pfSense

internet (Wan) -> pfsense-> LAN

Firewall

rules: for Wan and LAN. Block or pass các gói tin theo rules và theo thứ tự các rules

Firewall Schedules: Đặt lịch làm việc, sau đó khi áp dụng các rules, có thể thêm schedules vào để set time áp dụng với các rules

Pass, Block or Reject:

\* Reject sends a TCP RST or ICPM “Port Unreachable”

- Captive Portal: Tạo mạng truy cập công cộng. Đăng nhập bằng user và password được admin tạo khi kết nối tới mạng

- Hỗ trợ backup and restore

Rules: Group, floating ,NAT port forwarding

Floating rules. Tạo quy tắc áp dụng từ các vùng vào vùngkhác (VD. Cấm lan1, lan2 truy cập vào DMZ)

NAT-> outbound: NAT địa chỉ local qua pfSense qua địa chỉ mạng public.

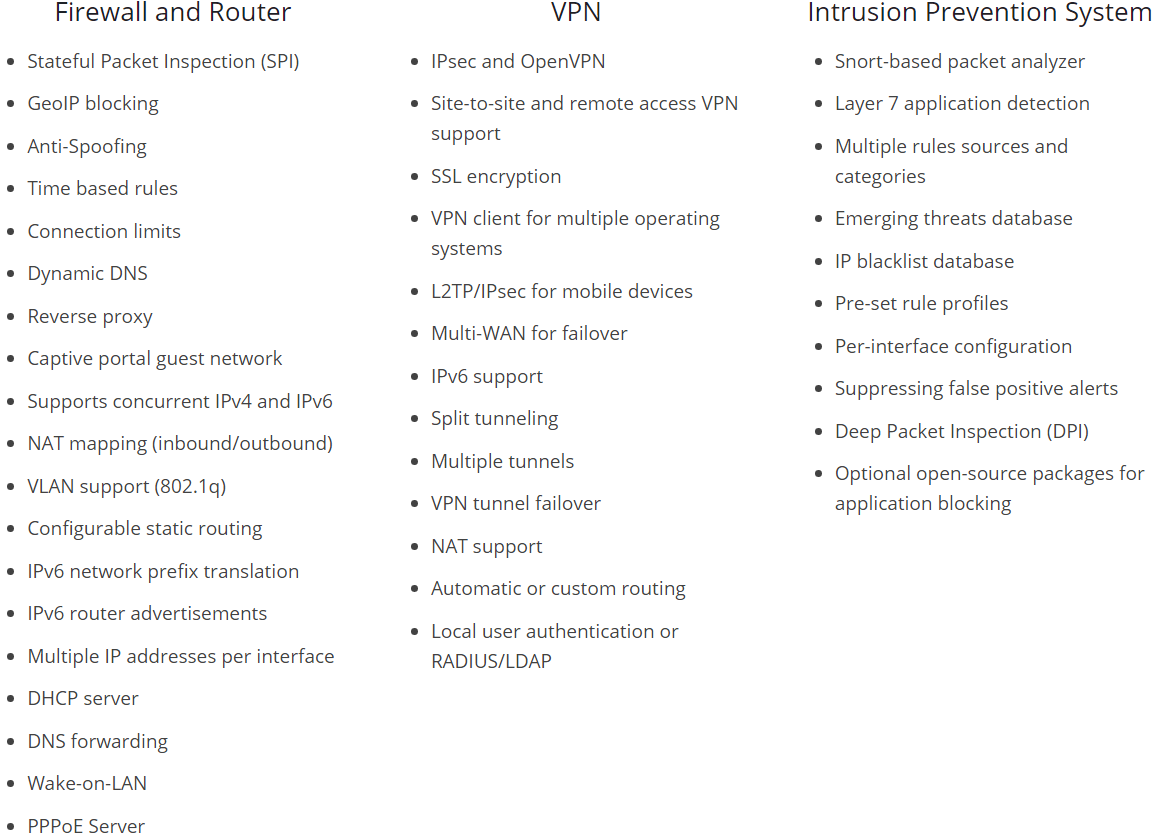
NAT -> port forwarding. Mở port tương ứng từ ngoài vào bên trong mạng nội bộ

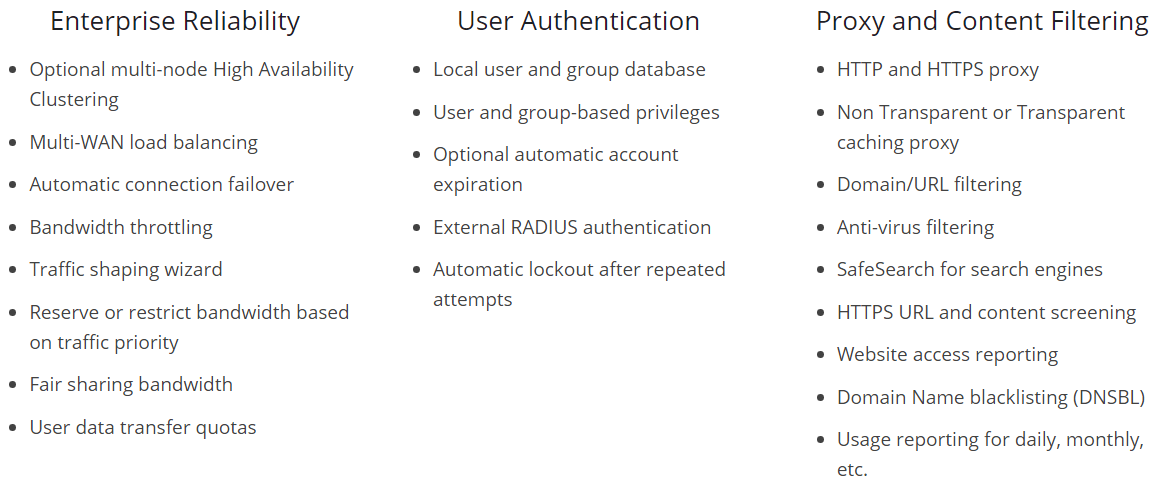
Firewall -> limmiter. Điều chỉnh băng thông giới hạn

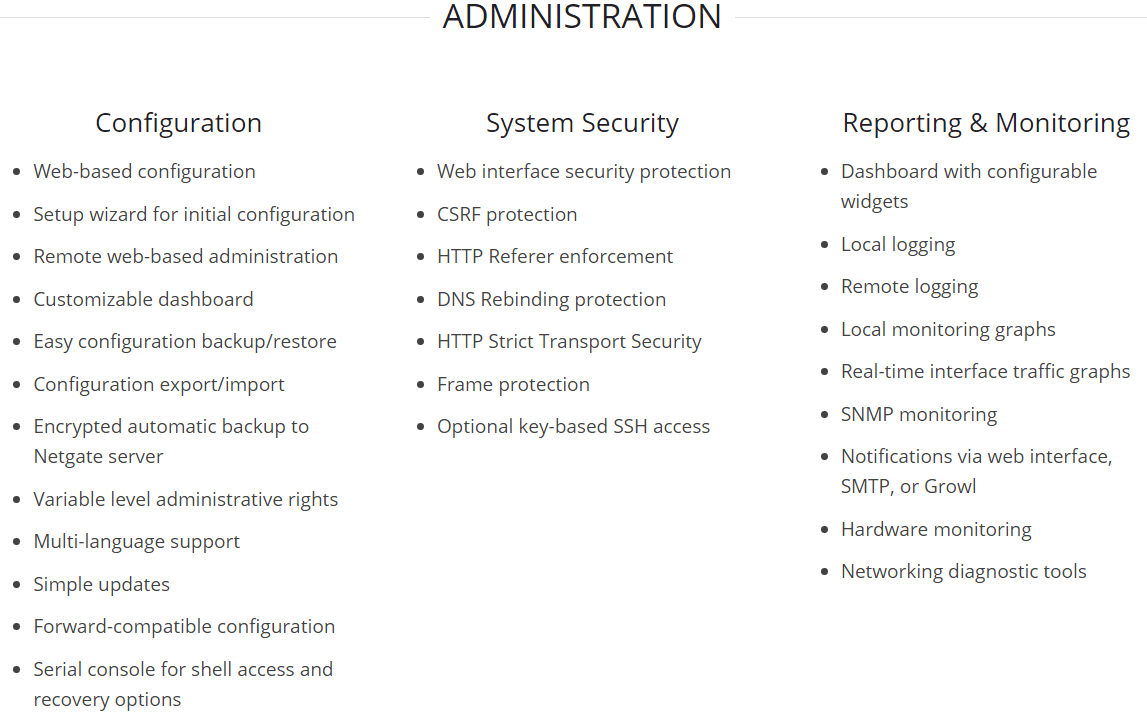
**COP-360: Thử nghiệm pfSense**

Phiên bản: 2.4.4-p3.

FEATURES







**I.Tổng quan**

**-** Mô tả:PfSense là dự án mã nguồn mở dựa trên FreeBSD được sự dụng như một tường lửa hoặc có thể sử dụng làm thiết bị định tuyến. PfSense có thể chạy trên thiết bị chuyên dụng của hãng hoặc người dùng thiết lập pfSense chạy trên máy tính cấu hình thấp ~ (cpu: 1 core, ram 512GB, hdd 5GB, ≥ 2 network card).

- Phương pháp triển khai thực tế: Với rất nhiều tính năng , pfSense được sử dụng cho nhiều mục đích khác nhau. Giá thành triển khai thấp hơn so với những thiết bị chuyên dụng cùng loại, hỗ trợ tính năng cơ bản và nâng cao: Load Balancing, Traffic Shaping, Captive Portal, UTM Device, DNS / DHCP Server, IDS / IPS, Transparent Caching Proxy, Web Content Filter, ... :

* Tường lửa: Với tính năng xử lý gói tin TCP/IP mạnh mẽ, nên pfSense được dùng như một tưởng lửa nhằm lọc những kết nối đến vùng mạng chỉ định.
* Thiết bị định tuyến mạng WAN/LAN: Đóng vai trò như một router, pfSense hỗ trợ các chức năng định tuyến như: PPPoE, BGP, OSPF, RIP,… phù hợp doanh nghiệp triển khai với giá thành thấp. PfSense có thể sử dụng thay thế switch layer 3
* Wireless Access Point
* Máy chủ VPN/DNS/DHCP/Sniffer.

Cài đặt: https://github.com/phamngocsonls/SVTT/blob/phamngocsonls/SONPN/pfSense/install\_pfSense.md

**II. Các tính năng cơ bản”**

1. **Cấu hình tường lửa**.

1.1 Alias: Phương thức đặt bí danh cho một hoặc nhiều IP/Network/URL/port.

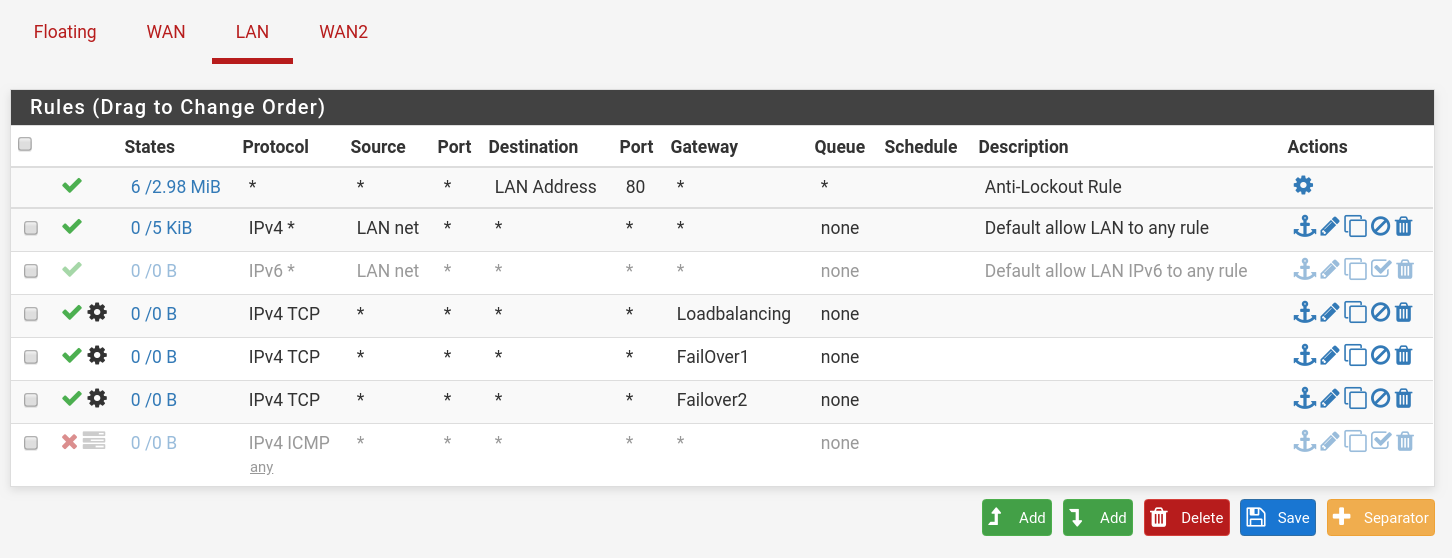
1.2NAT:

+ Port Forwarding: Quy định về loại gói tin khi nhận được sẽ mặc định chuyển đến cổng nào ở phía trong mạng LAN.

+ NAT 1:1 : Ánh xạ IP public với IP private.

+ Outbound: NAT địa chỉ IP private qua địa chỉ IP public.

1.3 Rules: Là thành cơ bản trong hệ thống tường lửa. Rule có 3 trạng thái: block, pass, reject(reject gửi gói TCP RST hoặcr ICPM “Port Unreachable). Đặt các rule phù hợp với mạng và yêu cầu, nên đặt các rule từ cơ bản đến rõ ràng. Giao diện rule có nhiều tùy chỉnh như hình dưới.



1.4 Schedules: Chức năng lập lịch trong pfSense cho phép cấu hình thời gian hoạt động của hệ thông một cách tự động. Qua thiết lập mặc định của Rule có người dùng gán lịch cụ thể cho các rule mong muốn.

1.5 Traffic Shaper: Được sử dụng trong môi trường có nhiều loại dịch vụ mạng cùng hoạt động như VoIP, data network, streaming … Thiết lập Traffic Shaper là quan trọng trong môi trường mạng lớn để đảm bảo tính ổn định cho các dịch vụ cần có độ ưu tiên cao. Có thể giới hạn băng thông tĩnh cho các mạng hoặc sử dụng các cơ chế lập lịch kiểm soát gói tin như:

* CBQ: Hoạt động dựa vào các chỉ số băng thông mạng như số phần trăm băng thông được sử dụng hoặc tổng dung lượng được sử dụng trong 1 giây. CBQ thực hiện phân mức ưu tiên cho các gói tin từ 0 đến 7. Các gói tin có độ ưu tiên cao hơn sẽ được xử lý trước.
* PRIQ: Cơ chế PRIQ dựa vào mức độ ưu tiên được chia thành 0 đến 15. Các dịch vụ cao hơn sẽ được xử lý trước. Một số dịch vụ có thể bị ngưng phục vụ do có chỉ số ưu tiên quá thấp.
* HFSC: Thuật toán Hierarchical Fair Service Curve được sử dụng nhằm đảm bảo các kết nối đều có thể ở một mức ổn định cho từng loại dịch vụ. Khi hoạt động pfSense sẽ ghi nhớ băng thông khi hoạt động của dịch vụ nhằm giới hạn các dịch vụ khác để đảm bảo hệ thống hoạt động tốt.

**2.Cân bằng tải:**

- PfSense hỗ trợ hai phương pháp cân bằng tải: gateway và server. Cân bằng tải gateway cho phép hệ thống mạng phân bố lưu lượng dữ liệu trên nhiều kết nối Wan. Cân bằng tải server cho phép phân bố việc sử dụng tài nguyên từ các máy chủ nội bộ và đảm bảo thừa tài nguyên cho hệ thống máy chủ phục vụ. Phương pháp này thường được sử dụng trong việc cân bằng tải các dịch vụ web, SMTP, DNS hoặc các dịch vụ sử dụng giao thức TCP trong việc truyền dữ liệu.

**2.1: Thử nghiệm cân bằng tải multi-WAN:**

Sử dụng multi-WAN giúp đảm bảo tính sẵn sẵng sàng, tăng băng thông khi sử dụng, giúp mạng luôn trong trạng thái hoạt động ổn định khi một trong 2 WAN bị chết.

Do môi trường không đủ và gặp một số lỗi nên sử dụng lab của link sau:

<https://github.com/phamngocsonls/thuctap012017/blob/master/TVBO/docs/Firewalls/pfsense/docs/pfsense-multi-wan.md>

**2.2: Cân bằng tải server:** Người dùng sẽ sử dụng 2 hoặc nhiều địa chỉ IP dự phòng chứa các web server. Khi server chính chết sẽ tự động sử dụng các IP dự phòng. Để làm được điều này cần tạo một Virtual IP gộp các IP dự phòng lại.

LAB: <https://github.com/phamngocsonls/SVTT/blob/phamngocsonls/SONPN/pfSense/server_LoadBalancing.md>

**2.3: Thử nghiệm High Availability Sync và CARP:**

High Availability Sync và CARP là giải pháp để tạo 1 cluster nhanh chóng. Với High Availability Sync sẽ đồng bộ hóa từ tường lửa chính đến tường lửa thứ cấp. Thay đổi trên bảng trạng thái của máy chính sẽ được gửi đến máy thứ cấp và ngược lại. Điều này giúp cấu hình CARP nhanh gọn cho hệ thống FailOver. Khi mất tín hiệu của máy Master thì các máy dự phòng khác sự tự đổi lên vai trò Master, đảm bảo tính HA của hệ thống. Tham khảo lab ở dưới:

LAB: <https://github.com/phamngocsonls/SVTT/blob/phamngocsonls/SONPN/pfSense/HA_CARP_failover.md>

**3. VPN:**

Ngoài ra, pfSense cũng cung cấp dịch vụ VPN để tạo đường hầm an toàn dành cho các máy có nhu cầu kết nối đến nhau trong môi trường mạng công cộng.

Do chưa thực hiện lab này nên có dẫn link của một thành viên khác đã thực hiện chức năng VPN của pfSense: <https://github.com/hocchudong/ghichep-pfSense/blob/master/docs/pfSense-OpenVPN-TAPmode.md>

**4. Captive portal**

Captive portal là một trang web hiển thị khi người dùng kết nối tới một vùng mạng đã được chỉ định. Đây là tính năng khá mạnh mã giúp quản lý truy cập người dùng. PfSense hỗ trợ 2 phương pháp chứng thực: pfSense user và chứng thực thông qua Radius server. Trong trường hơp mạng cần cung cấp dịch vụ truy cập tính phí, pfSense cung cấp giải pháp sinh mã voucher.

Lab ví dụ về dịch vụ Capitive portal:

<https://github.com/hocchudong/thuctap012017/blob/master/TVBO/docs/Firewalls/pfsense/docs/pfsense-captive-portal.md>

Ngoài ra pfSense còn hỗ trợ Package Manager để người dùng tải về các gói cài đặt ngoài nhằm tối ưu và thêm tính năng, hệ thống monitor dashboard với nhiều lựa chọn, khả năng xuất log các dịch vụ…