cổng truy nhập. |

## Kết luận.

Pfsense là một giải pháp tường lửa hiệu quả và tiết kiệm chi phí cho việc bảo vệ hệ thống mạng bên trong. Với khả năng định tuyến và tính năng tường lửa mạnh mẽ, pfSense cho phép mở rộng mạng mà vẫn đảm bảo sự bảo mật. Giao diện web dễ sử dụng và khả năng cài đặt thêm gói dịch vụ mở rộng tính năng làm cho pfSense trở thành một lựa chọn phổ biến cho mạng doanh nghiệp nhỏ.

Tuy nhiên, pfSense cũng có một số hạn chế. Một số tính năng được sử dụng trong các doanh nghiệp lớn có thể còn hạn chế và chưa được triển khai trên mô hình thực tế. Điều này đòi hỏi thời gian và điều kiện để nghiên cứu và triển khai những tính năng này. Một số tính năng cần được cải thiện và phát triển để đáp ứng được nhu cầu của các doanh nghiệp lớn.

Tuy nhiên, pfSense vẫn được coi là một giải pháp an toàn và hiệu quả trong việc quản lý thông tin và bảo vệ mạng văn phòng. Với sự phát triển tích cực của cộng đồng, mong đợi rằng những hạn chế và yêu cầu cải thiện sẽ được giải quyết và pfSense sẽ ngày càng phát triển và cung cấp nhiều tính năng mới.

**TÀI LIỆU KHAM THẢO**

[1] *Tham khảo - Firewall và các chức năng của Firewall*

[https://blogchiasekienthuc.com/dan-cong-nghe/firewall-la-gi-tim-hieu-ky-hon-ve-firewall.html#ii-co-may-loai-firewall](https://blogchiasekienthuc.com/dan-cong-nghe/firewall-la-gi-tim-hieu-ky-hon-ve-firewall.html" \l "ii-co-may-loai-firewall)

[2] *Tham khảo - Sự khác nhau giữa Firewall cứng và Firewall mềm*

<https://netsystem.vn/tim-hieu-ve-firewall-su-khac-nhau-giua-firewall-cung-va-mem-la-gi>

[3] *Tham khảo - Một số chức năng chính của Pfsense*

<https://viblo.asia/p/network-gioi-thieu-ve-pfsense-N0bDM6LXv2X4>

[4] *Tham khảo - Pfsense* <https://www.pfsense.org/>

[5] *Tham khảo - Pfsense Document* <https://docs.netgate.com/pfsense/en/latest/>