TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN &  
TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH & ĐIỆN TỬ**



ĐỒ ÁN CHUYÊN NGÀNH 3

**Tìm hiểu và triển khai hệ thống tường lửa PFSense**

Sinh viên: **NGUYỄN AN PHÚC** Mã: 21IT639

Giảng viên hướng dẫn: **THS.TRẦN THU THỦY**

Đà Nẵng, tháng 5 năm 2025

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN &  
TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH & ĐIỆN TỬ**

ĐỒ ÁN CHUYÊN NGÀNH 3

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

Sinh viên: **NGUYỄN AN PHÚC** Mã: 21IT639

Giảng viên hướng dẫn: **THS.TRẦN THU THỦY**

Đà Nẵng, tháng 5 năm 2025

**NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

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

LỜI CẢM ƠN

Để đề tài đạt được kết quả như hiện tại, em đã nhận được sự hỗ trợ,   
giúp đỡ, chỉ bảo tận tâm của cô. Với tình cảm sâu sắc, chân thành, cho phép   
chúng em được bày tỏ lòng biết ơn sâu sắc đến tất cả quý thầy cô đã tạo điều kiện   
giúp đỡ chúng em trong quá trình học tập và nghiên cứu.

Trước hết, chúng em xin gửi tới đội ngũ giảng viên trường Đại học Công nghệ thông tin và truyền thông Việt – Hàn lời chào trân trọng, lời chúc sức khỏe và   
lời cảm ơn sâu sắc nhất. Với sự quan tâm, chỉ bảo tận tình chu đáo, cũng như vốn  
kiến thức về nhiều lĩnh vực của mình, đội ngũ giảng viên của trường đã truyền tải cho chúng em được nhiều kiến thức, cũng như kỹ năng cần thiết, để đến ngày hôm nay,  
chúng em đã có thể hoàn thành được Đề tài của mình.

Đặc biệt, chúng em xin gửi lời cảm ơn chân thành tới THS.TRẦN THU THỦY,   
giảng viên đã quan tâm, giúp đỡ, chỉ bảo tận tình để em có thể hoàn thành tốt   
đề tài này trong suốt thời gian vừa qua.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế, đề tài này không thể tránh được những thiếu sót. Em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy/cô, để chúng em có điều kiện bổ sung, nâng cao kiến thức, kỹ năng   
của mình, phục vụ tốt hơn cho công tác thực tế sau này.

Chúng em xin trân trọng cảm ơn!

*Sinh viên,*

Nguyễn An Phúc

**MỤC LỤC**

[LỜI CẢM ƠN ii](#_Toc198276372)

[DANH MỤC HÌNH ẢNH vi](#_Toc198276373)

[DANH MỤC CÁC TỪ VIẾT TẮT viii](#_Toc198276374)

[MỞ ĐẦU x](#_Toc198276375)

[1. Giới thiệu x](#_Toc198276376)

[2. Mục tiêu của đề tài x](#_Toc198276377)

[3. Đối tượng, phạm vi và phương pháp tiếp cận xi](#_Toc198276378)

[4. Đóng góp của đề tài xi](#_Toc198276379)

[5. Bố cục của đề tài xi](#_Toc198276380)

[CHƯƠNG 1: TỔNG QUAN 1](#_Toc198276381)

[1. GIỚI THIỆU TỔNG QUAN VỀ PFSENSE 1](#_Toc198276382)

[1.1. PFSense là gì? 1](#_Toc198276383)

[1.2. Lịch sử phát triển của PFSense 1](#_Toc198276384)

[2. CÁC CHỨC NĂNG CỦA PFSENSE 1](#_Toc198276385)

[2.1. Aliases 1](#_Toc198276389)

[2.2. NAT 2](#_Toc198276390)

[2.3. Firewall Rules 3](#_Toc198276391)

[2.4. Quản lý băng thông và QoS 3](#_Toc198276392)

[2.5. Hỗ trợ VPN 3](#_Toc198276393)

[2.6. IDS/IPS và Giám sát lưu lượng 4](#_Toc198276394)

[2.7. Tính năng hỗ trợ DNS và DHCP 4](#_Toc198276395)

[3. SO SÁNH PFSENSE VỚI CÁC GIẢI PHÁP TƯỜNG LỬA KHÁC 4](#_Toc198276396)

[3.1. So sánh tổng quan 4](#_Toc198276397)

[3.2. Ưu điểm và nhược điểm của pfSense 4](#_Toc198276398)

[4. CÔNG CỤ MÔ PHỎNG VMWARE VÀ GNS3 5](#_Toc198276399)

[4.1. VMware – Công cụ ảo hóa mạnh mẽ 5](#_Toc198276400)

[4.2. GNS3 – Mô phỏng mạng chuyên sâu 6](#_Toc198276401)

[5. Kết chương 1 6](#_Toc198276402)

[CHƯƠNG 2: NGHIÊN CỨU CÁC CÔNG NGHỆ PFSENSE 7](#_Toc198276403)

[1. KIẾN TRÚC HỆ THỐNG PFSENSE 7](#_Toc198276404)

[1.1. Thành phần cốt lõi 7](#_Toc198276405)

[1.2. Luồng xử lý gói tin 8](#_Toc198276406)

[1.3. Sơ đồ kiến trúc tổng quan 9](#_Toc198276407)

[1.4. Ưu điểm và hạn chế của kiến trúc pfSense 9](#_Toc198276408)

[2. CÁC CHẾ ĐỘ HOẠT ĐỘNG CỦA PFSENSE 10](#_Toc198276409)

[2.1. Chế độ Router 10](#_Toc198276410)

[2.2. Chế độ Transparent Bridge 11](#_Toc198276411)

[2.3. Bảng so sánh Router Mode vs Bridge Mode 12](#_Toc198276412)

[3. Mô hình triển khai thực tế 13](#_Toc198276413)

[3.1. Mô hình mạng gia đình hoặc doanh nghiệp nhỏ (SOHO) 13](#_Toc198276414)

[3.2. Mô hình nhiều VLAN cho doanh nghiệp vừa và lớn 14](#_Toc198276415)

[3.3. Mô hình đa WAN – Cân bằng tải và dự phòng 14](#_Toc198276416)

[3.4. Mô hình kết nối VPN từ xa và site-to-site 15](#_Toc198276417)

[4. Công nghệ bảo mật tích hợp 16](#_Toc198276418)

[4.1. OpenVPN/Ipsec 16](#_Toc198276419)

[4.2. IDS/IPS – Phát hiện và ngăn chặn xâm nhập 17](#_Toc198276420)

[4.3. Captive Portal – Kiểm soát truy cập mạng công cộng 19](#_Toc198276421)

[4.4. DNS Resolver và DNS Forwarder 19](#_Toc198276422)

[4.5. Tính năng nâng cao khác 19](#_Toc198276423)

[5. Kết chương 2 20](#_Toc198276424)

[CHƯƠNG 3: XÂY DỰNG LAB TRIỂN KHAI PFSENSE 21](#_Toc198276425)

[1. Thiết kế mô hình phòng lab 21](#_Toc198276426)

[1.1. Mục tiêu triển khai 21](#_Toc198276427)

[1.2. Mô hình hệ thống thực nghiệm 21](#_Toc198276428)

[1.3. Phân vùng mạng chi tiết: 22](#_Toc198276429)

[2. Cài đặt Và cấu hình triển khai mô phỏng 22](#_Toc198276430)

[2.1. Cài đặt chi tiết 22](#_Toc198276431)

[2.2. Cấu hình chức năng cơ bản 24](#_Toc198276432)

[2.3. Trình bày sản phẩm 35](#_Toc198276433)

[3. Kết luận chương 38](#_Toc198276434)

[KẾT LUẬN 39](#_Toc198276435)

[1. Kết quả đạt được 39](#_Toc198276436)

[2. Những mặt đạt được và chưa đạt được 39](#_Toc198276438)

[3. Hướng nghiên cứu 40](#_Toc198276439)

[TÀI LIỆU THAM KHẢO 41](#_Toc198276440)

DANH MỤC HÌNH ẢNH

[Hình 1.1: Biểu tượng của PFSense 1](#_Toc197545334)

[Hình 2.1: Aliases 2](#_Toc197545335)

[Hình 2.2: NAT service 2](#_Toc197545336)

[Hình 2.3: Firewall rules 3](#_Toc197545337)

[Hình 3.1: So sánh pfSense với các tường lửa khác 4](#_Toc197545338)

[Hình 4.1: VMware 5](#_Toc197545339)

[Hình 4.2: GNS3 chạy trên nền VMware 6](#_Toc197545340)

[Hình 1.1: Sơ đồ luồng gói tin pfSense 9](#_Toc197545341)

[Hình 3.1: Mô hình mạng gia đình 13](#_Toc197545342)

[Hình 3.2: Mô hình nhiều VLAN cho doanh nghiệp vừa và lớn 14](#_Toc197545343)

[Hình 3.3: PfSense có thể triển khai các mô hình VPN như: 15](#_Toc197545344)

[Hình 3.4: Site-to-Site VPN 16](#_Toc197545345)

[Hình 4.1: VPN 16](#_Toc197545346)

[Hình 4.2: IPSec VPN 17](#_Toc197545347)

[Hình 4.3: Snort 18](#_Toc197545348)

[Hình 4.4: Suricata 18](#_Toc197545349)

[Hình 4.5: Captive Portal 19](#_Toc197545350)

[Hình 1.1: Sơ đồ mô hình hệ thống 21](#_Toc197545351)

[Hình 2.1: Lựa chọn phiên bản cài đặt 23](#_Toc197545352)

[Hình 2.2: Khởi động PFSense 23](#_Toc197545353)

[Hình 2.3: Tải PFSense 23](#_Toc197545354)

[Hình 2.4: Khởi động lại PFSense 24](#_Toc197545355)

[Hình 2.5: Cổng WAN được cấp dhcp 24](#_Toc197545356)

[Hình 2.6: Giao diện web GUI truy cập trên cổng WAN 25](#_Toc197545357)

[Hình 2.7: Giao diện cổng LAN 25](#_Toc197545358)

[Hình 2.8: Giao diện cổng DMZ 26](#_Toc197545359)

[Hình 2.9: Thiết lập alias 26](#_Toc197545360)

[Hình 2.10: Thiết lập NAT Outbound 27](#_Toc197545361)

[Hình 2.11: Cấu hình Nat port forward 28](#_Toc197545362)

[Hình 2.12: Floating Rule 28](#_Toc197545363)

[Hình 2.13: WAN Rule 29](#_Toc197545364)

[Hình 2.14: DMZ Rule 30](#_Toc197545365)

[Hình 2.15: Traffic Graph 31](#_Toc197545366)

[Hình 2.16: Thiết lập SNMP 32](#_Toc197545367)

[Hình 2.17: Thêm gói frr 32](#_Toc197545368)

[Hình 2.18: Cấu hình OSPF 33](#_Toc197545369)

[Hình 2.19: Thêm areas 34](#_Toc197545370)

[Hình 2.20: Thêm interface 34](#_Toc197545371)

[Hình 2.21: Ping để kiểm tra kết nối trên các mạng nội bộ 35](#_Toc197545372)

[Hình 2.22: Ping từ PC nội bộ không thành công 36](#_Toc197545373)

[Hình 2.23: Truy cập WAN cổng 9090 để vào Prometheus 36](#_Toc197545374)

[Hình 2.24: Truy cập WAN port 3000 vào grafana 37](#_Toc197545375)

[Hình 2.25: Xem giám sát thông qua Grafana 37](#_Toc197545376)

DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| TỪ VIẾT TẮT | ĐẦY ĐỦ | NỘI DUNG |
| IP | Internet Protocol | Giao thức định địa chỉ và truyền dữ liệu giữa các thiết bị mạng |
| LAN | Local Area Network | Mạng cục bộ – kết nối các thiết bị trong phạm vi gần (như văn phòng, nhà ở) |
| WAN | Wide Area Network | Mạng diện rộng – kết nối các mạng LAN ở khoảng cách lớn |
| NAT | Network Address Translation | Cơ chế chuyển đổi địa chỉ IP trong mạng nội bộ ra địa chỉ công cộng |
| SNMP | Simple Network Management Protocol | Giao thức giám sát và quản lý thiết bị mạng |
| MIB | Management Information Base | Cơ sở dữ liệu quản lý dùng trong SNMP để lưu thông tin thiết bị |
| pfSense | Packet Filter Sense | Hệ điều hành tường lửa mã nguồn mở dùng để định tuyến và bảo mật mạng |
| DNS | Domain Name System | Hệ thống phân giải tên miền thành địa chỉ IP |
| DHCP | Dynamic Host Configuration Protocol | Giao thức cấp phát địa chỉ IP động cho các thiết bị |
| GUI | Graphical User Interface | Giao diện người dùng đồ họa |
| RRD | Round Robin Database | Cơ sở dữ liệu dạng vòng dùng để lưu trữ số liệu thời gian (dùng trong biểu đồ) |
| ACL | Access Control List | Danh sách điều khiển truy cập |
| IDS | Intrusion Detection System | Hệ thống phát hiện xâm nhập |
| IPS | Intrusion Prevention System | Hệ thống ngăn chặn xâm nhập |
| HA | High Availability | Độ sẵn sàng cao – đảm bảo hệ thống luôn hoạt động ngay cả khi lỗi xảy ra |
| CPU | Central Processing Unit | Bộ xử lý trung tâm – thành phần chính xử lý dữ liệu |
| RAM | Random Access Memory | Bộ nhớ truy xuất ngẫu nhiên – lưu trữ dữ liệu tạm thời |
| VM | Virtual Machine | Máy ảo – mô phỏng máy tính chạy trên phần mềm ảo hóa |

MỞ ĐẦU

1. Giới thiệu

Trong thời đại số hóa và kết nối toàn cầu hiện nay, an toàn thông tin là một trong những vấn đề quan trọng hàng đầu đối với cá nhân, doanh nghiệp và tổ chức. Với sự phát triển mạnh mẽ của công nghệ thông tin, các mối đe dọa an ninh mạng ngày càng gia tăng, đòi hỏi các hệ thống mạng phải có những biện pháp bảo vệ hiệu quả để chống lại các cuộc tấn công từ bên ngoài.

Tường lửa (Firewall) là một trong những giải pháp quan trọng giúp bảo vệ hệ thống mạng trước các mối đe dọa từ Internet. Một trong những hệ thống tường lửa mã nguồn mở phổ biến hiện nay là **pfSense**, một nền tảng firewall mạnh mẽ, linh hoạt và dễ dàng triển khai. pfSense không chỉ cung cấp các tính năng bảo mật tiêu chuẩn mà còn hỗ trợ nhiều chức năng nâng cao như quản lý băng thông, VPN, lọc nội dung, phát hiện và ngăn chặn xâm nhập.

Nhận thấy tầm quan trọng của việc sử dụng tường lửa trong việc bảo vệ hệ thống mạng, em đã chọn đề tài: **"Tìm hiểu và triển khai hệ thống tường lửa pfSense"** với mục tiêu nghiên cứu, ứng dụng và triển khai pfSense vào thực tế. Thông qua đề tài này, em mong muốn nâng cao hiểu biết về bảo mật mạng cũng như góp phần giúp các tổ chức, cá nhân có thể áp dụng pfSense để bảo vệ hệ thống mạng của mình.

1. Mục tiêu của đề tài

Nhằm hoàn tất chương trình học và tiếp thu thêm nhiều kiến thức về bảo mật mạng, em đã chọn đề tài này với những mục tiêu cụ thể như sau:

* Tìm hiểu tổng quan về hệ thống tường lửa pfSense, các tính năng và ứng dụng của nó trong bảo mật mạng.
* Nghiên cứu các phương pháp triển khai pfSense trong các môi trường mạng thực tế.
* Thực hành cài đặt và cấu hình pfSense để bảo vệ hệ thống mạng.
* Đánh giá hiệu suất và hiệu quả của pfSense trong việc bảo vệ hệ thống mạng trước các mối đe dọa an ninh.

1. Đối tượng, phạm vi và phương pháp tiếp cận

**Đối tượng nghiên cứu:** Hệ thống tường lửa pfSense và các tính năng bảo mật của nó.

**Phạm vi nghiên cứu:**

* Tìm hiểu về pfSense và các tính năng chính của nó.
* Cấu hình và triển khai pfSense trong hệ thống mạng doanh nghiệp và cá nhân.
* Đánh giá hiệu quả bảo mật của pfSense qua các thử nghiệm thực tế.

**Phương pháp nghiên cứu:**

* Tìm hiểu lý thuyết qua các tài liệu khoa học, sách chuyên ngành và các bài báo về bảo mật mạng.
* Thực hành cài đặt, cấu hình và thử nghiệm pfSense trong môi trường mô phỏng và thực tế.
* Thu thập, phân tích và đánh giá kết quả thực nghiệm để đưa ra kết luận.

1. Đóng góp của đề tài

**Sau quá trình nghiên cứu và triển khai, đề tài sẽ đạt được các kết quả sau:**

* Hoàn thành báo cáo chi tiết về hệ thống tường lửa pfSense, từ lý thuyết đến thực hành.
* Xây dựng một hệ thống tường lửa hoàn chỉnh bằng pfSense có thể ứng dụng vào thực tế.
* Đánh giá hiệu quả của pfSense trong bảo vệ hệ thống mạng.
* Cung cấp tài liệu tham khảo và hướng dẫn triển khai pfSense cho các cá nhân, tổ chức quan tâm đến bảo mật mạng.

1. Bố cục của đề tài

Sau phần Mở đầu, báo cáo được trình bày trong ba chương, cụ thể như sau:

***Chương 1: Tổng quan về pfSense***

Chương này trình bày các khái niệm và tổng quan về pfSense, bao gồm lịch sử phát triển, các tính năng chính, tầm quan trọng của tường lửa trong bảo vệ mạng, so sánh pfSense với các giải pháp tường lửa khác và giới thiệu các công cụ mô phỏng như VMware và GNS3.

**Chương 2: Nghiên cứu các công nghệ pfSense**

Nội dung chương bao gồm kiến trúc hệ thống pfSense, các chế độ hoạt động, mô hình triển khai thực tế, cũng như các giao thức và công nghệ bảo mật tích hợp trong pfSense.

**Chương 3: Xây dựng lab triển khai pfSense**

Chương này trình bày các bước triển khai thực tế, bao gồm cài đặt pfSense trên môi trường máy ảo, cấu hình cơ bản như giao diện mạng, DHCP, NAT, triển khai các chính sách lọc lưu lượng, thiết lập và quản lý IPSEC, giám sát và phân tích lưu lượng mạng, kiểm tra và đánh giá hiệu quả hệ thống tường lửa.

Cuối cùng là phần **Kết luận, Tài liệu tham khảo và Phụ lục** liên quan đến đề tài.

# TỔNG QUAN

## GIỚI THIỆU TỔNG QUAN VỀ PFSENSE

### PFSense là gì?

pfSense là một hệ thống tường lửa mã nguồn mở, được phát triển dựa trên FreeBSD và được sử dụng rộng rãi trong nhiều mô hình mạng từ cá nhân, doanh nghiệp nhỏ đến các hệ thống lớn. pfSense ban đầu là một nhánh của dự án m0n0wall, được thiết kế để hoạt động như một tường lửa và bộ định tuyến mạnh mẽ, linh hoạt.



Hình 1.1: Biểu tượng của PFSense

### Lịch sử phát triển của PFSense

PFSense được phát triển từ dự án m0n0wall do Manuel Kasper sáng lập vào năm 2004. Nhận thấy nhu cầu về một hệ thống tường lửa mã nguồn mở mạnh mẽ và linh hoạt hơn, nhóm phát triển đã tạo ra pfSense vào năm 2006. Kể từ đó, pfSense đã trải qua nhiều phiên bản cải tiến với sự hỗ trợ của cộng đồng và công ty Netgate.

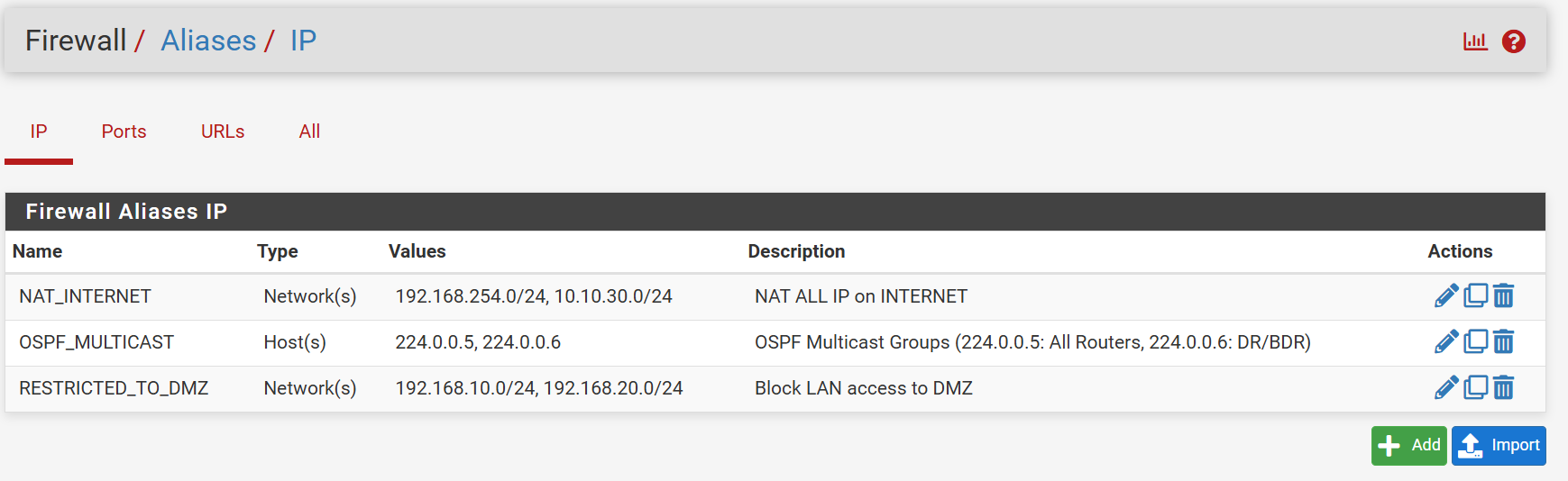
## CÁC CHỨC NĂNG CỦA PFSENSE

pfSense không chỉ đơn thuần là một tường lửa và router. Nó còn chứa đựng một loạt các tính năng hữu ích giúp nâng cao bảo mật, tối ưu hóa hiệu suất mạng, và cung cấp nhiều khả năng quản lý linh hoạt cho người dùng. Từ việc giám sát lưu lượng cho đến VPN và IDS/IPS, pfSense thật sự mang lại giá trị lớn trong việc quản lý và bảo vệ mạng.



### Aliases

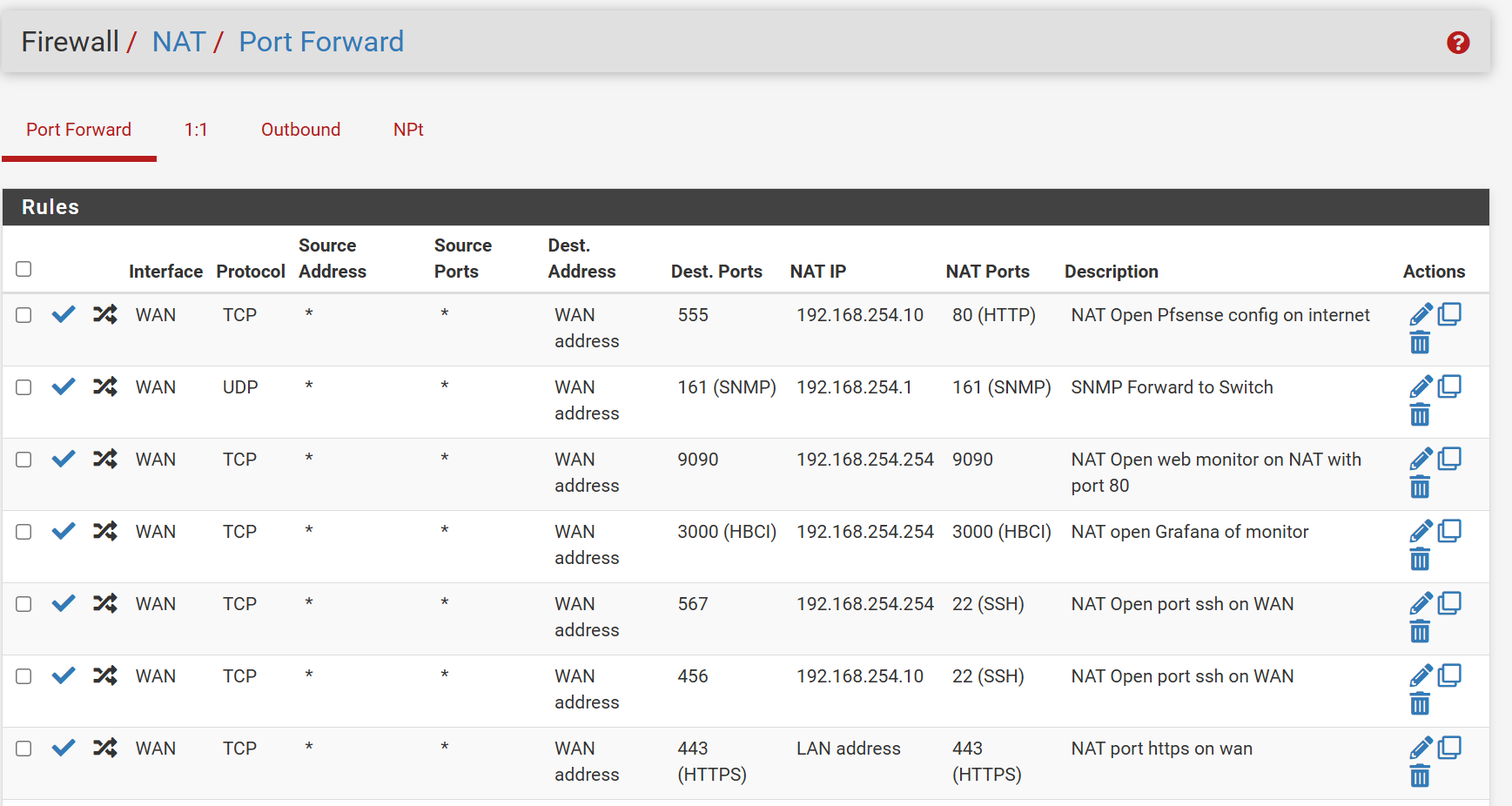
Trong pfsense, firewall không thể có 1 rule gồm nhiều nhóm IP hoặc 1 nhóm port. Vì vậy, điều ta cần làm là gom nhóm các IP, Port hoặc URL vào thành 1 alias . Một alias sẽ cho phép thay thế 1 host, 1 dải mạng, nhiều IP riêng biệt hay 1 nhóm port, URL … Alias giúp ta tiết kiệm được phần lớn thời gian nếu bạn sử dụng một cách chính xác như thay vì sử dụng hàng loạt rule để thiết lập cho nhiều địa chỉ, ta có thể sử dụng 1 rule duy nhất để gom nhóm lại.



Hình 2.1: Aliases

### NAT

Pfsense có hỗ trợ nat static dưới dạng nat 1:1. Điều kiện để thực hiện được nat 1:1 là ta phải có IP public. Khi thực hiện nat 1:1 thì IP private được nat sẽ luôn ra ngoài bằng IP public tương ứng và các port cũng tương ứng trên IP public.



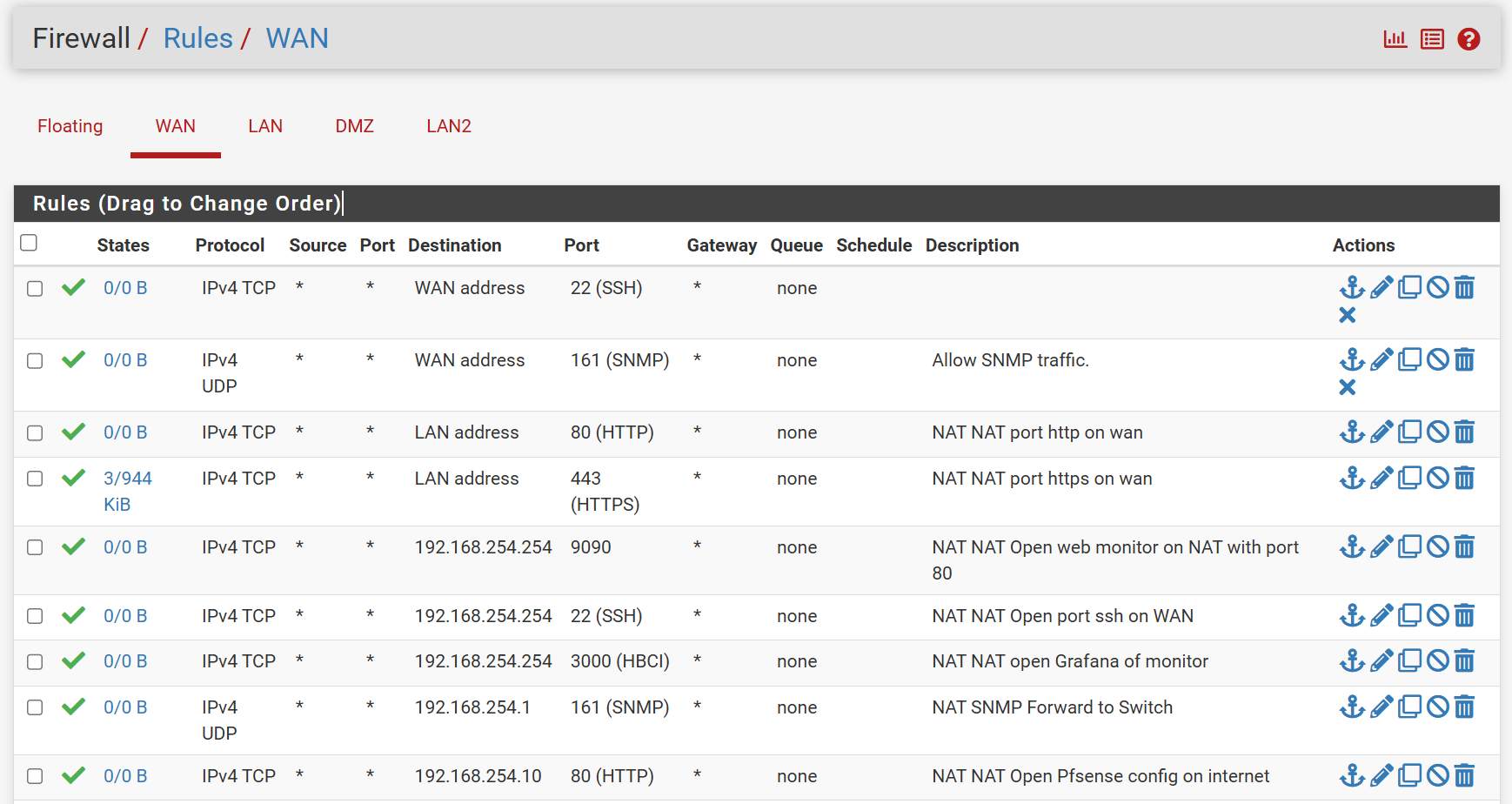
Hình 2.2: NAT service

Pfsense hỗ trợ nat outbound mặc định với Automatic outbound NAT rule generation. Để cấu hình thủ công, ta chọn Manual Outbound NAT rule generation (AON - Advanced Outbound NAT) và xóa các rule mặc định của pfsense đi đồng thời cấu hình thêm các rule outbound.

Ngoài 3 kiểu Nat: port forward, 1:1 và outbound, pfsense còn hỗ trợ NAT Npt. Phương thức này thực hiện NAT đối với Ipv6.

### Firewall Rules

Là nơi lưu trữ tất cả các luật ra, vào trên pfsense. Mặc định PfSense cho phép mọi kết nối ra, vào (tại cổng LAN có sẵn rule any à any). Ta phải tạo các rule để quản lý mạng bên trong.



Hình 2.3: Firewall rules

### Quản lý băng thông và QoS

Quản lý băng thông là một trong những tính năng quan trọng và hấp dẫn mà pfSense cung cấp. Với sự gia tăng nhanh chóng của số lượng thiết bị kết nối vào internet, việc đảm bảo băng thông được phân bổ hợp lý giữa các ứng dụng và dịch vụ trở thành điều cần thiết. pfSense có thể sử dụng Quality of Service (QoS) để khi định hình lưu lượng truy cập, giúp ưu tiên các loại dữ liệu nhất định.

### Hỗ trợ VPN

Một trong những điểm mạnh nổi bật của pfSense là khả năng hỗ trợ Virtual Private Network (VPN). VPN cho phép người dùng tạo kết nối an toàn giữa máy tính cá nhân và mạng nội bộ, mà qua đó họ có thể truy cập vào tài nguyên như máy chủ, dữ liệu mà không cần phải tiếp xúc trực tiếp với mạng mở.

pfSense hỗ trợ nhiều giao thức VPN khác nhau như OpenVPN, IPsec, và L2TP, cho phép người dùng chọn lựa phương án tốt nhất phù hợp với nhu cầu của họ.

### IDS/IPS và Giám sát lưu lượng

pfSense tích hợp hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS), giúp bảo vệ mạng khỏi các cuộc tấn công và sự cố bảo mật. Hệ thống này theo dõi và phân tích lưu lượng mạng để phát hiện các hành vi đáng ngờ, từ đó đưa ra cảnh báo hoặc tự động chặn các kết nối nguy hiểm.

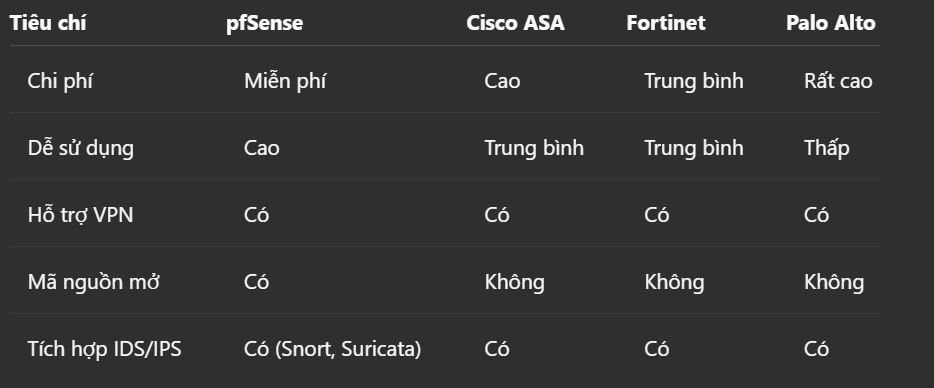
### Tính năng hỗ trợ DNS và DHCP

pfSense không chỉ hoạt động như một tường lửa hay router mà còn cung cấp tính năng quản lý DNS và DHCP mạnh mẽ. Việc tích hợp chức năng quản lý địa chỉ IP và tên miền trong cùng một giải pháp giúp đơn giản hóa cấu hình mạng và tiết kiệm thời gian cho người quản trị.

## SO SÁNH PFSENSE VỚI CÁC GIẢI PHÁP TƯỜNG LỬA KHÁC

### So sánh tổng quan

So với các giải pháp thương mại như Cisco ASA, Fortinet và Palo Alto, pfSense có một số ưu điểm và nhược điểm như sau:



Hình 3.1: So sánh pfSense với các tường lửa khác

### Ưu điểm và nhược điểm của pfSense

Ưu điểm:

* Hoàn toàn miễn phí và mã nguồn mở.
* Hỗ trợ nhiều tính năng nâng cao mà không cần trả phí.
* Cộng đồng lớn hỗ trợ phát triển liên tục.

#### Nhược điểm:

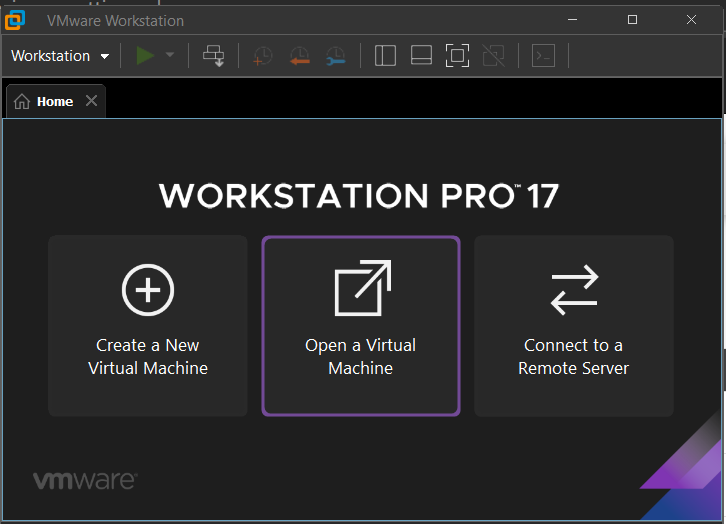
* Yêu cầu kiến thức kỹ thuật để cài đặt và quản lý.
* Hiệu suất có thể thấp hơn giải pháp thương mại nếu triển khai trên phần cứng yếu.
* Không có hỗ trợ chính thức từ hãng trừ khi sử dụng bản thương mại.

## CÔNG CỤ MÔ PHỎNG VMWARE VÀ GNS3

VMware và GNS3 được chọn do khả năng mô phỏng sát với môi trường thực tế, hỗ trợ kiểm thử pfSense trong các kịch bản mạng phức tạp.

### VMware – Công cụ ảo hóa mạnh mẽ

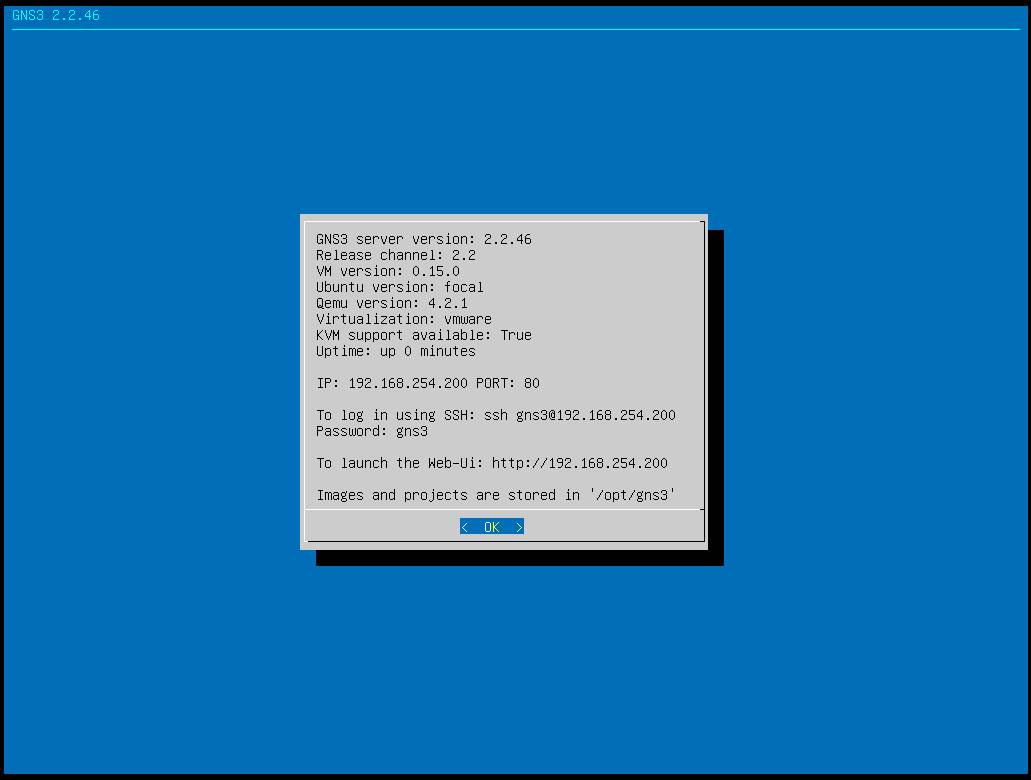
VMware là phần mềm ảo hóa chuyên nghiệp, cho phép tạo máy ảo chạy GNS3 để kiểm thử và triển khai trong môi trường mạng thực tế.



Hình 4.1: VMware

### GNS3 – Mô phỏng mạng chuyên sâu

GNS3 là công cụ mô phỏng mạng mạnh mẽ, giúp mô phỏng các thiết bị mạng và kiểm thử pfSense trong môi trường giả lập.



Hình 4.2: GNS3 chạy trên nền VMware

## Kết chương 1

Chương 1 đã cung cấp cái nhìn tổng quan về pfSense – một giải pháp tường lửa mã nguồn mở được đánh giá cao nhờ tính linh hoạt, hiệu suất và khả năng mở rộng. Qua việc tìm hiểu lịch sử phát triển, các tính năng chính, ưu điểm và nhược điểm, cũng như so sánh pfSense với các giải pháp tường lửa khác, người đọc có thể thấy được lý do tại sao pfSense ngày càng được tin dùng trong các hệ thống mạng hiện đại.

Bên cạnh đó, việc giới thiệu các công cụ mô phỏng như VMware và GNS3 cũng cho thấy tính khả thi và thuận tiện trong việc nghiên cứu, thử nghiệm và triển khai pfSense trong môi trường thực tế hoặc mô phỏng.

Những kiến thức cơ bản này đóng vai trò nền tảng quan trọng, giúp người học và người triển khai có sự chuẩn bị tốt trước khi đi sâu vào nghiên cứu các công nghệ bên trong pfSense cũng như quá trình triển khai thực tế sẽ được trình bày ở các chương tiếp theo.

# NGHIÊN CỨU CÁC CÔNG NGHỆ PFSENSE

## KIẾN TRÚC HỆ THỐNG PFSENSE

Kiến trúc của pfSense được thiết kế dựa trên nền tảng FreeBSD, kết hợp các thành phần mạng và bảo mật tiên tiến để tạo ra một hệ thống tường lửa linh hoạt, mạnh mẽ. Phần này phân tích chi tiết các thành phần cốt lõi, luồng xử lý gói tin và cơ chế hoạt động của pfSense.

### Thành phần cốt lõi

FreeBSD: Hệ điều hành mã nguồn mở tập trung vào hiệu suất và bảo mật, cung cấp:

Network Stack: Hỗ trợ TCP/IP stack tối ưu cho xử lý gói tin tốc độ cao.

GEOM Framework: Quản lý disk I/O, quan trọng cho hệ thống log và caching.

#### Nhân FreeBSD

* Nền tảng ổn định: FreeBSD cung cấp hiệu suất cao, khả năng xử lý đa nhiệm và hỗ trợ phần cứng đa dạng, từ máy chủ đến thiết bị nhúng (Raspberry Pi).
* Bảo mật mạnh mẽ: Tích hợp sẵn các cơ chế như jail, MAC (Mandatory Access Control), và IPFW để cách ly và kiểm soát tài nguyên.

#### Packet Filter (PF) – Bộ lọc gói tin

Vai trò: Là "trái tim" của pfSense, PF xử lý:

* Lọc gói tin (Firewall Rules).
* NAT (Network Address Translation) – Chuyển đổi địa chỉ mạng.
* Quality of Service (QoS) – Ưu tiên băng thông.

Ưu điểm:

* Hỗ trợ stateful inspection (theo dõi trạng thái kết nối).
* Cú pháp cấu hình linh hoạt, tương thích với OpenBSD.

#### Giao diện quản trị (Web GUI & CLI)

Web GUI:

* Trực quan, hỗ trợ cấu hình firewall rules, VPN, IDS/IPS qua trình duyệt.
* Tích hợp AJAX để giám sát thời gian thực (traffic, CPU, RAM).

Command Line Interface (CLI):

* Truy cập qua SSH hoặc console, dùng để khắc phục sự cố hoặc tự động hóa bằng script.

### Luồng xử lý gói tin

Quy trình xử lý gói tin trong pfSense tuân theo mô hình phân tầng, đảm bảo kiểm soát chặt chẽ từ lớp mạng đến ứng dụng. Dưới đây là các bước chi tiết:

Bước 1: Tiếp nhận gói tin từ interface

* Gói tin đến từ cổng mạng (ví dụ: WAN, LAN) được đưa vào driver network interface của FreeBSD.
* VLAN tagging: Hỗ trợ phân chia lưu lượng theo VLAN (nếu cấu hình).

Bước 2: Lọc gói tin bằng PF

* Stateful Inspection: PF kiểm tra gói tin dựa trên:
* Rule firewall (ví dụ: cho phép SSH từ IP cụ thể).
* Bảng trạng thái (state table): Ghi nhớ kết nối hợp lệ để giảm độ trễ.
* NAT/PAT:
* Outbound NAT: Chuyển đổi IP nội bộ thành IP công cộng.
* Port Forwarding: Chuyển hướng cổng (ví dụ: từ WAN:80 → LAN:192.168.1.100:80).

Bước 3: Xử lý bởi các module mở rộng

* VPN (OpenVPN/IPsec): Mã hóa gói tin nếu thuộc kết nối VPN.
* IDS/IPS (Snort/Suricata): Quét nội dung gói tin để phát hiện tấn công (ví dụ: SQL injection).
* QoS (Limiters): Áp dụng giới hạn băng thông cho từng dịch vụ (ví dụ: ưu tiên VoIP).

Bước 4: Forwarding hoặc chặn gói tin

* Gói tin hợp lệ được chuyển đến gateway hoặc máy đích.
* Gói tin vi phạm rule bị drop/log lại (ghi nhật ký tại /var/log/filter.log).

### Sơ đồ kiến trúc tổng quan

Lớp Ứng dụng: Web GUI, API, CLI

Lớp Dịch vụ: VPN, IDS/IPS, DHCP/DNS

Lớp Lõi: Packet Filter (PF), NAT, QoS

Lớp Phần cứng: Driver NIC, CPU Scheduling



Hình 1.1: Sơ đồ luồng gói tin pfSense

### Ưu điểm và hạn chế của kiến trúc pfSense

#### Ưu điểm

Modular Design: Dễ dàng mở rộng tính năng (thêm package như Squid cho caching).

Hiệu suất cao: Tận dụng tối đa phần cứng nhờ tối ưu hóa từ FreeBSD.

Tích hợp đa công nghệ: Hỗ trợ cả IPv4/IPv6, VLAN, VPN đa giao thức.

#### Hạn chế

Độ phức tạp: Cấu hình QoS hoặc IDS/IPS yêu cầu kiến thức chuyên sâu.

Tài nguyên phần cứng: Cần CPU mạnh nếu bật nhiều tính năng (ví dụ: Suricata + OpenVPN).

## CÁC CHẾ ĐỘ HOẠT ĐỘNG CỦA PFSENSE

Hệ thống pfSense hỗ trợ nhiều chế độ hoạt động linh hoạt, phù hợp với các yêu cầu khác nhau của mạng doanh nghiệp và cá nhân. Dưới đây là phân tích chi tiết về hai chế độ chính: Router Mode và Transparent Bridge Mode, bao gồm nguyên lý hoạt động, cấu hình cụ thể và ứng dụng thực tế.

### Chế độ Router

#### Tổng quan

Trong chế độ Router, pfSense hoạt động như một bộ định tuyến lớp 3 (Layer 3 Gateway), có khả năng:

* Định tuyến giữa các mạng con (subnet) hoặc VLAN.
* Hỗ trợ giao thức định tuyến động (OSPF, BGP).
* Áp dụng NAT/PAT để kết nối mạng nội bộ ra Internet.

1. Nguyên lý NAT (Network Address Translation):

SNAT (Source NAT): Thay đổi IP nguồn khi gói tin đi ra Internet.

* SNAT: 192.168.1.100:1234 → 203.0.113.5:5432

DNAT (Destination NAT): Chuyển hướng cổng (Port Forwarding)

* DNAT: 203.0.113.5:80 → 192.168.1.10:80

#### Định tuyến giữa các VLAN/Subnet

Nguyên lý hoạt động:

* Mỗi VLAN/subnet được gán vào một interface vật lý hoặc logical (VLAN tagging) trên pfSense.
* pfSense sử dụng bảng định tuyến (routing table) để chuyển tiếp gói tin giữa các VLAN.

#### Định tuyến động (OSPF/BGP)

1. OSPF (Open Shortest Path First):

* Sử dụng thuật toán Dijkstra để tính đường đi ngắn nhất.
* Area Design: Backbone Area (0.0.0.0) + Non-Backbone Areas.

Ưu điểm: Tự động cập nhật bảng định tuyến khi topology mạng thay đổi.

1. BGP (Border Gateway Protocol):

* Path Vector Protocol, sử dụng AS-Path để chọn route.
* Triển khai Multi-homing: eBGP (giữa các AS) + iBGP (trong AS).

#### So sánh OSPF vs BGP:

|  |  |  |
| --- | --- | --- |
| Tiêu chí | OSPF | BGP |
| Phạm vi | Mạng nội bộ (AS) | Liên AS (Internet) |
| Độ phức tạp | Dễ cấu hình | Yêu cầu kiến thức cao |
| Use-case | Doanh nghiệp vừa và nhỏ | ISP/Large Enterprise |

### Chế độ Transparent Bridge

#### Tổng quan

Trong chế độ này, pfSense hoạt động như một bridge lớp 2 có khả năng:

* Lọc lưu lượng dựa trên MAC address hoặc rule firewall.
* Không thay đổi IP client → Không ảnh hưởng đến cấu trúc mạng hiện có.

#### Nguyên lý hoạt động

Bridge Interfaces: Ghép 2+ interface mạng thành một bridge (ví dụ: em0 + em1).

Lọc gói tin: Áp dụng firewall rules trên bridge interface.

#### Ứng dụng thực tế

Triển khai trong mạng hiện có:

* Đặt pfSense giữa switch core và gateway để lọc lưu lượng mà không cần thay đổi IP.
* Ưu điểm: Không làm gián đoạn dịch vụ mạng.

Hạn chế:

* Không hỗ trợ NAT.
* Yêu cầu span port trên switch để giám sát lưu lượng.

### Bảng so sánh Router Mode vs Bridge Mode

|  |  |  |
| --- | --- | --- |
| Tiêu chí | Router Mode | Transparent Bridge Mode |
| Layer | Lớp 3 (IP) | Lớp 2 (MAC) |
| NAT hỗ trợ | Có | Không |
| Triển khai | Thay đổi IP client | Không thay đổi IP |
| Hiệu suất | Cao (xử lý bằng CPU) | Trung bình (phụ thuộc phần cứng) |
| Use-case | Gateway chính, Multi-VLAN | Lọc lưu lượng không xâm phạm |

## Mô hình triển khai thực tế

### Mô hình mạng gia đình hoặc doanh nghiệp nhỏ (SOHO)



Hình 3.1: Mô hình mạng gia đình

Đây là mô hình đơn giản, phù hợp với hộ gia đình hoặc văn phòng nhỏ, nơi yêu cầu cơ bản là NAT, DHCP, tường lửa và VPN.

#### Cấu hình cơ bản:

WAN: Kết nối đến modem nhà mạng.

LAN: Cấp phát DHCP cho các thiết bị nội bộ.

VPN: Cho phép người dùng truy cập từ xa vào mạng nội bộ.

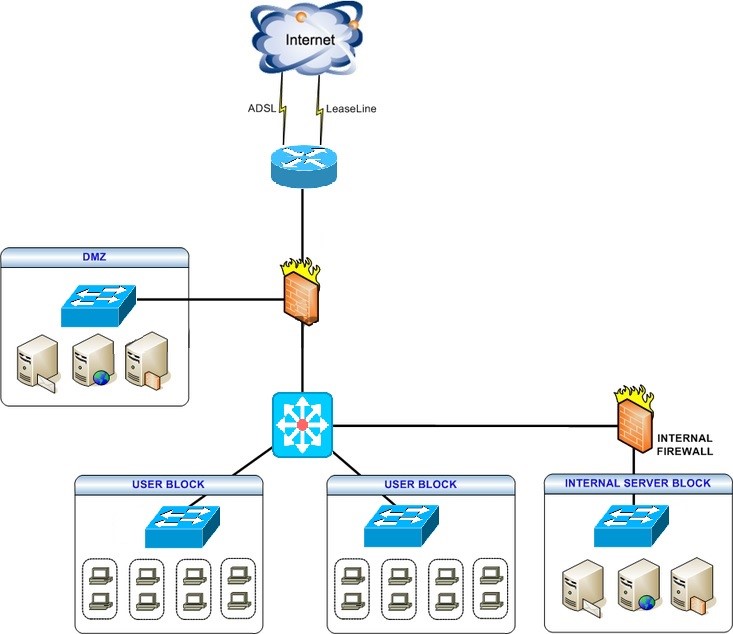
#### Lợi ích:

Tăng cường bảo mật mạng gia đình.

Hạn chế truy cập Internet theo thời gian, địa chỉ MAC/IP.

Triển khai VPN để truy cập từ xa.

### Mô hình nhiều VLAN cho doanh nghiệp vừa và lớn



Hình 3.2: Mô hình nhiều VLAN cho doanh nghiệp vừa và lớn

pfSense hỗ trợ cấu hình nhiều VLAN để phân chia mạng nội bộ theo chức năng hoặc phòng ban (ví dụ: VLAN cho kế toán, VLAN cho kỹ thuật, VLAN cho khách).

#### Cấu hình cơ bản:

Một card mạng vật lý có thể gắn nhiều VLAN.

Thiết lập các rule tường lửa giữa các VLAN để kiểm soát truy cập.

Có thể dùng Captive Portal cho VLAN khách.

#### Lợi ích:

Cô lập các nhóm người dùng, tăng bảo mật.

Dễ quản lý truy cập mạng giữa các phòng ban.

Tối ưu hiệu năng và giảm broadcast domain.

### Mô hình đa WAN – Cân bằng tải và dự phòng

pfSense hỗ trợ nhiều kết nối WAN và có thể cấu hình để:

Cân bằng tải (Load Balancing): Phân phối lưu lượng ra ngoài giữa nhiều đường truyền.

Dự phòng (Failover): Khi một WAN bị mất kết nối, WAN còn lại tự động đảm nhiệm lưu lượng.

#### Cấu hình cơ bản:

Cấu hình hai interface WAN với các gateway khác nhau.

Thiết lập Gateway Group để định nghĩa hành vi chuyển đổi tự động.

#### Lợi ích:

Tăng độ ổn định kết nối Internet.

Đảm bảo dịch vụ không bị gián đoạn khi một nhà mạng gặp sự cố.

### Mô hình kết nối VPN từ xa và site-to-site



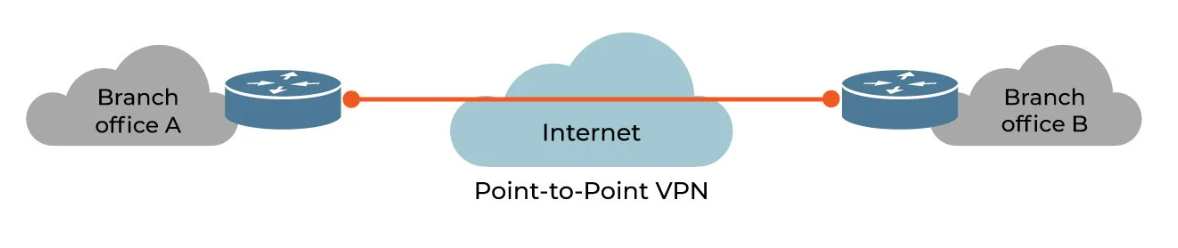
Hình 3.3: PfSense có thể triển khai các mô hình VPN như:

#### VPN truy cập từ xa (Remote Access)

Nhân viên có thể truy cập vào hệ thống nội bộ từ bên ngoài thông qua kết nối VPN an toàn.

Hỗ trợ OpenVPN, IPSec và L2TP.

#### VPN giữa các chi nhánh (Site-to-Site VPN)



Hình 3.4: Site-to-Site VPN

Kết nối nhiều chi nhánh với nhau qua Internet bằng đường hầm mã hóa VPN.

Đảm bảo truyền thông an toàn và riêng tư giữa các văn phòng.

**Lợi ích:**

Bảo mật thông tin trao đổi giữa trụ sở chính và chi nhánh.

Hỗ trợ làm việc từ xa hiệu quả, bảo vệ truy cập nội bộ.

## Công nghệ bảo mật tích hợp

PfSense không chỉ là một tường lửa đơn thuần mà còn là một giải pháp bảo mật toàn diện, được tích hợp nhiều giao thức và công nghệ hiện đại giúp bảo vệ hệ thống mạng trước các mối đe dọa từ bên ngoài cũng như kiểm soát truy cập bên trong. Dưới đây là các công nghệ và giao thức bảo mật quan trọng được pfSense hỗ trợ.

### OpenVPN/Ipsec

VPN là công nghệ cho phép thiết lập kết nối mạng riêng ảo qua hạ tầng mạng công cộng, giúp truyền dữ liệu an toàn và mã hóa.



Hình 4.1: VPN

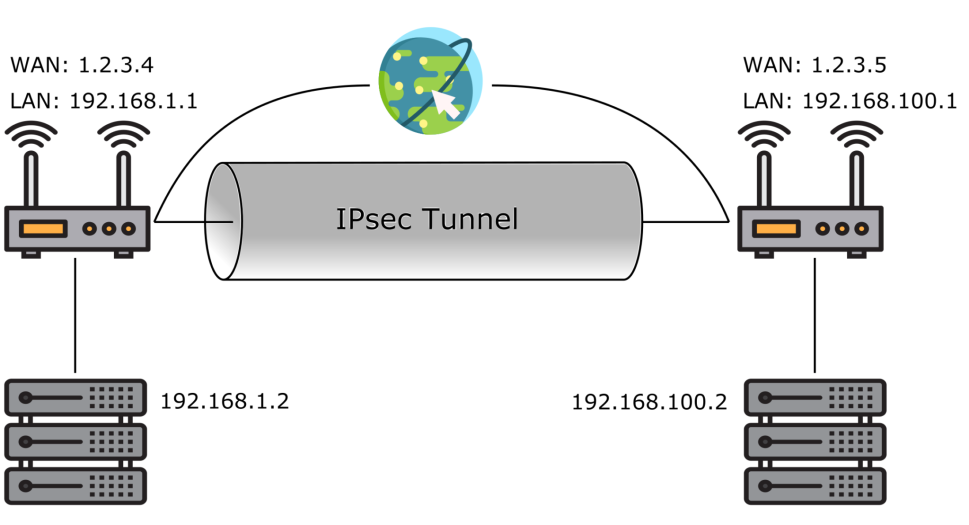
#### OpenVPN

Là giao thức VPN mã nguồn mở, bảo mật cao và linh hoạt.

Hỗ trợ chứng chỉ số (SSL/TLS) và xác thực người dùng.

Dễ cấu hình và tương thích với nhiều hệ điều hành (Windows, Linux, macOS, Android, iOS).

#### IPsec



Hình 4.2: IPSec VPN

Chuẩn VPN phổ biến trong doanh nghiệp, sử dụng để thiết lập VPN site-to-site hoặc truy cập từ xa.

Hỗ trợ các thuật toán mã hóa mạnh như AES, SHA, 3DES.

Có thể tích hợp với hệ thống xác thực LDAP/RADIUS.

#### L2TP/Ipsec

Kết hợp giữa L2TP và IPsec để tạo VPN với tính năng mã hóa mạnh và dễ triển khai cho người dùng cuối.

### IDS/IPS – Phát hiện và ngăn chặn xâm nhập

pfSense hỗ trợ các hệ thống phát hiện và ngăn chặn xâm nhập thông qua các gói mở rộng như Snort hoặc Suricata.

#### Snort



Hình 4.3: Snort

Là hệ thống phát hiện xâm nhập mã nguồn mở phổ biến.

Sử dụng các tập luật (ruleset) để phát hiện tấn công như DoS, Port Scan, SQL Injection,...

Có thể hoạt động ở chế độ phát hiện (IDS) hoặc ngăn chặn (IPS).

#### Suricata



Hình 4.4: Suricata

Là IDS/IPS thế hệ mới, hỗ trợ đa luồng, tốc độ cao.

Tích hợp hỗ trợ giao thức như HTTP, TLS, DNS, SMB để phân tích sâu gói tin.

### Captive Portal – Kiểm soát truy cập mạng công cộng



Hình 4.5: Captive Portal

Captive Portal cho phép pfSense kiểm soát truy cập mạng bằng cách chuyển hướng người dùng đến trang đăng nhập trước khi truy cập Internet.

Hữu ích trong các môi trường Wi-Fi công cộng, quán cà phê, khách sạn, trường học,...

Hỗ trợ xác thực qua tài khoản nội bộ, RADIUS hoặc voucher.

### DNS Resolver và DNS Forwarder

pfSense có thể hoạt động như một máy chủ DNS nội bộ với khả năng:

DNS Resolver (Unbound): Cho phép truy vấn DNS đệ quy trực tiếp đến root DNS server, tăng tính bảo mật và riêng tư.

DNS Forwarder: Chuyển tiếp truy vấn DNS đến máy chủ DNS được chỉ định (như Google DNS, Cloudflare).

Tính năng bổ sung:

Hỗ trợ DNSSEC (DNS Security Extensions) để xác thực truy vấn DNS.

Hỗ trợ Blacklist để chặn truy cập các tên miền độc hại.

### Tính năng nâng cao khác

* pfSense tích hợp **tính năng log chi tiết** cho Firewall, DHCP, VPN, Gateway, DNS, Captive Portal,...
* pfSense hỗ trợ nhiều thuật toán mã hóa và phương thức xác thực để bảo vệ dữ liệu
* Packet Filtering: Kiểm soát lưu lượng theo Layer 3/4.
* Traffic Shaping: Ưu tiên lưu lượng VoIP, video call,...
* GeoIP Blocking: Chặn lưu lượng từ các quốc gia cụ thể.
* Tự động cập nhật blacklist IP/domain từ nguồn bên ngoài (pfBlockerNG).

## Kết chương 2

Trong chương 2, báo cáo đã trình bày và phân tích các công nghệ cốt lõi cấu thành nên hệ thống pfSense – một nền tảng tường lửa mã nguồn mở mạnh mẽ và linh hoạt. Từ kiến trúc hệ thống, các chế độ hoạt động, các mô hình triển khai thực tế, đến việc tích hợp các giao thức và công nghệ bảo mật, pfSense cho thấy khả năng đáp ứng đa dạng nhu cầu bảo vệ mạng trong cả môi trường cá nhân và doanh nghiệp.

Bên cạnh đó, khả năng mở rộng qua các plugin và gói mở rộng như pfBlockerNG, Snort, Squid, Suricata,... giúp pfSense không chỉ dừng lại ở vai trò của một tường lửa mà còn trở thành một giải pháp toàn diện cho quản trị mạng, giám sát lưu lượng, và tăng cường an toàn thông tin.

Những nội dung được nghiên cứu trong chương này sẽ là cơ sở quan trọng để tiến hành triển khai thực tế pfSense trong chương tiếp theo. Qua đó, người đọc có thể hình dung rõ hơn về cách cấu hình, vận hành, và đánh giá hiệu quả hoạt động của hệ thống tường lửa pfSense trong môi trường thực tế.

# ****XÂY DỰNG LAB TRIỂN KHAI PFSENSE****

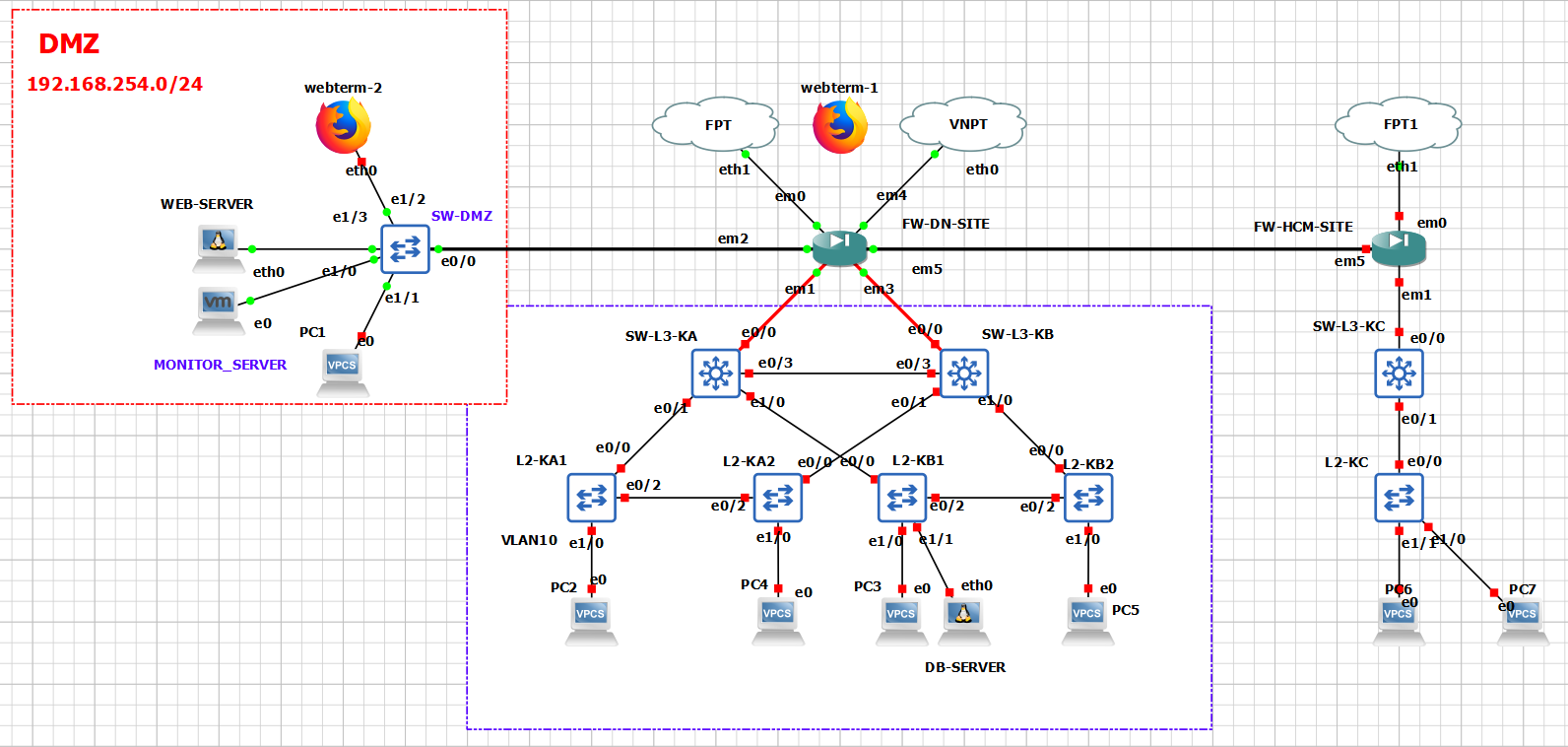
## ****Thiết kế mô hình phòng lab****

### Mục tiêu triển khai

Mục tiêu chính của chương này là xây dựng một môi trường thí nghiệm (lab) sử dụng pfSense để mô phỏng việc bảo vệ hệ thống mạng. Các mục tiêu cụ thể bao gồm:

* Cài đặt pfSense trong môi trường ảo hóa.
* Cấu hình các chức năng cơ bản: giao diện mạng, DHCP, NAT.
* Thiết lập các chính sách tường lửa và lọc lưu lượng.
* Cấu hình VPN IPsec để bảo vệ kết nối từ xa.
* Giám sát và phân tích lưu lượng nhằm đánh giá hiệu quả bảo mật.

### Mô hình hệ thống thực nghiệm



Hình 1.1: Sơ đồ mô hình hệ thống

PFSense Firewall: Là thiết bị trung tâm điều phối lưu lượng giữa các VLAN nội bộ, vùng DMZ và mạng bên ngoài (Internet). Đồng thời đảm nhận vai trò router, NAT, DHCP, VPN và quản lý chính sách bảo mật.

Switch Layer 3: Chịu trách nhiệm định tuyến nội bộ giữa các VLAN trong vùng LAN. Switch này giao tiếp trực tiếp với pfSense qua trunk port.

Switch Layer 2: Phân phối kết nối đến các máy trạm và server trong từng VLAN riêng biệt.

DB Server & Client: Được phân bố trong các VLAN khác nhau.

Switch DMZ: Quản lý kết nối đến vùng DMZ, nơi chứa các dịch vụ công khai và giám sát.

Monitor Server (192.168.254.254/24): Đóng vai trò theo dõi hoạt động mạng và tài nguyên hệ thống, được đặt trong vùng DMZ.

Web server chỉ phục vụ nội bộ – người dùng trong VLAN 10–40 có thể truy cập

### Phân vùng mạng chi tiết:

#### Vùng LAN (quản lý qua switch L3)

|  |  |  |
| --- | --- | --- |
| VLAN | Địa chỉ mạng | Mô tả |
| 10 | 192.168.10.0/24 | Nhóm người dùng văn phòng |
| 20 | 192.168.20.0/24 | Nhóm kỹ thuật |
| 30 | 192.168.30.0/24 | Nhóm máy chủ cơ sở dữ liệu |
| 40 | 192.168.40.0/24 | Phòng ban quản lý – IT admin |

#### Vùng DMZ

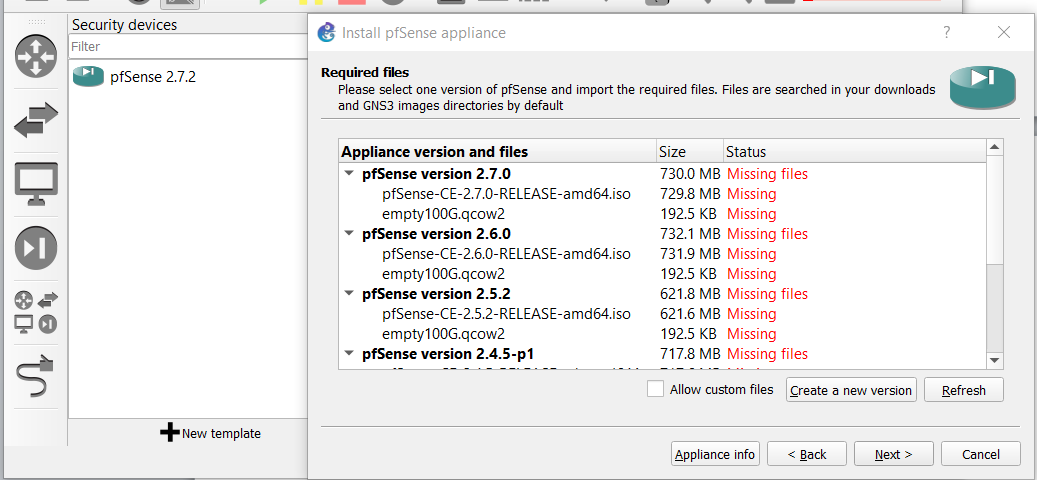
|  |  |  |
| --- | --- | --- |
| Thành phần | Địa chỉ IP | Mô tả |
| Switch DMZ | 192.168.254.1/24 | Quản lý thiết bị vùng DMZ |
| Monitor Server | 192.168.254.254/24 | Giám sát hệ thống |
| Web Server | 192.168.254.100/24 | Web nội bộ phục vụ người dùng |

## Cài đặt Và cấu hình triển khai mô phỏng

### Cài đặt chi tiết

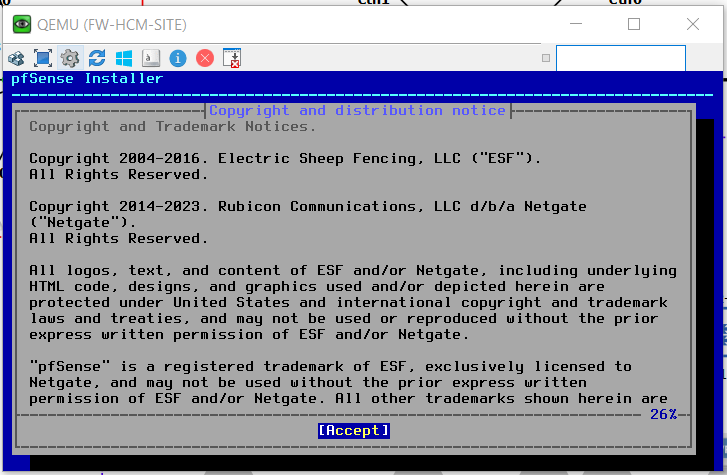
Bước 1: Chọn vào: New template ở phần security devices

Bước 2: Chọn lựa chọn phiên bản và tải đúng phiên bản từ trên internet



Hình 2.1: Lựa chọn phiên bản cài đặt

Bước 3: Khởi động PFSense và tiếp tục cấu hình



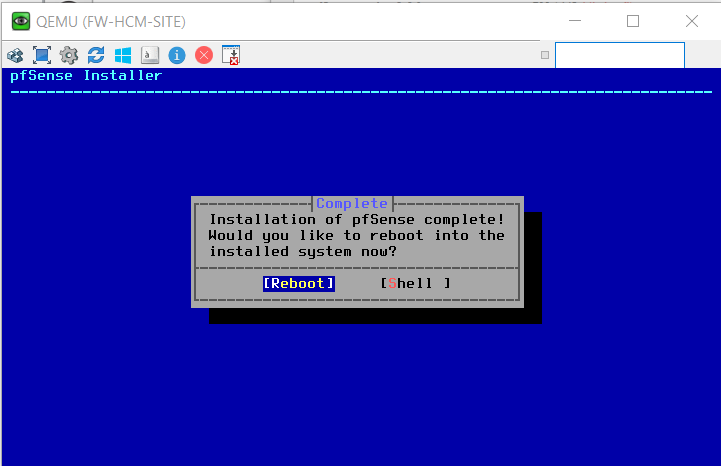
Hình 2.2: Khởi động PFSense

* Nhấn vào accept
* Tự động phân vùng và cài đặt



Hình 2.3: Tải PFSense

Bước 4: Sau khi cài đặt xong hãy reboot lại chuyển sang cấu hình



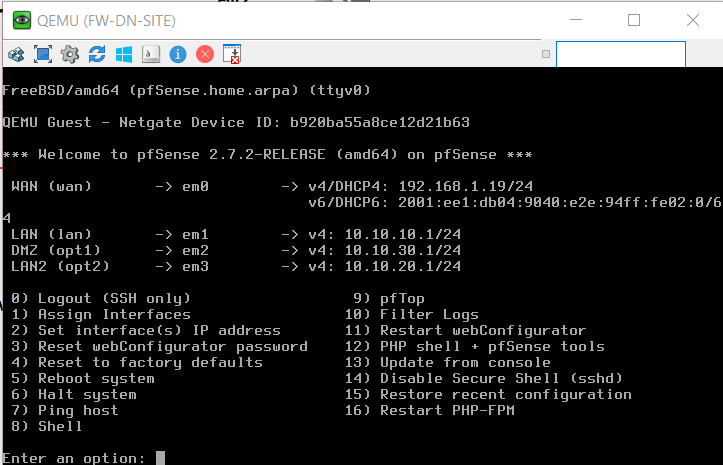
Hình 2.4: Khởi động lại PFSense

### Cấu hình chức năng cơ bản

#### Cấu hình giao diện mạng

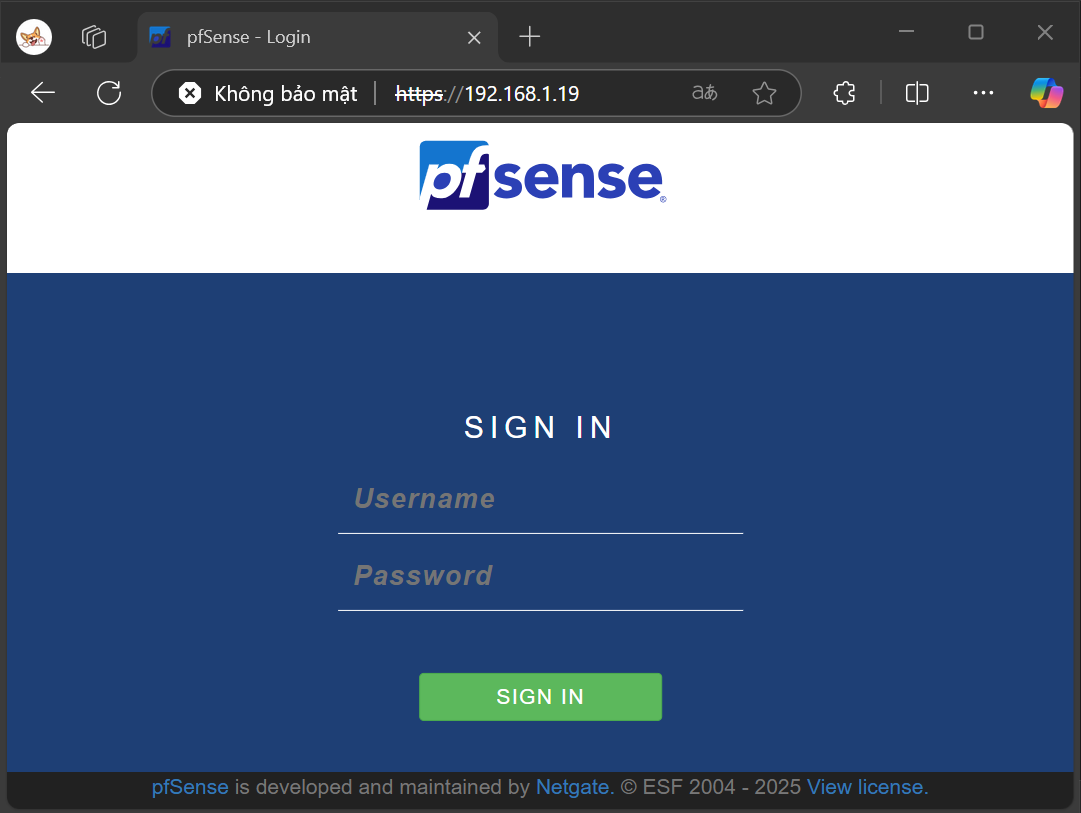
1. Cổng WAN (em0)

Cấu hình truy cập được tường lửa giao diện web với cổng wan với địa chỉ ip động được cấp là 192.168.1.19: giả sử đây là địa chỉ public được cấp từ nhà mạng.



Hình 2.5: Cổng WAN được cấp dhcp

Sau đó truy cập vào địa chỉ WAN trên web brower để truy cập Firewall GUI

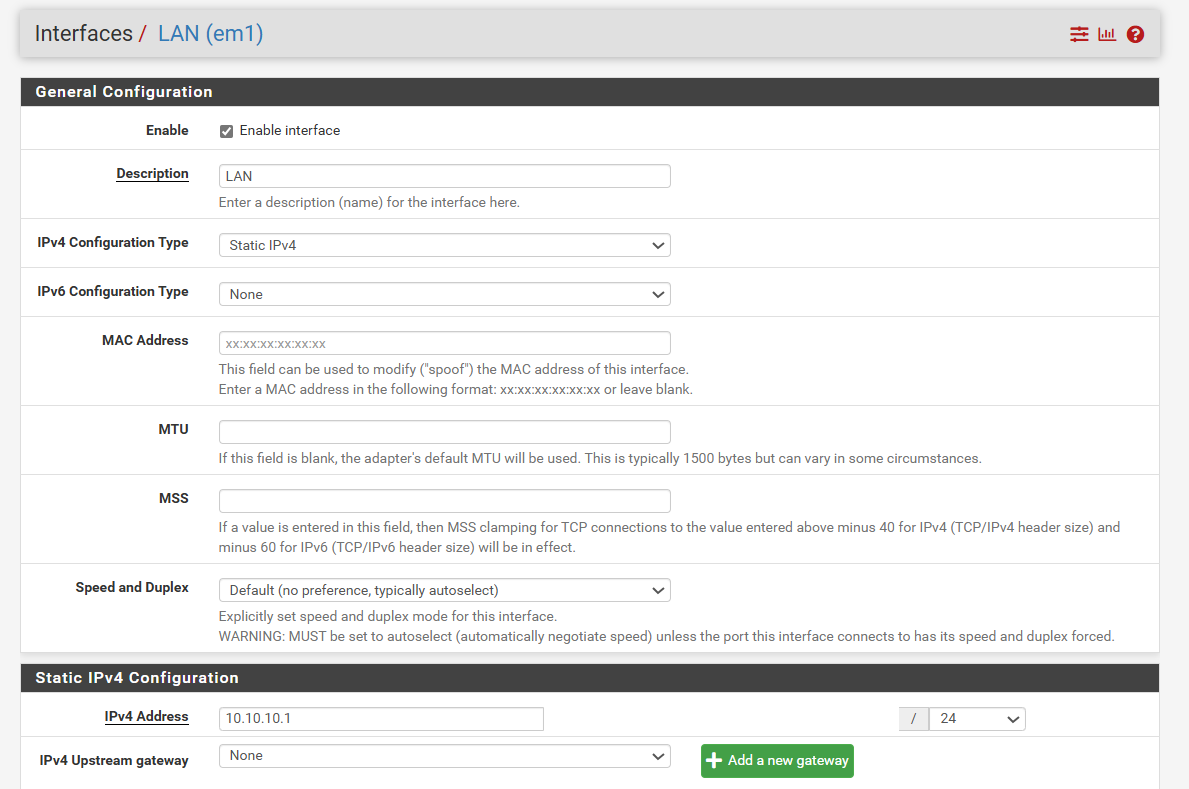


Hình 2.6: Giao diện web GUI truy cập trên cổng WAN

1. Cổng LAN (em1) và LAN2

Cổng LAN(em1)

Cấp IP tĩnh với địa chỉ 10.10.10.1/24, có thể truy cập nội bộ trang web của Firewall thông qua địa chỉ cổng này.



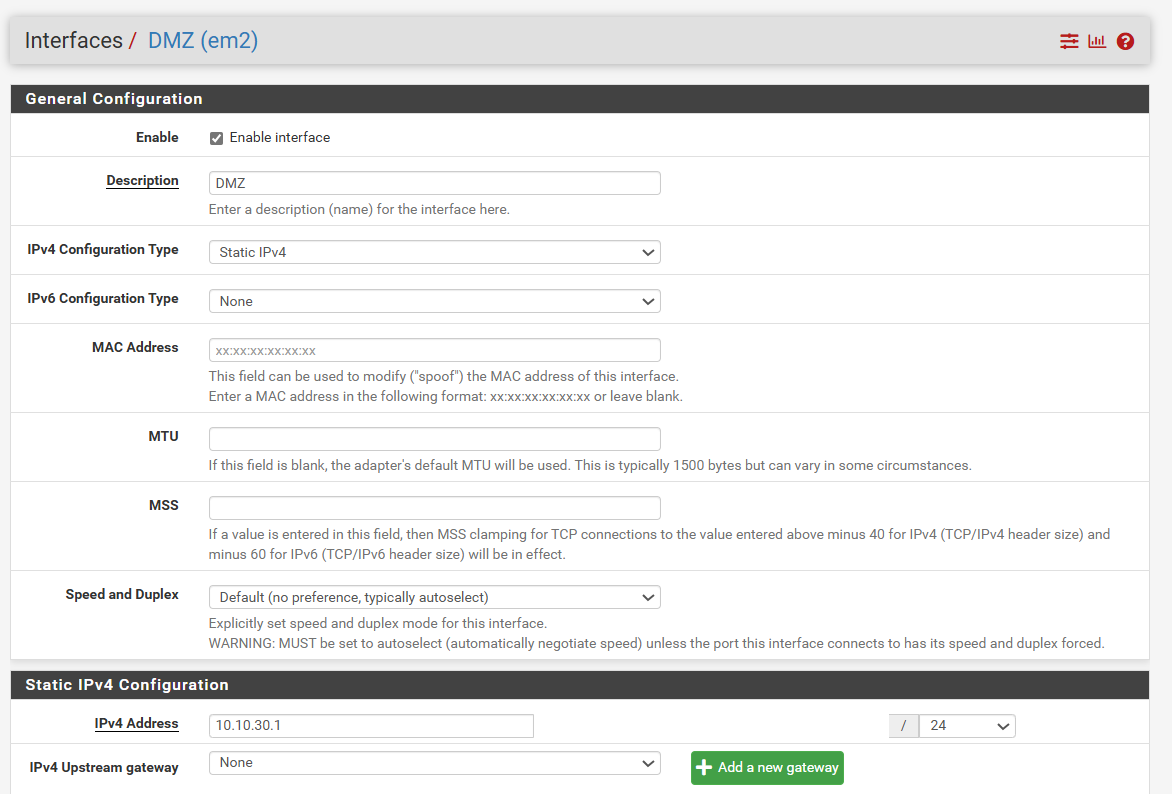
Hình 2.7: Giao diện cổng LAN

Cổng LAN2(em3)

Cổng này được cấp ip tĩnh 10.10.20.1/24, dùng để đưa các thiết bị nội bộ bên trong ra để truy cập được internet

1. Cổng DMZ(em2)

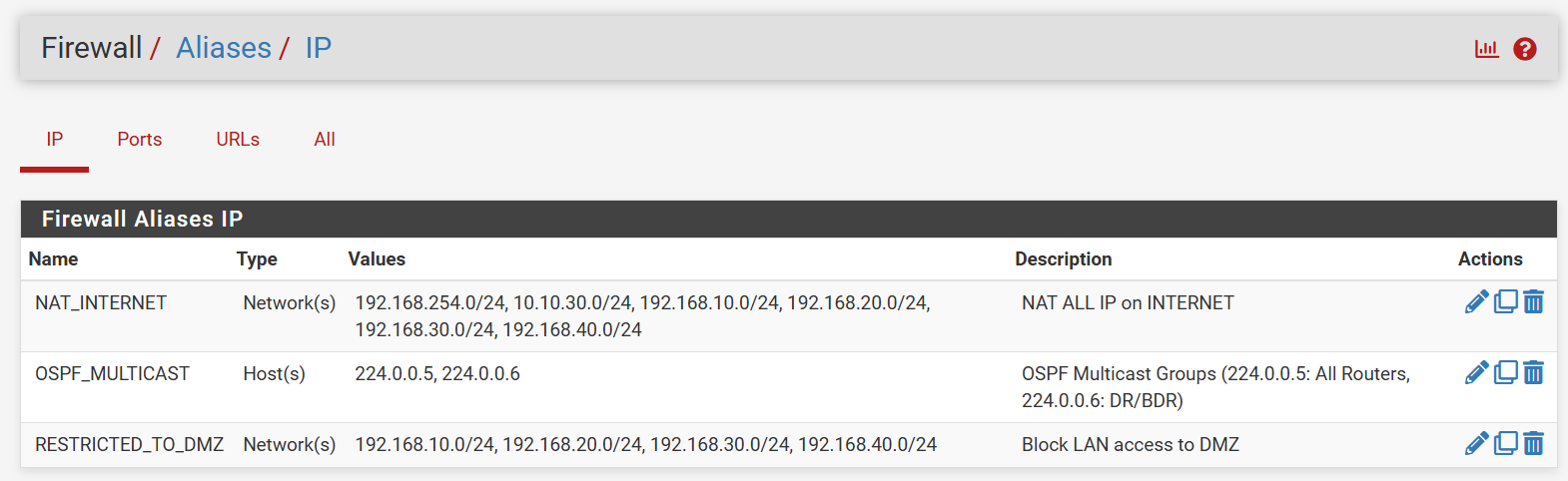
Cổng này được cấp ip tĩnh 10.10.30.1/24, cổng này dùng hiệu năng lớn giúp các thiết bị trong DMZ có thể truy cập cũng như lấy thông tin từ các thiết bị bên ngoài .



Hình 2.8: Giao diện cổng DMZ

#### Thiết lập alias

Để đơn giản hóa việc quản lý các dải mạng và nhóm địa chỉ IP trong quá trình cấu hình firewall, hệ thống sử dụng tính năng Alias trên pfSense. Ba alias chính được tạo như sau:



Hình 2.9: Thiết lập alias

1. NAT\_INTERNET

Ánh xạ NAT ra ngoài Internet cho toàn bộ các mạng nội bộ và vùng DMZ.

Với 4 VLAN và 1 VLAN DMZ

1. OSPF\_MULTICAST

Dùng trong quá trình định tuyến OSPF giữa các router với các giá trị

* 224.0.0.5 – OSPF All Routers
* 224.0.0.6 – OSPF DR/BDR

1. RESTRICTED\_TO\_DMZ

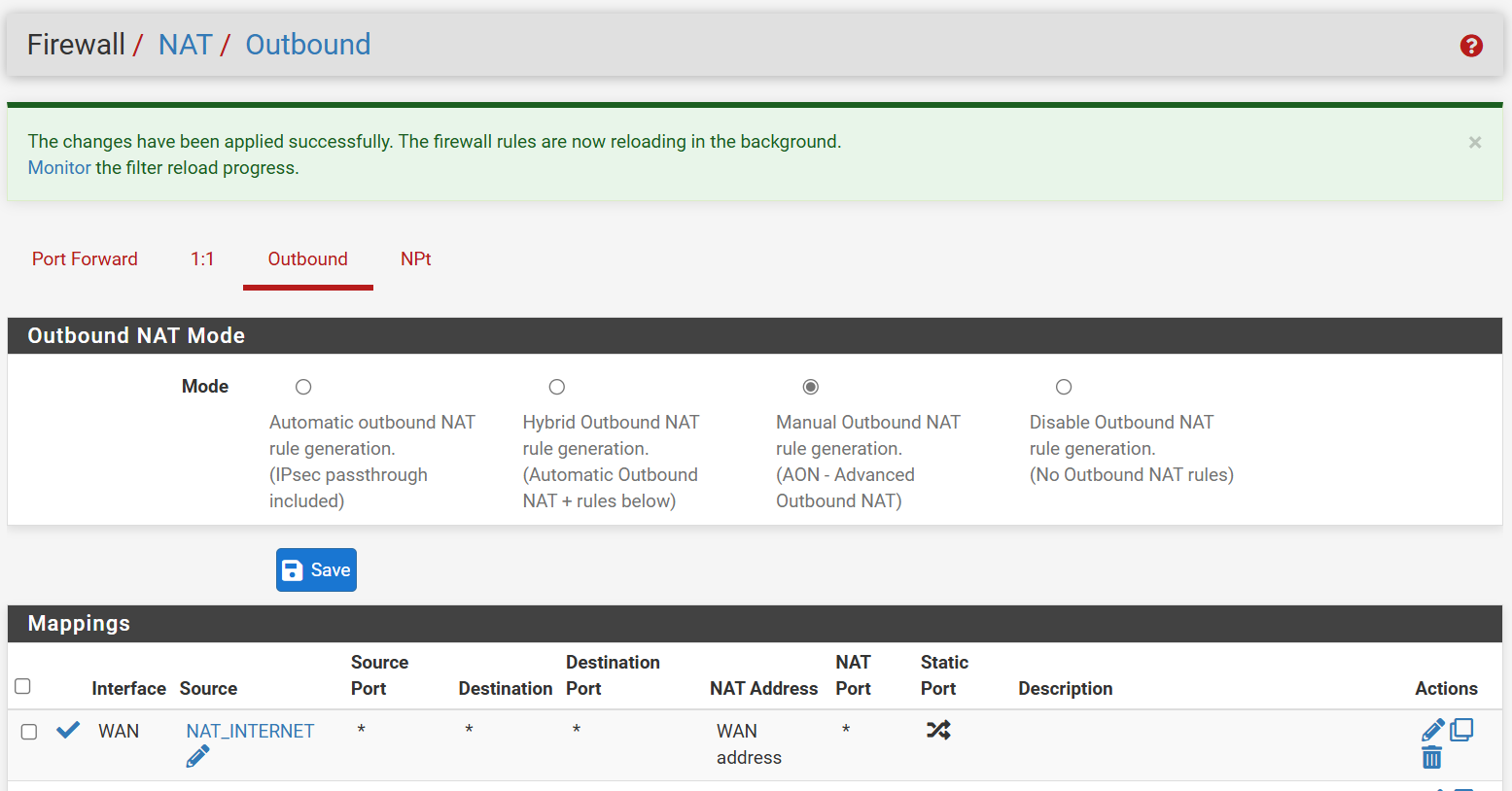
Dùng để giới hạn quyền truy cập từ các VLAN nội bộ vào vùng DMZ.

Với 4 VLAN nội bộ từ 10 đến 40

#### Thiết lập NAT

1. NAT outbound

Chỉnh sang chế độ Manual Outbound NAT để kiểm soát chính xác các mạng nội bộ nào được phép truy cập Internet.

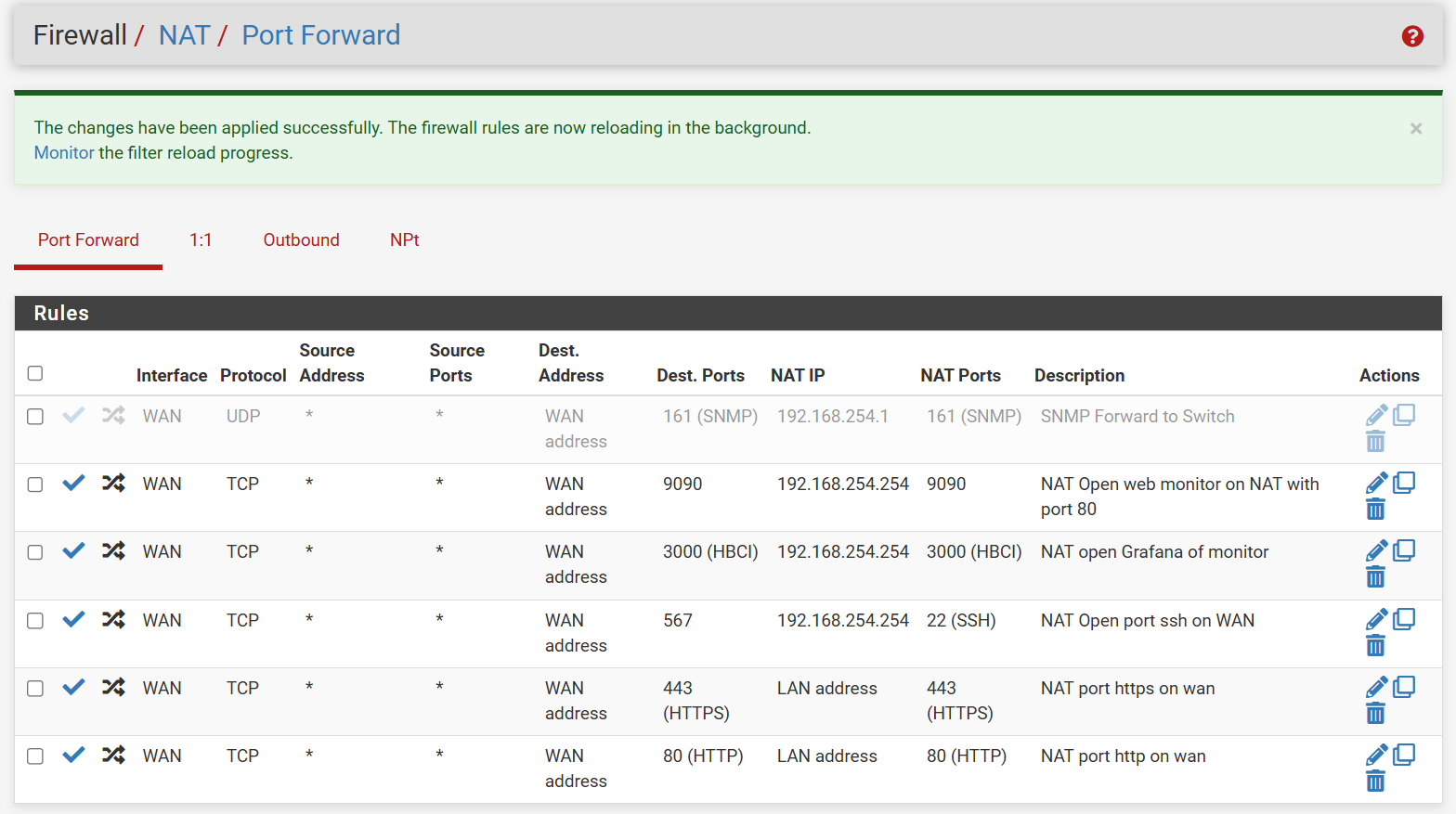


Hình 2.10: Thiết lập NAT Outbound

Cấu hình tạo cho phép Alias NAT\_INTERNET có thể đi ra địa chỉ WAN để truy cập Internet

1. NAT Forward

Nhằm mục đích công khai một số dịch vụ nội bộ ra bên ngoài Internet (trên interface WAN), hệ thống sử dụng chức năng Port Forward của pfSense. Dưới đây là các rule cụ thể đã được cấu hình:



Hình 2.11: Cấu hình Nat port forward

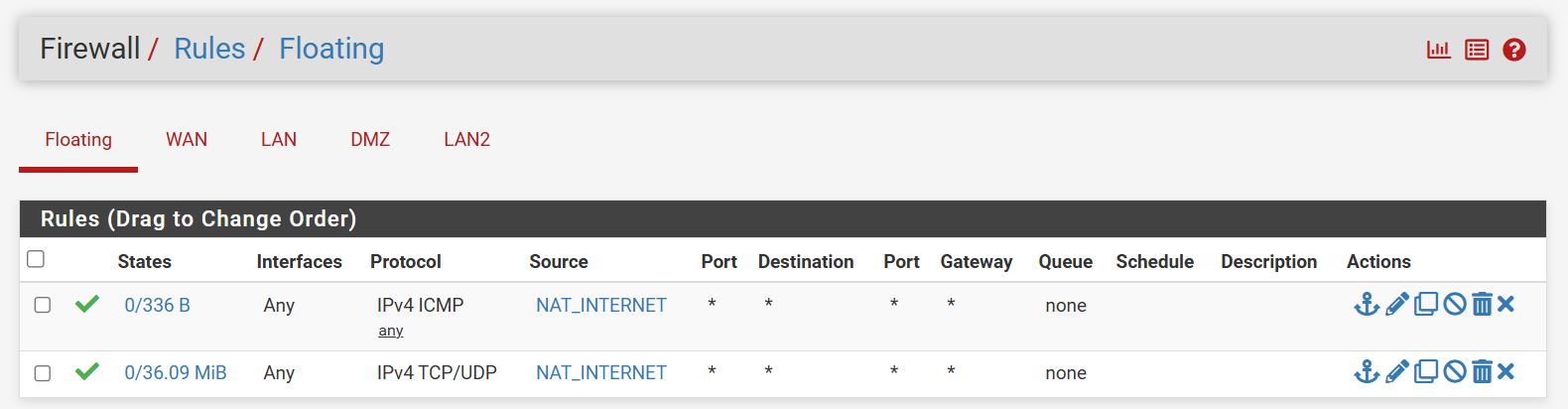
Với cấu hình trên mình cho phép 1 số trang web, dịch vụ bên trong mạng nội bộ ra ngoài thông qua cổng WAN và các port tùy chỉnh tương ứng.

Như cho phép truy cập Web Monitor từ Internet qua cổng 9090 hay Truy cập Grafana qua cổng 3000 cũng như thiết lập ssh để có thể kết nối được từ xa mà không cần ở mạng nội bộ

#### Thiết lập RULE

#### Trên Floating

Trong pfSense, các Floating Rules được sử dụng khi cần áp dụng quy tắc tường lửa trên nhiều interface cùng lúc, hoặc cho các luồng đặc biệt (inbound/outbound, pass/block theo chiều, QoS…). Hệ thống đã thiết lập các luật sau nhằm kiểm soát lưu lượng từ nhóm NAT ra Internet:



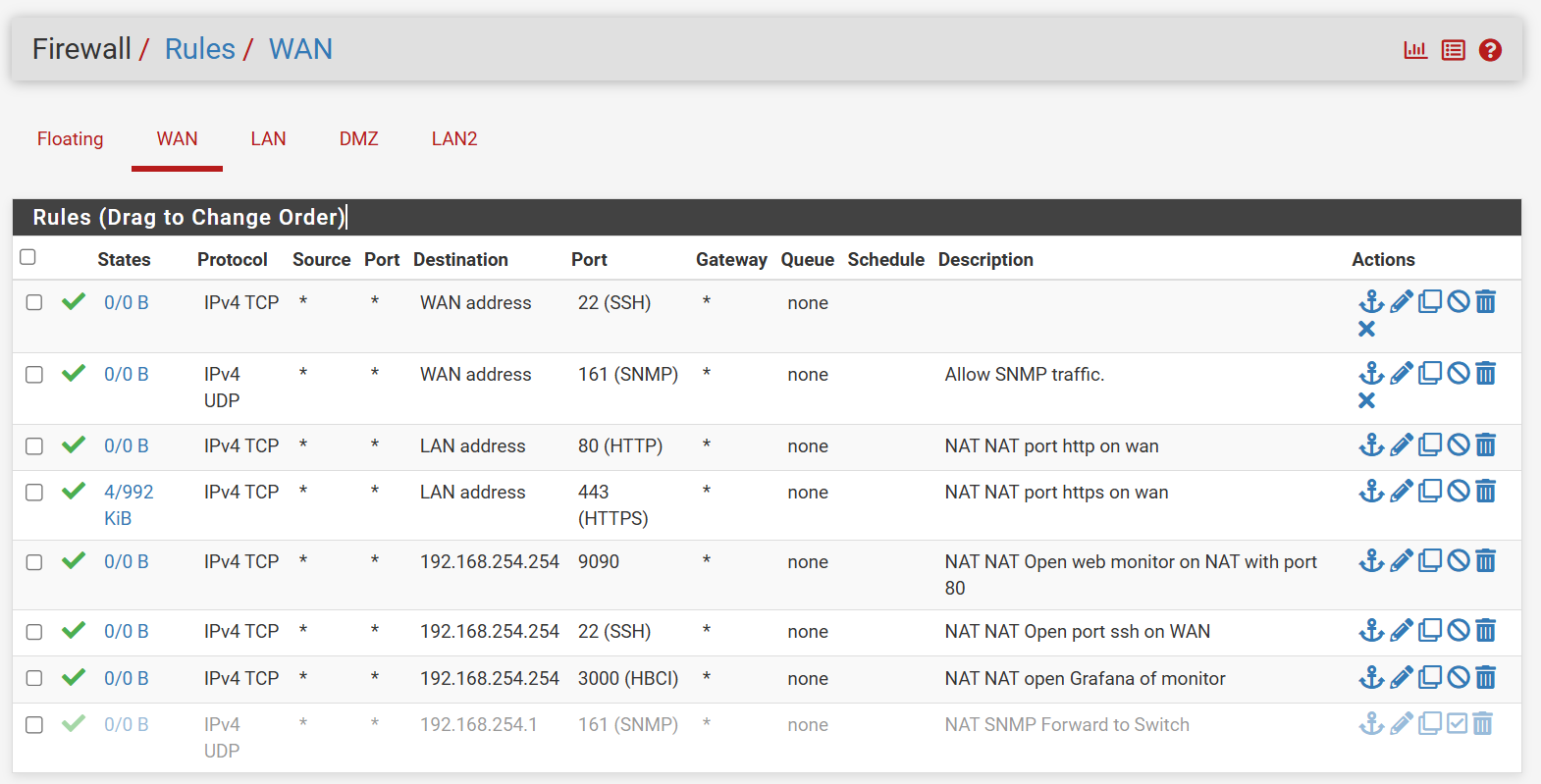
Hình 2.12: Floating Rule

Mục đích: Cho phép các thiết bị trong mạng nội bộ NAT có thể:

* Gửi ICMP để kiểm tra kết nối (ping).
* Sử dụng các dịch vụ TCP/UDP thông thường như HTTP, HTTPS, DNS, v.v.

1. Trên WAN

Vì đã thiết lập NAT Forward nên những cấu hình đã được thiết lập trên nó sẽ tự động thêm vào Rule



Hình 2.13: WAN Rule

Chi tiết: Các rule cho phép chuyển tiếp các cổng dịch vụ quan trọng:

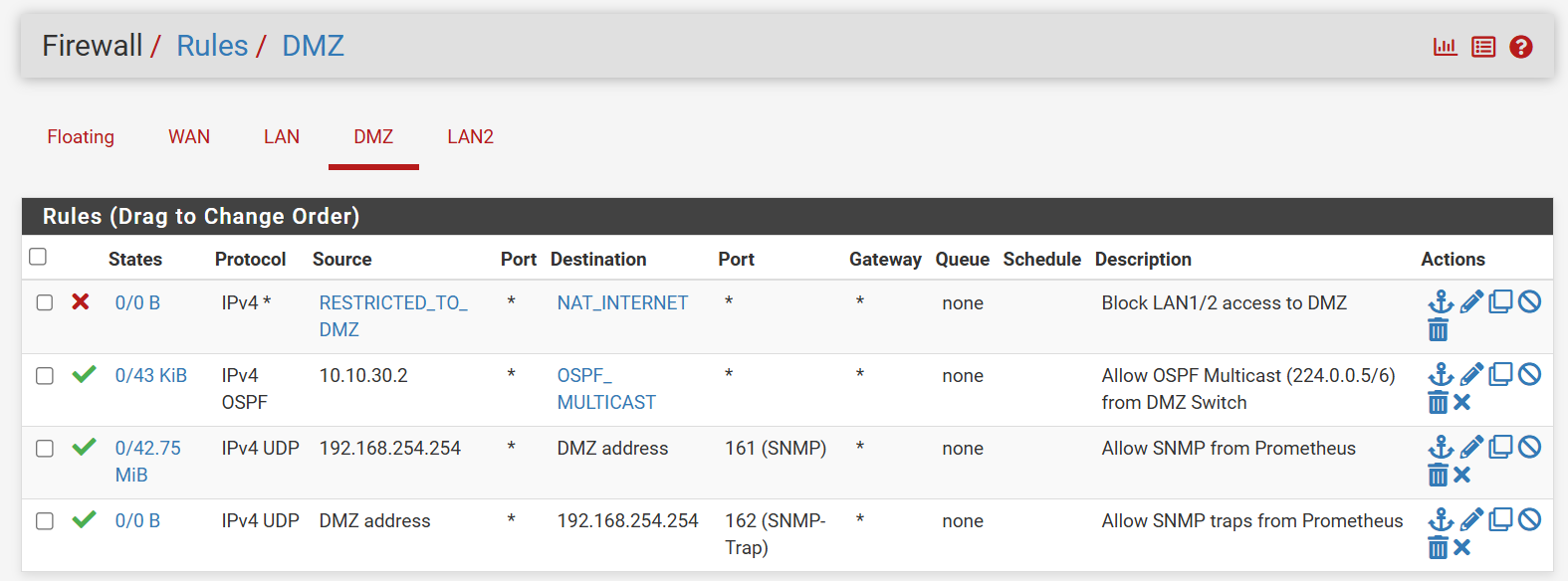
* SSH (22): Quản trị hệ thống từ xa.
* SNMP (161): Giám sát thiết bị.
* HTTP/HTTPS (80/443): Dịch vụ web.
* 9090 / 3000: Dùng cho công cụ giám sát như Grafana hoặc web monitor nội bộ.
* LAN address / WAN address: Cho phép ánh xạ từ địa chỉ WAN bên ngoài đến địa chỉ LAN hoặc thiết bị cụ thể trong mạng nội bộ.

Mục đích:

Cấu hình trên đảm bảo cho các dịch vụ nội bộ có thể được truy cập từ Internet qua NAT, đồng thời mở đúng port cần thiết để phục vụ giám sát và quản trị hệ thống từ xa.

1. Trên DMZ

Vùng DMZ được sử dụng để chứa các dịch vụ có thể được truy cập từ mạng bên ngoài mà không ảnh hưởng đến an ninh của mạng nội bộ. Các quy tắc tường lửa được thiết lập để kiểm soát chặt chẽ lưu lượng vào và ra khỏi DMZ, bao gồm các chính sách chặn truy cập không mong muốn và cho phép giao tiếp theo nhu cầu dịch vụ.



Hình 2.14: DMZ Rule

Chi tiết:

Rule 1: Từ nguồn RESTRICTED\_TO\_DMZ (đại diện cho các mạng LAN1/LAN2/LAN3/LAN4), toàn bộ lưu lượng đến NAT\_INTERNET bị chặn, nhằm đảm bảo các mạng nội bộ không thể truy cập DMZ trực tiếp.

Rule 2: Cho phép OSPF Multicast (224.0.0.5/6) từ địa chỉ 10.10.30.2 (thiết bị switch hoặc router), phục vụ cho việc định tuyến động trong mạng.

Rule 3 & 4: Thiết lập cho phép Prometheus thực hiện giám sát qua SNMP:

* Prometheus gửi yêu cầu SNMP đến thiết bị trong DMZ qua cổng 161.
* Thiết bị trong DMZ gửi SNMP trap về Prometheus qua cổng 162.

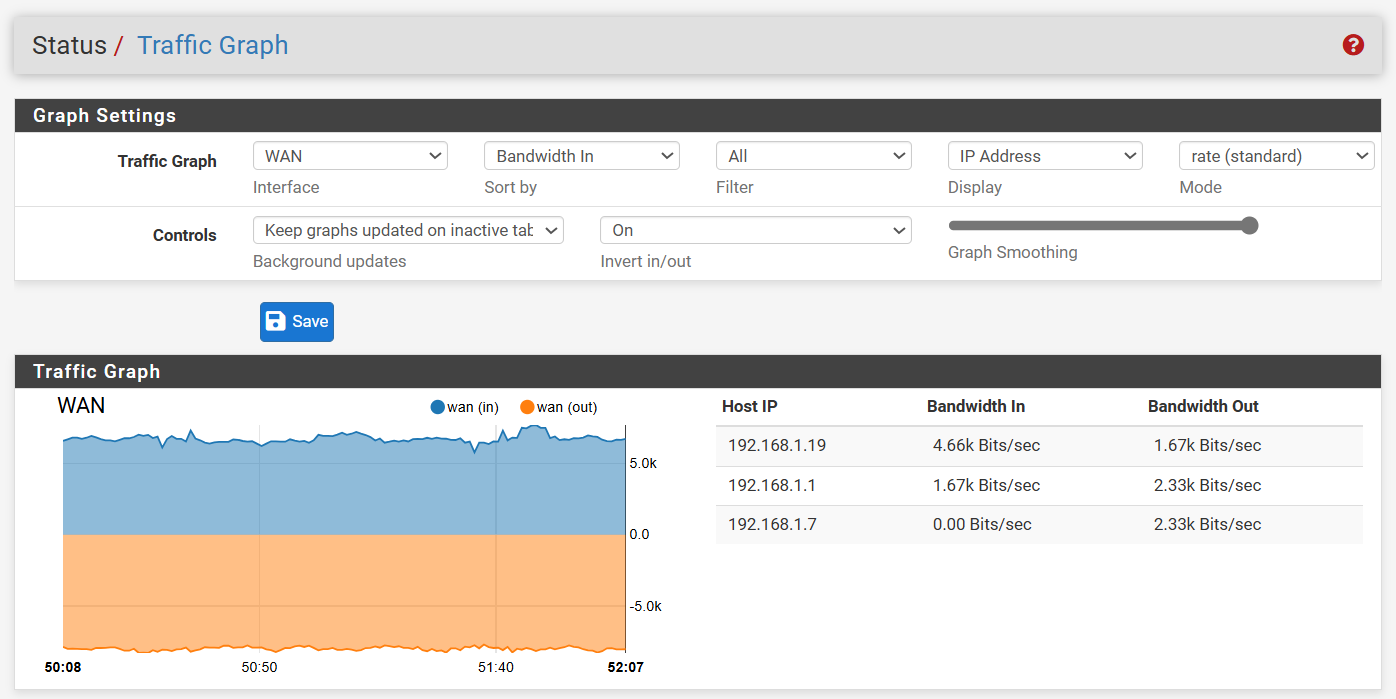
Mục đích:

* Đảm bảo cách ly vùng DMZ khỏi mạng nội bộ LAN.
* Hỗ trợ giám sát và định tuyến mạng động.
* Tăng cường bảo mật khi chỉ cho phép luồng dữ liệu cần thiết qua DMZ.

#### Thiết lập giám sát

1. Xem thông qua Traffic Graph

Sử dụng công cụ Traffic Graph để theo dõi lưu lượng dữ liệu theo thời gian thực giúp phát hiện các bất thường hoặc đánh giá hiệu suất mạng.



Hình 2.15: Traffic Graph

Tuy nhiên chỉ xem theo thời gian thực và không thể xem được CPU hay bộ nhớ hay các thông số kỹ thuật khác nên ta cần phải cấu hình SNMP sử dụng công cụ để giám sát chuyên nghiệp

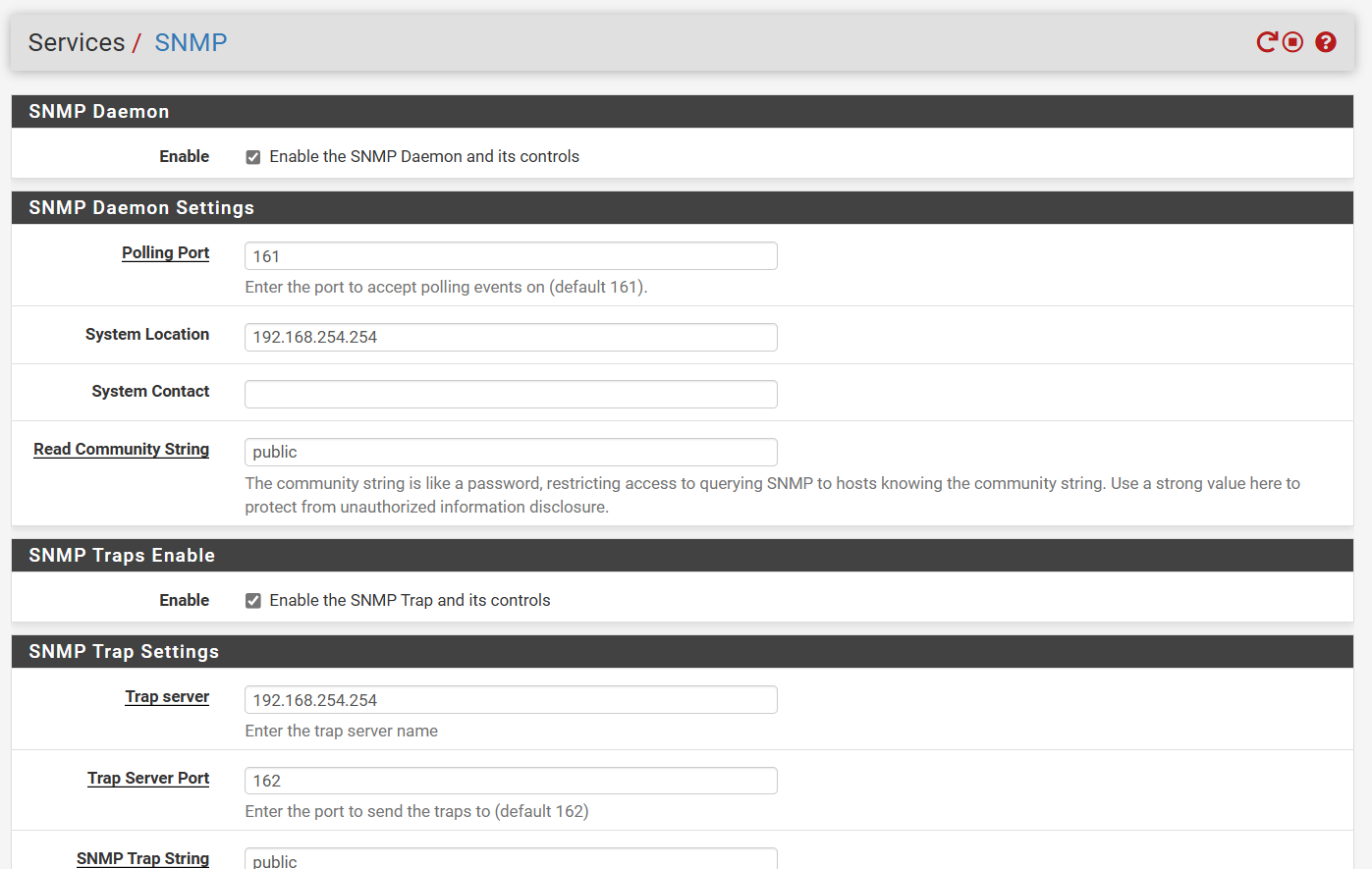
1. Kích hoạt dịch vụ SNMP:

Dịch vụ SNMP Daemon được bật để cho phép hệ thống phản hồi các truy vấn giám sát mạng. Các thiết lập bao gồm:

Polling Port: Cổng 161 (mặc định) được dùng để nhận các truy vấn từ trình giám sát.

System Location: Đặt là 192.168.254.254 – là địa chỉ IP của hệ thống quản lý tập trung hoặc thiết bị giám sát.

Read Community String: để mặc định là public – chuỗi này hoạt động như một mật khẩu đơn giản để giới hạn truy cập dữ liệu SNMP. Trong môi trường sản xuất nên đổi thành chuỗi mạnh hơn để tăng tính bảo mật.



Hình 2.16: Thiết lập SNMP

1. Kích hoạt và cấu hình SNMP Trap:

SNMP Trap giúp gửi cảnh báo chủ động đến máy chủ giám sát khi có sự kiện xảy ra.

Trap Server: đặt là 192.168.254.254 – IP máy chủ nhận cảnh báo SNMP.

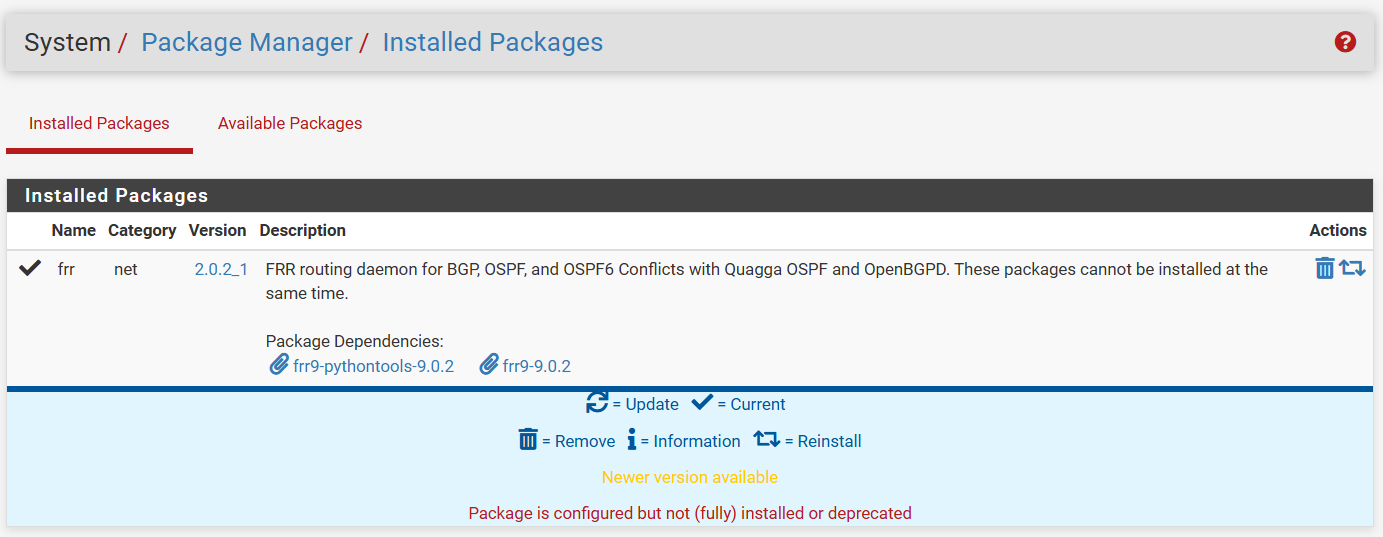
Trap Port: sử dụng cổng mặc định 162.

SNMP Trap String: sử dụng chuỗi public.

#### Thiết lập thêm các dịch vụ bên ngoài

1. Cài đặt thêm gói FRR

Để sử dụng được các giao thức định tuyến như OSPF, BGB



Hình 2.17: Thêm gói frr

#### Cấu hình OSPF

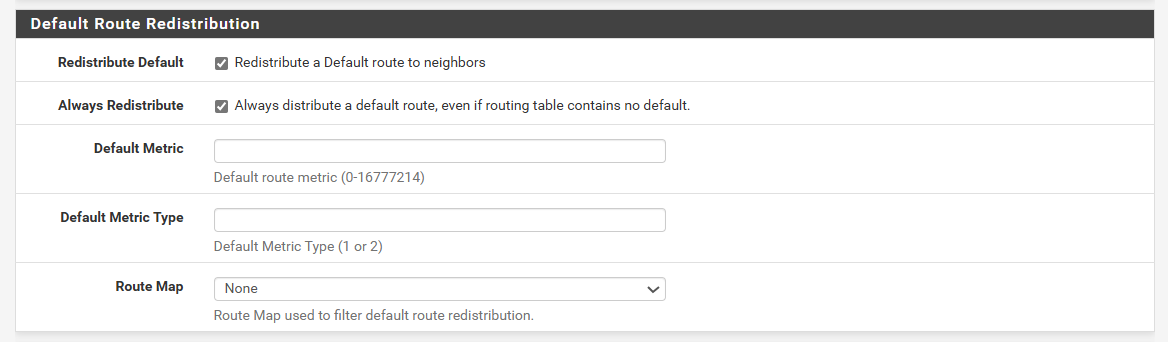
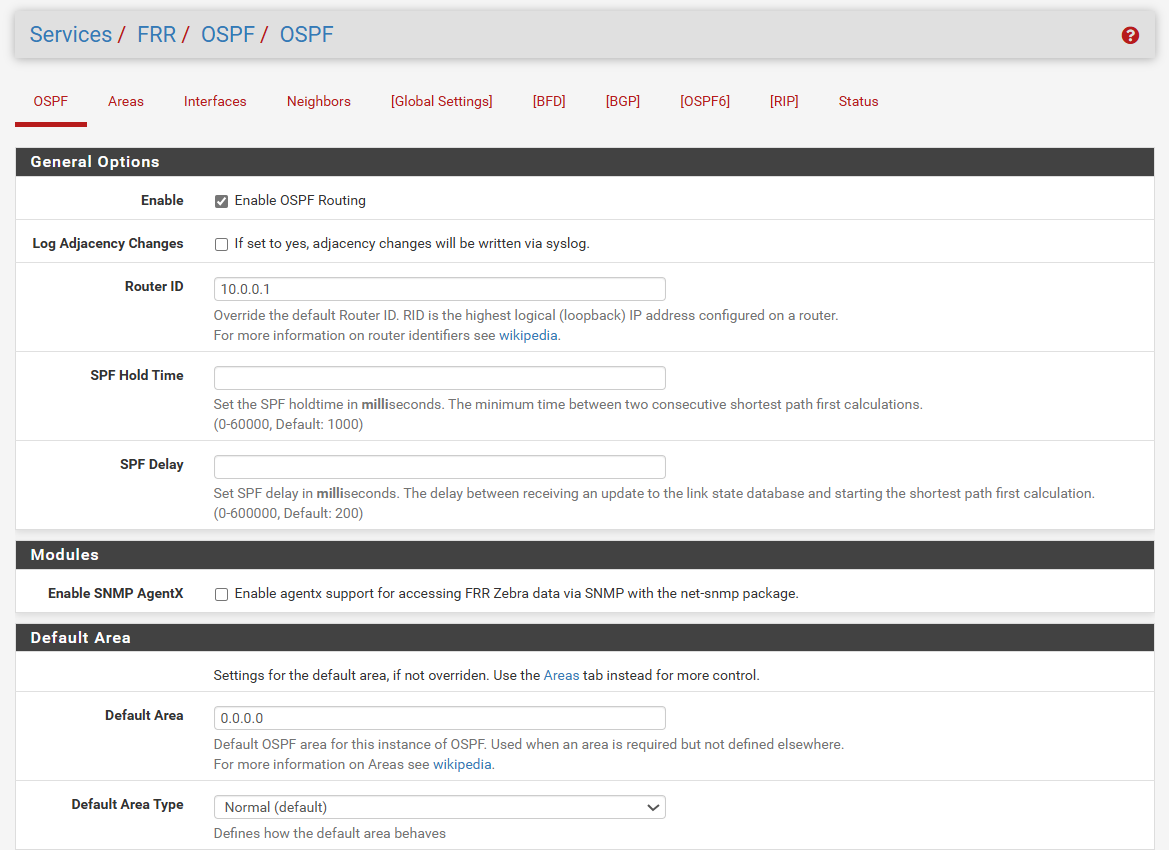
Đã bật OSPF Routing.

Router ID được đặt là 10.0.0.1.

Default Area: 0.0.0.0 với loại mặc định là Normal.

Chọn vào 2 ô Redistribute Default và Always Redistribute để

* Chỉ phân phối tuyến đường mặc định (0.0.0.0/0) nếu bảng định tuyến của router hiện tại đã có sẵn default route
* Luôn phân phối tuyến đường mặc định cho neighbor, ngay cả khi router không có default route trong bảng định tuyến.



Hình 2.18: Cấu hình OSPF

1. Thêm areas để xác định khu vực cần cấp OSPF.

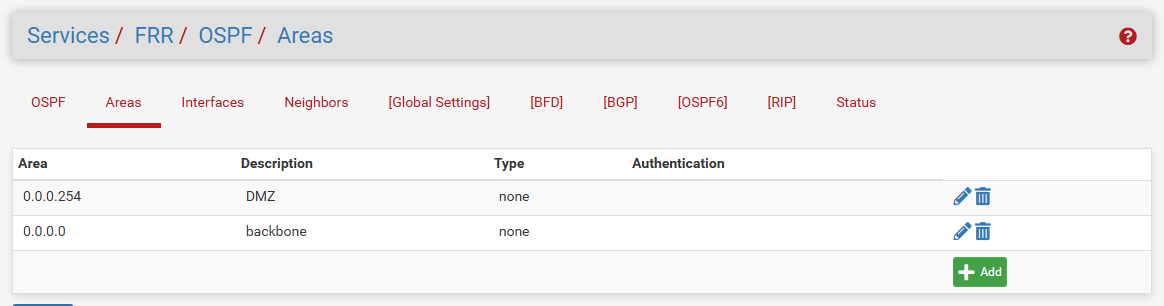
Phân vùng mạng logic.

Area 0.0.0.0 (Backbone):

* Là trung tâm kết nối mọi Area khác.
* Ví dụ: Trong ảnh, lan và opt2 thuộc Area 0 → Giao tiếp trực tiếp với nhau.

Area 0.0.0.254 (DMZ):

* Area non-backbone, thường dùng cho mạng DMZ (Public Servers).
* Traffic từ DMZ → LAN phải đi qua Area 0.

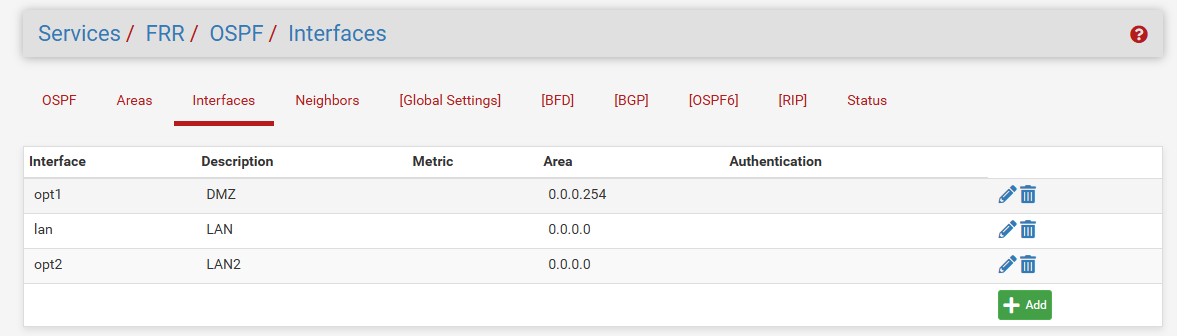


Hình 2.19: Thêm areas

1. Khai báo Interface tham gia định tuyến OSPF.

Các interface được liệt kê (opt1, lan, opt2) sẽ gửi/nhận OSPF Hello packets để thiết lập quan hệ neighbor.

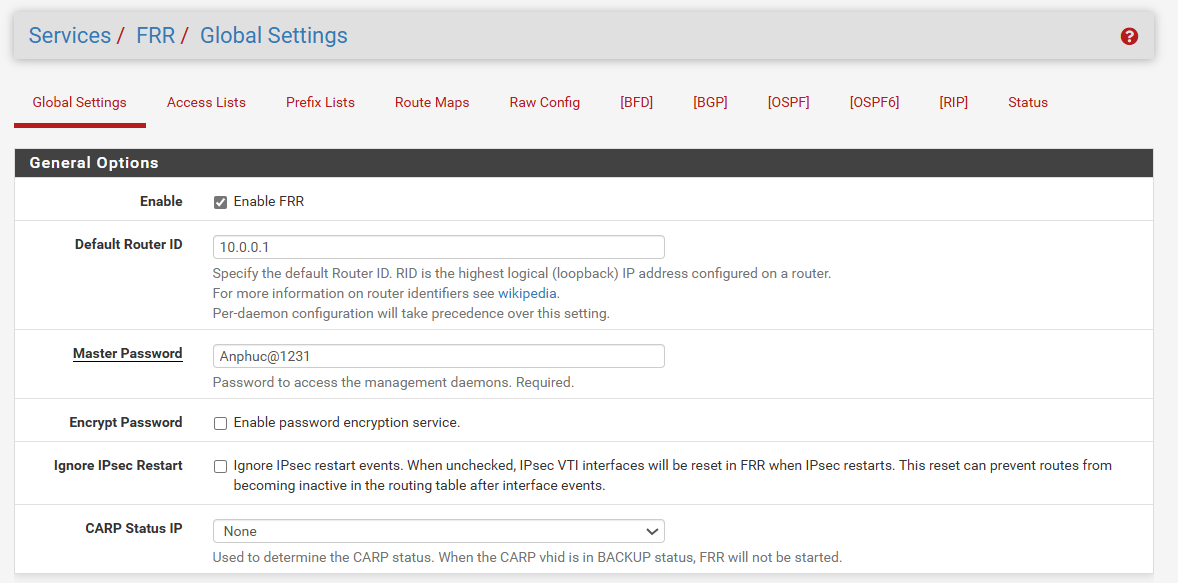
Quyết định network nào được quảng bá vào OSPF.



Hình 2.20: Thêm interface

1. Bật FRR để OSPF được hoạt động.

Bước cuối cùng là bật FRR để mọi dịch vụ cần sẽ được chạy trơn tru.



### Trình bày sản phẩm

#### Kiểm tra truy cập Internet từ các mạng nội bộ

Sau khi cấu hình định tuyến và NAT, các máy trong mạng nội bộ có thể truy cập Internet thông qua cổng của pfSense.

Sử dụng lệnh ping 8.8.8.8 hoặc truy cập một trang web từ máy trong mạng nội bộ để xác minh.

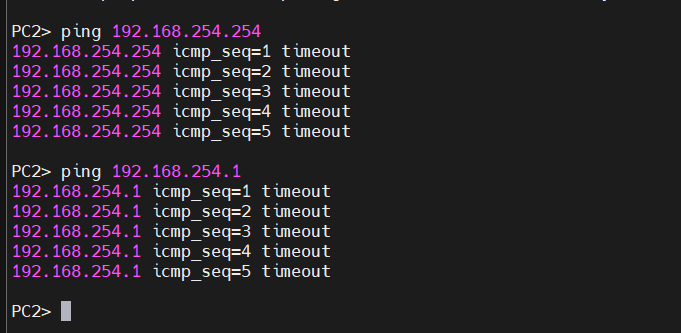
Kết quả: các gói tin đến và hồi đáp thành công.



Hình 2.21: Ping để kiểm tra kết nối trên các mạng nội bộ

#### Kiểm tra chặn mạng nội bộ vào vùng DMZ

Ping hay truy cập trang web monitoring để kiểm tra



Hình 2.22: Ping từ PC nội bộ không thành công

Kết quả: PC không thể ping tới và chặn thành công

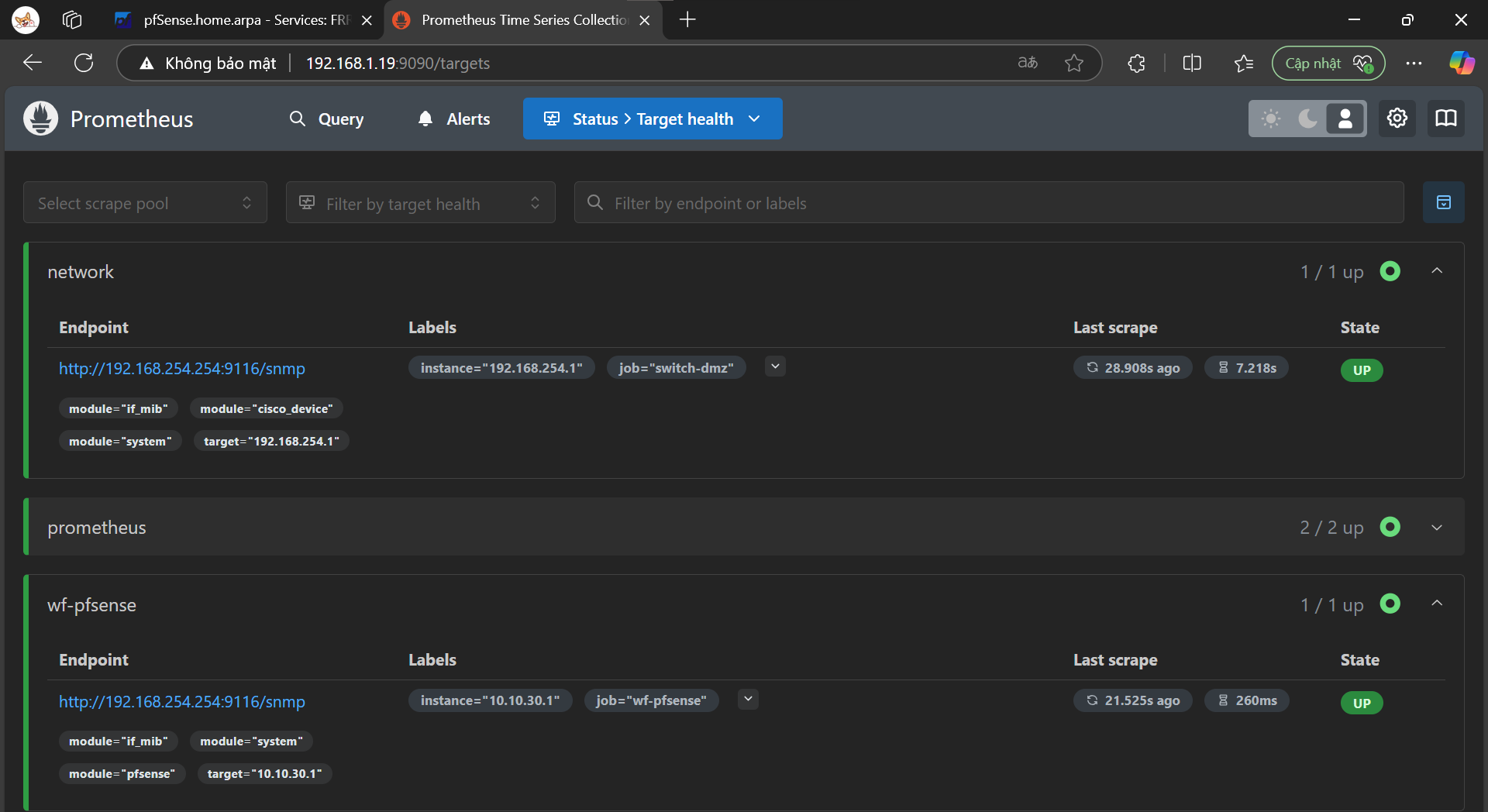
#### Kiểm tra chức năng NAT và Port Forward

Thực hiện NAT để chuyển tiếp port từ WAN đến một máy chủ trong mạng LAN, ví dụ như dịch vụ web nội bộ.

Cấu hình NAT Port Forward từ WAN port 8080 → máy chủ nội bộ port 80.

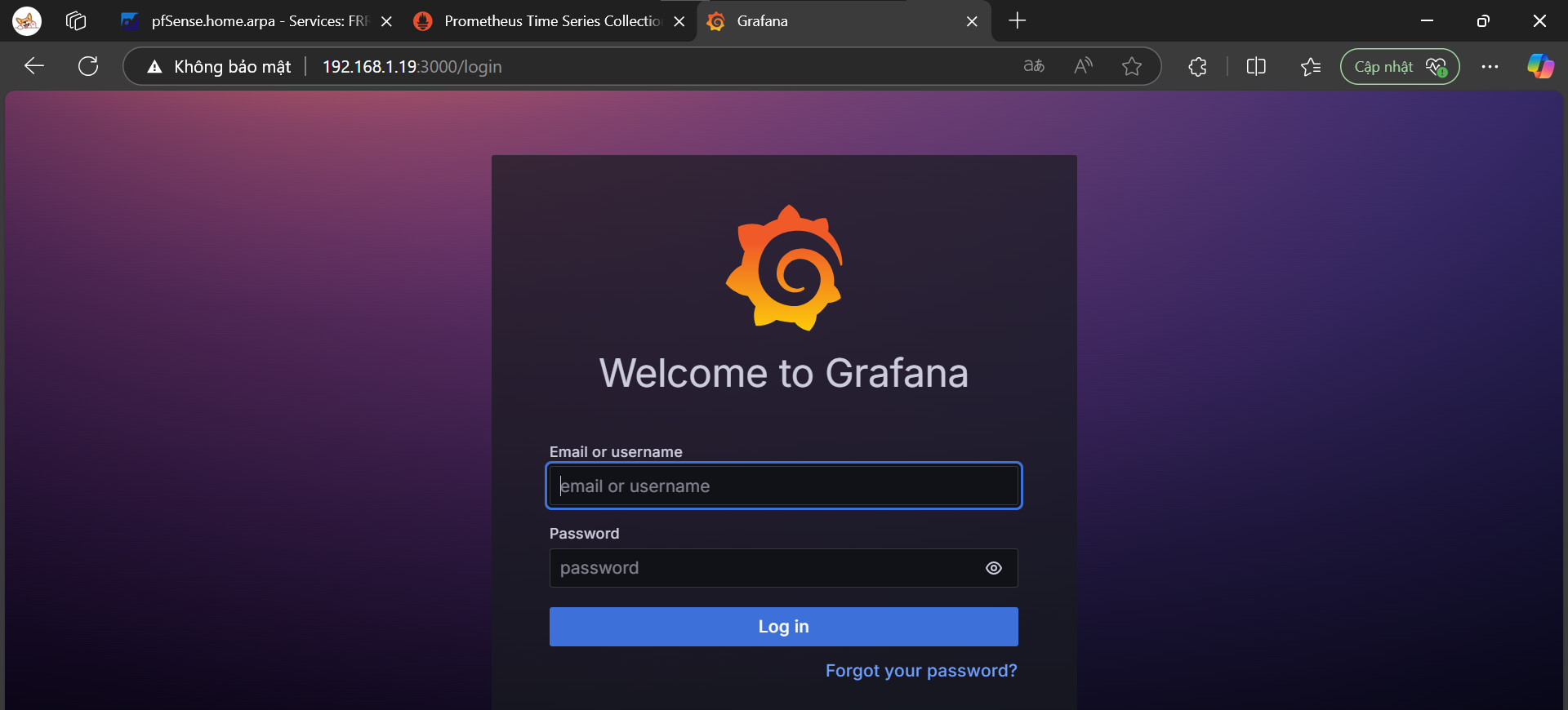
Từ bên ngoài, truy cập IP WAN:8080 để truy cập máy chủ nội bộ.

WAN port 9090 -> thiết bị giám sát port 9090



Hình 2.23: Truy cập WAN cổng 9090 để vào Prometheus

WAN port 3000 -> truy cập giao diện grafana để xem mô hình giám sát



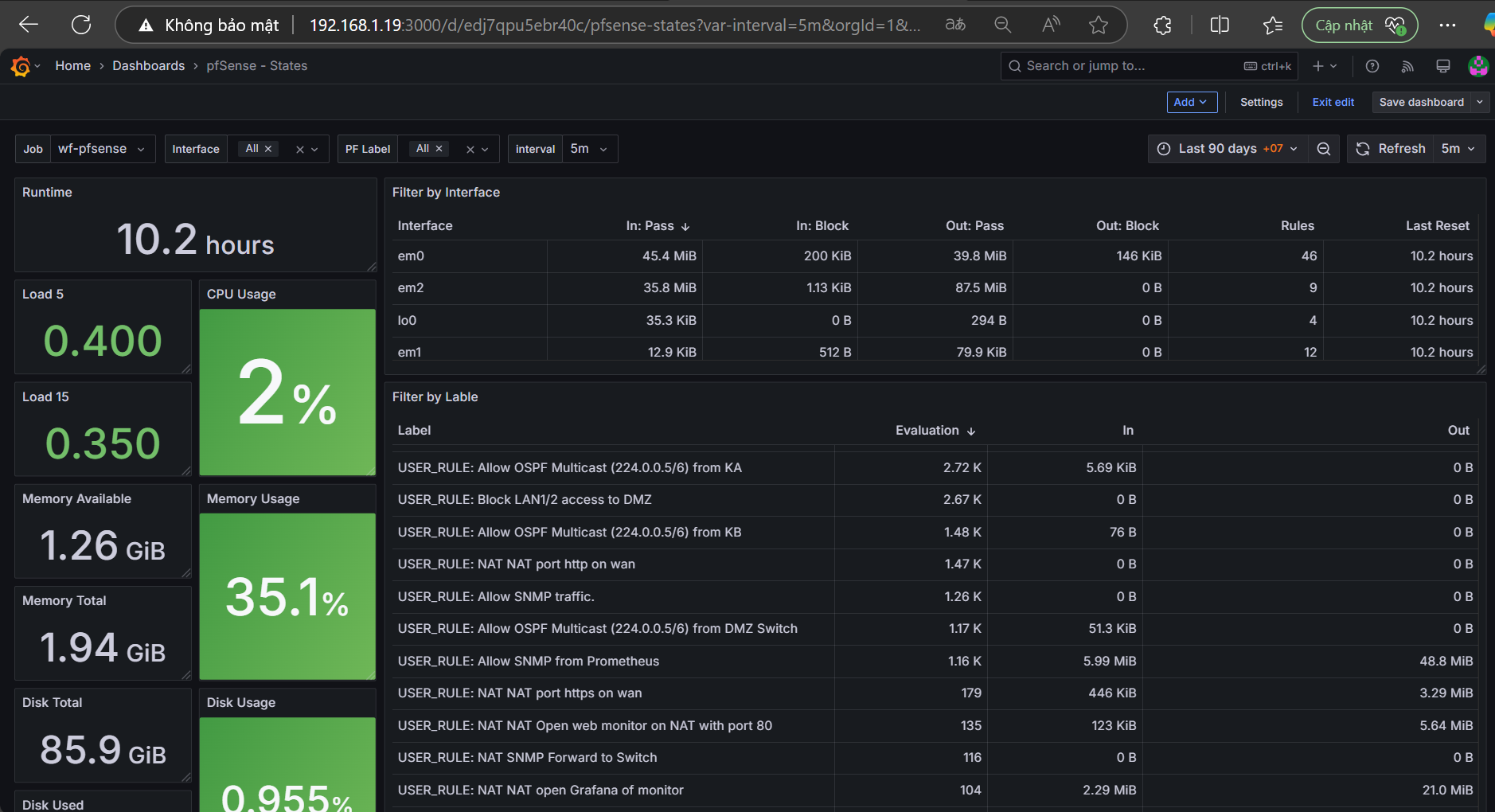
Hình 2.24: Truy cập WAN port 3000 vào grafana

#### Cấu hình và kiểm tra SNMP thông qua Grafana

Kích hoạt dịch vụ SNMP để cho phép phần mềm giám sát thu thập dữ liệu trạng thái hệ thống.

SNMP Daemon hoạt động với community string là public.

Dữ liệu như CPU, RAM, traffic interface được thu thập qua SNMP Walk/Prometheus



Hình 2.25: Xem giám sát thông qua Grafana

## Kết luận chương

Trong chương này, tôi đã tiến hành thiết kế và triển khai hệ thống mạng sử dụng pfSense làm tường lửa và cổng kết nối mạng chính. Quá trình thực hiện bao gồm cấu hình định tuyến, NAT, và các dịch vụ hỗ trợ như giám sát hệ thống thông qua giao thức SNMP.

Kết quả kiểm thử cho thấy:

* Các máy trong mạng nội bộ đã truy cập Internet thành công thông qua cấu hình định tuyến và NAT.
* Chức năng NAT và Port Forward hoạt động ổn định, đảm bảo khả năng truy cập dịch vụ nội bộ từ bên ngoài.
* Hệ thống giám sát đã được thiết lập hoàn chỉnh, thu thập được thông tin tình trạng thiết bị thông qua SNMP.
* SNMP Trap cũng đã được kích hoạt, cho phép gửi cảnh báo khi có sự kiện xảy ra về phía hệ thống quản lý.

Việc sử dụng pfSense mang lại hiệu quả cao trong việc xây dựng hệ thống mạng với chi phí thấp, đồng thời cung cấp khả năng kiểm soát truy cập và theo dõi hệ thống mạnh mẽ. Các công cụ như Traffic Graph giúp dễ dàng quan sát lưu lượng mạng theo thời gian thực.

Kết thúc chương này, tôi đã xây dựng được một hệ thống mạng ổn định, có khả năng giám sát và mở rộng, làm nền tảng cho các bước triển khai và tối ưu tiếp theo trong các chương sau.

KẾT LUẬN

* 1. Kết quả đạt được

Sau quá trình thực hiện đề tài “Tìm hiểu và triển khai hệ thống OpenStack Hybrid Cloud”, em xin rút ra một số kết luận như sau:

**THUẬN LỢI**

**Kiến thức chuyên môn: Đề tài giúp em củng cố và mở rộng kiến thức về ảo hóa, điện toán đám mây, mô hình hạ tầng dịch vụ (IaaS), đặc biệt là cơ chế hoạt động của các thành phần trong OpenStack.**

**Tài liệu đầy đủ: OpenStack có cộng đồng lớn, tài liệu chi tiết và nhiều nguồn học trực tuyến (Docs, GitHub, diễn đàn) hỗ trợ quá trình nghiên cứu và xử lý lỗi.**

**Môi trường mô phỏng linh hoạt: Việc triển khai trên VMware Workstation với DevStack cho phép dễ dàng kiểm thử, khôi phục hệ thống và thực hành cấu hình thực tế.**

**KHÓ KHĂN**

**Yêu cầu tài nguyên cao: Hệ thống OpenStack cần nhiều tài nguyên phần cứng, đặc biệt là RAM và CPU, gây khó khăn khi triển khai trên thiết bị cá nhân.**

**Thời gian triển khai dài: Quá trình cài đặt DevStack có thể mất nhiều thời gian, đặc biệt khi có lỗi phát sinh trong quá trình tải gói hoặc xung đột phiên bản.**

**Khó khăn trong quản trị mạng ảo: Cấu hình Open vSwitch với các bridge như br-ex, br-int đòi hỏi hiểu biết chuyên sâu về mạng ảo, định tuyến nội bộ và NAT.**

2. Những mặt đạt được và chưa đạt được

**Mặt đạt được:**

Triển khai thành công hệ thống IaaS: Bao gồm các dịch vụ cốt lõi Keystone, Glance, Nova, Neutron, Cinder, Horizon và mô hình mạng ảo hóa phức hợp.

Mô hình mạng ba lớp rõ ràng: Xây dựng kiến trúc mạng với các lớp Public, DMZ và Internal thông qua PFSENSE, đảm bảo phân vùng mạng an toàn và truy cập hợp lý.

Cấu hình lưu trữ linh hoạt: Thiết lập backend LVM để tạo volume, hỗ trợ boot từ volume và lưu trữ ổn định.

Demo hoàn chỉnh: Triển khai thành công các máy ảo Web Server, Database Server, truy cập được từ Internet thông qua Floating IP.

**Mặt chưa đạt:**

Chưa triển khai mô hình HA: Hệ thống hiện tại chỉ có một node duy nhất, chưa có giải pháp dự phòng hay phân tán.

Chưa tích hợp giám sát nâng cao: Hệ thống chưa kết nối với công cụ giám sát như Prometheus, Zabbix để thu thập và cảnh báo hiệu suất.

Giới hạn môi trường triển khai: Sử dụng DevStack nên hệ thống chỉ phù hợp với môi trường lab, không khuyến khích dùng trong môi trường production.

1. Hướng nghiên cứu

Trong tương lai, để hoàn thiện và mở rộng mô hình, em đề xuất một số hướng nghiên cứu:

Chuyển sang triển khai production: Sử dụng OpenStack bản ổn định (ví dụ Packstack, kolla-ansible hoặc OpenStack-Ansible) để xây dựng môi trường thật có độ ổn định cao.

Mở rộng tính khả dụng (HA): Triển khai nhiều node controller và compute, kết hợp với dịch vụ load balancing (HAProxy, Keepalived) để đảm bảo tính sẵn sàng.

Tích hợp giám sát và cảnh báo: Kết nối với hệ thống như Zabbix hoặc Prometheus để theo dõi tình trạng tài nguyên và dịch vụ.

Tự động hóa triển khai: Áp dụng Ansible hoặc Terraform để tự động hóa quá trình cài đặt và cấu hình OpenStack.

Phát triển hybrid thực sự: Kết nối OpenStack private cloud với public cloud như AWS hoặc Azure thông qua giải pháp federated identity hoặc VPN site-to-site.

TÀI LIỆU THAM KHẢO

[1] OpenStack Documentation – https://docs.openstack.org

[2] DevStack – A Tool for Installing OpenStack –https://docs.openstack.org/devstack/latest/

[3] Open vSwitch (OVS) – https://docs.openvswitch.org/en/latest/

[4] OpenStack Networking Guide – https://docs.openstack.org/neutron/latest/

[5] Volume Service (Cinder) – https://docs.openstack.org/cinder/latest/

[6] Zabbix Documentation – https://www.zabbix.com/documentation/

[7] Prometheus Documentation – https://prometheus.io/docs/introduction/overview/

[8] OpenStack HA Guide – https://docs.openstack.org/ha-guide/latest/

[9] Suricata IDS/IPS – https://suricata.io/docs/