BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

-------o0o-------

ISO 9001:2015

NGHIÊN CỨU TRIỂN KHAI GIẢI PHÁP ĐẢM BẢO AN NINH MẠNG TRÊN NỀN PFSENSE

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
-------o0o-------

NGHIÊN CỨU TRIỂN KHAI GIẢI PHÁP ĐẢM BẢO AN NINH MẠNG TRÊN NỀN PFSENSE

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

Sinh viên thực hiện : **Trần Văn Quyết**
Mã sinh viên : **1512101012**
Giáo viên hướng dẫn : **TS. Ngô Trường Giang**.

HẢI PHÒNG - 2019

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

-------o0o-------

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

Sinh viên: **Trần Văn Quyết** Mã sinh viên: **1512101012**

Lớp: **CT1901M** Ngành: **Công nghệ Thông tin**

Tên đề tài: Nghiên cứu triển khai giải pháp đảm bảo an ninh mạng trên nền Pfsense

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

a. Nội dung:

- Tìm hiểu tổng quan về an toàn an ninh mạng
- Tìm hiểu phần mềm nguồn mở pfsense
- Triển khai một số dịch vụ cơ bản trên pfsence để tăng cường an ninh.

b. Các yêu cầu cần giải quyết

- Tìm hiểu các vấn đề cơ bản về an ninh mạng máy tính.
- Tìm hiểu cấu hình phần mềm nguồn mở pfsense.
- Cấu hình một số dịch vụ cơ bản trên pfsence để tăng cường an ninh mạng.

2. Các số liệu cần thiết để thiết kế, tính toán

3. Địa điểm thực tập

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Người hướng dẫn thứ nhất:

Họ và tên: Ngô Trường Giang

Học hàm, học vị: Tiến sĩ.

Cơ quan công tác: Khoa Công nghệ Thông tin

Nội dung hướng dẫn:

- Tìm hiểu tổng quan về an toàn an ninh mạng
- Tìm hiểu phần mềm nguồn mở pfsense
- Triển khai một số dịch vụ cơ bản trên pfsence để tăng cường an ninh.

Người hướng dẫn thứ hai:

Họ và tên: …….....

Học hàm, học vị……

Cơ quan công tác: ……

Nội dung hướng dẫn: …….....

……..

……..

Đề tài tốt nghiệp được giao ngày 01 tháng 7 năm 2019

Yêu cầu phải hoàn thành trước ngày 21 tháng 9 năm 2019

Đã nhận nhiệm vụ: Đ.T.T.N	Đã nhận nhiệm vụ: Đ.T.T.N
Sinh viên	Cán bộ hướng dẫn Đ.T.T.N
Trần Văn Quyết	Ngô Trường Giang

Hải Phòng, ngày .....tháng.....năm 2019

HIỆU TRƯỞNG

GS.TS.NGUT Trần Hữu Nghị

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

PHIẾU NHẬN XÉT CỦA CÁN BỘ HƯỚNG DẪN TỐT NGHIỆP

Họ và tên: Ngô Trường Giang

Cơ quan công tác: Khoa Công nghệ Thông tin

Họ tên sinh viên: Trần Văn Quyết

Ngành: Công nghệ Thông tin

Nội dung hướng dẫn:

- Tìm hiểu tổng quan về an toàn an ninh mạng
- Tìm hiểu phần mềm nguồn mở pfsense
- Triển khai một số dịch vụ cơ bản trên pfsence để tăng cường an ninh.

1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp:
   - Sinh viên tích cực, chủ động tìm đọc các tài liệu liên quan tới đề tài
   - Chấp hành nghiêm túc kế hoạch, tiến độ đề ra.

2. Đánh giá chất lượng của đồ án (so với nội dung yêu cầu đã đề ra trong nhiệm vụ đề tài tốt nghiệp trên các mặt lý luận, thực tiễn, tính toán số liệu..):
   - Về mặt lý thuyết: Đồ án đã trình bày tổng quan về an ninh mạng máy tính, một số giải pháp tăng cường an ninh mạng máy tính.
   - Về mặt thực nghiệm: Đồ án đã triển khai cấu hình một số dịch vụ tăng cường an ninh mạng như: giới hạn truy cập, Giới hạn tốc độ download/upload cho từng client, Chứng thực user truy cập web, hệ thống backup Firewall, mạng riêng ảo Site – to – site và Client – to site.
   - Về hình thức: Báo cáo trình bày sáng sủa, bố cục hợp lý.
   - Đồ án đáp ứng được yêu cầu đề ra.
3. Ý kiến của cán bộ hướng dẫn:

Đạt ☐ Không đạt ☐ Điểm:……...

Ngày 30 tháng 9 năm 2019

Cán bộ hướng dẫn

TS. Ngô Trường Giang

QC20-B18

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN CHẤM PHẢN BIỆN

Họ và tên giảng viên: Phùng Anh Tuấn

Đơn vị công tác: khoa Công nghệ Thông tin - trường ĐHDL Hải Phòng

Họ và tên sinh viên: Trần Văn Quyết - Ngành: Công nghệ Thông tin

Đề tài tốt nghiệp: Nghiên cứu triển khai giải pháp đảm bảo an ninh mạng trên nền PFSENSE.

1. Phần nhận xét của giảng viên chấm phản biện

- An ninh mạng là vấn đề nóng trong lĩnh vực quản trị mạng do đó việc tăng cường an ninh cho hệ thống mạng là điều cần được quan tâm.
- Nội dung đồ án có tính ứng dụng thực tế tốt.
- Đáp ứng được yêu cầu của một đồ án tốt nghiệp ngành CNTT.

2. Những mặt còn hạn chế

- Kiến thức nền chỉ trình bầy lý thuyết và chưa có ví dụ minh họa.
- Hình ảnh minh họa cài đặt cấu hình pfsense mờ chưa rõ nét
- Kết quả thực nghiệm bước đầu mới chỉ thực hiện trên máy tính ảo.

3. Ý kiến của giảng viên chấm phản biện

Được bảo vệ ☐ Không được bảo vệ ☐ Điểm:…….

Hải Phòng, ngày 08 tháng 10 năm 2019

Giảng viên chấm phản biện

(Ký và ghi rõ họ tên)

LỜI CẢM ƠN

Sau hơn ba tháng nỗ lực tìm hiểu và thực hiện, đồ án "Nghiên cứu và triển khai hệ thống firewall mã nguồn mở cho doanh nghiệp vừa và nhỏ" đã được hoàn thành, ngoài sự cố gắng hết mình của bản thân, em còn nhận được nhiều sự động viên, khích lệ từ gia đình, thầy cô và bạn bè.

Em xin bày tỏ lòng biết ơn sâu sắc tới thầy Ngô Trường Giang đã tận tình hướng dẫn, chỉ bảo và dành rất nhiều thời gian quý báu của thầy cho em trong thời gian qua, đã giúp em hoàn thành đồ án đúng thời hạn.

Em xin cảm ơn các thầy cô giáo khoa Công nghệ thông tin trường Đại học Dân lập Hải Phòng đã giảng dạy, trang bị cho em những kiến thức chuyên ngành, chuyên môn, chuyên sâu trong suốt 4 năm qua.

Mặc dù em đã cố gắng hết sức để hoàn thành đồ án tốt nghiệp này, nhưng vì tham khảo ở nhiều nguồn tài liệu khác nhau, cộng thêm kiến thức còn nhiều hạn chế, do đó không thể tránh khỏi những thiếu sót. Em rất mong nhận được sự thông cảm và đóng góp, chỉ bảo tận tình của quý thầy cô và các bạn để đồ án ngày càng hoàn thiện hơn.

Em xin chân thành cảm ơn!

MỞ ĐẦU

Ngày nay, máy tính và mạng internet 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.

Xác định được tầm quan trọng trong việc bảo mật hệ thống mạng của doanh nghiệp nên em đã chọn và nghiên cứu đề tài "Nghiên cứu triển khai giải pháp đảm bảo an ninh mạng trên nền Pfsense" với mục đích tìm hiểu sâu sắc về cơ chế hoạt động của nó cũng như phát hiện ra những nhược điểm tìm giải pháp khắc phục những nhược điểm này để hệ thống mạng trong doanh nghiệp luôn được vấn hành trơn tru, an toàn và hạn chế sự cố xảy ra.

Đồ án được chia thành 3 nội dung chính :

- Chương 1 : An ninh mạng máy tính.
- Chương 2 : Giải pháp tăng cường an ninh mạng.
- Chương 3 : Giải pháp proxy server trên Pfsense.

MỤC LỤC

DANH MỤC HÌNH VẼ

CHƯƠNG 1: AN NINH MẠNG MÁY TÍNH

1.1 Các nguyên tắc nền tảng của an ninh mạng

An ninh mạng máy tính (network sevurity) là tổng thể các giải pháp về mặt tổ chức và kỹ thuật nhằm ngăn cản mọi nguy cơ tổn hại đến mạng.

Các tổn hại có thể xảy ra do:

- Lỗi của người sử dụng.
- Các lỗ hổng trong các hệ điều hành cũng như các chương trình ứng dụng.
- Các hành động hiểm độc.
- Các lỗi phần cứng.
- Các nguyên nhân khác từ tự nhiên.

An ninh mạng máy tính bao gồm vo số các phương pháp được sử dụng để ngăn cản các sự kiện trên, nhưng trước hết tập trung vào việc ngăn cản:

- Lỗi của người sử dụng.
- Các hành động hiểm độc.

Số lượng các mạng máy tính tăng lên rất nhanh. Ngày càng trở thành phức tạp và phải thực hiện các nhiệm vụ quan trọng hơn.

Mang lại những thách thức mới cho những ai sử dụng và quản lý chúng. Sự cần thiết phải hội nhập các dịch vụ vào cùng một hạ tầng cơ sở mạng tất cả trong một là một điều hiển nhiên, làm phát sinh nhanh chóng việc các công nghệ đưa vào các sản phẩm có liên quan đến an ninh còn non nớt. Do các nhà quản lý mạng phải cố gắng triển khai những công nghệ mới nhất vào hạ tầng cơ sở mạng của mình. Nên an ninh mạng trở thành một chức năng then chốt trong việc xây dựng và duy trì các mạng hiện đại của mọi tổ chức.

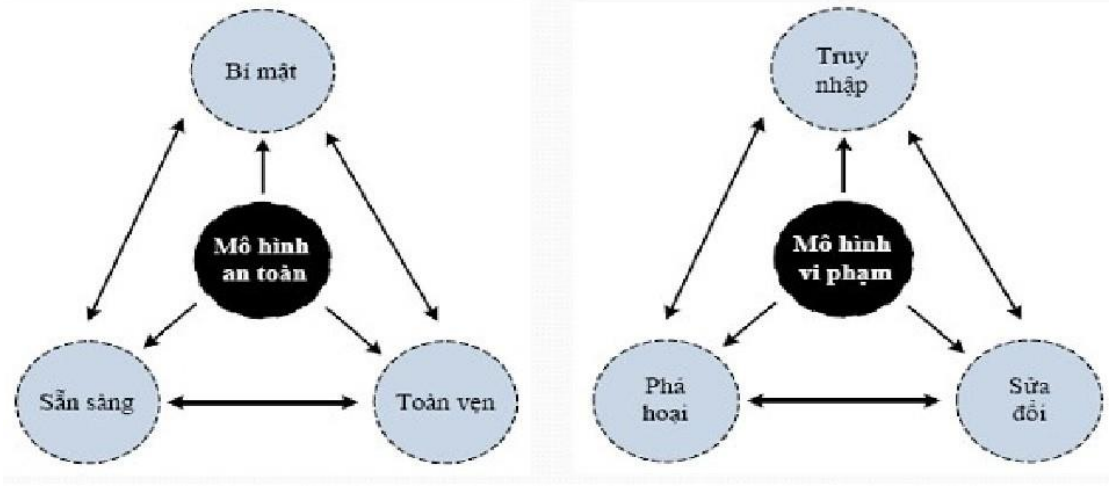
Các nguyên tắc nền tảng :

- Tính bí mật.
- Tính toàn vẹn.
- Tính sẵn sàng.

Tùy thuộc vào ứng dụng và hoàn cảnh cụ thể, mà một trong ba nguyên tắc này sẽ quan trọng hơn những cái khác.

1.1.1 Mô hình CIA

Confidentiality (tính bảo mật), Integrity (tính toàn vẹn), Availability (tính sẵn sàng), được gọi là: Mô hình bộ ba CIA. Ba nguyên tắc cốt lõi này phải dẫn đường cho tất cả các hệ thống an ninh mạng. Bộ ba CIA cũng cung cấp một công cụ đo (tiêu chuẩn để đánh giá) đối với các thực hiện an ninh. Mọi vi phạm bất kỳ một trong ba nguyên tắc này đều có thể gây hậu quả nghiêm trọng đối với tất cả các thành phần có liên quan.



Hình 1-1 Mô hình CIA

1.1.1.1 Tính bí mật

Bí mật là sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. Đó là khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhạy cảm đó được che giấu với người dùng không được

cấp phép. Đối với an ninh mạng thì tính bí mật rõ ràng là điều đầu tiên được nói đến và nó thường xuyên bị tấn công nhất.

1.1.1.2 Tính toàn vẹn

Toàn vẹn là sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó đảm bảo được sự chính xác của thông tin và hệ thống.

Có ba mục đích chính của việc đảm bảo tính toàn vẹn:

- Ngăn cản sự làm biến dạng nội dung thông tin của những người sử dụng không được phép.
- Ngăn cản sự làm biến dạng nội dung thông tin không được phép hoặc không chủ tâm của những người sử dụng được phép.
- Duy trì sự toàn vẹn dữ liệu cả trong nội bộ và bên ngoài.

1.1.1.3 Tính sẵn sàng

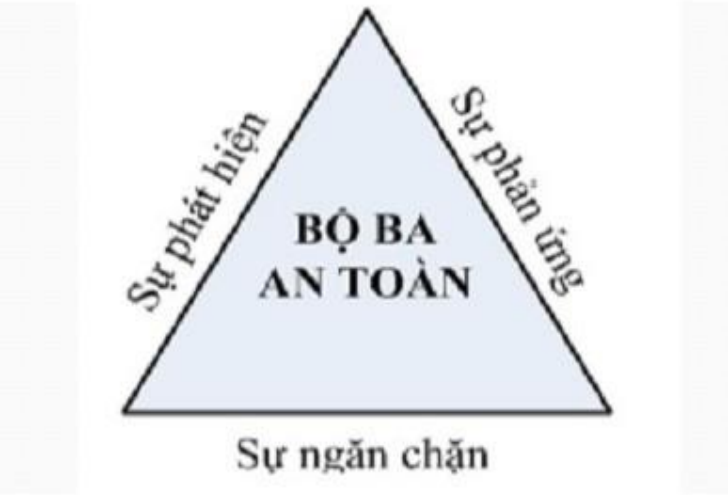
Tính sẵn sàng bảo đảm các người sử dụng hợp pháp của hệ thống có khả năng truy cập đúng lúc và không bị ngắt quãng tới các thông tin trong hệ thống và tới mạng. Tính sẵn sàng có liên quan đến độ tin cậy của hệ thống.

1.1.2 Mô hình bộ ba an ninh

Một mô hình rất quan trọng có liên quan trực tiếp đến quá trình phát triển và triển khai của mọi tổ chức là mô hình bộ ba an ninh (security trinity). Ba khía cạnh của mô hình bộ ba an ninh là:

- sự phát hiện (Detection).
- sự ngăn chặn (Prevention).
- sự phản ứng (Response).

Chúng kết hợp thành các cơ sở của an ninh mạng.



Hình 1-2 Mô hình bộ ba an toàn

1.1.2.1 Sự ngăn chặn

Nền tảng của bộ ba an ninh là sự ngăn chặn. Nó cung cấp mức độ an ninh cần thiết nào đó để thực hiện các biện pháp ngăn chặn sự khai thác các lỗ hổng. Trong khi phát triển các giải pháp an ninh mạng, các tổ chức cần phải nhấn mạnh vào các biện pháp ngăn chặn hơn là vào sự phát hiện và sự phản ứng vì sẽ là dễ dàng, hiệu quả và có giá trị nhiều hơn để ngăn chặn một sự vi phạm an ninh hơn là thực hiện phát hiện hoặc phản ứng với nó.

1.1.2.2 Sự phát hiện

Cần có các biện pháp cần thiết để thực hiện phát hiện các nguy cơ hoặc sự vi phạm an ninh trong trường hợp các biện pháp ngăn chặn không thành công. Một sự vi phạm được phát hiện sớm sẽ dễ dàng hơn để làm mất tác hại và khắc phục nó. Như vậy, sự phát hiện không chỉ được đánh giá về mặt khả năng, mà còn về mặt tốc độ, tức là phát hiện phải nhanh.

1.1.2.3 Sự phản ứng

Phải phát triển một kế hoạch để đưa ra phản ứng phù hợp đối với một số lỗ hổng an ninh. Kế hoạch đó phải được viết thành văn bản và phải xác định ai là người chịu trách nhiệm cho các hành động nào và khi thay đổi các phản ứng và các mứcđộ cần tăng cường. Tính năng phản ứng của một hệ thống an

ninh không chỉ là năng lực, mà còn là vấn đề tốc độ.Ngày nay các cuộc tấn công mạng rất đa dạng, sẽ không thể đoán chắc được chúng sẽ xảy ra khi nào, ở đâu, dạng nào và hậu quả của chúng. Vì vậy để đảm bảo an ninh cho một mạng thì cần:

- Phát hiện nhanh.
- Phản ứng nhanh.
- Ngăn chặn thành công mọi hình thức tấn công.

Đây là một nhiệm vụ hết sức khó khăn cho các nhà quản lý và các nhà cung cấp dịch vụ mạng.

1.2 Các nguy cơ mất an ninh mạng

1.2.1 Các nguy cơ

- Các người bên ngoài và các hacker.
- Các người đang làm việc trong công ty.
- Các ứng dụng mà cán bộ và nhân viên của công ty sử dụng để thực hiện các nhiệm vụ thương mại của họ.
- Các hệ điều hành chạy trên các máy tính cá nhân, các máy chủ, cũng như các thiết bị khác.
- Hạ tầng cơ sở mạng được sử dụng để truyền tải dữ liệu qua mạng, như là các bộ định tuyến (router), các bộ chuyển mạch (switch), các bộ tập trung (hub), các bức tường lửa (firewall) và các thiết bị khác.
- Sử dụng cách tiếp cận phân chia và chinh phục (divide-and-conquer).
- Các điểm yếu trong việc hoạch định chính sách.
- Các điểm yếu trong các công nghệ máy tính.
- Các điểm yếu trong các cấu hình thiết bị.

1.2.2 Các điểm yếu trong giao thức mạng

- Các điểm yếu trong giao thức mạng có liên quan đến các lỗ hổng trong các giao thức mạng đang vận hành và các ứng dụng sử dụng các giao thức này.
- Một bộ giao thức phổ biến và được sử dụng nhiều nhất trên mạng là TCP/IP. TCP/IP là một bộ các giao thức, bao gồm các giao thức IP, TCP, UDP, ICMP, OSPF, IGRP, EIGRP, ARP, RARP, ….

1.2.3 Các điểm yếu trong hệ điều hành

Mỗi một hệ điều hành đang sử dụng đều có một hoặc nhiều các lỗ hổng an ninh trong đó. Đây là một sự thật hiển nhiên của các hệ điều hành được sử dụng rộng rãi, vì thế các hacker hướng vào các lỗ hổng này để tấn công.

1.2.4 Các điểm yếu trong thiết bị mạng

Các điểm yếu trong các thiết bị mạng được xem là các nguy cơ an ninh dễ bị tổn thương (bị tấn công) đối với các thiết bị mạng như là các router, các switch, các firewall, …, chúng cũng hoạt động dựa trên các hệ điều hành.

1.2.5 Các điểm yếu trong các cấu hình thiết bị

Các điểm yếu trong các cấu hình thiết bị là một trong các vấn đề an ninh khó giải quyết nhất, bởi vì các điểm yếu này có liên quan trực tiếp đến các lỗi do con người vô tình gây ra khi cấu hình thiết bị hoặc không hiểu được thiết bị cần phải cấu hình như thế nào. Phải quan tâm tới các mật khẩu:

- Các mật khẩu có dễ dàng đoán ra không ?
- Các mật khẩu có thường xuyên được thay đổi không ?
- Các mật khẩu có truyền qua mạng trong dạng bản rõ không ?

1.3 Giải pháp kỹ thuật trong lập kế hoạch an ninh mạng

1.3.1 Sử dụng các nền tảng khác nhau

Một trong các vấn đề khó khăn nhất mà sẽ phải đối mặt khi thiết kế một giải pháp an ninh là khi cố gắng tìm kiếm một giải pháp "một phù hợp cho tất

cả" (one-sizefits-all), hay nói một cách khác là việc cố gắng tích hợp tất cả các sản phẩm an ninh mạng chỉ từ một nhà cung cấp, với hệ thống quản lý mà nó dễ dàng cho phép thực hiện các chính sách an ninh thông qua tất cả các sản phẩm an ninh của mình. Vì thế, giải pháp an ninh phải chứa đựng nhiều dạng thiết bị phần cứng, cũng như các ứng dụng phần mềm. Sau đây đưa ra một danh sách nhỏ của một vài dạng thiết bị mà giải pháp an ninh có liên quan đến:

- Các máy tính để bàn và các máy tính xách tay chạy các hệ điều hành Windows 2000, 2003, XP, Vista, 7, cũng như các hệ điều hành UNIX, Macintosh….
- Các máy chủ chạy các hệ điều hành Windows NT, 2000, 2003, NetWare, Linux, Solaris, HP-UX, …. - Các máy tính lớn (Maiframe) chạy Multiple Virtual Storage (MVS) và Vitual Machine (VM);
- Các thiết bị định tuyến của các hãng Cisco, Juniper, Nortel, Lucent,….
- Các thiết bị chuyển mạch của các hãng Cisco, Foundry, Extreme, ….

1.3.2 Sử dụng các mô hình an ninh mạng

Một bước quan trọng nhất trong thiết kế và phân tích các hệ thống an ninh là mô hình an ninh, bởi vì nó tích hợp chính sách an ninh mà bắt buộc phải tuân thủ trong hệ thống. Một mô hình an ninh là một sự miêu tả tượng trưng của một chính sách an ninh. Nó ánh xạ các yêu cầu của chính sách an ninh tạo thành các luật và các quy tắc của một hệ thống mạng. Một chính sách an ninh là một tập hợp các mục tiêu tổng quan và các yêu cầu mức cao, còn mô hình an ninh sẽ thực hiện nó. Các mô hình an ninh có ba phương án cơ bản được sử dụng để phát triển một mô hình an ninh mạng. Thông thường,

các tổ chức thực hiện một sự kết hợp nào đó của ba phương án để đảm bảo an ninh mạng. Ba phương án thực hiện là:

- Mô hình an ninh nhờ sự mù mờ (security by obscurity model).
- Mô hình bảo vệ vòng ngoài (perimeter defense model).
- Mô hình bảo vệ theo chiều sâu (defense in depth model).

1.3.3 Sử dụng các nguyên tắc an ninh

Quyền hạn tối thiểu: nguyên tắc cơ bản nhất của một hệ thống an ninh mạng là cơ chế đặc quyền tối thiểu. Nguyên tắc này hạn chế phơi bày các yếu điểm của hệ thống và giảm các rủi ro có thể xảy ra và rủi ro do bị tấn công.

Phòng thủ theo chiều sâu: tức là phòng thủ cần có nhiều lớp, nhiều hệ thống phòng thủ để chúng hỗ trợ lẫn nhau.

Nút thắt: nút thắt đặt tại các cổng vào/ra xác định, cơ chế này bắt buộc đối phương chỉ có thể thâm nhập vào hệ thống qua một kênh hẹp (nơi này có thể giám sát và điều khiển được).

Điểm yếu nhất: phải xác định được chỗ nào là điểm yếu nhất của hệ thống để tăng cường an ninh, vì các hacker thường tìm mọi cách để phát hiện ra những điểm yếu này và tập trung mọi tấn công vào đó.

Cơ chế tự động ngắt khi có sự cố: trong những trường hợp xấu khi một phân hệ bảo vệ của toàn hệ thống gặp sự cố, hệ thống có thể tự tắt hoặc ngắt phần bị sự cố để ngăn chặn sự truy cập của đối phương vào hệ thống hoặc các vùng khác.

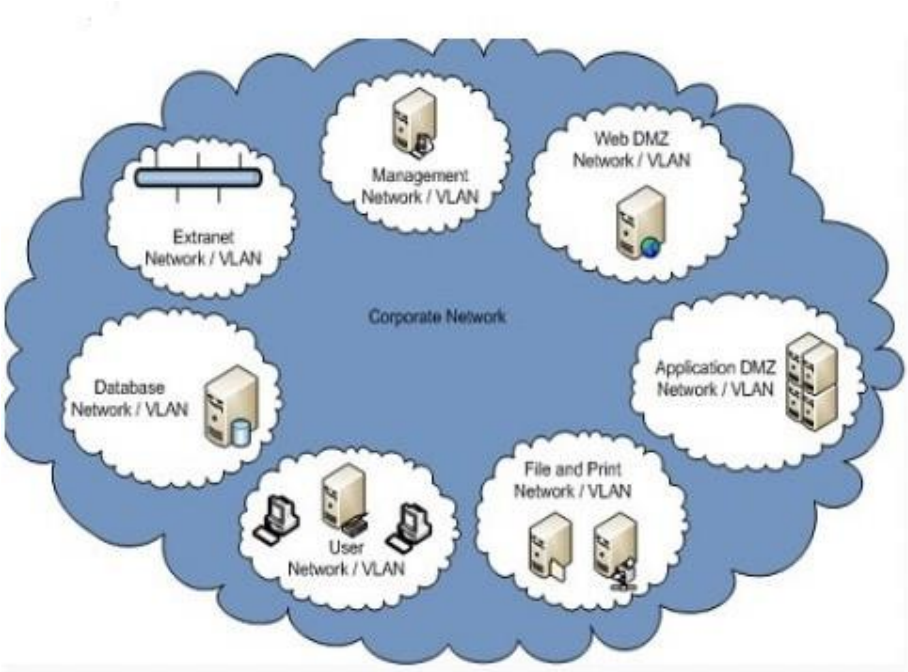
Mọi thành phần đều phải tham gia chế độ an ninh: tất cả các thành phần của hệ thống đều phải kết hợp thành một hệ thống bảo vệ hỗ trợ và kiểm soát lẫn nhau. Nếu có một số phân hệ không tham gia chế độ an ninh, thì toàn bộ hệ thống đó coi như không được an ninh.

Tính đa dạng của hệ thống phòng thủ: mức độ an ninh của hệ thống sẽ tăng lên nếu sử dụng nhiều môđun hoặc nhiều phương án phòng thủ khác nhau.

Tính đơn giản: một hệ thống phức tạp thường có nhiều lỗi và rất khó kiểm soát do đó cần phải đơn giản hóa một hệ thống bảo vệ.

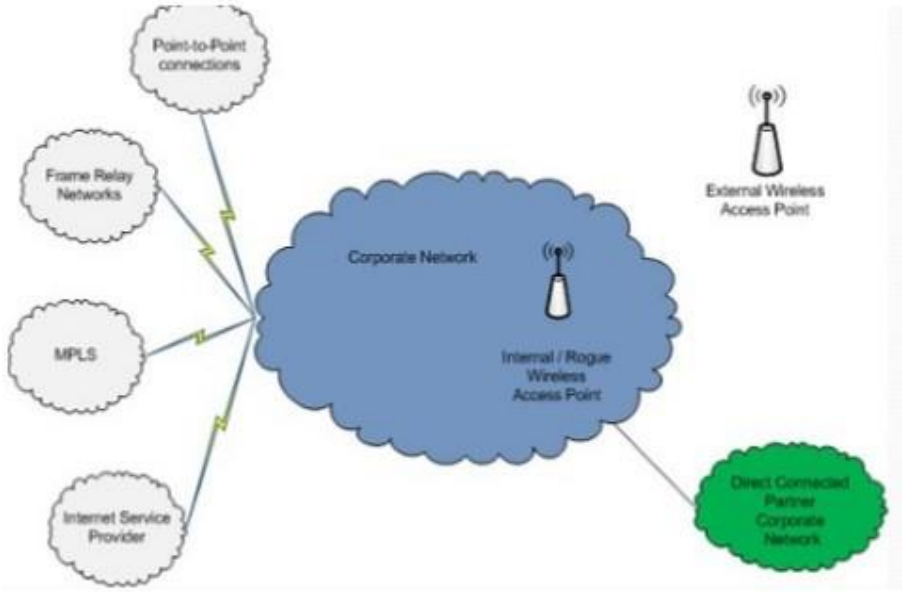
1.3.4 Sử dụng các giải pháp an ninh

- Giải pháp phân mảnh mạng.



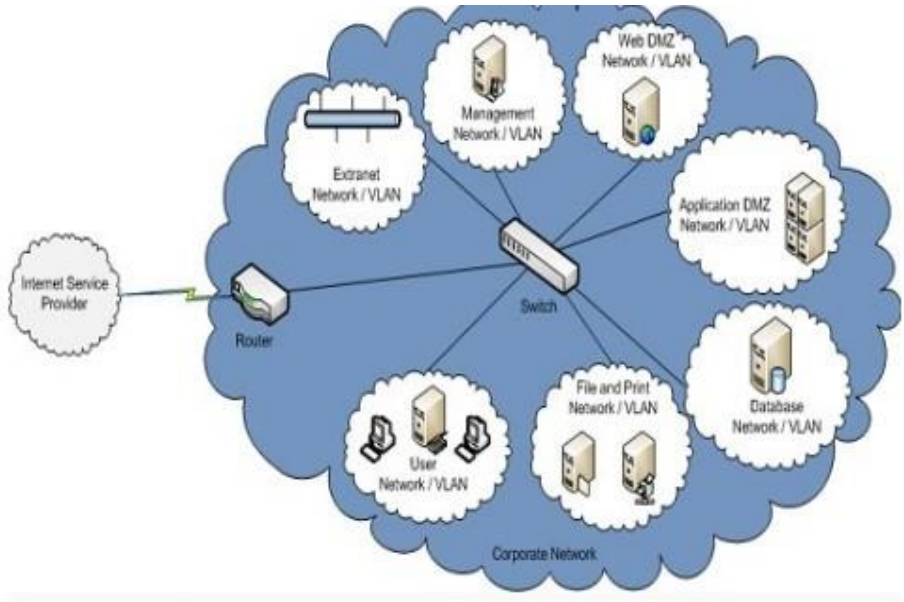
Hình 1-3 Mô hình giải pháp an ninh mạng

- Quản lý các điểm truy nhập.



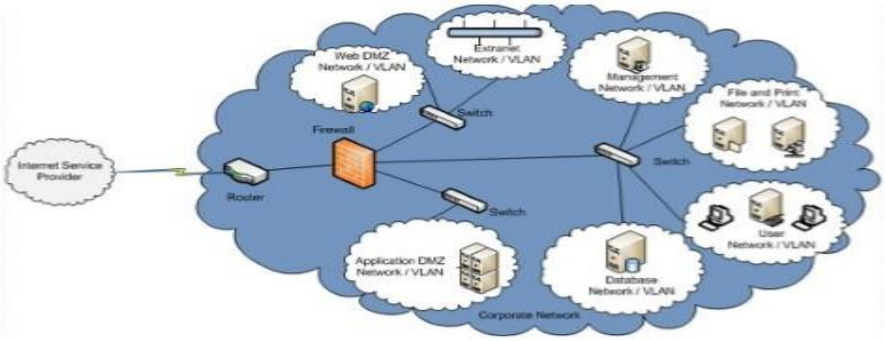
Hình 1-4 Mô hình quản lý các điểm truy cập

- Các bộ định tuyến và chuyển mạch.



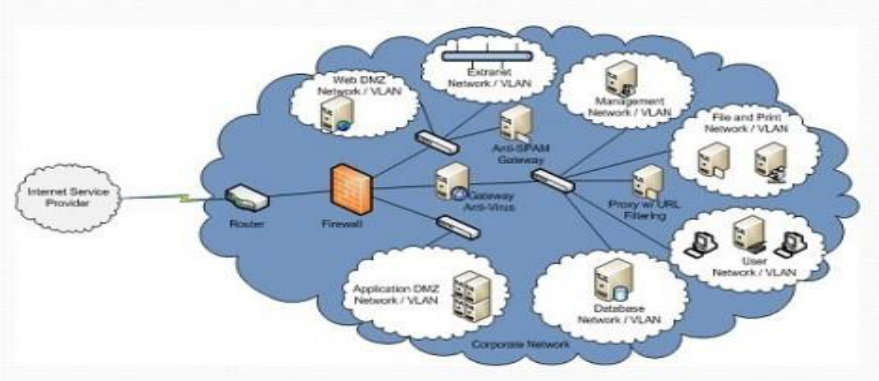
Hình 1-5 Mô hình định tuyến và chuyển mạch

- Giải pháp bức tường lửa.



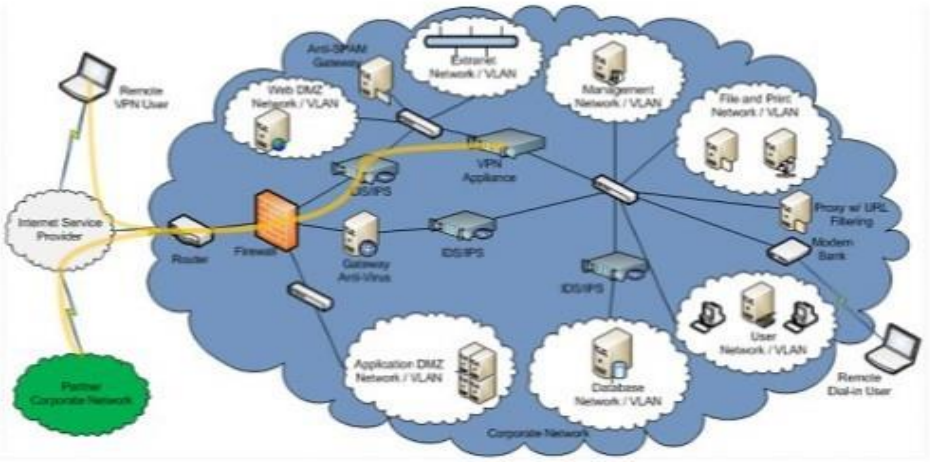
Hình 1-6 Mô hình bức tường lửa

- Giải pháp lọc nội dung.



Hình 1-7 Mô hình giải pháp lọc nội dung

- Điều khiển truy nhập từ xa.



Hình 1-8 Mô hình điều khiển truy cập từ xa

Một số giải pháp khác:

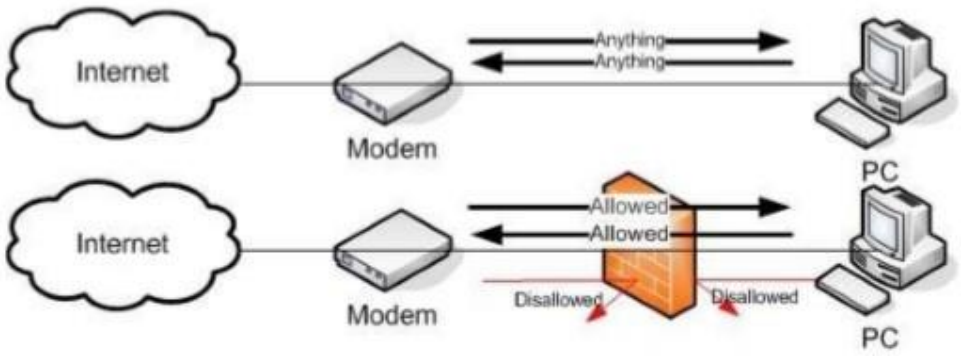
- Các chính sách an ninh.
- Giải pháp phòng chống mã độc (AntiMalware)
- Điều khiển truy nhập mạng (Network Admission Control – NAC).
- Các dịch vụ xác thực (Authentication Services).
- Quản lý các miếng vá (Patch Management).
- Các cổng lớp ứng dụng (Application Layer Gateway).
- Giải pháp phát hiện và phòng chống xâm nhập.
- Quản lý các sự kiện an ninh.
- Quản lý các tổn thương.
- Giải pháp mật mã.

CHƯƠNG 2: GIẢI PHÁP TĂNG CƯỜNG AN NINH MẠNG

2.1 Hệ thống tường lửa (Firewall)

2.1.1 Khái niệm về Firewall

Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát lưu lượng truy cập vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Nó kiểm soát các truy cập đến nguồn lực của mạng thông qua một mô hình kiểm soát chủ động. Nghĩa là, chỉ những lưu lượng truy cập phù hợp với chính sách được định nghĩa trong tường lửa mới được truy cập vào mạng, mọi lưu lượng truy cập khác đều bị từ chối.



Hình 2-1 Firewall

2.1.2 Chức năng chính của Firewall

Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet.

Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet.

Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).

Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).

Theo dõi luồng dữ liệu mạng giữa Internet và Intranet. Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.

Kiểm soát người sử dụng và việc truy nhập của người sử dụng. Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng.

2.1.3 Phân loại Firewall

Firewall được chia làm 2 loại gồm: Firewall cứng và Firewall mềm.

2.1.3.1 Đặc điểm Firewall mềm

Firewall mềm được cài đặt trên các máy tính cá nhân trên mạng. Không giống như Firewall cứng, Firewall mềm có thể dễ dàng phân biệt các chương trình trên máy tính, điều này cho phép dữ liệu vào một chương trình trong khi chặn một chương trình khác. Firewall mềm cũng có thể lọc dữ liệu gửi đi, cũng như các phản hồi từ xa cho các yêu cầu gửi đi. Nhược điểm chính của Firewall mềm cho một doanh nghiệp là: yêu cầu cài đặt, cập nhật và quản trị trên mỗi máy tính cá nhân.

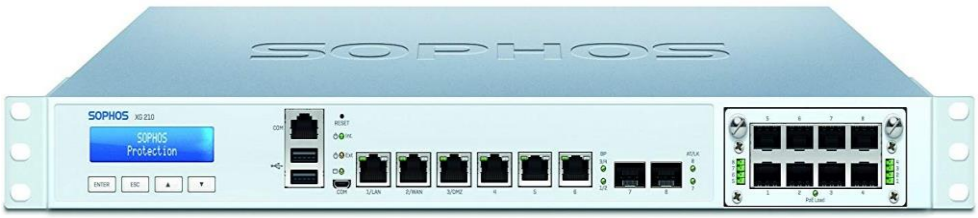
Firewall mềm được cài đặt trên các máy chủ riêng lẻ giúp chặn mỗi yêu cầu kết nối và sau đó xác định xem yêu cầu có hợp lệ hay không. Firewall xử lý tất cả các yêu cầu bằng cách sử dụng tài nguyên máy chủ.

Trong khi so sánh với Firewall cứng, Firewall mềm hoặc Firewall Opensource (tường lửa mã nguồn mở) dễ cấu hình và thiết lập hơn.

Firewall mềm cung cấp cho người dùng quyền kiểm soát hoàn toàn lưu lượng truy cập Internet của họ thông qua giao diện thân thiện với người dùng yêu cầu ít hoặc không có kiến thức.

2.1.3.2 Đặc điểm Firewall cứng

Firewall cứng nằm giữa mạng máy tính cục bộ và Internet, Firewall cứng sẽ kiểm tra tất cả các dữ liệu đến từ Internet, đi qua các gói dữ liệu an toàn trong khi chặn các gói dữ liệu nguy hiểm tiềm ẩn



Hình 2-2 Firewall cứng

Để bảo vệ đúng mạng mà không cản trở hiệu suất, tường lửa firewall cứng yêu cầu người thiết lập phải có kiến thức chuyên sâu và do đó có thể không phải là giải pháp khả thi cho các công ty không có bộ phận công nghệ thông tin chuyên dụng. Tuy nhiên, đối với các doanh nghiệp có nhiều máy tính, có thể kiểm soát an ninh mạng từ một thiết bị đơn giản hóa công việc.

Các doanh nghiệp thường có tường lửa phần cứng chuyên dụng có nhiều công cụ khác nhau để giúp chặn các mối đe dọa ở ngoại vi của mạng. Bằng cách này, người quản trị có thể lọc email và lưu lượng truy cập web (trong số những thứ khác) cho tất cả mọi người.

Tường lửa phần cứng được tích hợp vào bộ định tuyến nằm giữa máy tính và Internet. Người quản trị thường sử dụng lọc gói, có nghĩa là họ quét tiêu đề gói để xác định nguồn gốc, nguồn gốc, địa chỉ đích và kiểm tra với quy tắc người dùng hiện có được xác định để đưa ra quyết định cho phép / từ chối.

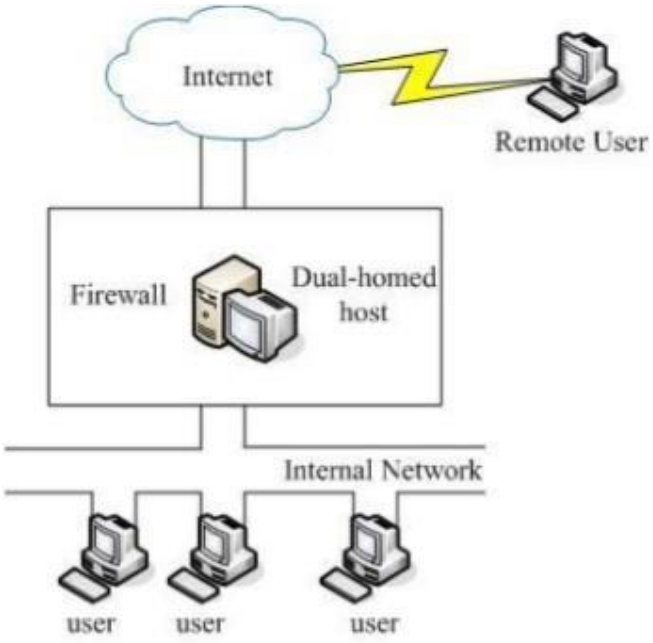
Tường lửa phần cứng được thiết lập cho thời gian phản hồi nhanh hơn do phần cứng và phần mềm được đồng bộ một cách tối đa giúp phát huy hết hiệu năng của tường lửa phần cứng giúp nó có thể xử lý nhiều lưu lượng truy cập hơn.

Tường lửa có hệ điều hành riêng ít bị tấn công hơn, điều này lần làm giảm nguy cơ bảo mật và ngoài ra, tường lửa phần cứng có các điều khiển bảo mật nâng cao.

Tường lửa phần cứng là một thành phần mạng nội bộ, nó có thể được quản lý tốt hơn.

2.1.4 Kiến trúc cơ bản của FireWall

2.1.4.1 Kiến trúc Dual-homed Host



Hình 2-3 Kiến trúc Dual-homed Host

Dual-homed Host là hình thức xuất hiện đầu tiên trong việc bảo vệ mạng nội bộ. Dual-homed Host là một máy tính có hai giao tiếp mạng (Network interface): một nối với mạng cục bộ và một nối với mạng ngoài (Internet).

Hệ điều hành của Dual-home Host được sửa đổi để chức năng chuyển các gói tin (Packet forwarding) giữa hai giao tiếp mạng này không hoạt động. Để làm việc được với một máy trên Internet, người dùng ở mạng cục bộ trước hết phải login vào Dual-homed Host, và từ đó bắt đầu phiên làm việc. [2]

Đánh giá về Dual-homed Host:

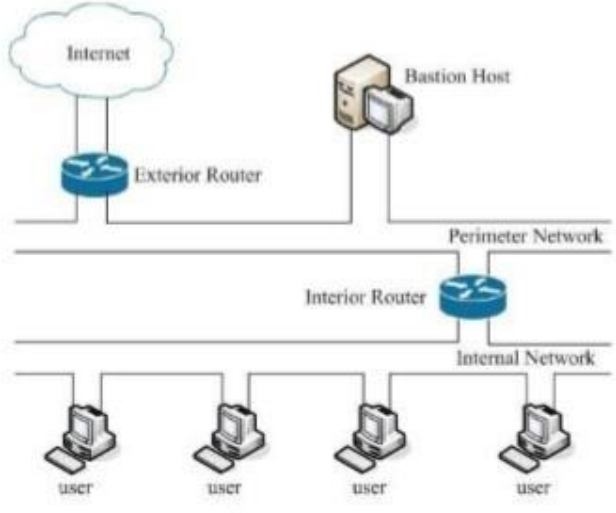
Để cung cấp dịch vụ cho những người sử dụng mạng nội bộ có một số giải pháp như sau:

- Kết hợp với các Proxy Server cung cấp những Proxy Service.
- Cấp các tài khoản người dùng trên máy dual-homed host này và khi mà người sử dụng muốn sử dụng dịch vụ từ Internet hay dịch vụ từ external network thì họ phải logging in vào máy này.

Phương pháp cấp tài khoản người dùng trên máy dual-homed host khá phức tạp, vì mỗi lần người dùng muốn sử dụng dịch vụ thì phải logging in vào máy khác (dual-homed host) khác với máy của họ, đây là vấn đề rất không thuận tiện với người sử dụng.

Nếu dùng Proxy Server: khó có thể cung cấp được nhiều dịch vụ cho người sử dụng vì phần mềm Proxy Server và Proxy Client không phải loại dịch vụ nào cũng có sẵn. Hoặc khi số dịch vụ cung cấp nhiều thì khả năng đáp ứng của hệ thống có thể giảm xuống vì tất cả các Proxy Server đều đặt trên cùng một máy.

2.1.4.2 Kiến trúc Screend Subnet Host



Hình 2-4 Kiến trúc Screend Subnet Host

Với kiến trúc này, hệ thống này bao gồm hai Packet-Filtering Router và một máy chủ. Kiến trúc này có độ an toàn cao nhất vì nó cung cấp cả mức bảo mật: Network và Application trong khi định nghĩa một mạng perimeter network. Mạng trung gian (DMZ) đóng vai trò của một mạng nhỏ, cô lập đặt giữa Internet và mạng nội bộ. Cơ bản, một MẠNG TRUNG GIAN được cấu hình sao cho các hệ thống trên Internet và mạng nội bộ chỉ có thể truy nhập được một số giới hạn các hệ thống trên mạng MẠNG TRUNG GIAN, và sự truyền trực tiếp qua mạng MẠNG TRUNG GIAN là không thể được.

Và những thông tin đến, Router ngoài (Exterior Router) chống lại những sự tấn công chuẩn (như giả mạo địa chỉ IP), và điều khiển truy nhập tới mạng trung gian. Nó chỉ cho phép hệ thống bên ngoài truy nhập máy chủ. Router trong (Interior Router) cung cấp sự bảo vệ thứ hai bằng cách điều khiển mạng trung gian truy nhập vào mạng nội bộ chỉ với những truyền thông bắt đầu từ Bastion Host (máy chủ).

Với những thông tin đi, Router điều khiển mạng nội bộ truy nhập tới mạng trung gian. Nó chỉ cho phép các hệ thống bên trong truy nhập tới máy chủ. Quy luật Filtering trên Router ngoài yêu cầu sử dụng dịch vụ Proxy bằng cách chỉ cho phép thông tin ra bắt nguồn từ Máy chủ.

Đánh giá về kiến trúc Screend Subnet Host :

- Đối với những hệ thống yêu cầu cung cấp dịch vụ nhanh, an toàn cho nhiều người sử dụng đồng thời cũng như khả năng theo dõi lưu thông của mỗi người sử dụng trong hệ thống và dữ liệu trao đổi giữa các người dùng trong hệ thống cần được bảo vệ thì kiến trúc cơ bản trên phù hợp.
- Để tăng độ an toàn trong mạng nội bộ, kiến trúc screened subnet ở trên sử dụng thêm một mạng DMZ (DMZ hay perimeter network) để che

phần nào lưu thông bên trong mạng nội bộ. Tách biệt mạng nội bộ với Internet.

- Sử dụng 2 Screening Router (bộ định tuyến lọc): Router ngoài và Router trong.
- Áp dụng qui tắc dư thừa có thể bổ sung thêm nhiều mạng trung gian (DMZ và perimeter network) càng tăng khả năng bảo vệ càng cao.
- Ngoài ra, còn có những kiến trúc biến thể khác như: sử dụng nhiều Bastion Host (máy chủ) (Máy chủ), ghép chung Router trong và Router ngoài, ghép chung Bastion Host (máy chủ) (Máy chủ) và Router ngoài.[2]

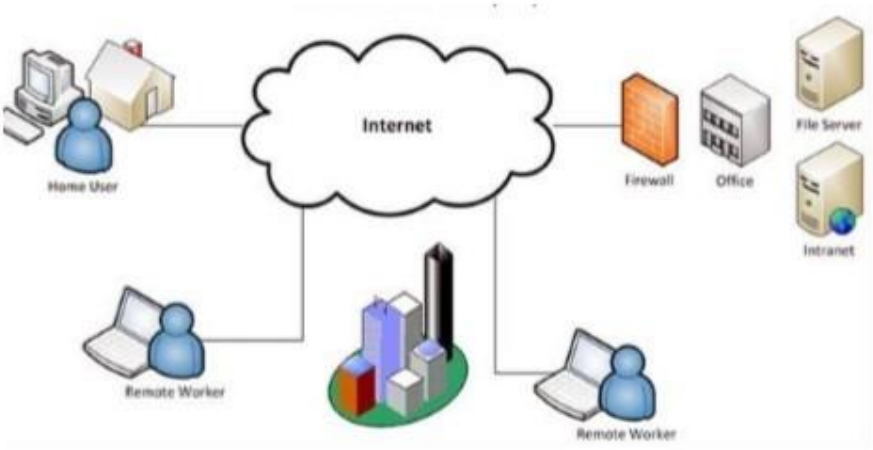
2.2 Mạng riêng ảo

2.2.1 Định nghĩa VPN

VPN được hiểu như là một giải pháp mở rộng một mạng riêng thông qua một mạng chung (thường là Internet). Mỗi VPN sẽ kết nối với một VPN khác, các site khác hay nhiều người dùng từ xa. Thay thế cho kết nối thực như leased – line, VPN sử dụng các kết nối ảo được dẫn từ các mạng nội bộ tới các site của người dùng từ xa.

Các giải pháp VPN được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì phạm vi hoạt động rộng (toàn quốc hay toàn cầu). Tài nguyên ở trung tâm có thể kết nối đến từ nhiều nguồn giúp tiết kiệm chi phí và thời gian.

VPN được gọi là mạng ảo bởi chúng chỉ sử dụng các kết nối tạm thời. Những kết nối bảo mật được thiết lập giữa các host, giữa host với mạng hay giữa hai mạng với nhau.



Hình 2-5 Mô hình mạng VPN

2.2.2 Các thành phần tạo nên VPN

2.2.2.1 VPN client

VPN client có thể là một máy tính hoặc một bộ định tuyến. Loại VPN khách hàng sử dụng cho mạng của công ty phụ thuộc vào nhu cầu cá nhân của công ty đó.

Mặt khác, nếu công ty có một vài nhân viên thường xuyên đi công tác xa và cần phải truy cập vào mạng của công ty trên đường đi, máy tính xách tay của nhân viên có thể thiết lập như VPN client.

Về mặt kỹ thuật, bất kỳ hệ điều hành đều có thể hoạt động như một VPN Client miễn là nó có hỗ trợ các giao thức như: giao thức đường hầm điểm-điểm PPTP (Point to Point Tunneling Protocol), giao thức đường hầm lớp 2 L2TP (Layer 2 Tunneling Protocol) và giao thức bảo mật Internet IPSec (Internet Protocol Security). Ngày nay, với các phiên bản Windows mới thì khả năng truy cập mạng VPN càng được phát triển tối ưu hơn, do đó vấn đề không tương thích với các phiên bản hệ điều hành hiện nay là không tồn tại.

2.2.2.2 VPN server

VPN server hoạt động như một điểm kết nối cho các VPN client. Về mặt kỹ thuật, một máy chủ VPN có thể được cài đặt trên một số hệ điều hành như Window Server, Linux …

VPN Server khá đơn giản. Nó là một máy chủ được cài đặt dịch vụ máy chủ định tuyến và truy cập từ xa RRAS (Routing and Remote Access Server). Khi một kết nối VPN đã được chứng thực, các máy chủ VPN chỉ đơn giản là hoạt động như một bộ định tuyến cung cấp cho khách hàng VPN có thể truy cập đến một mạng riêng

2.2.2.3 Firewall

Các thành phần khác theo yêu cầu của mạng riêng ảo VPN (Virtual Private Network) là một tường lửa tốt. Máy chủ VPN chấp nhận kết nối từ mạng ngoài, nhưng điều đó không có nghĩa là mạng ngoài cần phải có quyền truy cập đầy đủ đến máy chủ VPN. Chúng ta phải sử dụng một tường lửa để chặn bất kỳ cổng nào không sử dụng.

Yêu cầu cơ bản cho việc thiết lập kết nối VPN là địa chỉ IP của máy chủ VPN có thông qua tường lửa để tiếp cận với máy chủ VPN.

Chúng ta có thể đặt một máy chủ ISA giữa tường lửa và máy chủ VPN. Ý tưởng là có thể cấu hình tường lửa để điều chỉnh tất cả lưu lượng truy cập VPN có liên quan đến ISA Server chứ không phải là máy chủ VPN. ISA Server sau đó hoạt động như một proxy VPN. Cả hai VPN Client và VPN Server chỉ giao tiếp với máy chủ ISA mà không bao giờ giao tiếp trực tiếp với nhau. Điều này có nghĩa là ISA Server che chắn các VPN Server từ các VPN Client truy cập đến, vì thế cho VPN Server sẽ có thêm một lớp bảo vệ.

2.2.2.4 Giao thức đường hầm (Tunneling Protocol)

VPN client truy cập vào một máy chủ VPN qua một đường hầm ảo. Đường hầm ảo này là một lối đi an toàn qua môi trường công cộng (như Internet). Để có được đường hầm, cần phải sử dụng một trong các giao thức đường hầm. Một số giao thức để lựa chọn để tạo đường hầm như: IPSec, L2TP, PPTP và GRE. Nhưng để lựa chọn một giao thức đường hầm phù hợp cho một mô hình mạng ở một công ty hay một doanh nghiệp bất kỳ là một

quyết định quan trọng khi lập kế hoạch để triển khai hệ thống VPN cho doanh nghiệp, công ty đó.

Lợi thế lớn nhất mà L2TP hơn PPTP là nó dựa trên IPSec. IPSec mã hóa dữ liệu, cung cấp xác thực dữ liệu, dữ liệu của người gửi sẽ được mã hóa và đảm bảo không bị thay đổi nội dung trong khi truyền.

Mặc dù L2TP có vẻ là có lợi thế hơn so với PPTP, nhưng PPTP cũng có lợi thế riêng đó là khả năng tương thích. PPTP hoạt động tốt với các hệ điều hành Windows hơn L2TP. [3]

2.2.3 Ưu và nhược điểm của VPN

2.2.3.1 Ưu điểm

VPN mang lại lợi ích thực sự và tức thời cho các công ty. Có thể dùng VPN để đơn giản hoá việc thông tin giữa các nhân viên làm việc ở xa, người dùng từ xa, mở rộng Intranet đến từng văn phòng, chi nhánh, không những chúng ta có thể triển khai Extranet đến tận khách hàng và các đối tác chủ chốt mà còn làm giảm chi phí cho các công việc trên thấp hơn nhiều so với việc mua thiết bị và đường dây cho mạng WAN riêng. Những lợi ích này dù trực tiếp hay gián tiếp đều bao gồm: tiết kiệm chi phí, tính mềm dẻo, khả năng mở rộng và một số ưu điểm khác.

2.2.3.2 Nhược điểm

Mặc dù phổ biến nhưng mạng riêng ảo VPN (Virtual Private Network) khi triển khai hệ thống cần lưu ý một số hạn chế.

VPN đòi hỏi sự hiểu biết chi tiết về vấn đề an ninh mạng, việc cấu hình và cài đặt phải cẩn thận, chính xác đảm bảo tính an toàn trên hệ thống mạng Internet công cộng.

Độ tin cậy và hiệu suất của một VPN dựa trên Internet không phải là dưới sự kiểm soát trực tiếp của công ty, vì vậy giải pháp thay thế là hãy sử dụng một nhà cung cấp dịch vụ Internet tốt và chất lượng.

Việc sử dụng các sản phẩm VPN và các giải pháp của các nhà cung cấp khác nhau không phải lúc nào cũng tương thích do các vấn đề về tiêu chuẩn công nghệ VPN. Khi sử dụng pha trộn và kết hợp các thiết bị sẽ có thể gây ra những vấn đề kỹ thuật hoặc nếu sử dụng không đúng cách sẽ lãng phí rất nhiều chi phí triển khai hệ thống.

Một hạn chế hay nhược điểm rất khó tránh khỏi của VPN đó là vấn đề bảo mật cá nhân, bởi vì việc truy cập từ xa hay việc nhân viên kết nối với hệ thống văn phòng bằng máy tính xách tay, máy tính riêng, khi đó nếu các máy tính của họ thực hiện hàng loạt các ứng dụng khác, ngoài việc kết nối tới văn phòng làm việc thì những tin tặc có thể lợi dụng yếu điểm từ máy tính cá nhân của họ tấn công vào hệ thống của công ty. Vì vậy việc bảo mật cá nhân luôn được các chuyên gia khuyến cáo phải đảm bảo an toàn.

2.2.4 Mạng Site – to – Site VPNs

Bên cạnh Remote-acess VPN là site-to-site VPN, đây là cách kết nối nhiều văn phòng trụ sở xa nhau thông qua các thiết bị chuyên dụng và một đường truyền được mã hoá ở qui mô lớn hoạt động trên nền Internet. Site-to-Site VPN gồm 2 loại:

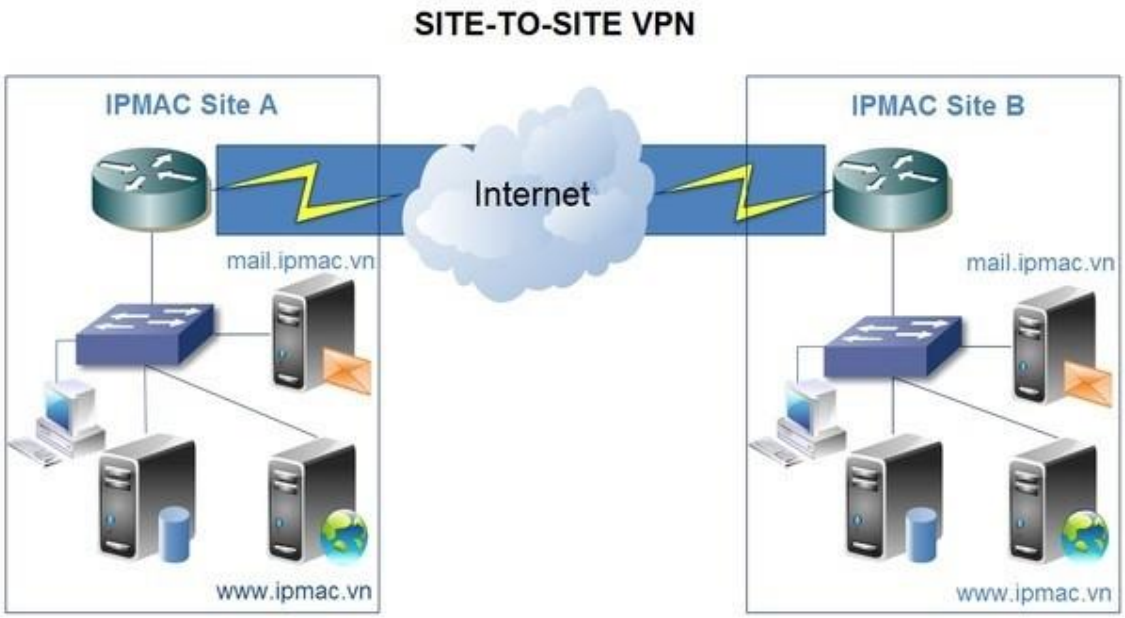
- Intranet-based: nếu công ty có các trụ sở xa nhau và muốn kết nối lại thành một mạng riêng duy nhất thì có thể tạo intranet VPN và nối kết Lan-to-Lan.
- Extranet-based: khi công ty có quan hệ mật thiết với công ty khác (ví dụ như một đối tác, nhà cung cấp hay khách hang) họ có thể xây dựng một extranet VPN nhằm kết nối Lan-to-Lan và cho phép các công ty này cùng làm việc trao đổi trong một môi trường chia sẻ riêng biệt (tất nhiên vẫn trên nền Internet).

VPN có thể được phát triển trên nhiều môi trường khác nhau: X.25, Frame Relay, ATM, Internet. Tuy nhiên trên các môi trường khác nhau thì sự

phát triển của VPN có các đặc điểm khác nhau về mặt kỹ thuật cũng như về mặt đáp ứng yêu cầu của khách hàng.

2.2.5 Mạng VPN cục bộ (Intranet-based VPN)

Các VPN cục bộ được sử dụng để bảo mật các kết nối giữa các địa điểm khác nhau của một công ty. Mạng VPN liên kết trụ sở chính, các văn phòng, chi nhánh trên một cơ sở hạ tầng chung sử dụng các kết nối luôn được mã hoá bảo mật. Điều này cho phép tất cả các địa điểm có thể truy nhập an toàn các nguồn dữ liệu được phép trong toàn bộ mạng của công ty. Những VPN này vẫn cung cấp những đặc tính của mạng WAN như khả năng mở rộng, tính tin cậy và hỗ trợ cho nhiều kiểu giao thức khác nhau với chi phí thấp nhưng vẫn đảm bảo tính mềm dẻo. Kiểu VPN này thường được cấu hình như là một VPN Site- to- Site.



Hình 2-6 Mô hình VPN Site-to-Site (Intranet Based)

Những ưu điểm chính của mạng cục bộ dựa trên giải pháp VPN bao gồm:

- Các mạng lưới cục bộ hay toàn bộ có thể được thiết lập (với điều kiện mạng thông qua một hay nhiều nhà cung cấp dịch vụ).
- Giảm được số nhân viên kỹ thuật hỗ trợ trên mạng đối với những nơi xa.
- Bởi vì những kết nối trung gian được thực hiện thông qua mạng Internet, nên nó có thể dễ dàng thiết lập thêm một liên kết ngang cấp mới.
- Tiết kiệm chi phí thu được từ những lợi ích đạt được bằng cách sử dụng đường ngầm VPN thông qua Internet kết hợp với công nghệ chuyển mạch tốc độ cao. Ví dụ như công nghệ Frame Relay, ATM.

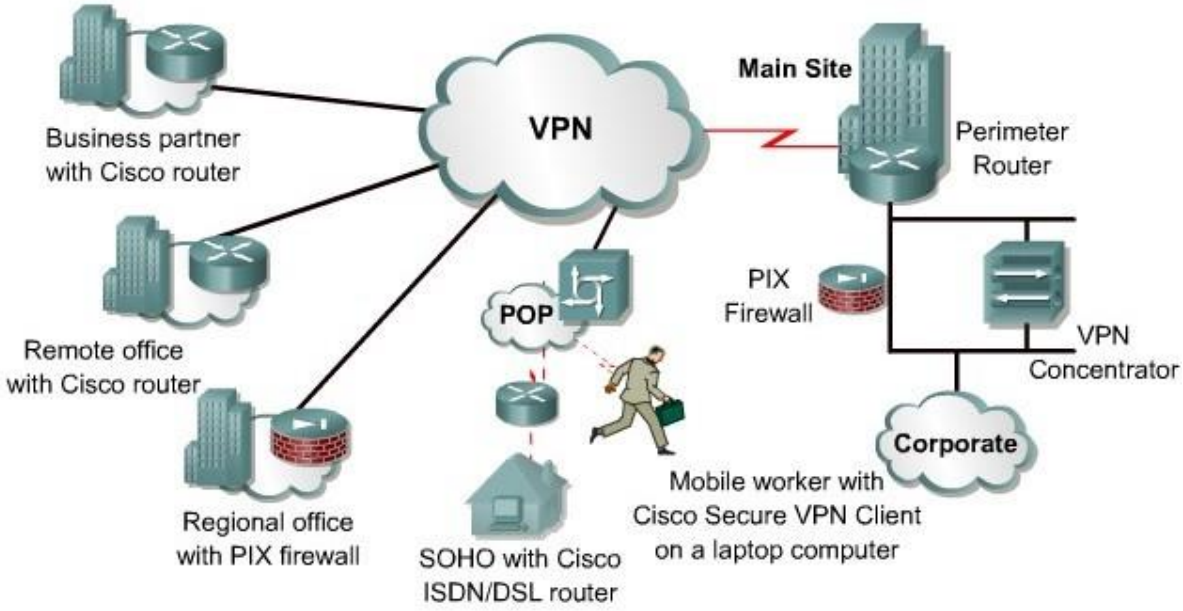
Tuy nhiên mạng cục bộ dựa trên giải pháp VPN cũng có những nhược điểm đi cùng như:

- Bởi vì dữ liệu được truyền "ngầm" qua mạng công cộng – mạng Internet – cho nên vẫn còn những mối "đe dọa" về mức độ bảo mật dữ liệu và mức độ chất lượng dịch vụ (QoS).
- Khả năng các gói dữ liệu bị mất trong khi truyền dẫn vẫn còn khá cao.
- Trường hợp truyền dẫn khối lượng lớn dữ liệu, như là đa phương tiện, với yêu cầu truyền dẫn tốc độ cao và đảm bảo thời gian thực là thách thức lớn trong môi trường Internet.

2.2.6 Mạng VPN mở rộng (Extranet-based VPN)

Thực tế mạng VPN mở rộng cung cấp khả năng điều khiển truy nhập tới những nguồn tài nguyên mạng cần thiết để mở rộng những đối tượng kinh doanh như là các đối tác, khách hàng, và các nhà cung cấp… . Các VPN mở rộng cung cấp một đường hầm bảo mật giữa các khách hàng, các nhà cung cấp và các đối tác qua một cơ sở hạ tầng công cộng. Kiểu VPN này sử dụng các kết nối luôn luôn được bảo mật và được cấu hình như một VPN Site–to–

Site. Sự khác nhau giữa một VPN cục bộ và một VPN mở rộng đó là sự truy cập mạng được công nhận ở một trong hai đầu cuối của VPN.



Hình 2-7 Mô hình VPN Site-to-Site (Extranet-Based VPN)

Những ưu điểm chính của mạng VPN mở rộng:

- Chi phí cho mạng VPN mở rộng thấp hơn rất nhiều so với mạng truyền thống.
- Dễ dàng thiết lập, bảo trì và dễ dàng thay đổi đối với mạng đang hoạt động.
- Vì mạng VPN mở rộng được xây dựng dựa trên mạng Internet nên có nhiều cơ hội trong việc cung cấp dịch vụ và chọn lựa giải pháp phù hợp với các nhu cầu của mỗi công ty hơn.
- Bởi vì các kết nối Internet được nhà cung cấp dịch vụ Internet bảo trì, nên giảm được số lượng nhân viên kỹ thuật hỗ trợ mạng, do vậy giảm được chi phí vận hành của toàn mạng.

Bên cạnh những ưu điểm ở trên giải pháp mạng VPN mở rộng cũng còn những nhược điểm đi cùng như:

- Khả năng bảo mật thông tin, mất dữ liệu trong khi truyền qua mạng công cộng vẫn tồn tại.
- Truyền dẫn khối lượng lớn dữ liệu, như là đa phương tiện, với yêu cầu truyền dẫn tốc độ cao và đảm bảo thời gian thực, là thách thức lớn trong môi trường Internet.
- Làm tăng khả năng rủi ro đối với các mạng cục bộ của công ty.

2.3 Hệ thống phát hiện chống xâm nhập

2.3.1 Hệ thống phát hiện xâm nhập (IDS).

IDS (Intrusion Detection Systems) là một hệ thống phòng chống nhằm phát hiện các hành động tấn công vào một mạng mục đích của nó là phát hiện và ngăn ngừa các hành động phá hoại đối với vấn đề bảo mật hệ thống hoặc những hành động trong tiến trình tấn công như sưu tập, quét các cổng một tính năng chính của hệ thống này là cung cấp thông tin nhận biết về những hành động không bình thường và đưa ra các báo cảnh thông báo cho quản trị viên mạng khóa các kết nối đang tấn công này thêm vào đó công cụ IDS cũng có thể phân biệt giữa những tấn công bên trong từ bên trong tổ chức (từ chính nhân viên hoặc khách hàng) và tấn công bên ngoài (tấn công từ hacker).

2.3.2 Hệ thống chống xâm nhập (IPS).

IPS (Intrusion Prevention Systems) là hệ thống theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn.

Chức năng chính của IPS là xác định các hoạt động nguy hại, lọu giữ các thông tin này. Sau đó kết hợp với firewall để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên.

Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tọơng tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn

có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS.

Nguyên lý hoạt động của một hệ thống phát hiện và chống xâm nhập đợợc chia làm 5 giai đoạn chính: Giám sát mạng, Phân tích lưu thông, Liên lạc giữa các thành phần, Cảnh báo về các hành vi xâm nhập và cuối cùng có thể tiến hành phản ứng lại tùy theo chức năng của từng IDS.

2.3.2.1 Giám sát mạng (monotoring)

Giám sát mạng là quá trình thu thập thông tin về lưu thông trên mạng. Việc này thông thường đợợc thực hiện bằng các Sensor. Yêu cầu đòi hỏi đối với giai đoạn này là có được thông tin đầy đủ và toàn vẹn về tình hình mạng. Đây cũng là một vấn đề khó khăn, bởi vì nếu theo dõi toàn bộ thông tin thì sẽ tốn khá nhiều tài nguyên, đồng thời gây ra nguy cơ tắc nghẽn mạng. Nên cần thiết phải cân nhắc để không làm ảnh hưởng đến toàn bộ hệ thống. Có thể sử dụng phương án là thu thập liên tục trong khoảng thời gian dài hoặc thu thập theo từng chu kì. Tuy nhiên khi đó những hành vi bắt được chỉ là những hành vi trong khoảng thời gian giám sát. Hoặc có thể theo vết những lợu thông TCP theo gói hoặc theo liên kết. Bằng cách này sẽ thấy được những dòng dữ liệu vào ra được phép. Nhưng nếu chỉ theo dõi những liên kết thành công sẽ có thể bỏ qua những thông tin có giá trị về những liên kết không thành công mà đây lại thường là những phần quan tâm trong một hệ thống IDS, ví dụ như hành động quét cổng.

2.3.2.2 Phân tích lưu thông (Analyzing)

Khi đã thu thập được những thông tin cần thiết từ những điểm trên mạng. IDS tiến hành phân tích những dữ liệu thu thập được. Mỗi hệ thống cần có một sự phân tích khác nhau vì không phải môi trường nào cũng giống nhau. Thông thường ở giai đoạn này, hệ thống IDS sẽ dò tìm trong dòng traffic mang những dấu hiệu đáng nghi ngờ dựa trên kỹ thuật đối sánh mẫu hoặc phân tích hành vi bất thường.

2.3.2.3 Cảnh báo (Alert)

Sau khi đã phân tích xong dữ liệu, hệ thống IDS cần phải đưa ra được những cảnh báo. Ví dụ như:

- Cảnh báo địa chỉ không hợp lệ.
- Cảnh báo khi máy cố gắng kết nối đến những máy nằm trong danh sách cần theo dõi ở trong hay ngoài mạng.

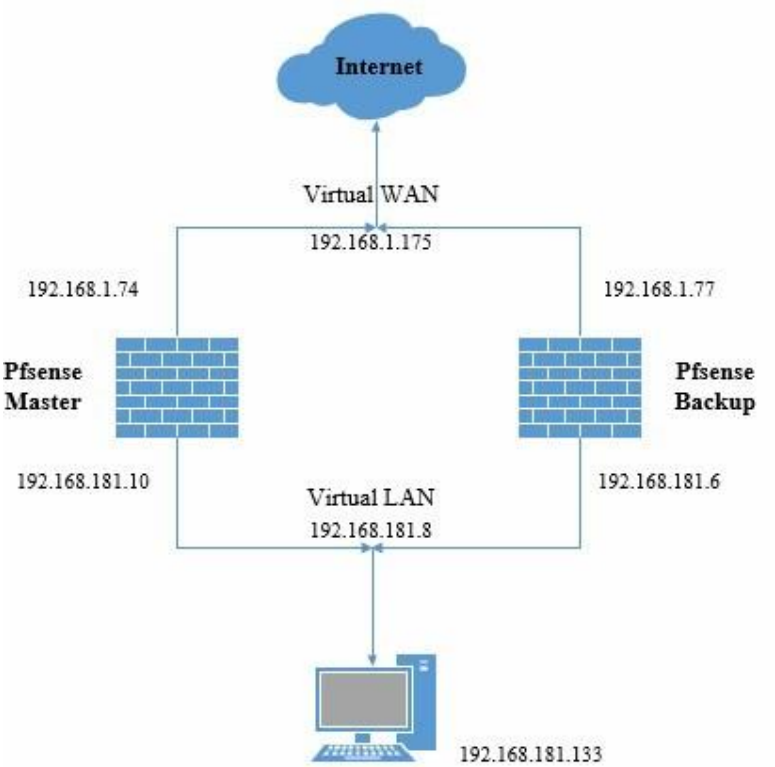
2.3.2.4 Phản ứng (Response)

Trong một số hệ thống IDS tiên tiến hiện nay, sau khi các giai đoạn trên phát hiện được dấu hiệu tấn công, hệ thống không những cảnh báo cho ngọời quản trị mà còn đưa ra các hành vi phòng vệ ngăn chặn hành vi tấn công đó. Điều này giúp tăng cường khả năng tự vệ của Mạng, vì nếu chỉ cần cảnh báo cho người quản trị thì đôi khi cuộc tấn công sẽ tiếp tục xảy ra gây ra các tác hại xấu. Một hệ thống IDS có thể phản ứng lại trước những tấn công phải được cấu hình để có quyền can thiệp vào hoạt động của Firewall, Switch và Router. Các hành động mà IDS có thể đưa ra như:

- Ngắt dịch vụ.
- Gián đoạn phiên.
- Cấm địa chỉ IP tấn công.
- Tạo log.

CHƯƠNG 3: TRIỂN KHAI PROXY SERVER TRÊN PFSENSE

3.1 Mô hình triển khai



Hình 3-1 Mô hình triển khai Pfsense thực nghiệm

3.2 Pfsense

3.2.1 Giới thiệu

PfSense là một ứng dụng có chức năng định tuyến, tường lửa và miễn phí, ứng dụng này sẽ cho phép bạn mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Bắt đầu vào năm 2004, khi m0n0wall mới bắt đầu chập chững – đây là một dự án bảo mật tập trung vào các hệ thống nhúng – pfSense đã có hơn 1 triệu lượt download và được sử dụng để bảo vệ các mạng có tất cả kích cỡ, từ mạng gia đình đến các mạng lớn của các công ty/doanh nghiệp. Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi lần phát hành nhằm cải thiện hơn nữa tính bảo mật, sự ổn định và khả năng linh hoạt của nó. Và là một trong số ít những

firewall có tính năng trạng thái, chỉ thường xuất hiện ở những firewall thương mại lớn như Cisco ASA, Checkpoint, Juniper …

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

PfSense hỗ trợ lọc bởi địa chỉ nguồn và địa chỉ đích, cổng nguồn hoặc cổng đích hay địa chỉ IP. Nó cũng hỗ trợ chính sách định tuyến và cơ chế hoạt động trong chế độ brigde hoặc transparent, cho phép bạn chỉ cần đặt pfSense ở giữa các thiết bị mạng mà không cần đòi hỏi việc cấu hình bổ sung. PfSense cung cấp cơ chế NAT và tính năng chuyển tiếp cổng, tuy nhiên ứng dụng này vẫn còn một số hạn chế với Point-to-Point Tunneling Protocol (PPTP), Generic Routing Encapsulation (GRE) và Session Initiation Protocol (SIP) khi sử dụng NAT.

PfSense được dựa trên FreeBSD và giao thức Common Address Redundancy Protocol (CARP) của FreeBSD, cung cấp khả năng dự phòng bằng cách cho phép các quản trị viên nhóm hai hoặc nhiều tường lửa vào một nhóm tự động chuyển.

Vì nó hỗ trợ nhiều kết nối mạng diện rộng (WAN) nên có thể thực hiện việc cân bằng tải. Tuy nhiên có một hạn chế với nó ở chỗ chỉ có thể thực hiện cân bằng lưu lượng phân phối giữa hai kết nối WAN và không thể chỉ định được lưu lượng cho qua một kết nối.

3.2.2 Cài đặt Pfsense

3.2.2.1 Phần cứng yêu cầu

- CPU Pentium II trở lên.
- RAM 512 MB.

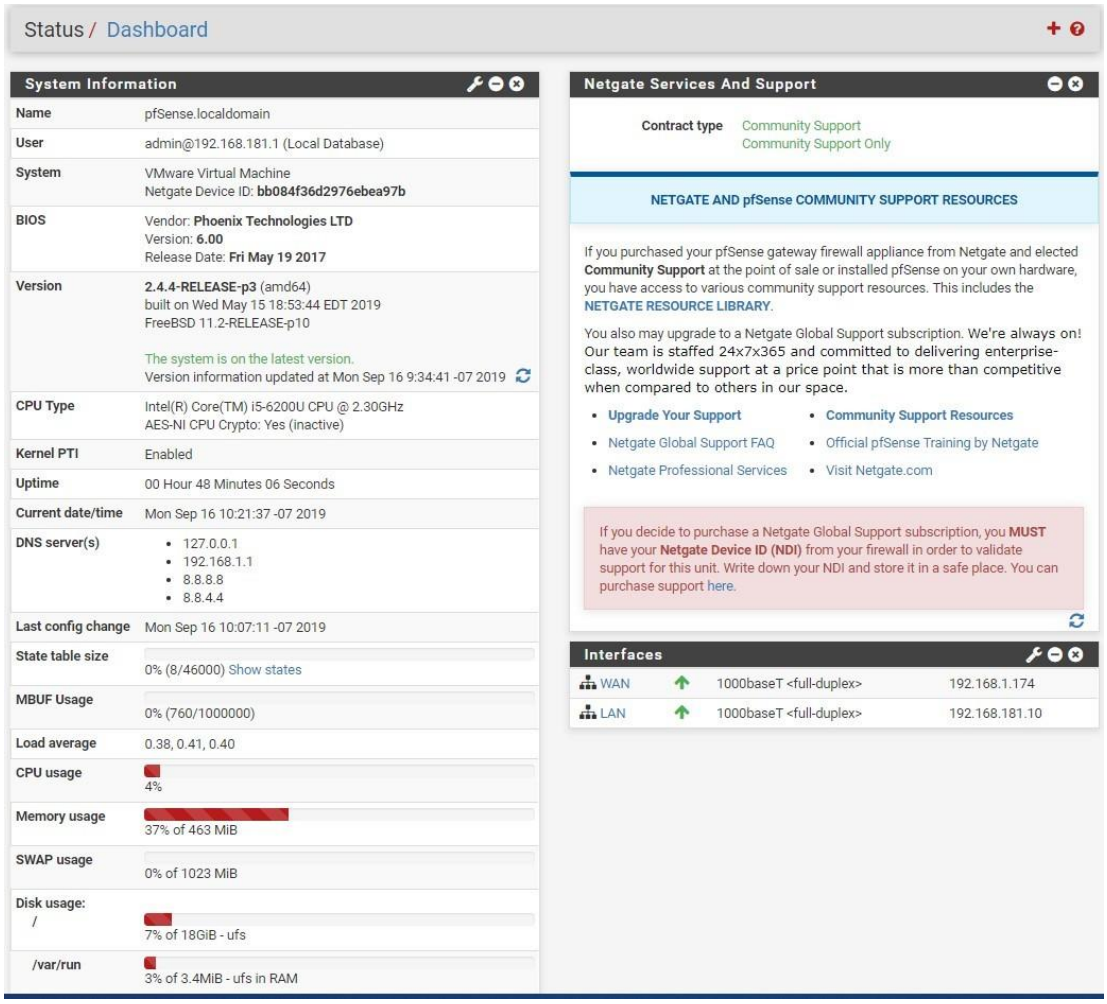
- Disk drive (SSD, HDD, etc).
- PCI Network 2 cái : 1 dùng WAN, 1 dùng LAN.

3.2.2.2 Cài đặt Pfsense trên PC

Vào trang chủ của Pfsense để download :

https://www.pfsense.org/download/

Hình 3-2 Download Pfsense



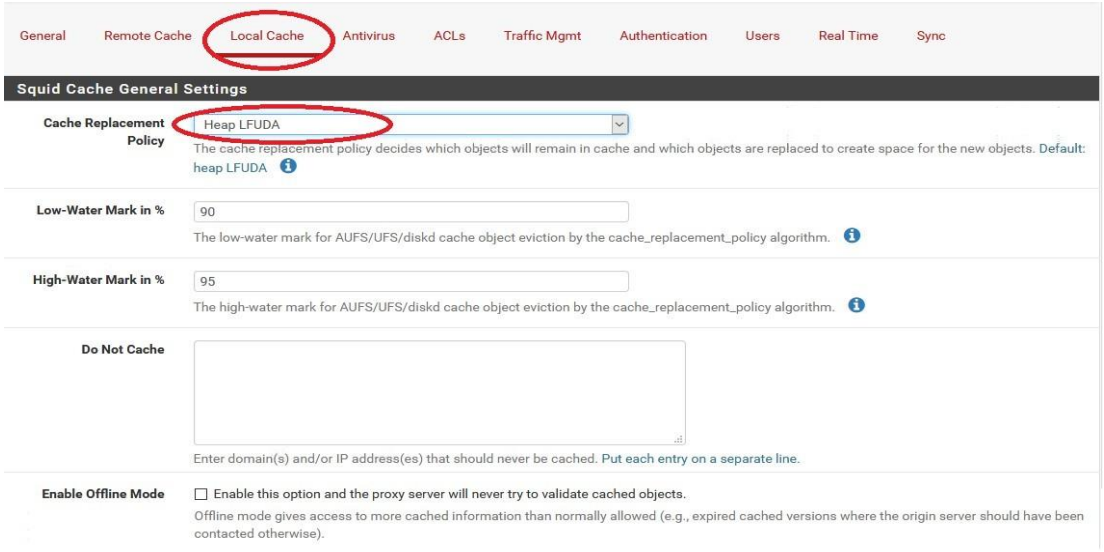
Hình 3-3 Giao diện Status Dashboard

3.3 Giải pháp proxy server trên Pfsense

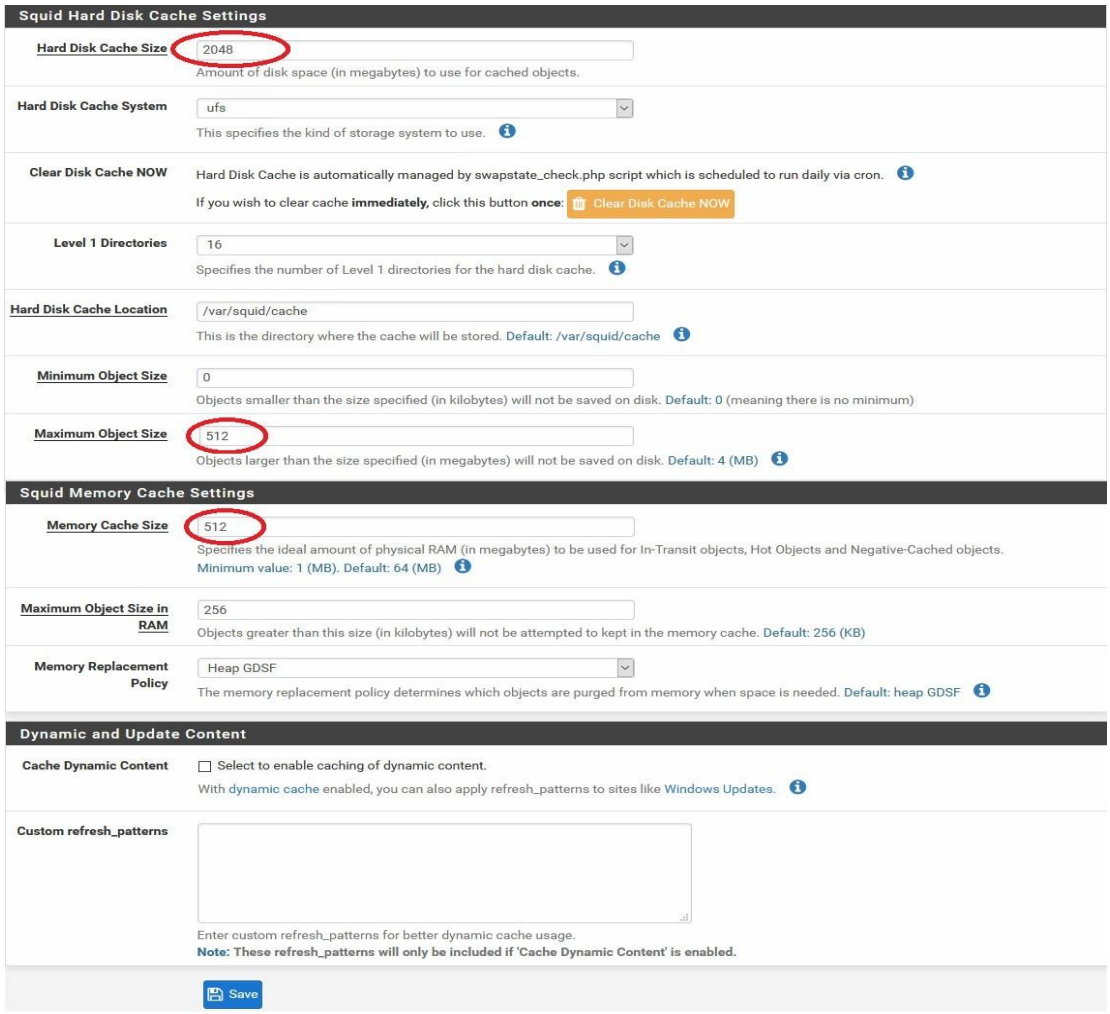
3.3.1 Cấu hình Proxy Server

3.3.1.1 Cấu hình Squid proxy

- Bước 1 : Cấu hình Local Cache. Vào "Services" > Squid Proxy Server > Local Cache. Mục Cache Replacement: Heap LFUDA, Hard Disk Cache Size: 2048, Maximum Object Size: 512, Memory Cache size: 512-> Click "Save" để lưu cấu hình.

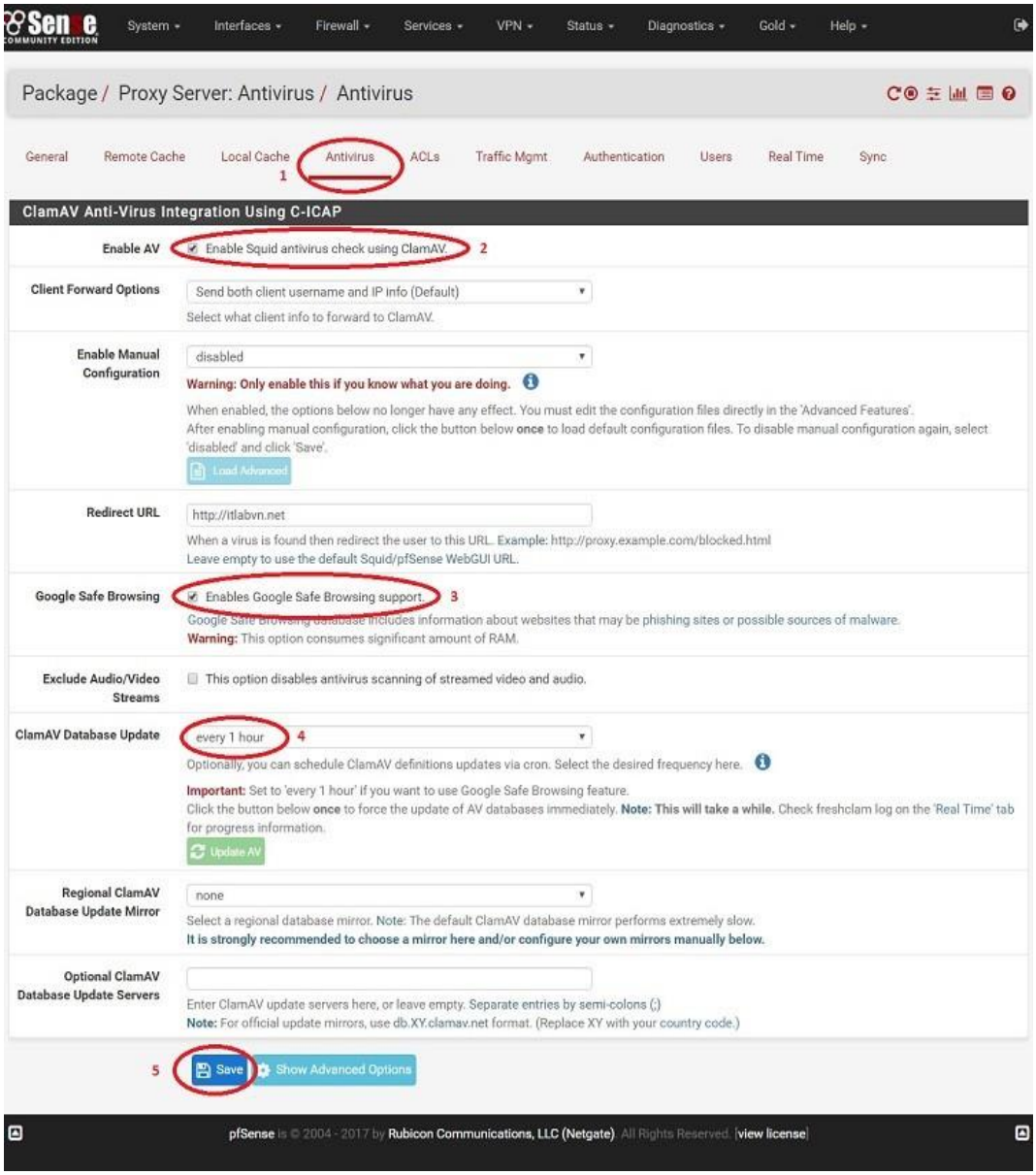


Hình 3-4 Cấu hình Squid proxy



Hình 3-5 Cấu hình Squid proxy

- Bước 2: Cấu hình tích hợp antivirus. Chọn "Services > Squid Proxy > Antivirus Tab" .Tích vào "Enable Squid antivirus check using ClamAV" , Tích "Enable Google Safe Browsing support", "ClamAV Database Update : every 1 hour" -> Click "Save" để lưu cấu hình.



Hình 3-6 Cấu hình Antivirus

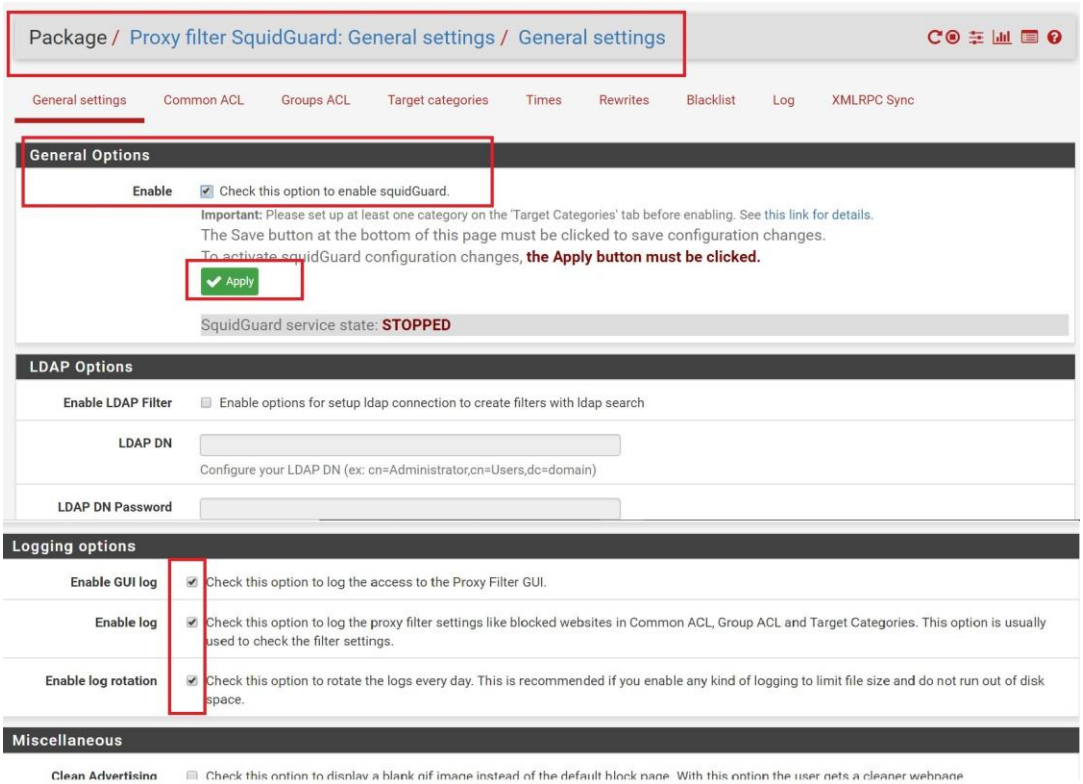
ClamAV là một mã nguồn mở (GPL), bộ công cụ chống virus, đặc biệt là cho thư điện tử quét trên cổng email. Phát hiện hơn 750.000 virus, worms, trojan, bao gồm cả Microsoft Office virus macro, phần mềm độc hại di động

và mối đe dọa khác.Mdaemon các bạn cũng sẽ thấy nó dùng ClamAV để quét mail.

3.3.1.2 Cấu hình Squid Guard

Squid Guard có tính năng chính để lọc web đen,web cấm, facebook , để thực hiện việc này thì nó tạo ra access list rồi kết hợp với Squid Proxy để các user bên trong pfsense không truy cập được các website bị cấm.

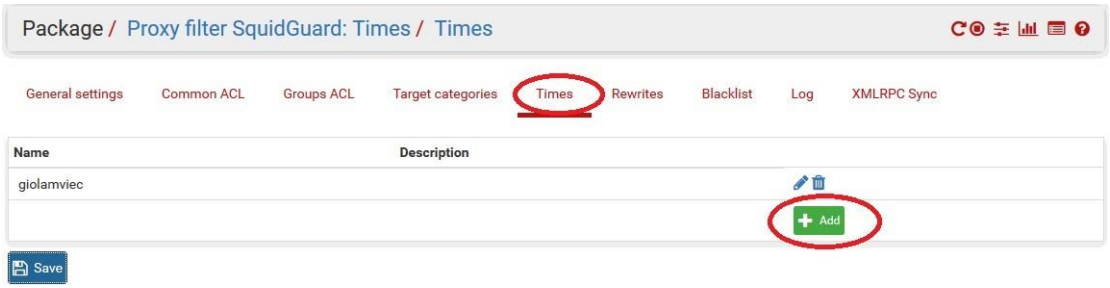
Truy cập Services -> SquidGuard Proxy Filter ->General Settings bật Enable ->Apply



Hình 3-7 Cấu hình Squid Guard

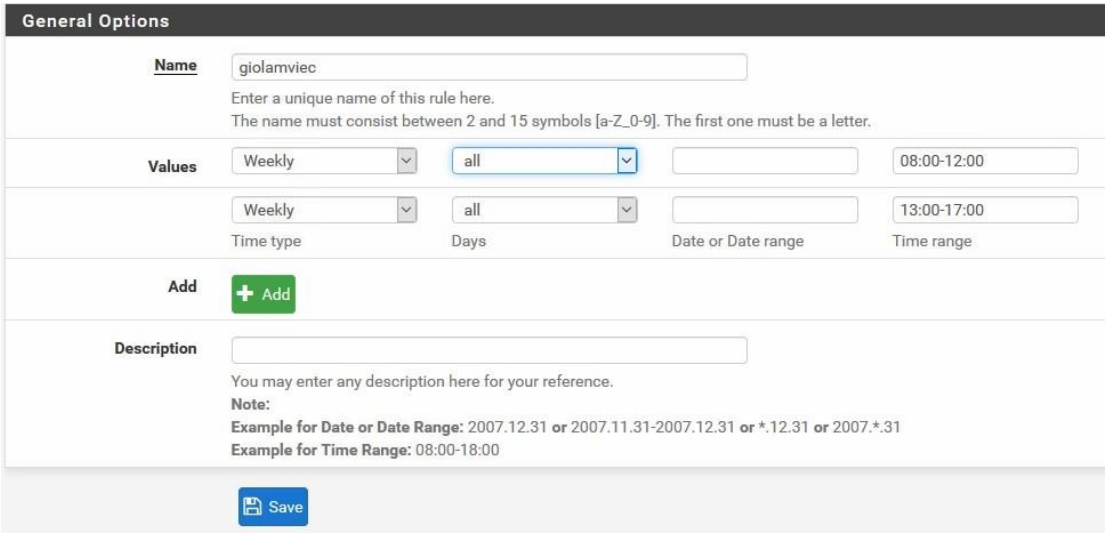
3.3.2 Giới hạn giờ truy cập web

- Bước 1: Chọn menu Services, sau đó chọn SquidGuard Proxy Filter, tiếp tục chuyển sang tab Times. Đây là tab cho phép ta cấu hình chặn lọc có sự can thiệp của thời gian. Chọn Add để thêm mới một khoảng thời gian.



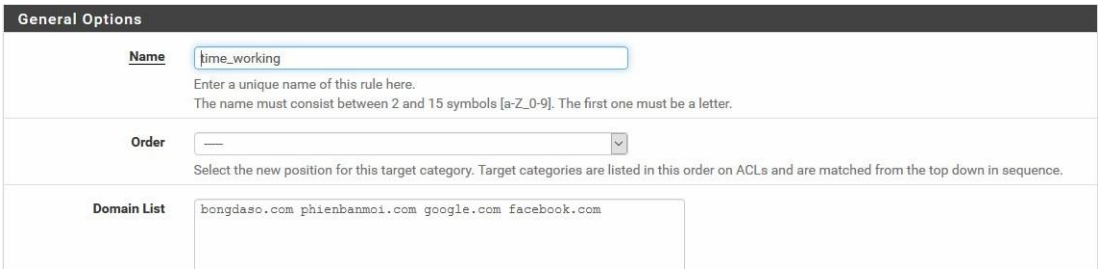
Hình 3-8 Tạo mới một khoảng thời gian

- Bước 2. Giả sử, ta sẽ thực hiện chặn các trang website đã quy định ở nội dung trên với những yêu cầu đề ra như sau: Thực hiện chặn truy cập vào các ngày làm việc từ thứ 2 cho đến thứ 6. Thời gian từ 8:00 đến 12:00 và 13:30 đến 17:30. Trong giờ làm việc, ta chỉ được phép truy cập các trang website ngoại trừ bongdaso.com, phienbanmoi.com, google.com. Các thời gian khác, truy cập bình thường.



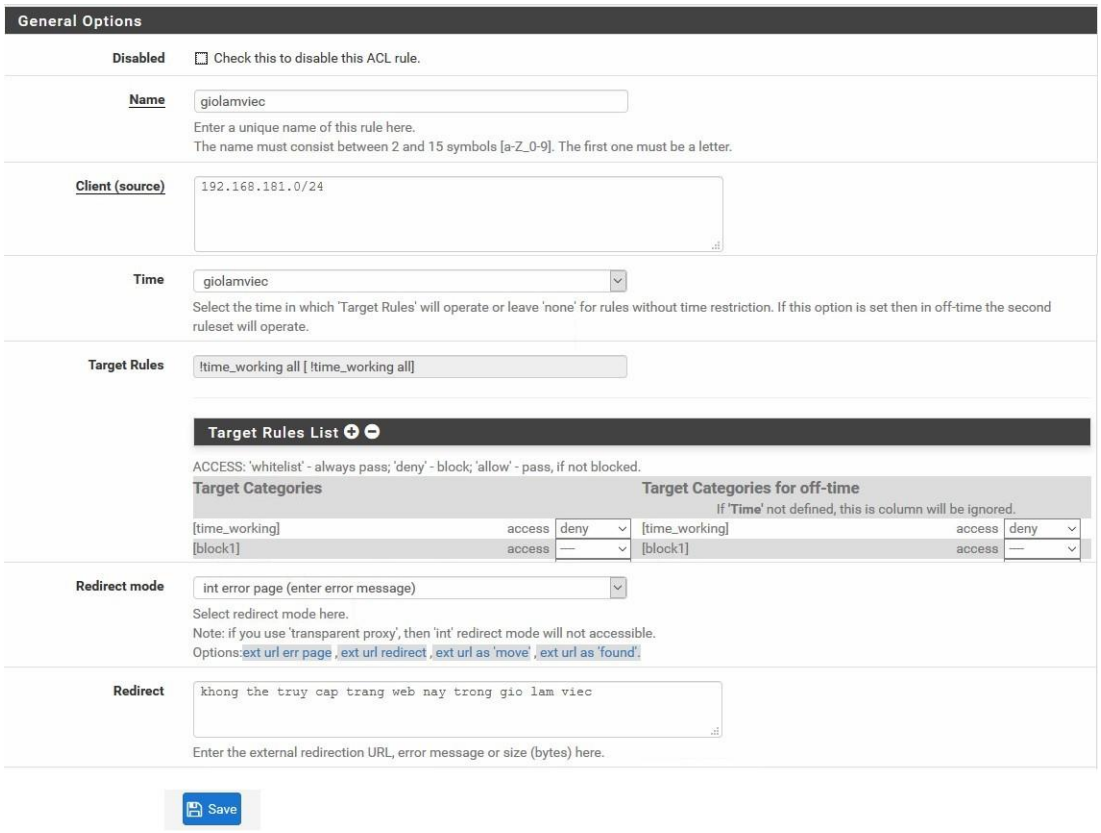
Hình 3-9 Chặn truy cập theo ngày giờ

- Bước 3. Chuyển sang tab Target categories. Ta sẽ thực hiện tạo ra một categories chưa danh sách các website bị chặn. Thực hiện lựa chọn các giá trị và điền thông tin tương tự như sau:



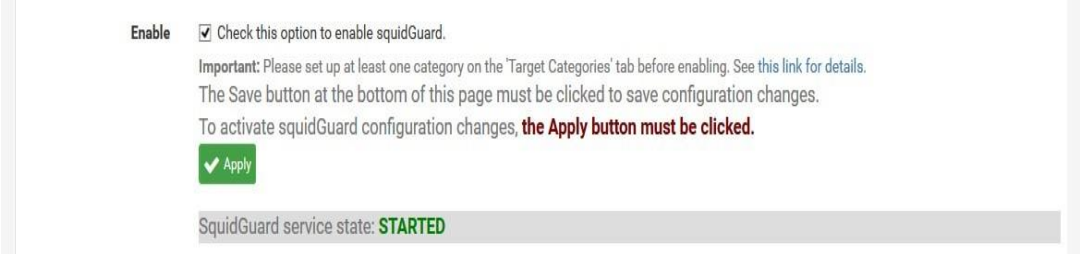
Hình 3-10 Tạo danh sách các web bị chặn

- Bước 4. Tiếp tục chuyển sang tab Groups ACL. Chọn Add để thêm mới một ACL (Access Control List). Thực hiện lựa chọn và điền các thông tin như sau:



Hình 3-11 Cấu hình Group ACL

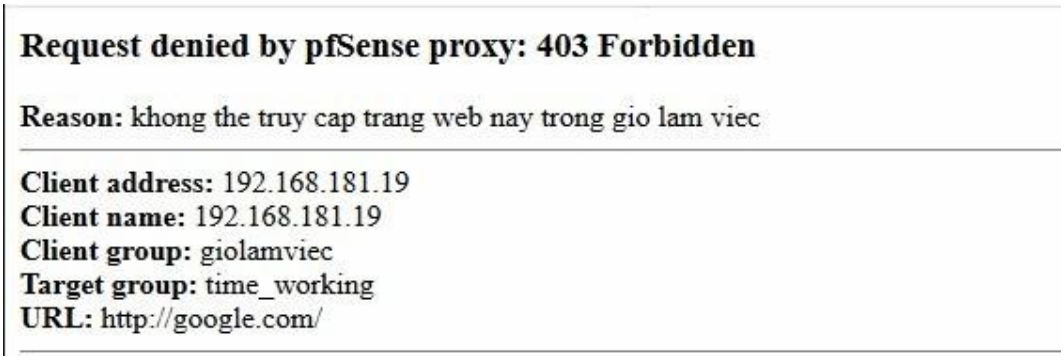
- Bước 5. Thực hiện chuyển sang tab General settings. Ta chọn Apply để chấp nhận thay đổi cấu hình:



Hình 3-12 Xác nhận thay đổi cấu hình

Kiểm tra kết quả của cấu hình :

- Khi truy cập vào trang web google.com :

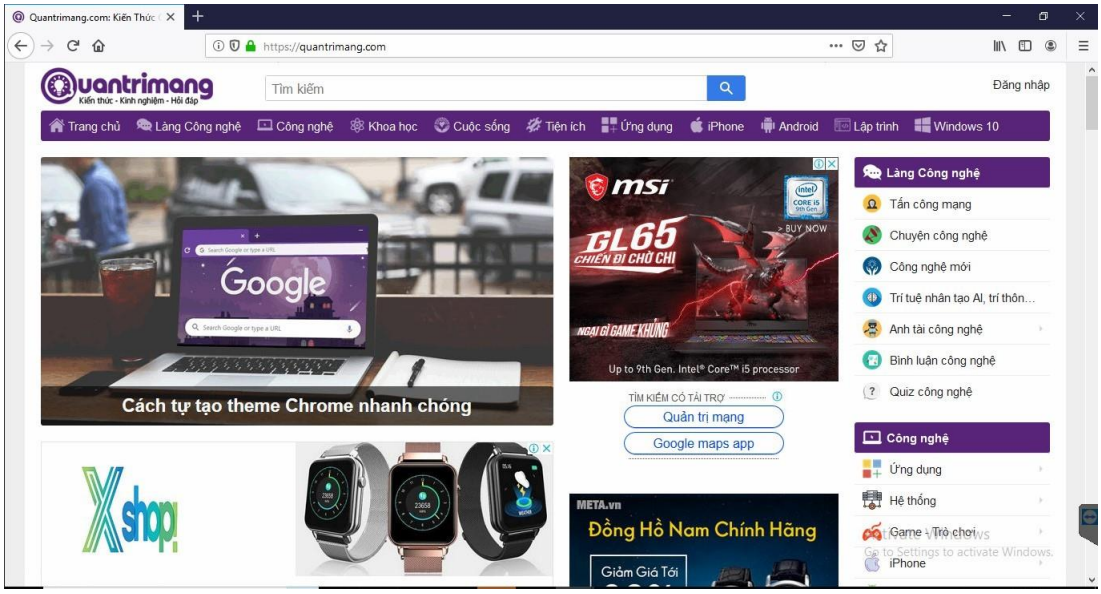


Hình 3-13 Truy cập vào google.com

- Khi truy cập vào phienbanmoi.com

Hình 3-14 Truy cập vào phienbanmoi.com

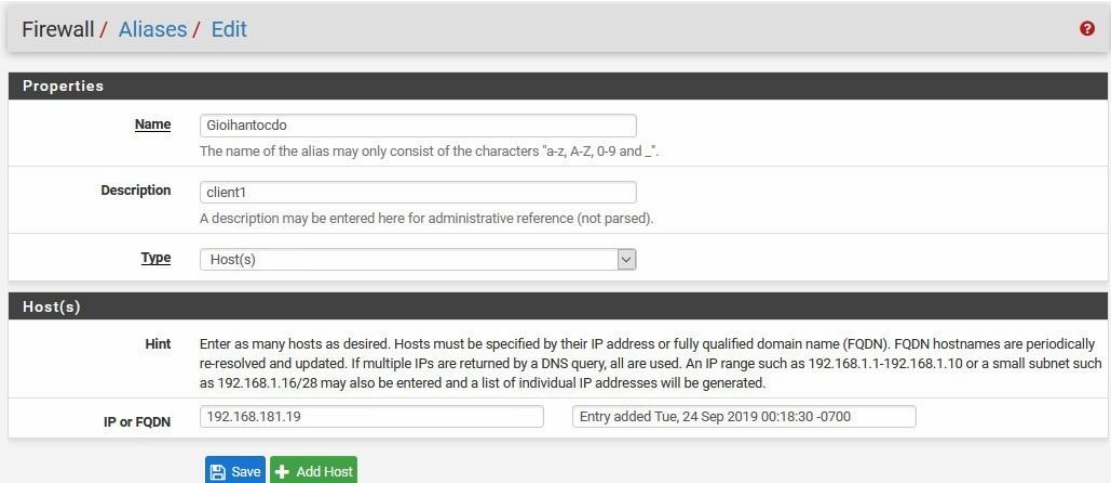
- Khi truy cập vào các trang web khác:



Hình 3-15 Khi truy cập vào trang web khác

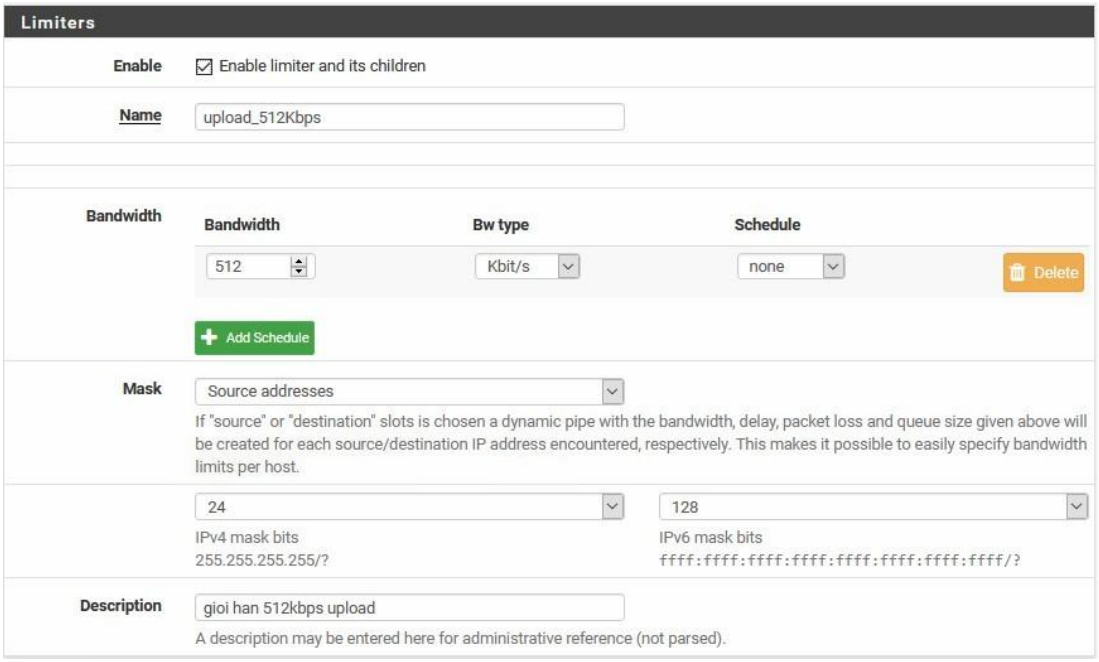
3.3.3 Giới hạn tốc độ download/upload cho từng client

- Bước 1:Tạo Alias chứa danh sách các IP cần giới hạn tốc độ : Firewall > Alias > Add :

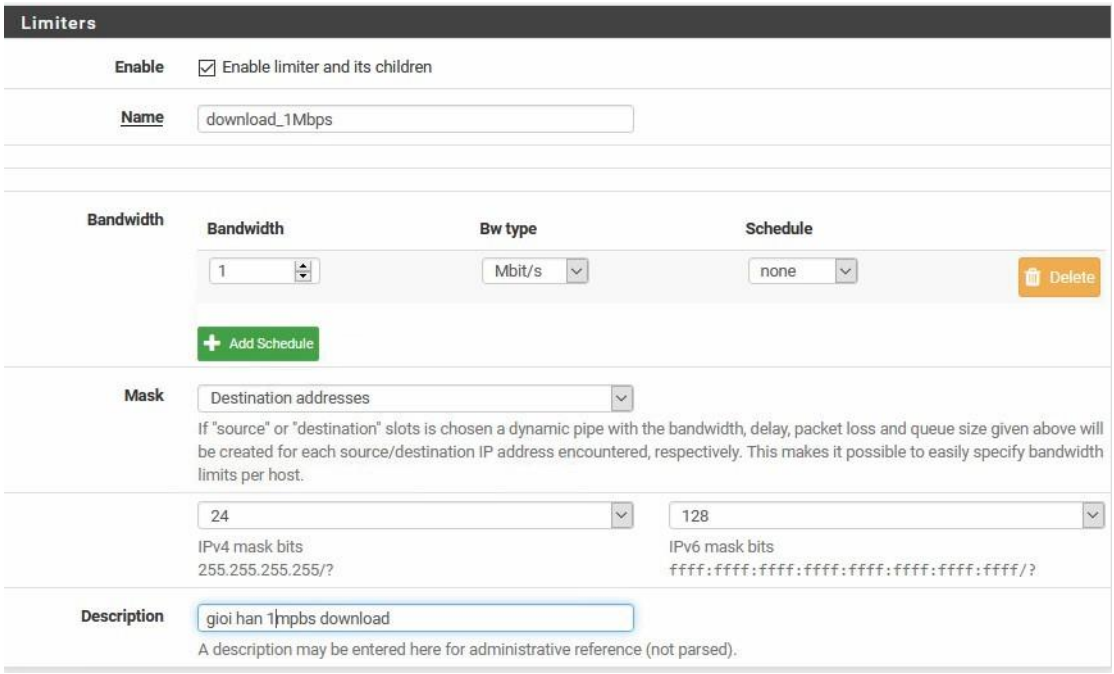


Hình 3-16 Tạo alias chứa danh sách IP

- Bước 2 :Tạo Limiter để qui định tốc độ được giới hạn. Chúng ta sẽ tạo 2 limiter tương ứng với 2 hướng upload và download.



Hình 3-17 Tạo limiter upload



Hình 3-18 Tạo limiter download

3.3.4 Chứng thực user truy cập web sử dụng Captive Portal

Captive portal là một trang Web trung gian, dùng để bảo vệ hệ thống mạng. Khi người dùng muốn tham gia vào hệ thống mạng sẽ được yêu cầu nhập tên và mật khẩu hợp lệ (đôi khi chỉ cần click tham gia), chức năng này

thường được sử dụng ở những hệ thống mạng không dây. Chúng cũng có thể được sử dụng trên kết nối có dây cho trung tâm thương mại, tiệm internet hoặc ở nhà.

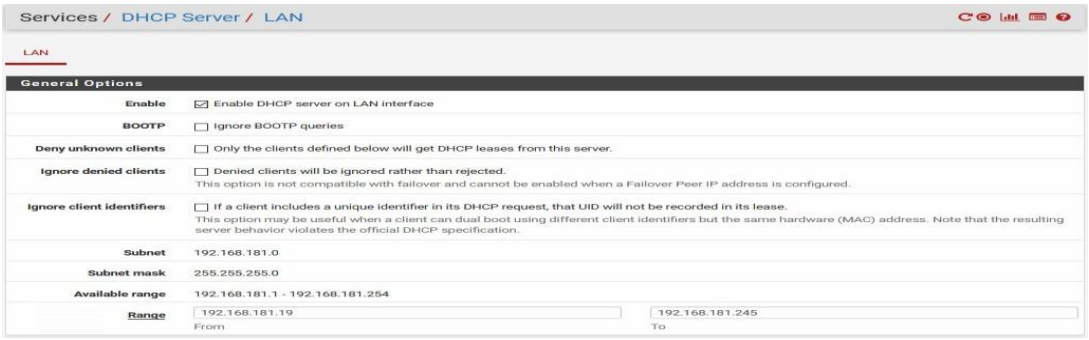
Một khi portal được kích hoạt thì bất kỳ máy tính nào trỏ đến pfSense như là gateway sẽ được chuyển hướng tự động tới trang portal.Portal cơ bản không có xác thực.

Captive portal pfsense mang đến một giải pháp cấu hình dễ dàng. Sử dụng một trang trung gian để yêu cầu người dùng chứng thực, giúp nâng cao khả năng bảo mật. Trang Web trung gian này có thể thiết kế đơn giản, với hướng dẫn và điều khoản sử dụng, hoặc sử dụng ô Username và Password để đăng nhập.

Khi đã cấu hình captive portal pfsense, bất cứ máy tính nào sử dụng pfSense làm gateway đều được chuyển hướng đến trang portal đích. [4]

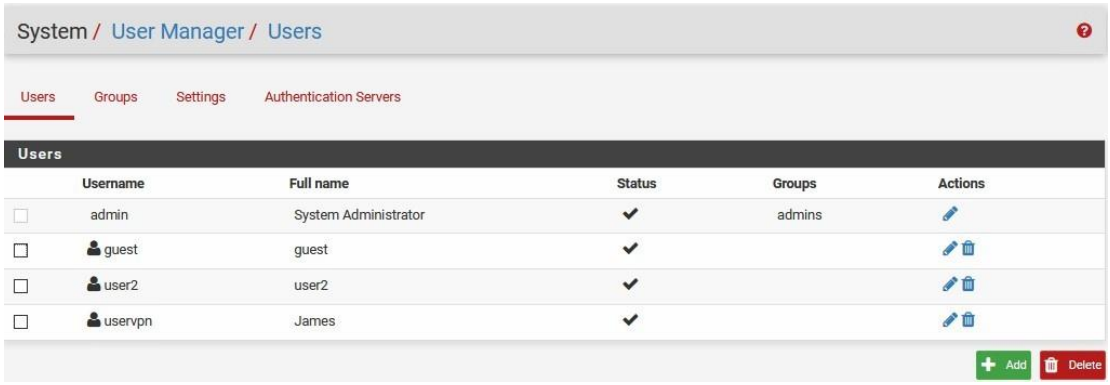
Các bước thực hiện lần lượt được thực hiện như sau:

- Bước 1: Thực hiện enable DHCP Server. Điều này là cần thiết nếu như ta cung cấp sử dụng tính năng kết hợp với Wi-Fi cho các thiết bị không dây và tránh trường hợp các thiết bị sử dụng có địa chỉ IP giống nhau gây phát sinh lỗi. Tại giao diện Web Interface quản lý của pfSense. Ta chọn Services rồi chọn DHCP Server. Hãy thực hiện điền thông tin tương tự như hình dưới sau đó chọn Save để lưu lại cấu hình.



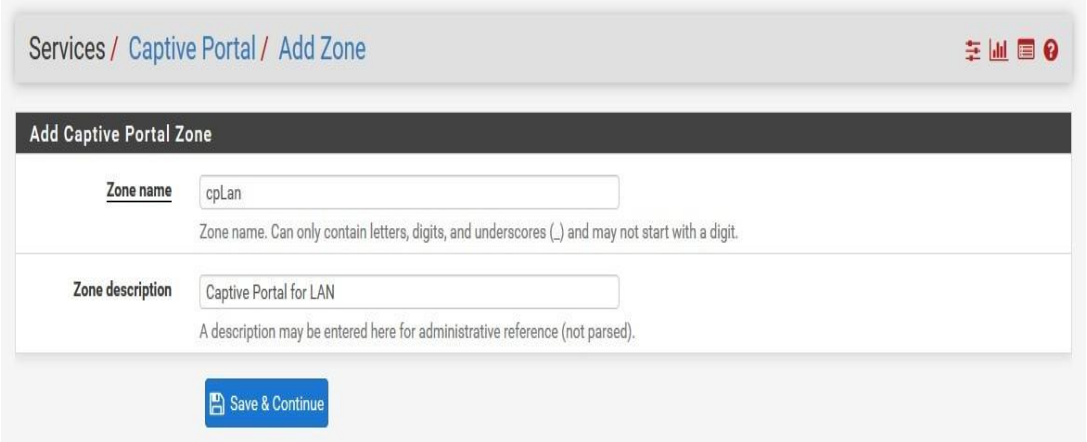
Hình 3-19 Enable DHCP

- Bước 2: Tạo tài khoản người dùng cung cấp cho người sử dụng có thể xác thực để truy cập internet. Cách thực hiện như sau: Chọn System, sau đó chọn User Manager > Add :



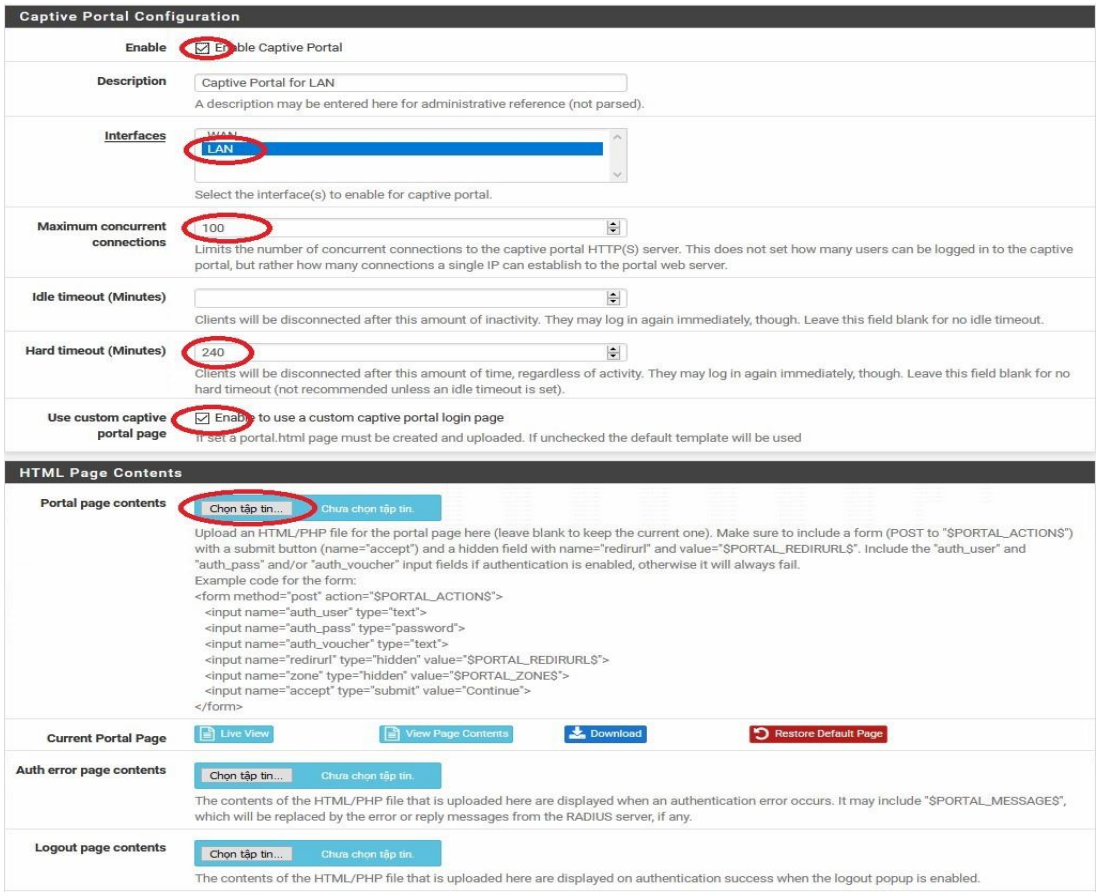
Hình 3-20 Tạo User

- Bước 3. Cấu hình Captive Portal bằng các thực hiện như sau: Chọn Services, tiếp tục chọn Captive Portal sau đó chọn Add. Nhập thông tin tương tự như hình sau để tạo ra Captive Portal Zone: Chọn Save & Continue để lưu lại thông tin.



Hình 3-21 Tạo 1 Zone mới

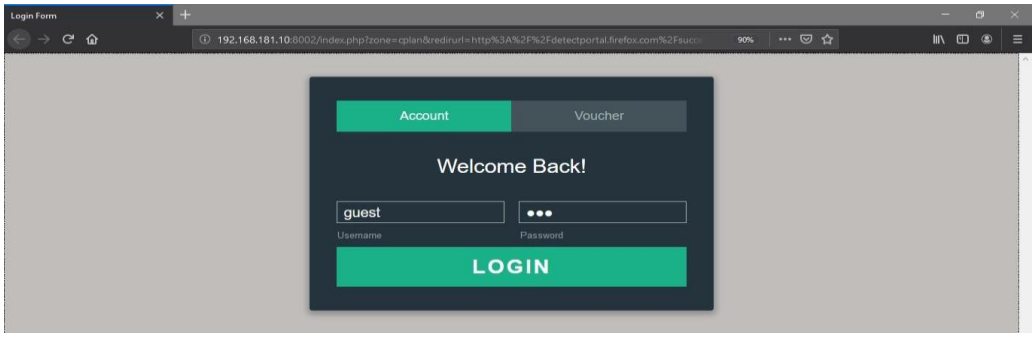
Bước 4 :Tiếp tục nhập thông tin tương tự như hình dưới đây:



Hình 3-22 Upload giao diện trang Portal

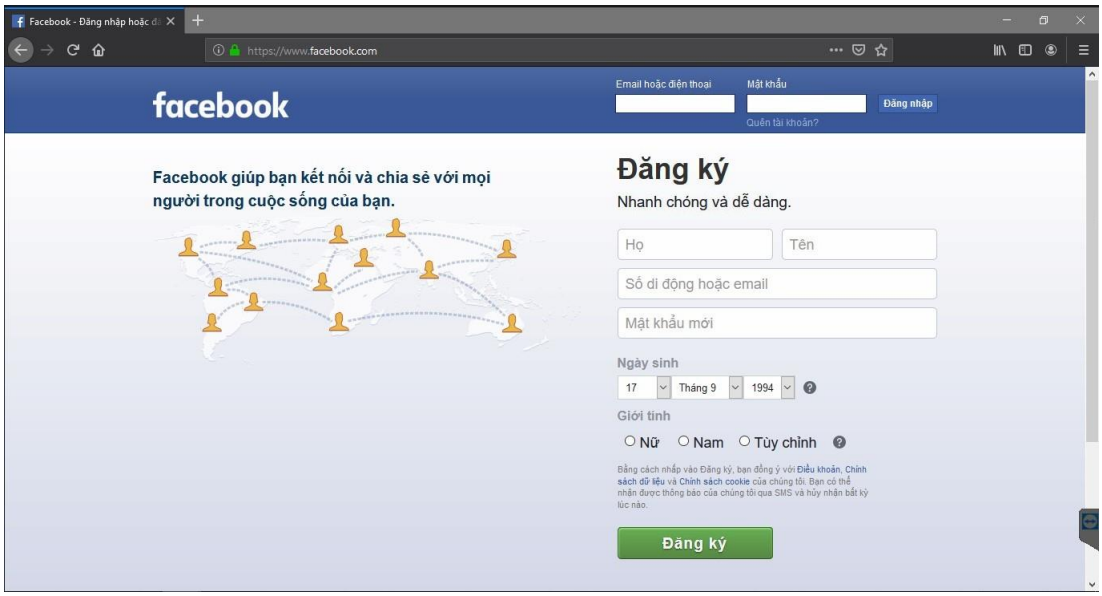
Kết quả thực nghiệm:

- Khi ta gõ địa chỉ của một trang web bất kì nào đó sẽ yêu cầu phải xác thực



Hình 3-23 Màn hình đăng nhập Portal

- Sau khi gõ username và password chúng ta có thể truy cập web như bình thường:



Hình 3-24 Sau khi đăng nhập

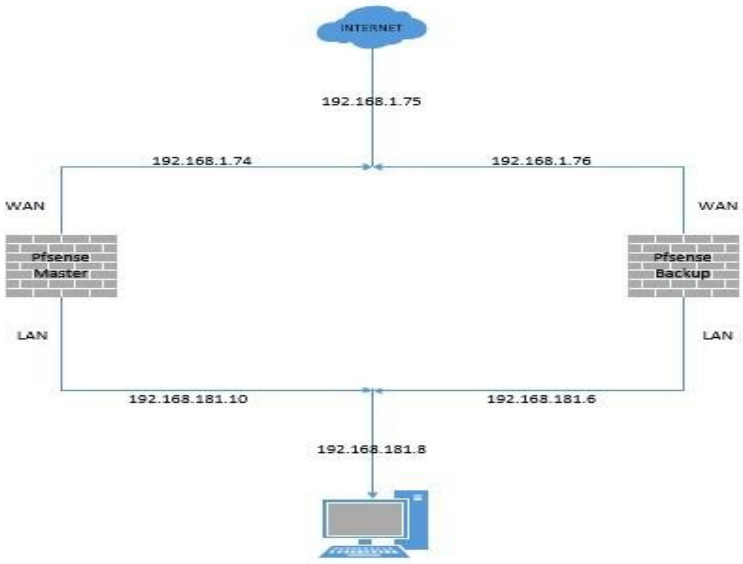
3.3.5 Xây dựng hệ thống 2 Firewall – failover đáp ứng các máy trong mạng LAN luôn truy cập được internet

3.3.5.1 Vai trò, chức năng

- Vai trò của việc cấu hình pfSense Cluster là đảm bảo cho việc cung cấp firewall ở mức ổn định nhất có thể. Phòng trường hợp khi phát sinh lỗi buộc firewall ngừng hoạt động gây ra sự trì trệ trong hệ thống.
- Với tính năng đồng bộ và sao lưu cấu hình cần thiết như các rule, pfSense Cluster là một giải pháp toàn vẹn nhất tính đến thời điểm hiện tại.
- Việc đồng bộ sử dụng giao thức CARP, dữ liệu đồng bộ được gửi qua http(s).

3.3.5.2 Mô hình

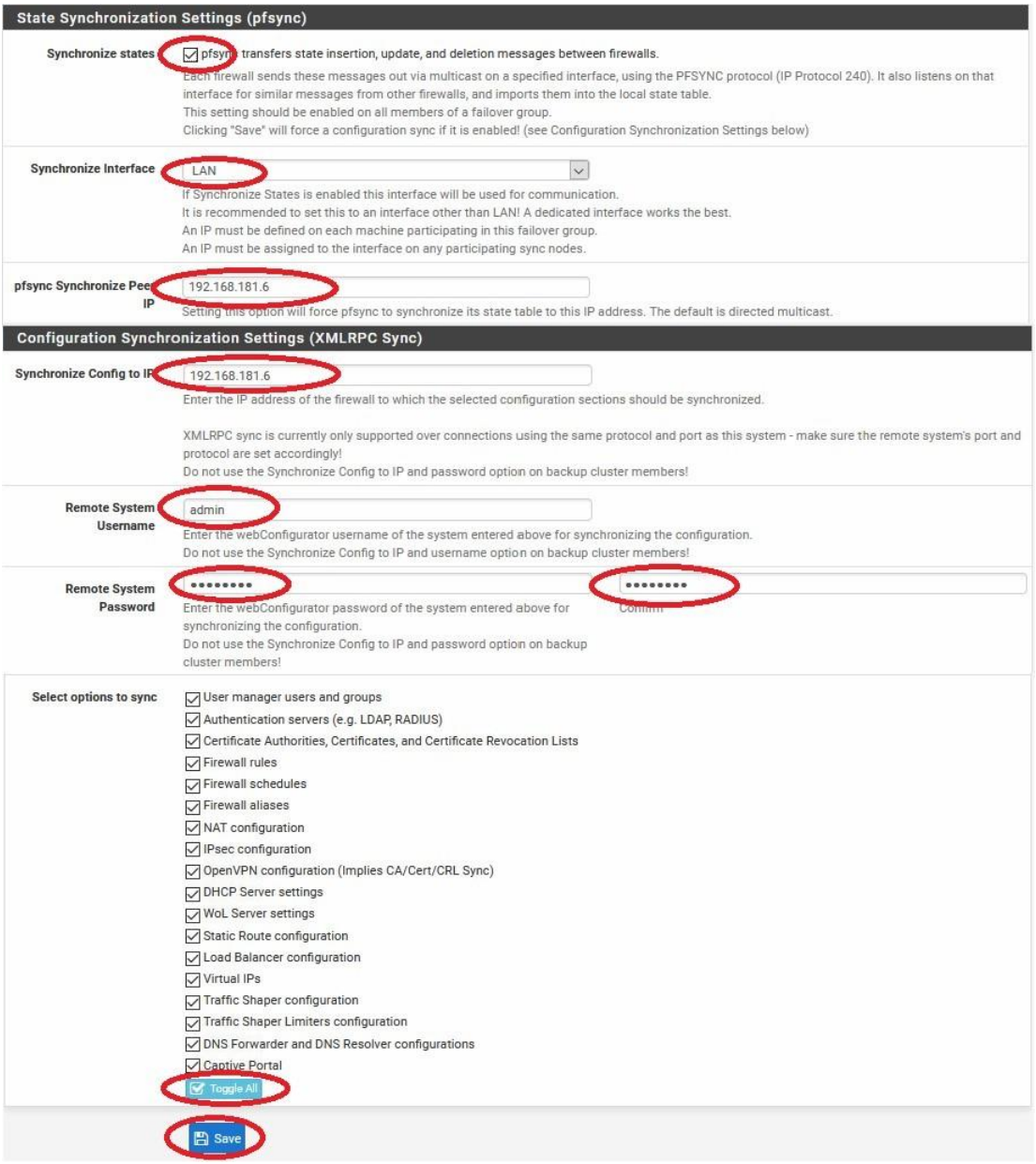
Mô hình thực hiện cấu hình có thể mô tả giống như hình sau:



Hình 3-25 Mô hình hệ thống 2 firewall - failover

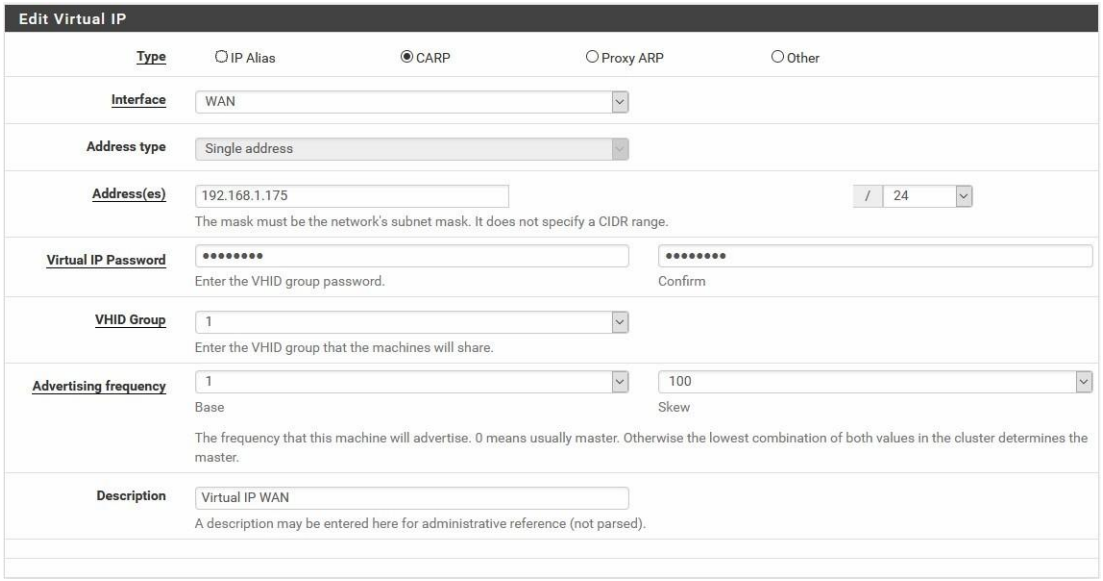
3.3.5.3 Thực hiện cấu hình

- Bước 1: Thực hiện cấu hình CARP trên pfSense master. Cách thực hiện như sau: Chọn menu System > High Avail. Sync > điền thông tin tương tự như hình sau đây:

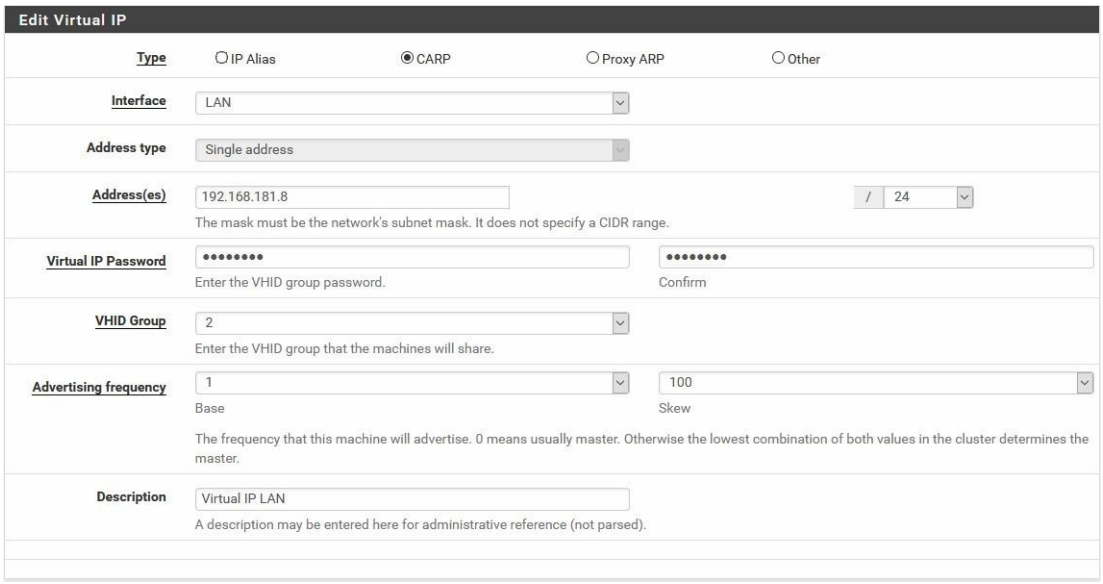


Hình 3-26 Cấu hình CARP

- Bước 2. Tạo Virtual IP WAN và Virtual IP LAN. Việc thực hiện chỉ cần thực hiện trên pfSense master. Vì lúc này, quá trình đồng bộ đã bắt đầu xảy ra. Cách thực hiện như sau: Chọn Firewall > Virtual Ips > Add để thêm mới một Virtual IP cho WAN. Nhập thông tin tương tự như sau:



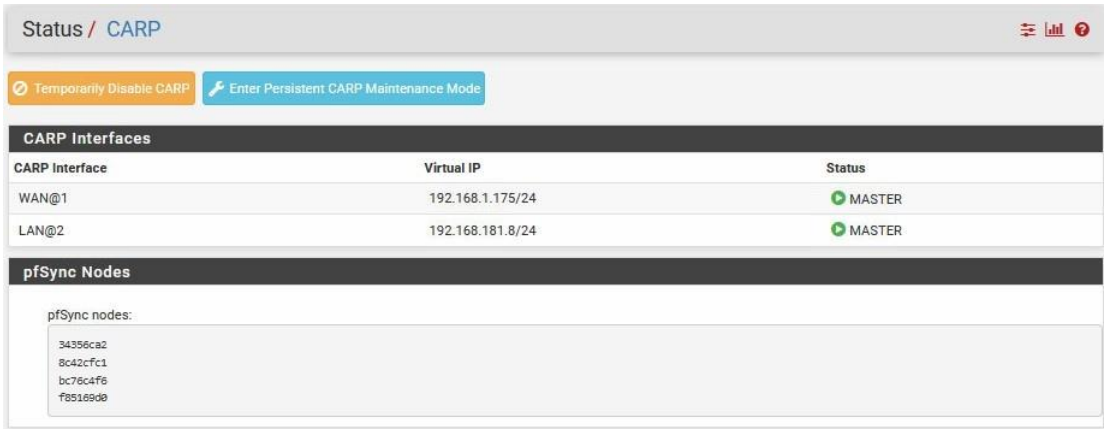
Hình 3-27 Tạo Virtual Ips WAN



Hình 3-28 Tạo Virtual Ips LAN

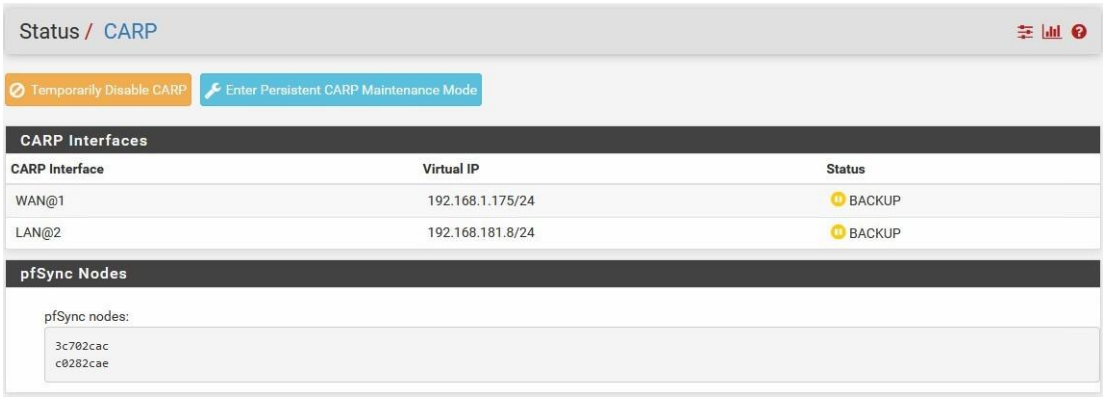
- Bước 3: Kiểm tra kết quả. Để kiểm tra kết quả của quá trình thực hiện cấu hình và quá trình đồng bộ. Ta thực hiện như sau: Chọn menu Status sau đó chọn CARP (failover). Kết quả:

  - Trên máy chủ pfSense master ta sẽ thấy như sau:



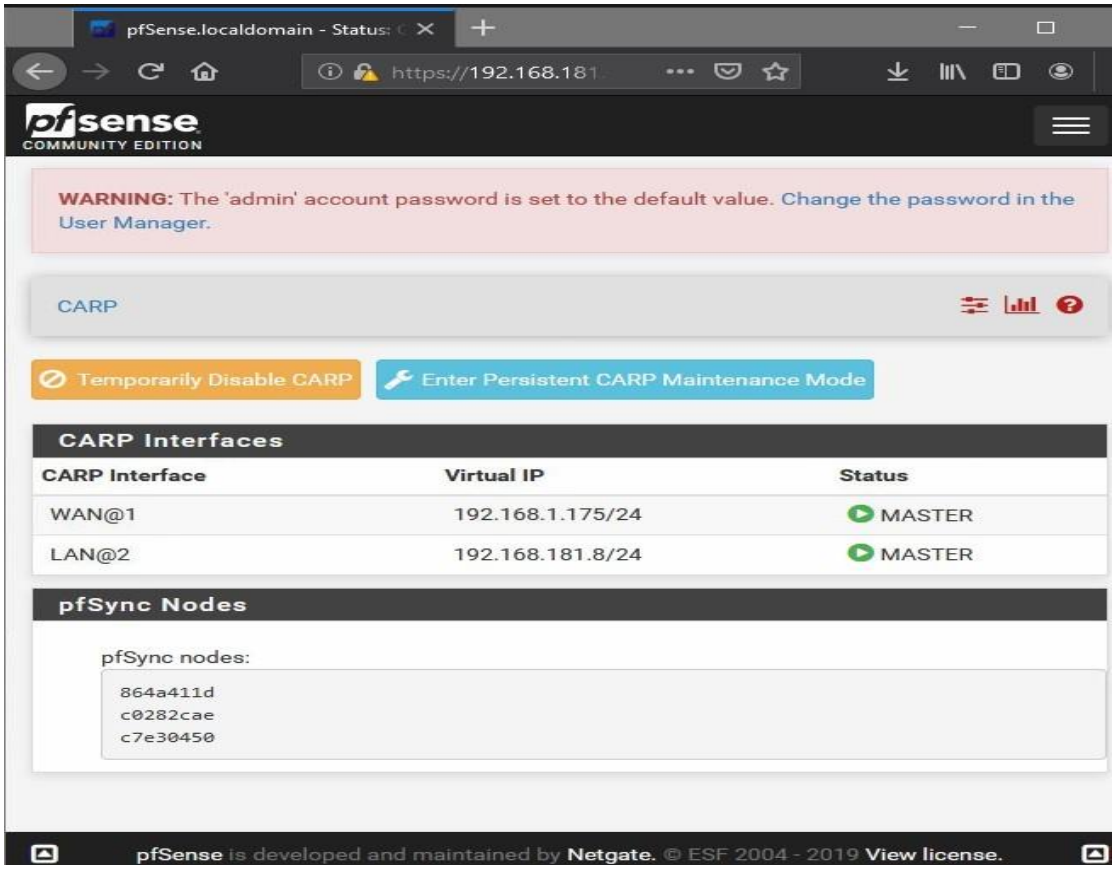
Hình 3-29 Trên máy pfsense master

- Trên máy chủ pfSense backup :



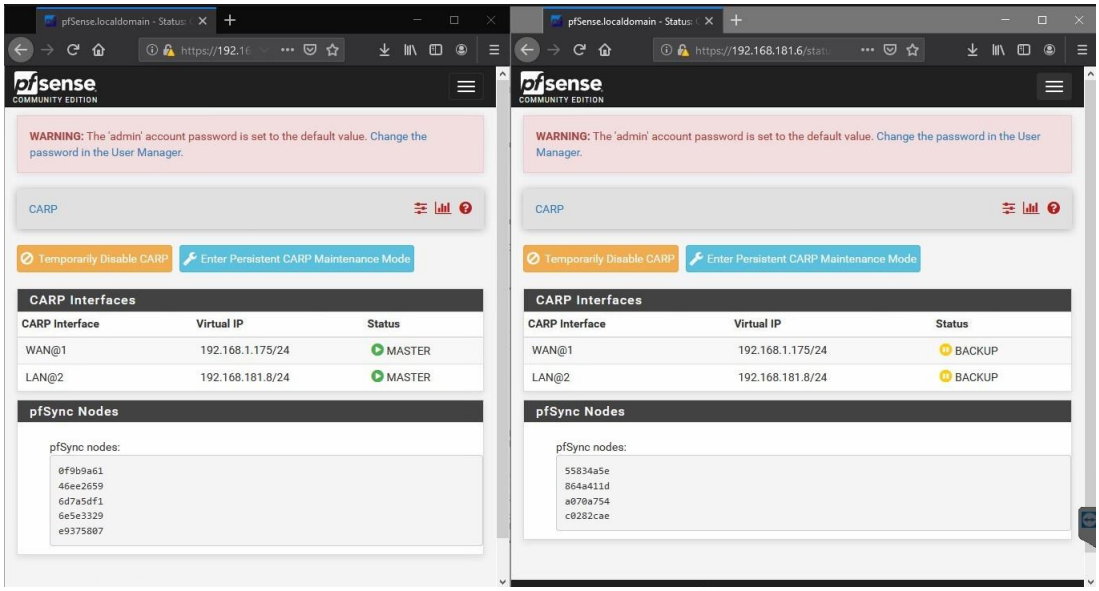
Hình 3-30 Trên máy pfsense backup

- Khi ta tắt máy chủ pfSense master, ngay lập tức CARP status máy chủ pfSense backup sẽ trở thành master:



Hình 3-31 Màn hình CARP status của pfSense backup

- Khi máy chủ pfSense master được bật lại:

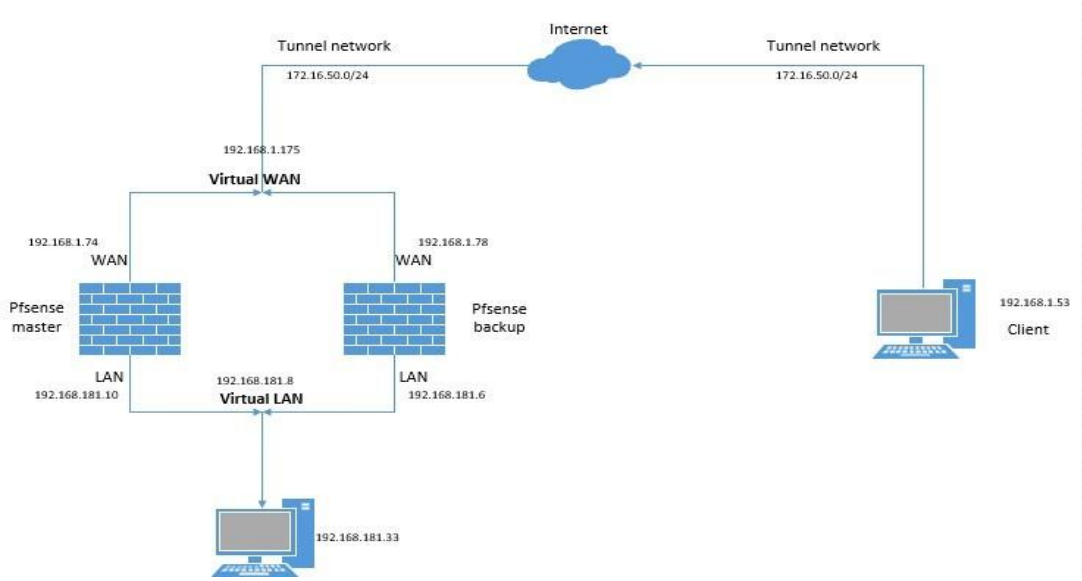


Hình 3-32 Màn hình CARP status của 2 máy chủ

3.3.6 Giải pháp mạng riêng ảo trên Pfsense

3.3.6.1 VPN Client to site

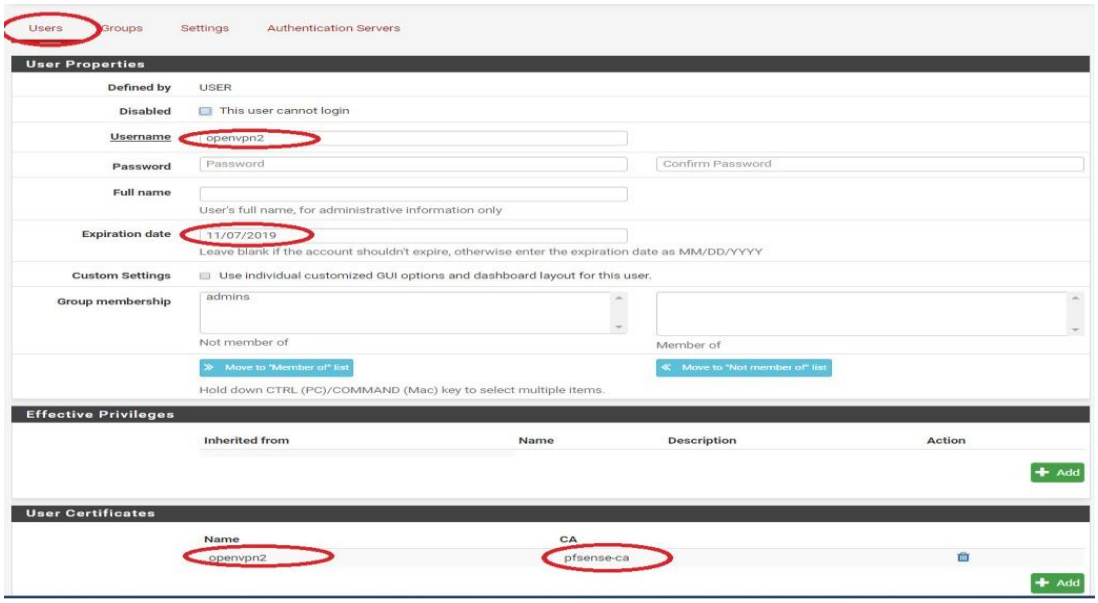
Mô hình thực hiện



Hình 3-33 Mô hình thực hiện

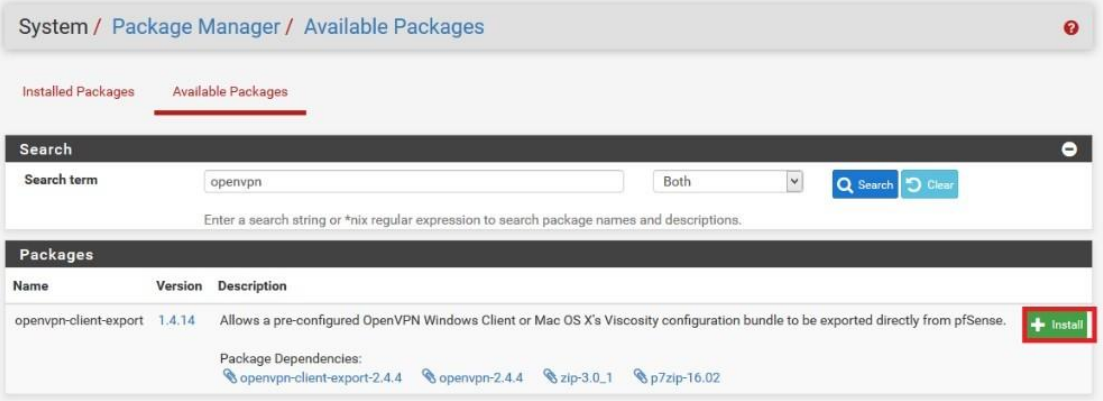
Các bước thực hiện

- Bước 1: Tạo người dùng cho phép sử dụng tài khoản để đăng nhập VPN. Thực hiện như sau: Chọn System > User Manager > chọn Add rồi nhập thông tin giống như hình sau:



Hình 3-34 Tạo user đăng nhập VPN

- Bước 2: Cài đặt package openvpn-client-export bằng việc thực hiện như sau: chọn System > Packet manager > Chọn tab Available Packages > nhập openvpn vào ô tìm kiếm và chọn Search > Install.



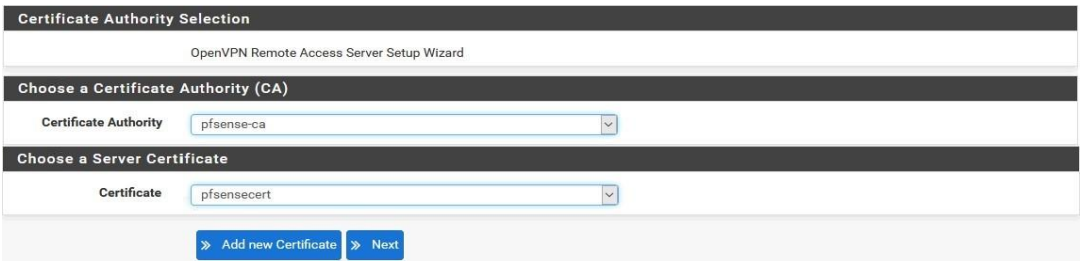
Hình 3-35 Cài đặt gói openvpn-client

- Bước 3. Tạo server VPN sử dụng pfSense. Cách thực hiện như sau:

  - Ta chọn menu VPN sau đó chọn openVPN rồi chuyển sang tab Wizards. Kết quả nhận được như sau:

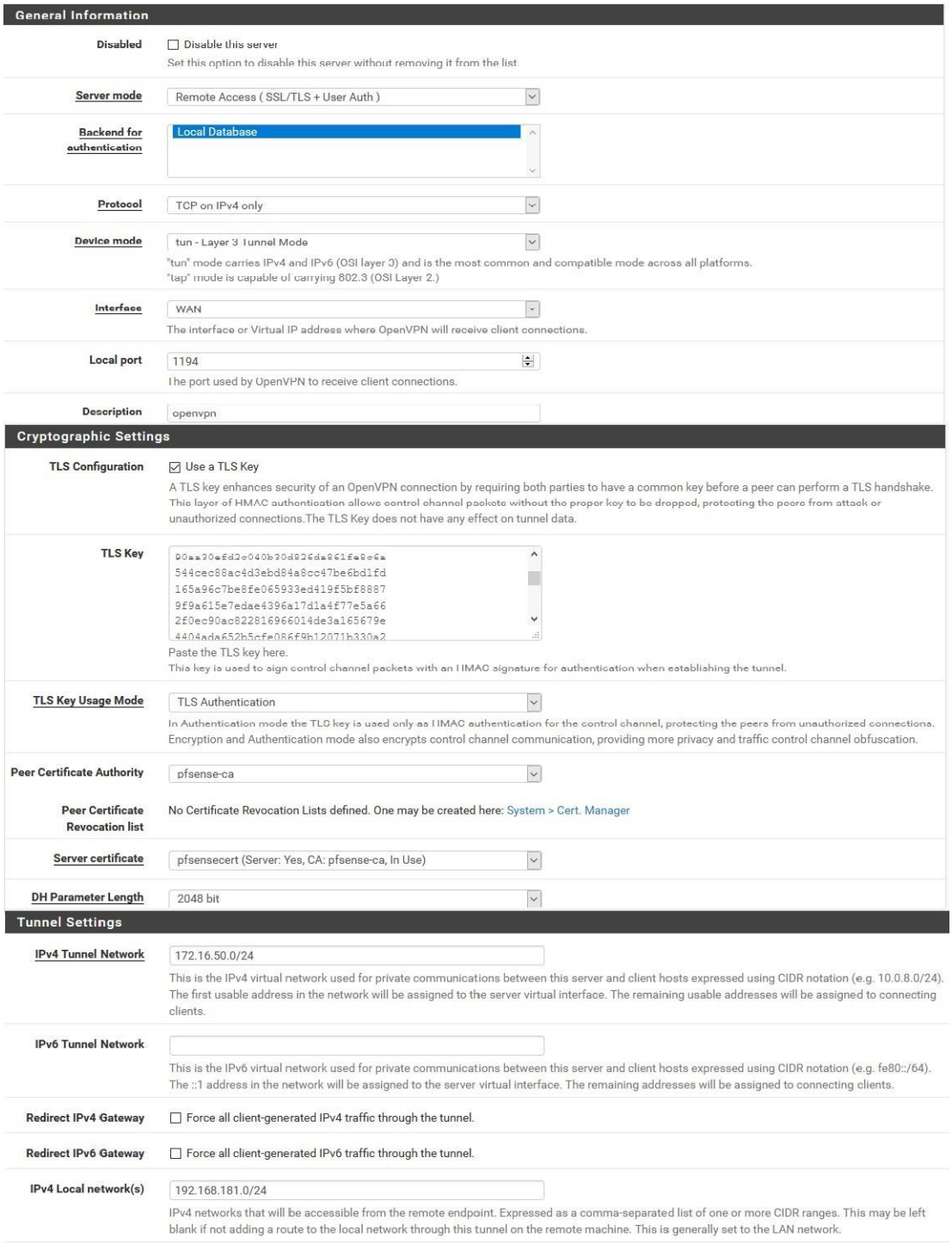
Hình 3-36 Tạo OpenVPN remote access

  - Chọn một CA và Certificate cho server openVPN sử dụng trong quá trình xác thực:



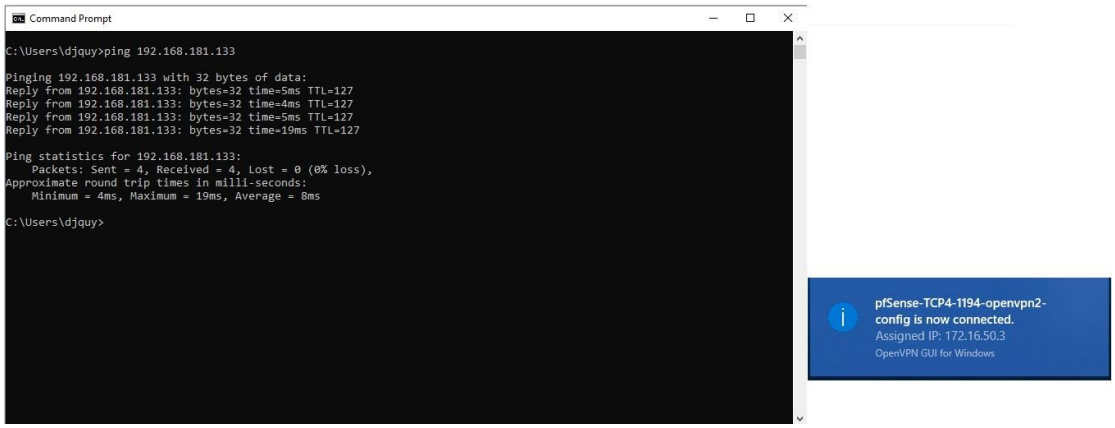
Hình 3-37 Chọn CA và Certificate

- Tiếp tục điền các thông tin như hình dưới:



Hình 3-38 Điền các thông số cho VPN

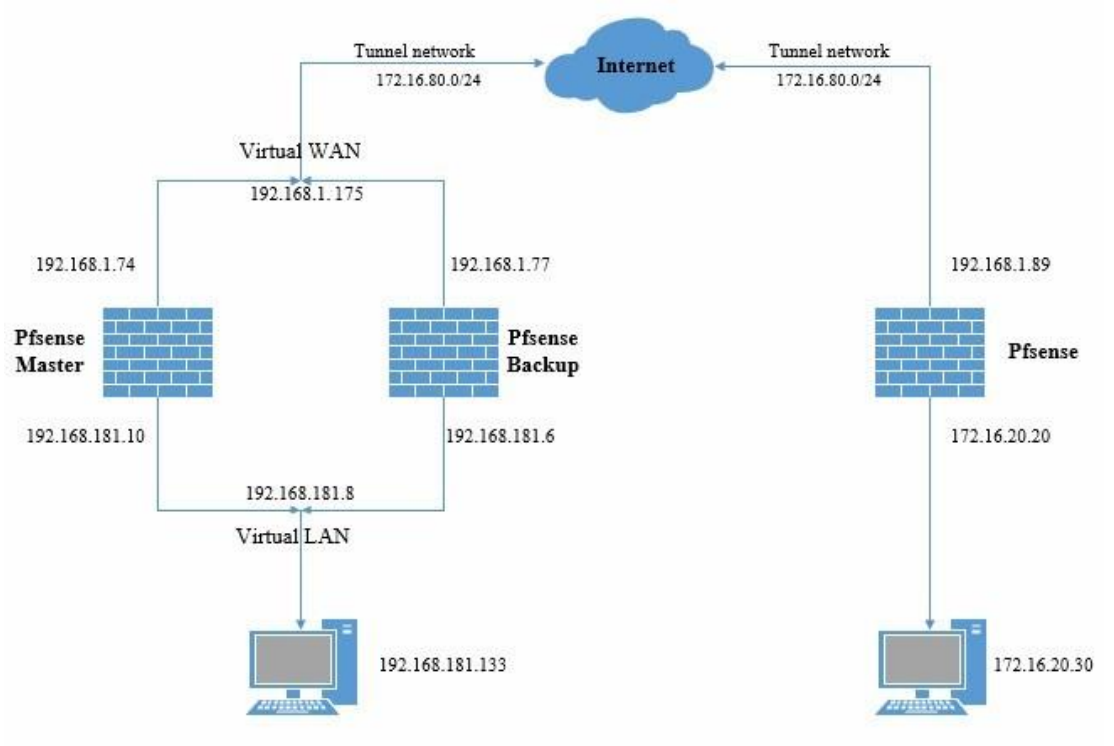
- Bước 4: Từ máy client đã cài đặt openVPN GUI, ta thực hiện kết nối đến server với tài khoản người dùng là openvpn2 để kiểm tra kết quả :



Hình 3-39 Thực hiện ping đến 1 máy trong mạng Lan của pfSense

3.3.6.2 VPN Site to site

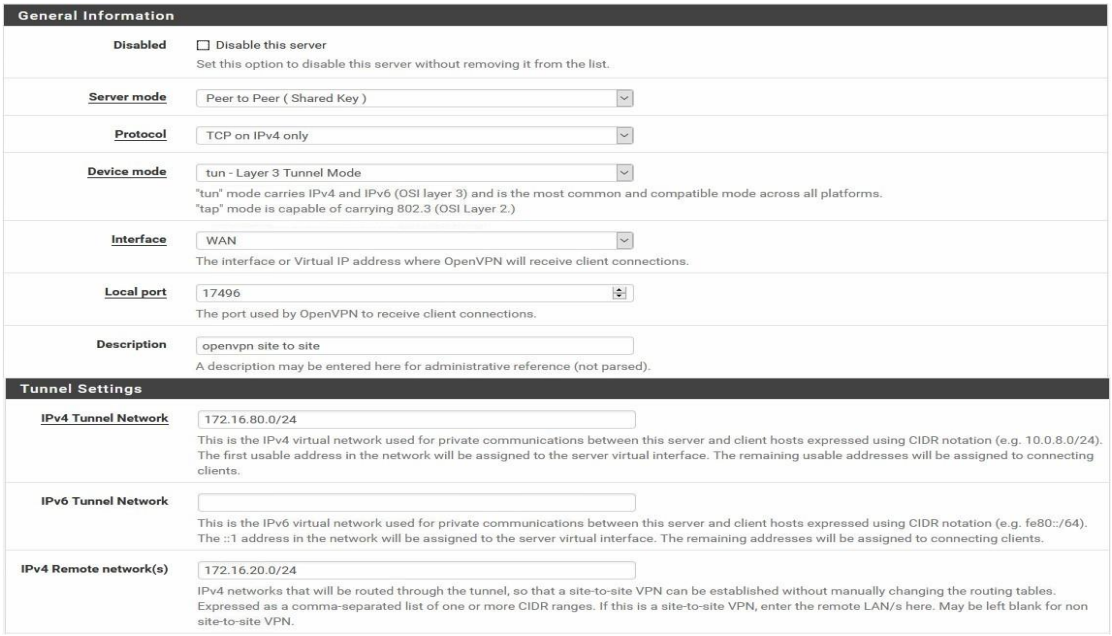
Mô hình thực hiện



Hình 3-40 Mô hình VPN site to site

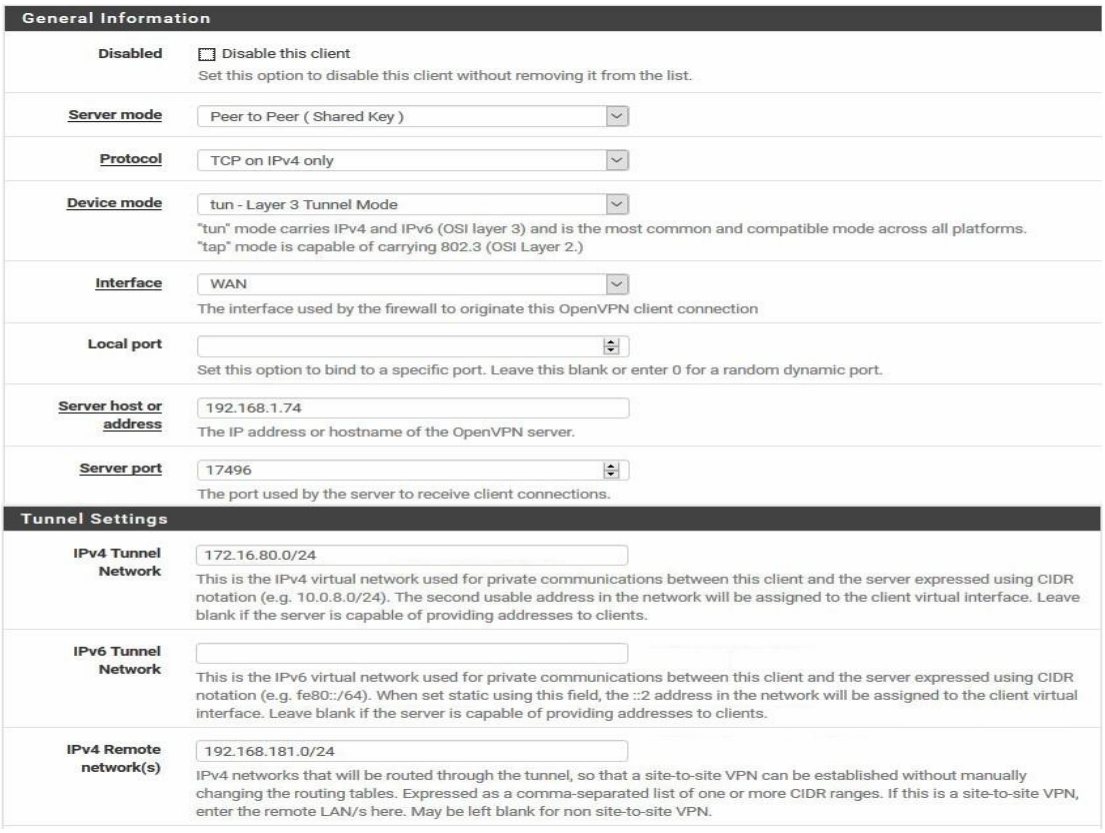
Các bước thực hiện:

- Bước 1 : Tại pfSense Master, chọn tab VPN > OpenVPN > Server , khai báo các thông số như sau :



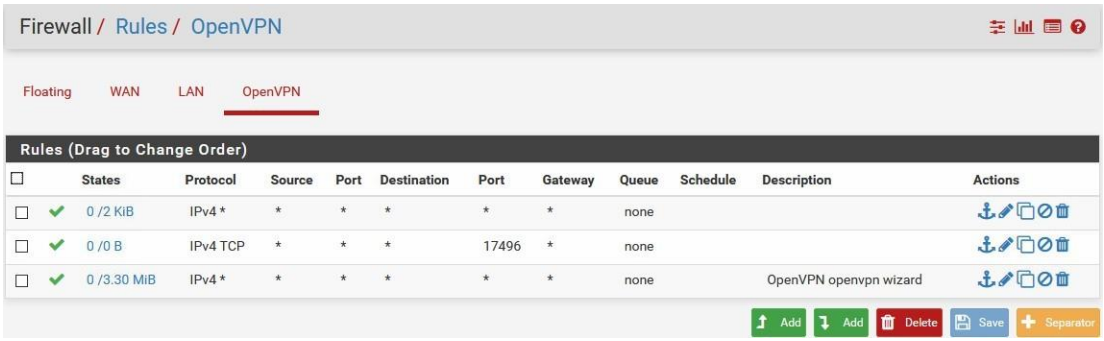
Hình 3-41 Tạo kết nối VPN trên pfSense Master

- Bước 2: Tại máy chủ pfSense 3, chọn tab VPN > OpenVPN > Client > điền các thông số như sau:



Hình 3-42 Tạo kết nối tại Pfsense 3

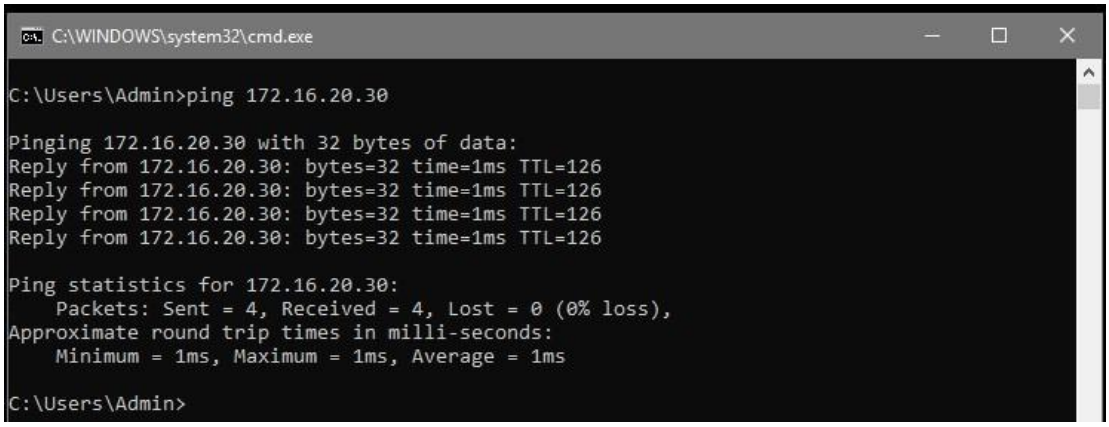
- Bước 3: Tạo rule cho phép kết nối 2 đầu VPN



Hình 3-43 Tạo rule cho OpenVPN

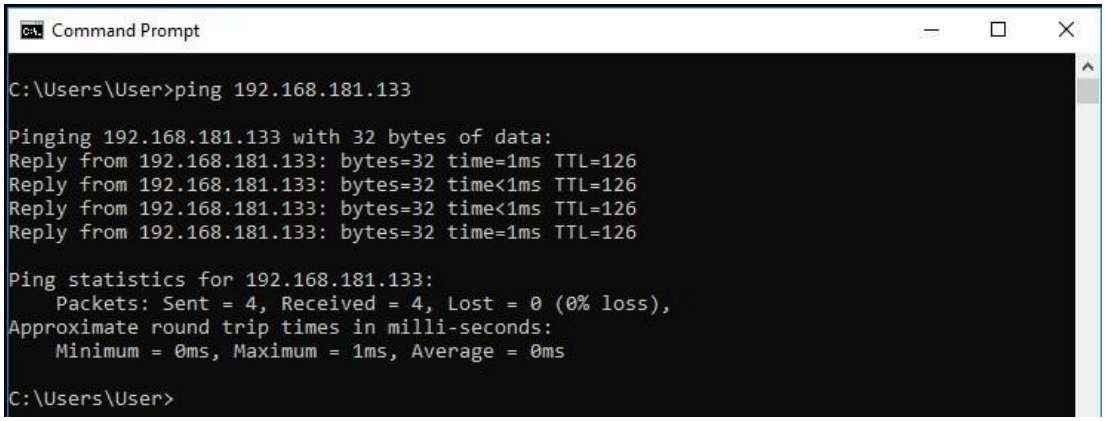
- Bước 4: Kiểm tra kết quả

  - Tại site pfSense Master ta ping đến site pfSense 3:



Hình 3-44 Kiểm tra kết nối

- Tại site pfSense 3, ta ping đến site pfSense Master:



Hình 3-45 Kiểm tra kết quả

KẾT LUẬN

Đồ án "Nghiên cứu triển khải giải pháp đảm bảo an ninh mạng trên nền pfSense" đã đạt được những kết quả sau :

Về lý thuyết đồ án đã trình bày và hiểu được :

- Tổng quan về an ninh – an toàn thông tin mạng. Các phương thức tấn công, các biện pháp giải phòng tránh khi bị tấn công.
- Nêu lên một số giải pháp về Firewall hiện nay.
- Hệ thông phát hiện chống xâm nhập.
- Tìm hiểu về Mạng riêng ảo VPN, các giao thức của VPN, ưu điểm và nhược điểm của VPN.

Về thực thi, đồ án đã tiến hành :

- Giới hạn giờ truy cập web.
- Giới hạn tốc độ download/upload cho từng client.
- Chứng thực user truy cập web sử dụng Captive Portal.
- Xây dựng hệ thống backup Firewall.
- Cấu hình VPN Site – to – site và Client – to site trên pfSense.

Với thời gian và điều kiện thực tế còn nhiều hạn chế, đề tài chỉ dừng lại ở khả năng nghiên cứu và triển khai được những chức năng cần thiết. Em rất mong nhận được sự đóng góp ý kiến của thầy cô để có thể khắc phục và hoàn thiện nội dung đồ án cũng như tiếp tục nghiên cứu sâu hơn phục vụ cho quá trình làm việc về sau.

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Công Nhật (2008), Giáo trình an toàn thông tin.

[2]. Nguyễn Tấn Phương (2010), Tìm hiểu Firewall, Khoa CNTT – Đại học Duy Tân.

[3]. ThS. Trần Công Hùng (2002), Kỹ thuật mạng riêng ảo, NXB Bưu Điện.

[4]. https://congnghe.club