BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

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

TÌM HIỂU GIẢI PHÁP AN NINH MẠNG VỚI FIREWALL

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-------

TÌM HIỂU GIẢI PHÁP AN NINH MẠNG VỚI FIREWALL

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

Sinh viên thực hiện **: Cù Thế Huy**

Mã sinh viên **: 1512101005**

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: **Cù Thế Huy** Mã sinh viên**:** **1512101005**

Lớp: **CT1901** Ngành**: Công nghệ Thông tin**

Tên đề tài:

"TÌM HIỂU GIẢI PHÁP AN NINH MẠNG VỚI FIREWALL"

LỜI CẢM ƠN

Trong thời gian làm đồ án tốt nghiệp, em đã nhận được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, gia đình và bạn bè.

Em xin gửi lời cảm ơn chân thành đến T.s Ngô Trường Giang, giảng viên khoa Công nghê thông tin - trường ĐHDL Hải Phòng người đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình làm đồ án.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong trường Đại Học Dân Lập Hải Phòng đã hết lòng dạy bảo chúng em trong những năm học Đại Học, giúp chúng em có những kiến thức và kinh nghiệm quý báu trong chuyên môn và cuộc sống, giúp chúng em bước những bước đi đầu tiên trong hành trang vào đời.

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

Hải Phòng, tháng 6 năm 2019

Sinh Viên

LỜI MỞ ĐẦU

Ngày nay, việc duy trì hệ thống mạng nội bộ hoạt động ổn định, nhanh chóng, an toàn và tin cậy đang là vấn đề được các tổ chức và doanh nghiệp đặc biệt quan tâm.Trong đó, yếu tố an toàn mạng luôn được đặt lên hàng đầu. Nắm bắt được nhu cầu của các tổ chức và doanh nghiệp, một số tập đoàn công nghệ thông tin và truyền thông hàng đầu trên thế giới đã đưa ra nhiều giải pháp bảo mật cũng như các Firewall (cả phần cứng lẫn phần mềm) để bảo vệ môi trường mạng được trong sạch và an toàn.

Hiện nay, các tổ chức và doanh nghiệp chọn cho mình cách bảo vệ hệ thống mạng của họ bằng nhiều cách khác nhau như sử dụng Router Cisco, dùng tường lửa Microsoft như ISA …. Tuy nhiên những thành phần kể trên tương đối tốn kém. Vì vậy để tiết kiệm chi phí và có một tường lửa bảo vệ hệ thống mạng bên trong (mạng nội bộ) khi mà chúng ta giao tiếp vối hệ thống mạng bên ngoài (Internet) thì Firewall mã nguồn mở là một giải pháp tương đối hiệu quả đối với người dùng.

Đồ án tốt nghiệp đã **"tìm hiểu giải pháp an ninh mạng với FireWall**" nhằm mục đích tìm hiểu sâu sắc về cơ chế hoạt động của nó. Sau đó áp dụng vào thực tiễn giúp tăng cường an ninh mạng nội bộ cho các công ty, doanh nghiệp. Giúp dữ liệu cá nhân của các nhân, công ty luôn nằm trong vùng an toàn. Quản lí điều tiết lưu lượng mạng một cách hợp lí để tránh lãng phí tài nguyên và giảm chi phí về an ninh mạng một cách tối đa.

Đồ án gồm 3 nội dung chính:

Chương 1: Tổng quan về an toàn thông tin và an ninh mạng

Chương 2: Tổng quan về Firewall và Pfsense

Chương 3: Thực nghiệm Firewall trên Pfsense

MỤC LỤC

DANH MỤC HÌNH VẼ

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN THÔNG TIN VÀ AN NINH MẠNG

1.1 An toàn thông tin mạng

Ngày nay với sự phát triển bùng nổ của công nghệ, hầu hết các thông tin của doanh nghiệp như chiến lược kinh doanh, các thông tin về khách hàng, nhà cung cấp, tài chính, mức lương nhân viên đều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của doanh nghiệp là những đòi hỏi ngày càng cao của môi trường kinh doanh yêu cầu doanh nghiệp cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua Internet hay Intranet. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài chính, danh tiếng của công ty và quan hệ khách hàng.

1.1.1 Một số khái niệm

An toàn thông tin: Bảo mật + toàn vẹn + khả dụng + chứng thực.

An toàn máy tính: tập hợp các công cụ được thiết kế để bảo vệ dữ liệu và chống hacker.

An toàn mạng: các phương tiện bảo vệ dữ liệu khi truyền chúng.

An toàn Internet: các phương tiện bảo vệ dữ liệu khi truyền chúng trên tập các mạng liên kết với nhau. Mục đích của môn học là tập trung vào an toàn Internet gồm các phương tiện để bảo vệ, chống, phát hiện, và hiệu chỉnh các phá hoại an toàn khi truyền và lưu trữ thông tin.

1.1.2 Nhu cầu an toàn thông tin

An toàn thông tin đã thay đổi rất nhiều trong thời gian gần đây. Trước kia hầu như chỉ có nhu cầu an toàn thông tin, nay đòi hỏi thêm nhiều yêu cầu mới như an ninh máy chủ và trên mạng.

Các phương pháp truyền thống được cung cấp bởi các cơ chế hành chính và phương tiện vật lý như nơi lưu trữ bảo vệ các tài liệu quan trọng và cung cấp giấy phép được quyền sử dụng các tài liệu mật đó.

Máy tính đòi hỏi các phương pháp tự động để bảo vệ các tệp và các thông tin lưu trữ. Nhu cầu an toàn rất lớn và rất đa dạng, có mặt khắp mọi nơi, mọi lúc. Do đó không thể không đề ra các qui trình tự động hỗ trợ bảo đảm an toàn thông tin.

Việc sử dụng mạng và truyền thông đòi hỏi phải có các phương tiện bảo vệ dữ liệu khi truyền. Trong đó có cả các phương tiện phần mềm và phần cứng, đòi hỏi có những nghiên cứu mới đáp ứng các bài toán thực tiễn đặt ra.

1.2 An ninh mạng

Luật an ninh mạng định nghĩa: An ninh mạng là sự đảm bảo hoạt động trên không gian mạng không gây hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Mục đích chính an ninh mạng

- Bảo đảm an toàn thông tin tại máy chủ
- Bảo đảm an toàn cho phía máy trạm
- An toàn thông tin trên đường truyền

1.3 Phân loại tấn công phá hoại thông tin

1.3.1 Tấn công vào máy chủ hoặc máy trạm độc lập (Standalone workstation or server)

Cách đơn giản nhất để tấn công một hệ điều hành là lợi dụng một máy tính đang ở trạng thái đăng nhập (logged-on) của một người nào đó khi người đó bỏ ra ngoài hoặc bận làm việc khác. Máy trạm hoặc máy chủ không được bảo vệ theo cách này là mục tiêu dễ nhất để tấn công khi không có người xung quanh. Đôi khi các máy chủ cũng là các mục tiêu tấn công, vì quản trị viên hoặc người điều hành máy chủ cũng có thể đi ra ngoài bỏ lại máy chủ trong trạng thái đăng nhập với một tài khoản có đặc quyền của quản trị viên mà bất cứ ai cũng có thể sử dụng. Thậm chí cả những máy chủ đặt trong các phòng máy được khoá cẩn thận, thì máy chủ này cũng trở thành một mục tiêu

tấn công cho bất cứ ai vào được phòng đó, những người này có thể là những lập trình viên, những nhà quản lý, thợ điện, nhân viên bảo trì, …

1.3.2 Tấn công bằng cách phá mật khẩu.

Quá trình truy trập vào một hệ điều hành có thể được bảo vệ bằng một tài khoản người dùng và mật khẩu. Những kẻ tấn công có rất nhiều cách khác phức tạp hơn để tìm mật khẩu truy nhập. Kẻ tấn công có trình độ đều biết rằng luôn có những tài khoản người dùng quản trị chính, ví dụ như tài khoản Administrator trong các hệ điều hành Windows, tài khoản root trong các hệ điều hành Unix và Linux, tài khoản Admin trong NetWare và các tài khoản đặc quyền Admin trong hiều hành Mac OS X(MacOS). Những kẻ tấn công sẽ cố gắng đăng nhập bằng các tài khoản này một cách cục bộ hoặc từ trên mạng, bằng chương trình Telnet chẳng hạn. Telnet là một giao thức trong tầng ứng dụng của mô hình TCP/IP cho phép truy nhập và cấu hình từ xa từ trên mạng hoặc trên Internet. Nếu một kẻ tấn công tìm kiếm một tài khoản để truy nhập, thì kẻ đó phải sử dụng hệ thống tên miền DNS trong một mạng kết nối với Internet để tìm những ra được những tên tài khoản có thể. Sau khi tìm ra được tên tài khoản người dùng, kẻ tấn công này sẽ sử dụng một phần mềm liên tục thử các mật khẩu khác nhau có thể như (Xavior, Authforce và Hypnopaedia). Phần mềm này sẽ tạo ra các mật khẩu bằng cách kết hợp các tên, các từ trong từ điển và các số

1.3.3 Virus và worm

Virus là một chương trình gắn trong các ổ đĩa hoặc các tệp và có khả năng nhân bản trên toàn hệ thống. Một số virus có thể phá hoại các tệp hoặc ổ đĩa, còn một số khác chỉ nhân bản mà không gây ra một sự phá hoại thường trực nào. Một số virus hoặc e-mail chứa các hướng dẫn cách xoá một tệp được cho là một virus nguy hiểm – nhưng thực chất tệp này lại là một tệp hệ thống. Nếu làm theo “cảnh báo” này có thể sẽ mắc phải các lỗi hệ thống hoặc có thể cài đặt lại tệp đó.

Worm (sâu mạng) là một chương trình nhân bản không ngừng trên cùng một máy tính hoặc gửi chính nó đến các máy tính khác trong mạng. Sự khác nhau giữa Worm (sâu mạng) và Virus là Worm (sâu mạng) tiếp tục tạo các tệp mới, còn virus thì nhiễm ổ đĩa hoặc tệp rồi ổ đĩa hoặc tệp đó sẽ nhiễm các ổ đĩa hoặc các tệp khác. Worm (sâu mạng) là một chương trình có vẻ là hữu ích và vô hại, nhưng thực tế lại gây hại cho máy tính của người dùng. Worm (sâu mạng) thường được thiết kế để cho phép kẻ tấn công truy nhập vào máy tính mà nó đang chạy hoặc cho phép kẻ tấn công kiểm soát máy tính đó. Ví dụ, các Worm (sâu mạng) như Trojan.Idly, B02K và NetBus là các Worm (sâu mạng) được thiết kế để cho phép kẻ tấn công truy nhập và điều khiển một hệ điều hành. Cụ thể, Trojan.Idly được thiết kế để chuyển cho kẻ tấn công tài khoản người dùng và mật khẩu để truy nhập máy tính nạn nhân.

1.3.4 Tấn công bộ đệm (buffer attack)

Rất nhiều hệ điều hành sử dụng bộ đệm (buffer) để lưu dữ liệu cho đến khi nó sẵn sàng được sử dụng. Giả sử, một máy chủ với một kết nối tốc độ cao đang truyền dữ liệu đa phương tiện tới một máy trạm trên mạng, và máy chủ truyền nhanh hơn máy trạm có thể nhận. Khi đó giao diện mạng của máy trạm sẽ sử dụng phần mềm lưu tạm (đệm) thông tin nhận được cho đến khi máy trạm sẵn sàng xử lý nó. Các thiết bị mạng như switch cũng sử dụng bộ đệm để khi lưu lượng mạng quá tải nó sẽ có chỗ để lưu dữ liệu cho đến khi chuyển tiếp xong dữ liệu đến đích. Tấn công bộ đệm là cách mà kẻ tấn công lừa cho phần mềm đệm lưu trữ nhiều thông tin trong bộ đệm hơn kích cỡ của nó (trạng thái này gọi là tràn bộ đệm). Phần thông tin thừa đó có thể là một phần mềm giả mạo sau đó sẽ truy nhập vào máy tính đích.

1.3.5 Tấn công từ chối dịch vụ.

Tấn công từ chối dịch vụ (DoS) được sử dụng để can thiệp vào quá trình truy nhập đến một máy tính, một trang web hay một dịch vụ mạng bằng cách làm tràn dữ liệu mạng bằng các thông tin vô ích hoặc bằng các frame

hay packet chứa các lỗi mà một dịch vụ mạng không nhận biết được. Ví dụ, một tấn công dịch vụ có thể nhắm vào các dịch vụ truyền thông dùng giao thức HTTP hoặc giao thức FTP trên một trang web. Mục đích chính của tấn công DoS là chỉ làm sập một trang cung cấp thông tin hoặc làm tắt một dịch vụ chứ không làm hại đến thông tin hoặc các hệ thống.

Nhiều khi một tấn công DoS vào một hệ điều hành được thực hiện trong chính mạng nội bộ mà hệ điều hành đó được cài đặt. Kẻ tấn công giành quyền truy nhập với tài khoản Administrator của Windows 2003 Server và dừng các dịch vụ trên máy trạm và máy chủ, làm cho người dùng không thể truy nhập vào máy chủ đó. Tệ hại hơn, kẻ tấn công có thể gỡ bỏ một dịch vụ hoặc cấu hình để cấm dịch vụ đó. Một cách khác đó là làm đầy ổ đĩa trên các hệ thống không cài đặt chức năng Disk quota (hạn ngạch đĩa) làm cho các ổ đĩa bị tràn bởi các tệp. Vấn đề này trước đây thường xảy ra đối với các hệ thống máy chủ không có các tuỳ chọn quản lý hạn ngạch đĩa.

Một kẻ tấn công từ xa (không khởi tạo tấn công từ trong mạng cục bộ) có thể thực hiện một dạng tấn công đơn giản đó là làm tràn dữ liệu mạng một hệ thống bằng nhiều gói tin. Ví dụ, chương trình Ping of Death sử dụng tiện ích Ping có trong các hệ điều hành Windows và Unix để làm tràn dữ liệu mạng một hệ thống bằng các gói tin quá cỡ, ngăn chặn truy nhập tới hệ thống đích. Ping là một tiện ích mà người dùng mạng và các quản trị viên thường sử dụng để kiểm tra kết nối mạng. Trong một số loại tấn công, máy tính khởi tạo tấn công có thể làm cho rất nhiều máy tính khác gửi đi các gói tin tấn công. Các gói tin tấn công có thể nhắm vào một trang web, một máy đích hay nhiều máy tính có thể tấn công nhiều máy đích. Kiểu tấn công này được gọi là tấn công từ chối dịch vụ phân tán DdoS.

1.3.6 Tấn công định tuyến nguồn (source routing attack).

Trong định tuyến nguồn, người gửi gói sẽ xác định chính xác tuyến đường mà gói sẽ đi qua để đến được đích. Thực chất, định tuyến nguồn chỉ sử dụng trong các mạng token ring và để gỡ rối các lỗi mạng. Ví dụ, tiện ích gỡ rối Traceroute trong các hệ điều hành Windows, UNIX, Mac OS và NetWare sử dụng định tuyến nguồn để xác định tuyến đường mà gói tin đi từ một điểm tới một điểm khác trên một mạng.

Trong tấn công định tuyến nguồn, kẻ tấn công sửa đổi địa chỉ nguồn và thông tin định tuyến làm cho gói tin có vẻ như đến từ một địa chỉ khác, ví dụ một địa chỉ tin cậy để truyền thông trên một mạng. Ngoài việc đóng giả làm một người tin cậy trong mạng, kẻ tấn công còn có thể sử dụng định tuyến nguồn để thăm dò thông tin của một mạng riêng, ví dụ một mạng được bảo vệ bởi một thiết bị mạng sử dụng chức năng chuyển đổi địa chỉ (NAT). NAT(Network Address Translation) có thể chuyển đổi địa chỉ IP của gói tin từ một mạng riêng thành một địa chỉ IP khác được sử dụng trên mạng công cộng hay mạng Internet – đây là kỹ thuật vừa để bảo vệ định danh của các máy tính trong một mạng riêng vừa để bỏ qua yêu cầu sử dụng các địa chỉ IP duy nhất trên toàn cầu trên mạng riêng.

* Chú ý: Những kẻ tấn công có thể lách được một thiết bị NAT bằng cách sử dụng một dạng định tuyến nguồn gọi là làm sai lệch bản ghi định tuyến nguồn (LSRR – Loose Source Record Route). Dạng định tuyến này không xác định một tuyến đầy đủ cho gói tin, mà chỉ một phần – ví dụ, một hoặc hai chặng (hop) hay thiết bị mạng trong tuyến đi qua thiết bị NAT.

1.3.7 Tấn công giả mạo.

Tấn công giả mạo làm cho địa chỉ nguồn của gói tin bị thay đổi làm cho có vẻ như được xuất phát từ một địa chỉ (máy tính) khác. Sử dụng tấn công giả mạo, kẻ tấn công có thể truy nhập được vào một hệ thống được bảo vệ.

Tấn công định tuyến nguồn cũng được coi là một dạng tấn công giả mạo. Ngoài ra, tấn công DoS làm tràn dữ liệu mạng một máy đích bằng các gói tin có địa chỉ nguồn giả mạo cũng là một dạng tấn công giả mạo.

1.3.8 Tấn công sử dụng e-mail

Một cuộc tấn công e-mail có vẻ như xuất phát từ một nguồn thân thiện, hoặc thậm chí là tin cậy như: một công ty quen, một người thân trong gia đình hay một đồng nghiệp. Người gửi chỉ đơn giản giả địa chỉ nguồn hay sử dụng một tài khoản e-mail mới để gửi e-mail phá hoại đến người nhận. Đôi khi một e-mail được gửi đi với một tiêu đề hấp dẫn như "Congratulation you've just won free software. Những e-mail phá hoại có thể mang một tệp đính kèm chứa một virus, một Worm (sâu mạng) hay một trojan horse. Một tệp đính kèm dạng văn bản word hoặc dạng bảng tính có thể chứa một macro (một chương trình hoặc một tập các chỉ thị) chứa mã độc. Ngoài ra, e-mail cũng có thể chứa một liên kết tới một web site giả.

Tấn công có tên Ganda được thực hiện dưới dạng một e-mail và tệp đính kèm được gửi đi dưới rất nhiều dạng khác nhau, nhưng nó luôn mang một thông báo kêu gọi một hành động như "Stop Nazis" hoặc "Save kittens - Hãy cứu lấy lũ mèo con". Khi người dùng mở tệp đính kèm, Worm (sâu mạng) Ganda sẽ được kích hoạt. Ngoài việc tạo ra các tệp, Worm (sâu mạng) này còn can thiệp vào các tiến trình đã khởi động, ví dụ các tiến trình của phần mềm diệt virus và bức tường lửa. Một ví dụ khác là một e-mail giả được gửi cho các người dùng của một công ty đăng ký web site nổi tiếng trên internet, yêu cầu người nhận cung cấp tên, địa chỉ và thông tin thẻ tín dụng lấy cớ là cập nhật các bản ghi của công ty. Nhưng mục đích thực của nó là bí mật thu thập dữ liệu về thẻ tín dụng.

1.3.9 Quét cổng

Truyền thông bằng giao thức TCP/IP sử dụng các cổng TCP hoặc cổng UDP nếu giao thức UDP được sử dụng cùng với giao thức IP. Cổng TCP hoặc UDP là một con đường để truy nhập hệ thống đích, thông thường nó liên quan đến một dịch vụ, một tiến trình hay một chức năng nhất định. Một cổng tương tự như một mạch ảo kết nối giữa 2 dịch vụ hoặc 2 tiến trình truyền thông với nhau giữa 2 máy tính hoặc 2 thiết bị mạng khác nhau. Các dịch vụ này có thể là FTP, e-mail, … Có 65535 cổng trong giao thức TCP và UDP. Ví dụ, dịch vụ DNS chạy trên cổng 53, FTP chạy trên cổng 20.

Port No	Purpose	Port No	Purpose
1	Multiplexing	53	DNS server application
5	RJE applications	79	Find active user application
9	Transmission discard	80	HTTP web browsing
15	Status of network	93	Device controls
20	FTP data	102	Service access point (SAP)
21	FTP commands	103	Standadized e-mail service
23	Telnet applications	104	Standadized e-mail exchange

25	SNMTP e-mail applications	119	Usenet news transfers
37	Time transactions	139	NetBIOS applications

Một số cổng TCP/IP và mục đích

Sau khi một kẻ tấn công đã biết được một hoặc nhiều địa chỉ IP của các hệ thống đang sống (tồn tại) trên mạng, kẻ tấn công sẽ chạy phần mềm quét cổng để tìm ra những cổng quan trọng nào đang mở, những cổng nào chưa được sử dụng. Có 2 phần mềm quét cổng thông dụng đó là Nmap và Strobe. Nmap thường được sử dụng để quét các máy tính chạy hệ điều hành Unix/Linux, ngoài ra còn một phiên bản được sử dụng cho các máy chủ và máy trạm Windows. Một cách để ngăn chặn truy nhập thông qua một cổng mở là dừng các dịch vụ hoặc các tiến trình hệ điều hành không sử dụng hoặc chỉ cấu hình khởi động các dịch vụ một cách thủ công bằng chính hiểu biết của mình.

1.3.10 Tấn công không dây

Các mạng không dây thường rất dễ bị tấn công, vì rất khó để biết được người nào đó đã xâm hại đến mạng này. Đôi khi các tấn công trên mạng không dây còn được gọi là war-drives, vì kẻ tấn công có thể lái xe lòng vòng quanh một khu vực, dùng một máy tính xách tay để thu thập các tín hiệu không dây. Tuy nhiên, kẻ tấn công cũng có thể làm điều đó bằng cách đi bộ hoặc ở một nơi nào đó với chiếc máy tính xách tay của mình.

Hai thành phần quan trọng được sử dụng trong các tấn công không dây là một card mạng không dây và một ăng ten đa hướng, có thể thu tín hiệu từ tất cả các hướng. Một thành phần khác đó là phần mềm war-driving được sử dụng để bắt và chuyển đổi các tín hiệu từ ăng ten qua card mạng không dây. Các tấn công không dây thường được thực hiện bằng cách quét rất nhiều kênh sử dụng cho các truyền thông không dây.

1.4 Các biện pháp phát hiện khi bị tấn công

Không có một hệ thống nào có thể đảm bảo an toàn tuyệt đối, mỗi một dịch vụ đều có những lỗ hổng bảo mật tiềm tàng. Người quản trị hệ thống không những nghiên cứu, xác định các lỗ hổng bảo mật mà còn phải thực hiện các biện pháp kiểm tra hệ thống có dấu hiệu tấn công hay không. Một số biện pháp cụ thể:

- Kiểm tra các dấu hiệu hệ thống bị tấn công: Hệ thống thường bị treo bằng những thông báo lỗi không rõ ràng. Khó xác định nguyên nhân do thiếu thông tin liên quan. Trước tiên, xác định các nguyên nhân có phải phần cứng hay không, nếu không phải nghĩ đến khả năng máy tính bị tấn công.
- Kiểm tra các tài khoản người dùng mới lạ, nhất là các tài khoản có ID bằng không.
- Kiểm tra sự xuất hiện của các tập tin lạ. Người quản trị hệ thống nên có thói quen đặt tên tập tin theo mẫu nhất định để dễ dàng phát hiện tập tin lạ.
- Kiểm tra thời gian thay đổi trên hệ thống.
- Kiểm tra hiệu năng của hệ thống: Sử dụng các tiện ích theo dõi tài nguyên và các tiến trình đang hoạt động trên hệ thống.
- Kiểm tra hoạt động của các dịch vụ hệ thống cung cấp.
- Kiểm tra truy nhập hệ thống bằng các tài khoản thông thường, đề phòng trường hợp các tài khoản này bị truy nhập trái phép và thay đổi quyền hạn mà người sử dụng hợp pháp không kiểm soát được.
- Kiểm tra các file liên quan đến cấu hình mạng và dịch vụ, bỏ các dịch vụ không cần thiết.

- Kiểm tra các phiên bản của sendmail, ftp, … tham gia các nhóm tin về bảo mật để có thông tin về lỗ hổng bảo mật của dịch vụ sử dụng.

Các biện pháp này kết hợp với nhau tạo nên một chính sách về bảo mật đối với hệ thống.

1.5 Công cụ an ninh mạng

1.5.1 Thực hiện an ninh mạng từ cổng truy nhập dùng tường lửa

Tường lửa cho phép quản trị mạng điều khiển truy nhập, thực hiện chính sách đồng ý hoặc từ chối dịch vụ và lưu lượng đi vào hoặc đi ra khỏi mạng. Tường lửa có thể được sử dụng để xác thực người sử dụng nhằm đảm bảo chắc chắn rằng họ đúng là người như đã khai báo trước khi cấp quyền truy nhập tài nguyên mạng.

Tường lửa còn được sử dụng để phân chia mạng thành những phân đoạn mạng và thiết lập nhiều tầng an ninh khác nhau trên các phân đoạn mạng khác nhau để có thể đảm bảo rằng những tài nguyên quan trọng hơn sẽ được bảo vệ tốt hơn, đồng thời tường lửa còn hạn chế lưu lượng và điều khiển lưu lượng chỉ cho phép chúng đến những nơi chúng được phép đến.

1.5.2 Mã hóa thông tin

Mã hóa (Cryptography) là quá trình chuyển đổi thông tin gốc sang dạng mã hóa. Có hai cách tiếp cận để bảo vệ thông tin bằng mật mã: theo đường truyền và từ nút-đến-nút (End-to-End).

Trong cách thứ nhất, thông tin được mã hóa để bảo vệ luồng thông giữa hai nút không quan tâm đến nguồn và đích của thông tin đó. Ưu điểm của cách này là có thể bí mật được luồng thông tin giữa nguồn và đích và có thể ngăn chặn được toàn bộ các vi phạm nhằm phân tích thông tin trên mạng. Nhược điểm là vì thông tin chỉ được mã hóa trên đường truyền nên đòi hỏi các nút phải được bảo vệ tốt.

Ngược lại, trong cách thứ hai, thông tin được bảo vệ trên toàn đường đi từ nguồn tới đích. Thông tin được mã hóa ngay khi được tạo ra và chỉ được giải mã khi đến đích. Ưu điểm của tiếp cận này là người sử dụng có thể dùng nó mà không ảnh hưởng gì tới người sử dụng khác. Nhược điểm của phương pháp này là chỉ có dữ liệu người sử dụng được mã hóa, còn thông tin điều khiển phải giữ nguyên để có thể xử lý tại các nút.

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

Có thể nói nhiệm vụ khó khăn nhất có liên quan đế an ninh mạng là giai đoạn lập kế hoạch, mà trong đó cần phải phát triển các giải pháp để đáp ứng các chính sách thương mại của công ty, cũng như các nhu cầu an ninh phải giải quyết. Khi khảo sát một hệ thống mạng để xác định các thành phần và các vùng không an ninh, cần tiếp cận một chính sách an ninh từ các nhận thức khác nhau:

- Các mục tiêu thương mại và các nhu cầu của người sử dụng.
- Con người và quan điểm của người khảo sát.
- Các vấn đề kỹ thuật.

1.6.1 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. Đây là một số 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,nVista, 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, ….

1.6.2 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.

1.6.3 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).

1.6.3.1 **Mô hình an ninh nhờ sự mù mờ**

Mô hình an ninh nhờ sự mù mờ dựa trên sự che giấu để bảo vệ mạng. Quan niệm đứng sau của mô hình này là nếu kẻ tấn công không có thông tin về hệ thống mạng thì sẽ không thể thực hiện tấn công. Hi vọng chính trong việc che giấu mạng hoặc ít nhất không quảng bá sự tồn tại của nó sẽ giống như việc đảm bảo an ninh thành công. Vấn đề chính với phương án này là mạng không thể hoạt động trong một thời gian dài mà không bị phát hiện và khi bị phát hiện thì mạng sẽ bị tổn thương hoàn toàn.

1.6.3.2 **Mô hình bảo vệ vòng ngoài**

Mô hình bảo vệ vòng ngoài giống tương tự như một pháo đài được bao quanh bởi một đường hào. Khi sử dụng mô hình này trong đảm bảo an ninh mạng, các tổ chức sẽ gia cố hoặc tăng cường sức mạnh của các hệ thống vòng ngoài hoặc có thể "che giấu" hệ thống mạng sau một bức tường lửa dùng để phân cách giữa mạng được bảo vệ và mạng không an ninh. Các tổ chức không thực hiện nhiều biện pháp để để bảo vệ các hệ thống trên mạng. Vì giả thiết là mô hình bảo vệ vòng ngoài đã đủ hiệu quả để ngăn chặn bất kỳ kiểu thâm nhập nào và vì vậy các hệ thống bên trong sẽ an ninh.

Hạn chế của mô hình này là không thực hiện bất kỳ biện pháp nào để bảo vệ các hệ thống bên trong đối với các tấn công nội bộ. Mà các tấn công nội bộ có thể là nguy cơ nghiêm trọng nhất trong mạng của mọi tổ chức.

1.6.3.3 **Mô hình bảo vệ theo chiều sâu**

Phương án an ninh nhất để sử dụng là mô hình bảo vệ theo chiều sâu. Phương án bảo vệ theo chiều sâu cố gắng thực hiện bảo vệ an ninh nhờ sự gia cố và giám sát mỗi hệ thống, mỗi hệ thống sẽ là một vùng được tự bảo vệ. Các biện pháp bên ngoài cũng sử dụng các hệ thống bảo vệ vòng ngoài, nhưng sự an ninh của các hệ thống bên trong không chỉ dựa hoàn toàn vào vòng bảo vệ bên ngoài. Phương án này là khó hơn để đảm bảo rằng tất cả các hệ thống và các người quản trị đều là thành phần của nó. Tuy nhiên, với mô

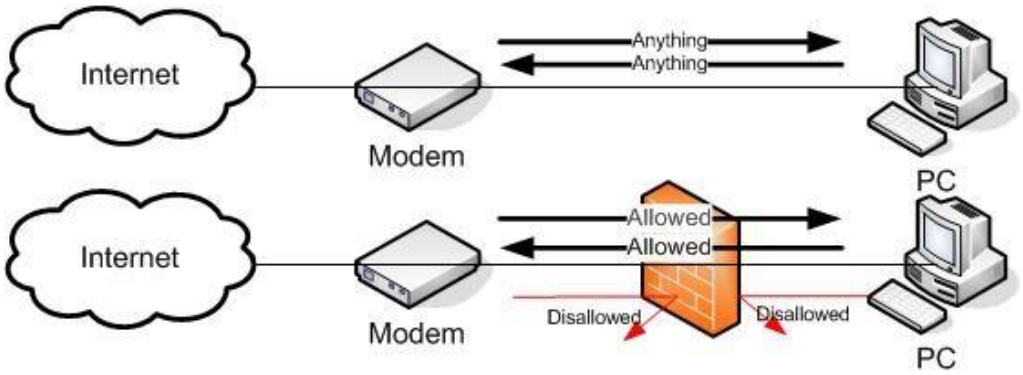
hình này các hệ thống bên trong có khả năng phát hiện bất kỳ sự tấn công từ cá hệ thống độc hại. Phương án này cũng hỗ trợ sự bảo vệ tốt hơn chống lại các kẻ tấn công bên trong. Hành động của các kẻ tấn công bên trong cũng dễ dàng được phát hiện hơn.

CHƯƠNG 2: TỔNG QUAN VỀ FIREWALL VÀ PFSENSE

2.1 Tổng quan về FireWall

2.1.1 Khái niệm về Firewall

Firewall (Tường lửa) 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 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.

2.1.3.2 **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.

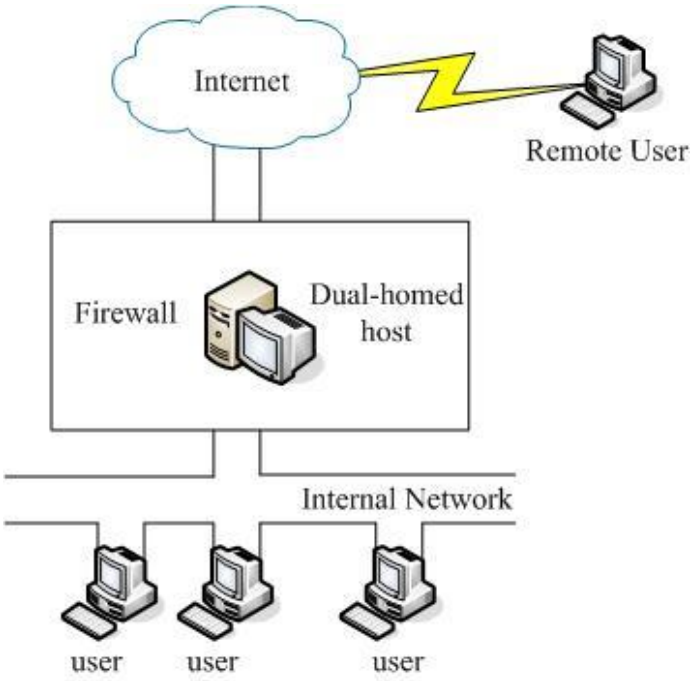
Firewall mềm được cài đặt trên các máy chủ riêng lẻ giúp chặn mỗi yêu cầu kết nối và sau đó xác định xem yêu cầu có hợp lệ hay không. Firewall xử lý tất cả các yêu cầu bằng cách sử dụng tài nguyên máy chủ.

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.

2.1.4 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.

❖ Ưu điểm của Dual-homed Host:

Cài đặt dễ dàng, không yêu cầu phần cứng hoặc phần mềm đặc biệt.

Dual-homed Host chỉ yêu cầu cấm khả năng chuyển các gói tin, do vậy, thông thường trên các hệ Unix, chỉ cần cấu hình và dịch lại nhân (Kernel) của hệ điều hành là đủ.

❖ Nhược điểm của Dual-homed Host:

Không đáp ứng được những yêu cầu bảo mật ngày càng phức tạp, cũng như những hệ phần mềm mới được tung ra thị trường.

Không có khả năng chống đỡ những đợt tấn công nhằm vào chính bản thân nó, và khi Dual-homed Host đó bị đột nhập, nó sẽ trở thành đầu cầu lý tưởng để tấn công vào mạng nội bộ

❖ 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:

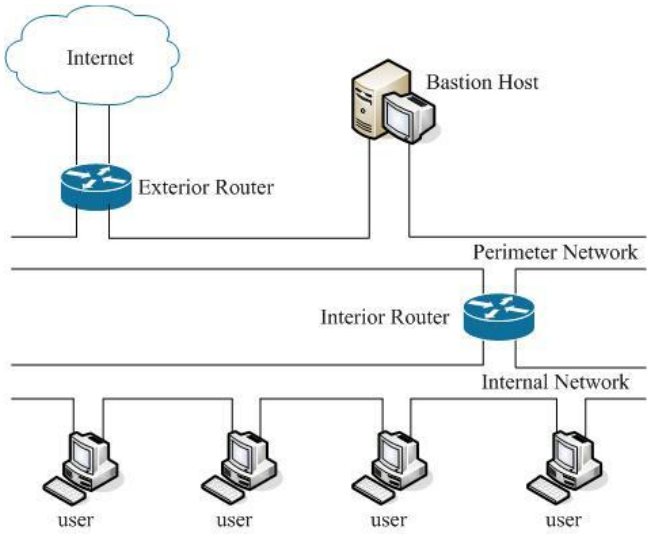
- Kết hợp với các Proxy Server cung cấp những Proxy Service.
- Cấp các tài khoản người dùng trên máy dual-homed host này và khi mà người sử dụng muốn sử dụng dịch vụ từ Internet hay dịch vụ từ external network thì họ phải logging in vào máy này.

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.

Một khuyết điểm cơ bản của hai mô hình trên nữa là : khi mà máy dual-homed host nói chung cũng như các Proxy Server bị đột nhập vào. Người tấn công (attacker) đột nhập được vào hệ thống sẽ hiểu các dịch vụ trên hệ thống đó, nắm bắt được các điểm yếu và thực hiện các hành vi phá hoại tinh vi hơn. Trong các hệ thống mạng dùng Ethernet hoặc Token Ring thì dữ liệu lưu thông trong hệ thống có thể bị bất kỳ máy nào nối vào mạng đánh cắp dữ liệu cho nên kiến trúc này chỉ thích hợp với một số mạng nhỏ.

2.1.4.2 **Kiến trúc Screend Subnet Host**



Hình 2-4Kiến trúc Screened Subnet

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.

❖ Ưu điểm:

- Ba tầng bảo vệ: Router ngoài, Máy chủ, và Router trong.
- Chỉ có một số hệ thống đã được chọn ra trên mạng trung gian là được biết đến bởi Internet qua bảng thông tin định tuyến và trao đổi thông tin định tuyến DNS (Domain Name Server).
- Đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ Proxy.

❖ 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.

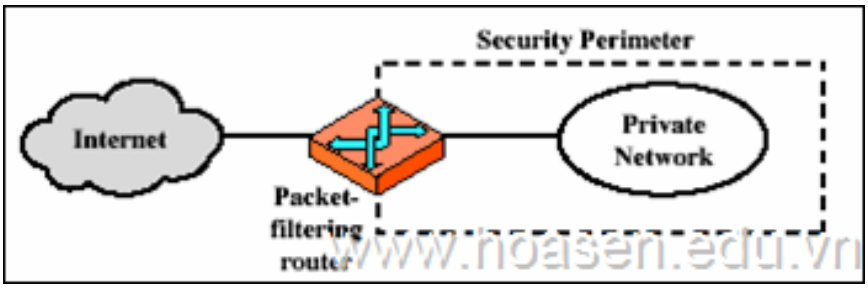
- Sử dụng 2 Screening Router (bộ định tuyến lọc): Router ngoài và Router trong.
- Áp dụng qui tắc dư thừa có thể bổ sung thêm nhiều mạng trung gian (DMZ và perimeter network) càng tăng khả năng bảo vệ càng cao.
- Ngoài ra, còn có những kiến trúc biến thể khác như: sử dụng nhiều Bastion Host (máy chủ)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

2.1.5 Các thành phần cơ bản của Firewall

2.1.5.1 **Packet Filtering – Bộ lọc gói tin**

Bộ lọc gói tin cho phép hay từ chối gói tin mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong các số các luật hay không. Các luật này dựa trên các thông tin ở packet header(tiêu đề gói tin) bao gồm các thông tin sau:

- Địa chỉ IP nguồn (IP Source Address).
- Địa chỉ IP đích (IP Destination Address).
- Protocol (TCP, UDP, ICMP, IP tunnel)
- TCP/UDP source port
- TCP/UDP destination port
- Dạng thông báo ICMP (ICMP message type)
- Cổng gói tin đến (Incomming interface of packet)
- Cổng gói tin đi (Outcomming interface of packet)



Hình 2-5 Packet Filtering

Nếu các luật lọc gói được thỏa mãn thì packet được chuyển qua firewall, nếu không packet sẽ bị bỏ đi. Nhờ vậy mà firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Ngoài ra, việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó hoặc những dịch vụ nào đó (SSH, SMTP, FTP…) được phép mới chạy được trên hệ thống mạng cục bộ.

Ưu điểm:

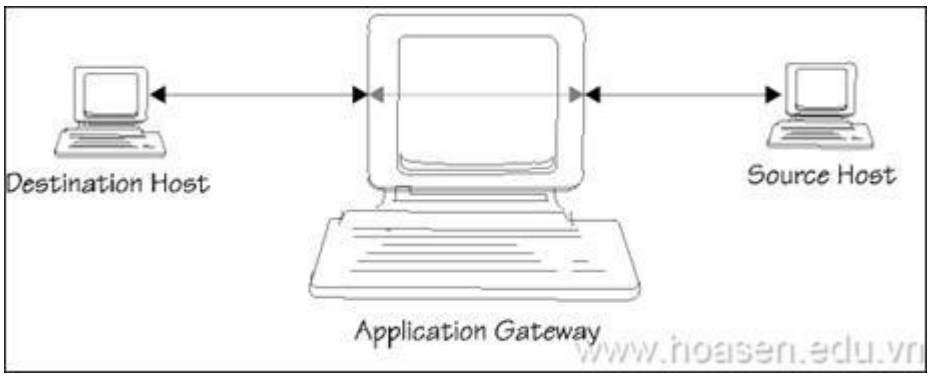
- Đa số các hệ thống firewall đều được sử dụng bộ lọc gói tin. Một trong những ưu điểm của phương pháp dùng bộ lọc gói là chi phí thấp vì cơ chế lọc gói đã có sẵn trong các router.
- Ngoài ra, bộ lọc gói là trong suốt đối với người sử dụng và các ứng dụng vì vậy nó không yêu cầu người sử dụng phải thao tác gì cả.

Nhược điểm:

- Việc định nghĩa các chế độ lọc gói là một việc khá phức tạp, nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ internet, các dạng packet header. Khi yêu cầu về lọc gói tin càng lớn, các rules càng trở nên phức tạp do đó rất khó quản lý và điều khiển.
- Do làm việc dựa trên header của các packet nên bộ lọc không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

2.1.5.2 **Application Gateway – Cổng ứng dụng**

Đây là một loại firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là proxy service. Proxy service là các bộ code đặc biệt cài đặt trên cổng ra (gateway) cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy service cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị cho là chấp nhận được trong khi từ chối những đặc điểm khác.



Hình 2-6 Application Gateway

Một cổng ứng dụng thường được coi như là một Bastion Host (máy chủ) (Máy chủ) bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài.

Những biện pháp đảm bảo an ninh của một Bastion Host (máy chủ) (máy chủ) là:

- Bastion Host (máy chủ) luôn chạy các phiên bản an toàn (secure version) của các phần mềm hệ điều hành (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào hệ điều hành (Operating system) cũng như là đảm bảo sự tích hợp firewall.

- Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên máy chủ, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ telnet, DNS, FTP, SMTP và xác thực tài khoản người dùng là được cài đặt trên máy chủ.
- Máy chủ có thể yêu cầu nhiều mức độ khác nhau ví dụ như tài khoản và mật khẩu hay thẻ thông minh (thẻ từ).
- Mỗi proxy được cài đặt cấu hình để cho phép truy nhập chỉ một số các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.
- Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của dữ liệu mạng đi qua nó. Điều này có nghĩ là bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.
- Mỗi proxy đều độc lập với các proxy khác trên Bastion Host (máy chủ). Điều này cho phép dễ dàng cài đặt một proxy mới hay tháo gỡ một proxy.

Ưu điểm:

- Cho phép người quản trị hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy cá nhân nào có thể truy cập bởi các dịch vụ.
- Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt và nó có nhậy ký ghi chép lại thông tin về truy cập hệ thống.
- Các tập luật lọc cho cổng ứng dụng dễ dàng cấu hình và kiểm tra hơn so với bộ lọc gói.

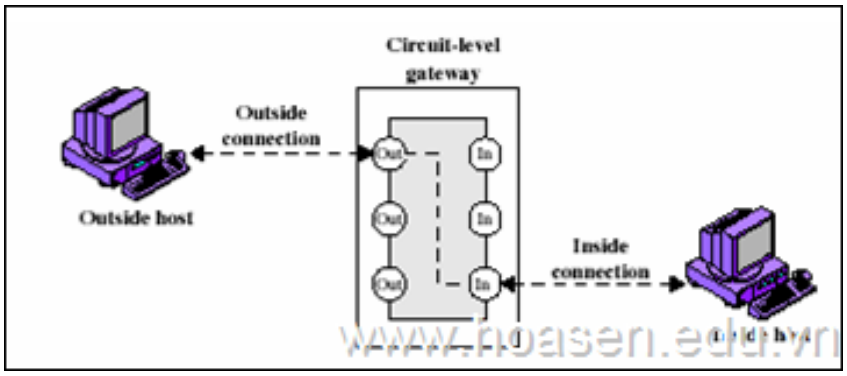
Nhược điểm:

- Cần phải có sự cấu hình trên máy user để user truy cập vào các dịch vụ proxy. Ví dụ telnet

2.1.5.3 **Circuit Level Gate – Cổng mạch**

Circuit Level Gateway là một chức năng đặc biệt có thể thực hiện bởi một cổng ứng dụng. Cổng mạch đơn giản chỉ là chuyển tiếp các kết nối TCP mà không thực hiện bất kì một hành động xử lý hay lọc gói nào.

Hình sau minh họa một hành động sử dụng kết nối telnet qua cổng mạch. Cổng mạch đơn giản chuyển tiếp kết nối telnet qua firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục telnet nào. Cổng mạch làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong và các kết nối bên ngoài. Tuy nhiên vì sự kết nối này xuất hiện từ hệ thống firewall nên nó che dấu thông tin về mạng nội bộ.



Hình 2-7 Circuit Level Gateway

Cổng vòng thường được sử dụng cho những kết nối ra ngoài. Ưu điểm lớn nhất là một Bastion Host (máy chủ) có thể được cấu hình để cung cấp cổng ứng dụng cho những kết nối đến và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống firewall dễ dàng sử dụng cho người dùng trong mạng nội bộ muốn trực tiếp truy cập tới các dịch vụ internet, trong khi vẫn cung cấp chức năng bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

2.2 PFSENSE

2.2.1 Giới thiệu PFSENSE

PfSense là một ứng dụng có chức năng định tuyến và tường lửa mạnh và miễn phí, ứng dụng này sẽ cho phép người dùng 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 download và được sử dụng để bảo vệ các mạng ở tất cả kích cỡ, từ các mạng gia đình đến các mạng lớn của của các công ty. Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi phát hành nhằm cải thiện hơn nữa tính bảo mật, sự ổn định và khả năng linh hoạt của nó.

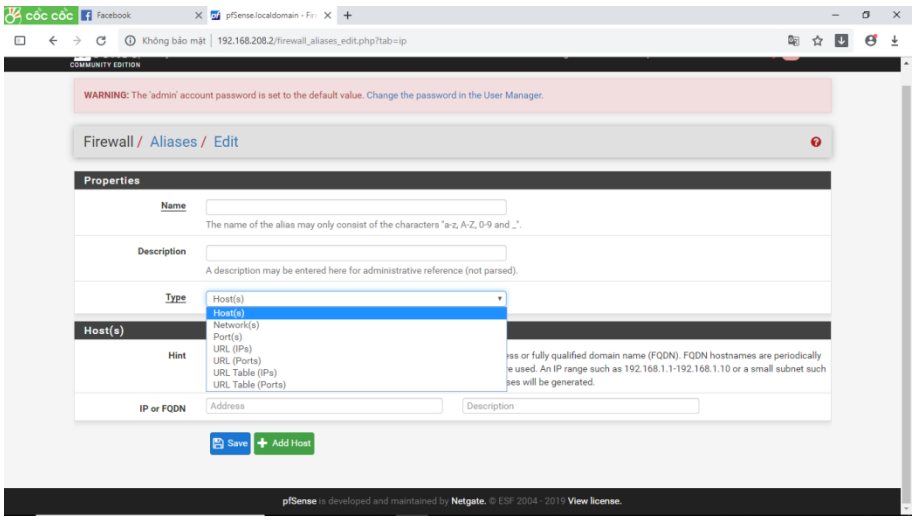
Pfsense bao gồm nhiều tính năng mà người dùng vẫn thấy trên các thiết bị tường lửa hoặc router thương mại, chẳng hạn như GUI trên nền Web tạo sự quản lý một cách dễ dàng. pfSense được dựa trên FreeBSD và giao thức Common Address Redundancy Protocol (CARP) của FreeBSD, cung cấp khả năng dự phòng bằng cách cho phép các quản trị viên nhóm hai hoặc nhiều tường lửa vào một nhóm tự động chuyển đổi dự phòng. Vì nó hỗ trợ nhiều kết nối mạng diện rộng (WAN) nên có thể thực hiện việc cân bằng tải

Đặc điểm khá quan trọng là cấu hình để cài đặt sử dụng phần mềm Pfsense không đòi hỏi cao. Chúng ta chỉ cần một máy tính Ram 128MB, HDD 1GB cũng đủ để dựng được tường lửa Pfsense. Tuy nhiên đặc thù Pfsense là tường lửa ngăn các nguy hại giữa mạng WAN và mạng LAN nên máy cài đặt Pfsense yêu cầu tối thiểu 2 card mạng.

2.2.2 Một số chức năng chính của FireWall PFSense

2.2.2.1 Aliases

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



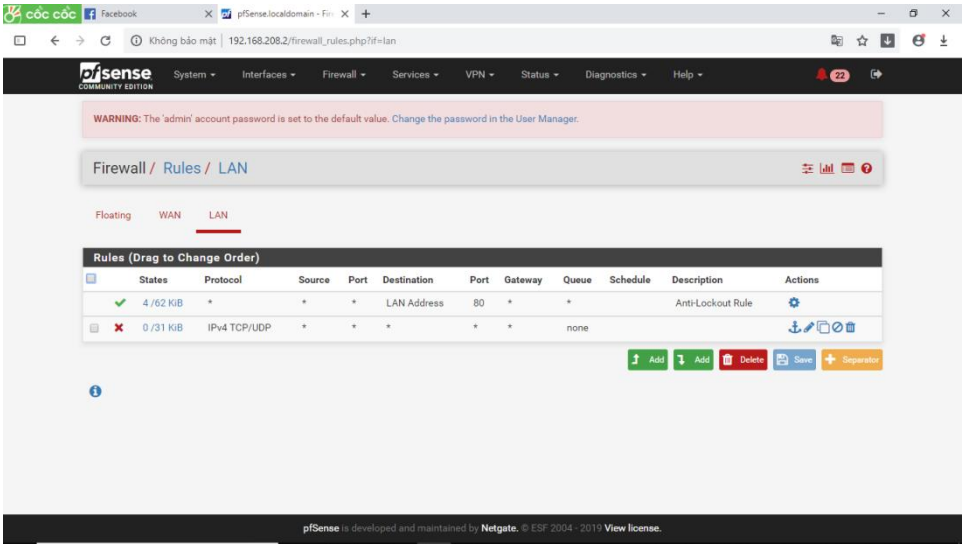
Hình 2-8 Thiết lập Firewall: Aliases

Các thành phần trong Aliases:

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

2.2.2.2 **Rules**

Nơi lưu các rules (Luật) của Firewall. Để vào Rules của pfSense, ta vào Firewall → Rules.



Hình 2-9 Chức năng Firewall: Rules

Mặc định pfSense cho phép mọi lưu lượng truy cập ra/vào hệ thống. Người quản trị phải tạo các rules để quản lý mạng bên trong Firewall.

Một số lựa chọn trong Destination và Source.

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

- **PPPoE clients**: Các clients thực hiện kết nối VPN sử dụng giao thức PPPoE

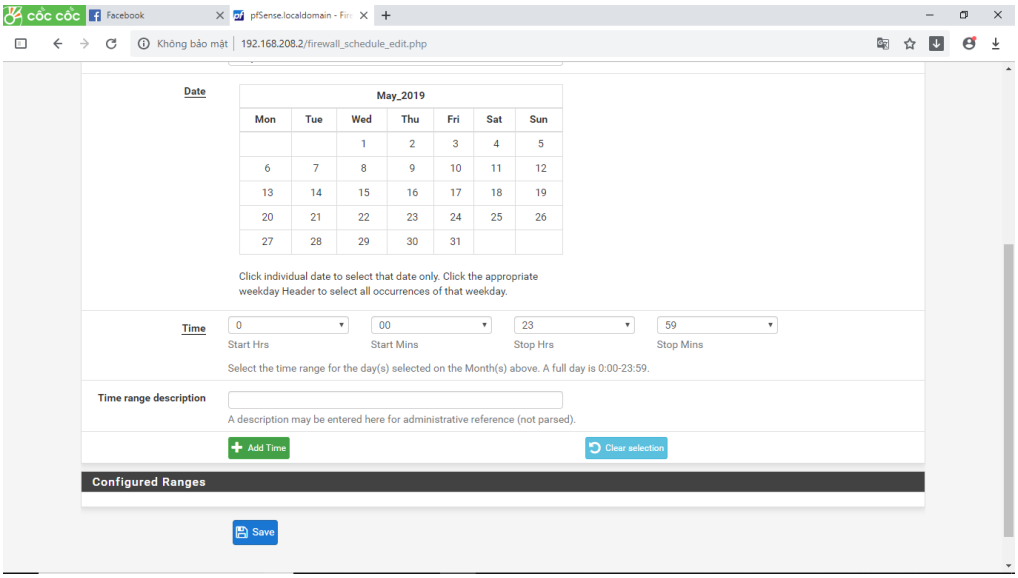
2.2.2.3 **Schedule**

Các Firewall rules có thể được sắp xếp để nó chỉ hoạt động vào các thời điểm nhất định trong ngày hoặc vào những ngày nhất định cụ thể hoặc các ngày trong tuần.

Đây là một cơ chế rất hay vì nó thực tế với những yêu cầu của các doanh nghiệp muốn quản lí nhân viên sử dụng internet trong giờ hành chính.

Đề tạo một Schedules mới, ta vào Firewall → Schedules: Nhấn dấu +

Ví dụ:



Hình 2-10 Thiết lập chức năng Firewall Schedules

2.2.3 Cài đặt PfSense trên máy ảo

Đầu tiên chuẩn bị để cài PfSense cần phải chuẩn bị:

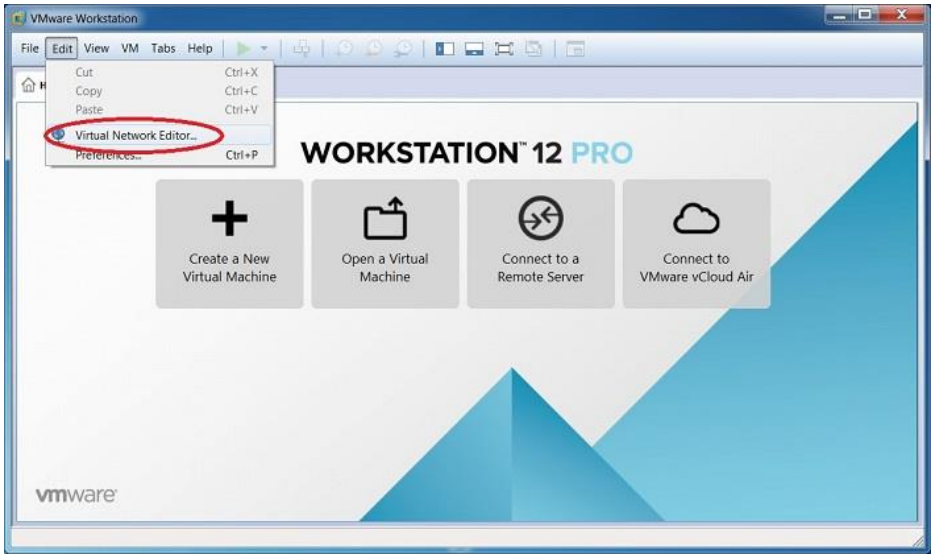
Dowload và cài đặt Vmware Workstation 12 tại địa chỉ:

http://www.mediafire.com/file/71ui47fpf7h3ujn/VMware+Workstation+12.rar

Tải pfsense.iso tại https://www.pfsense.org

Tiến hành cài đặt

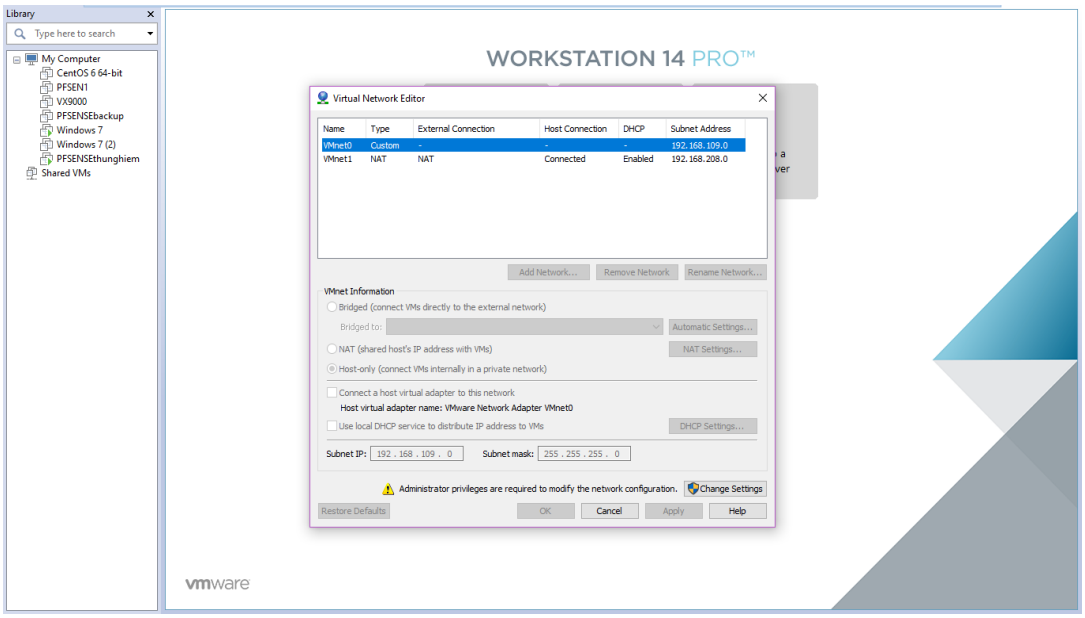
Thiết lập lại "Virtual Network Editor" bằng cách chọn "**Edit -> Virtual Network Editor**"



Hình 2-11 Cài đặt ban đầu

Thêm Vmnet0 và thiết lập ở chế độ "Bridged" với card mạng "Wireless" của Laptop thật

Chỉnh lại **Vmnet1** thiết lập ở chế độ "**NAT**"

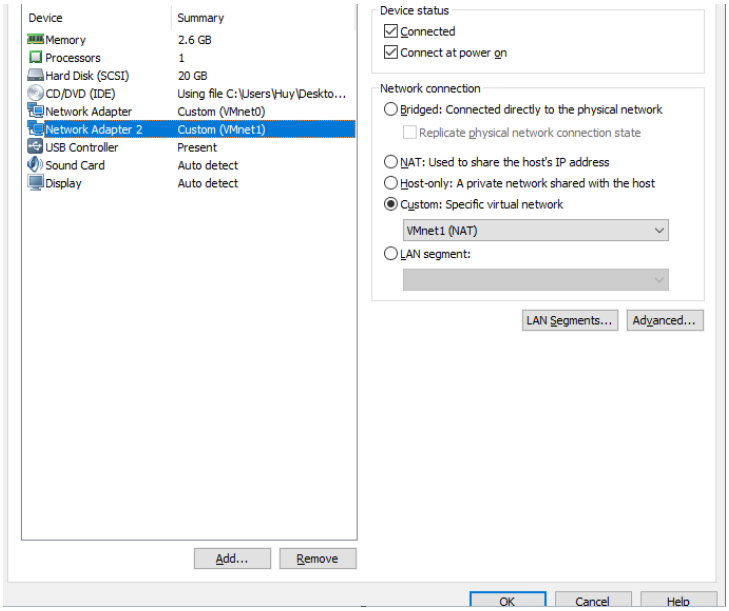


Hình 2-12 Thiết lập card Vmnet1

Tạo 1 máy ảo mới (New Virtual Machine Wizard (Ctrl+N)). Chọn "**Typical**" -> "**Next**"

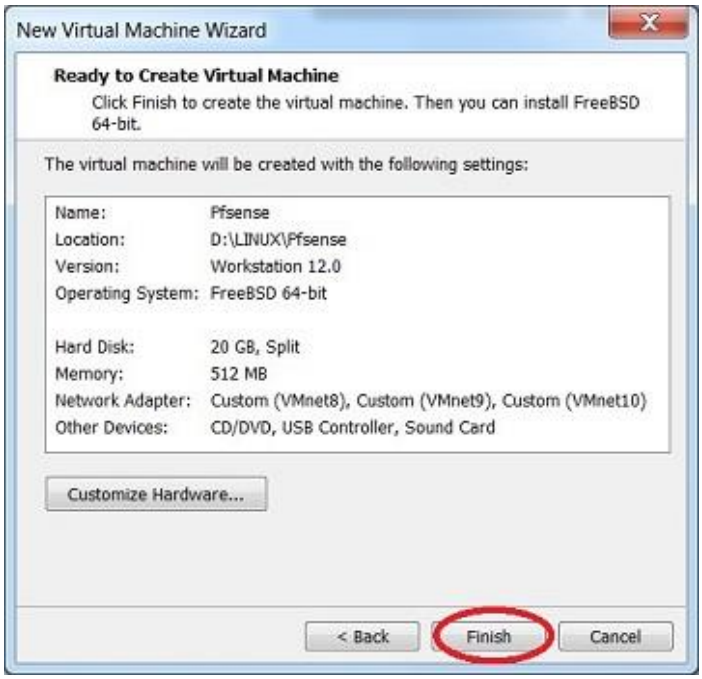
Hình 2-13 Tạo máy ảo Pfsense

Chọn "Add" và thêm 2 card mạng "Vmnet0", "Vmnet1″ cho máy ảo pfSense -> chọn **"Close"**



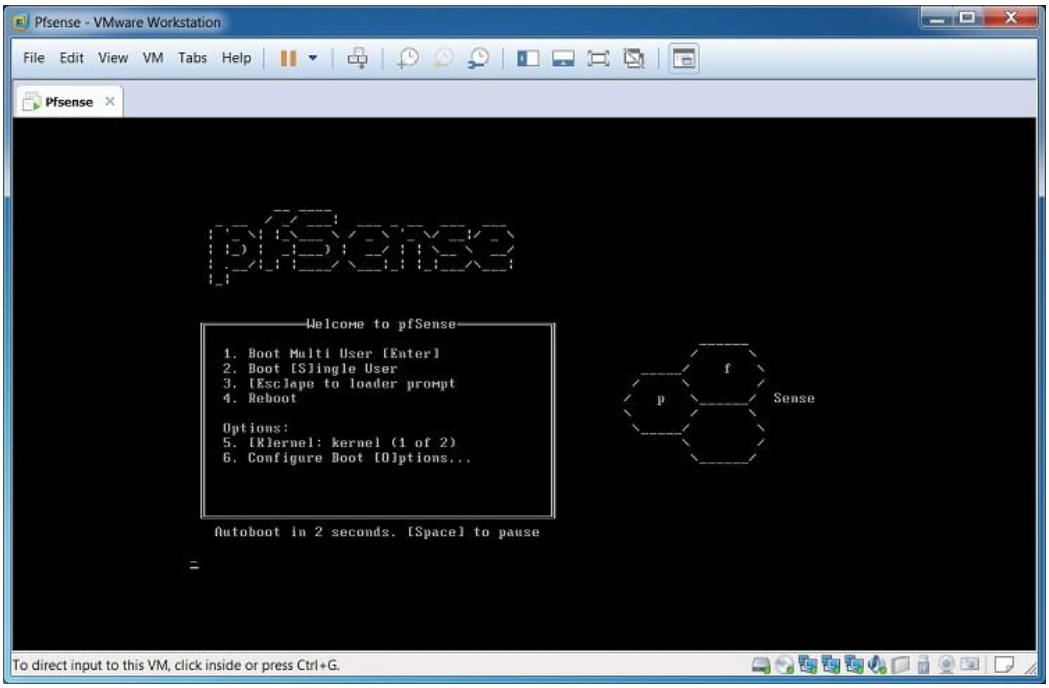
Hình 2-14 Thêm card mạng cho Pfsense

Chọn "**Finished**" để kết thúc quá trình cài đặt pfSense



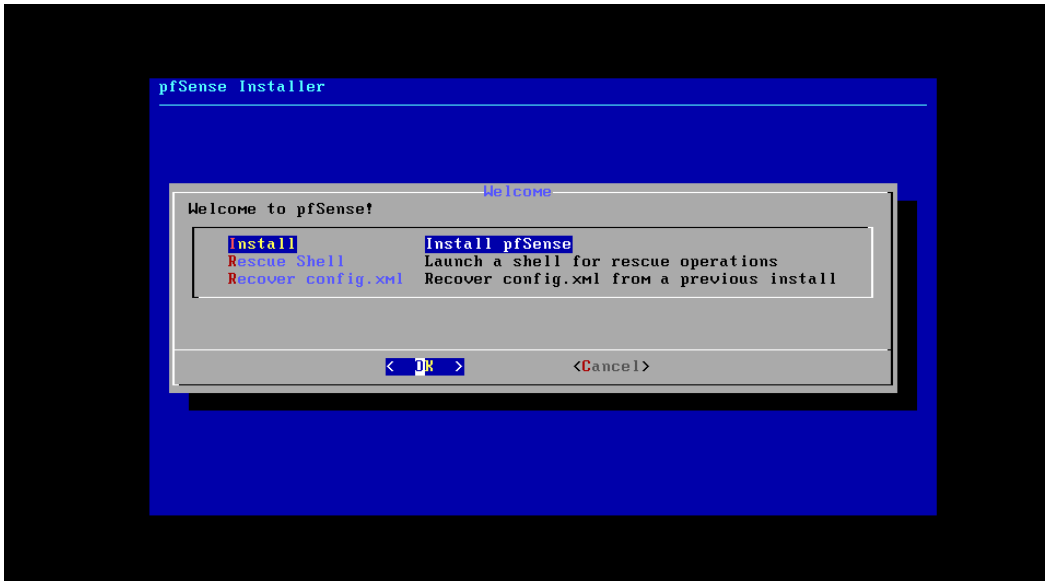
Hình 2-15 Kết thúc cài đặt cơ bản

Pfsense sẽ tự chọn mode khởi động



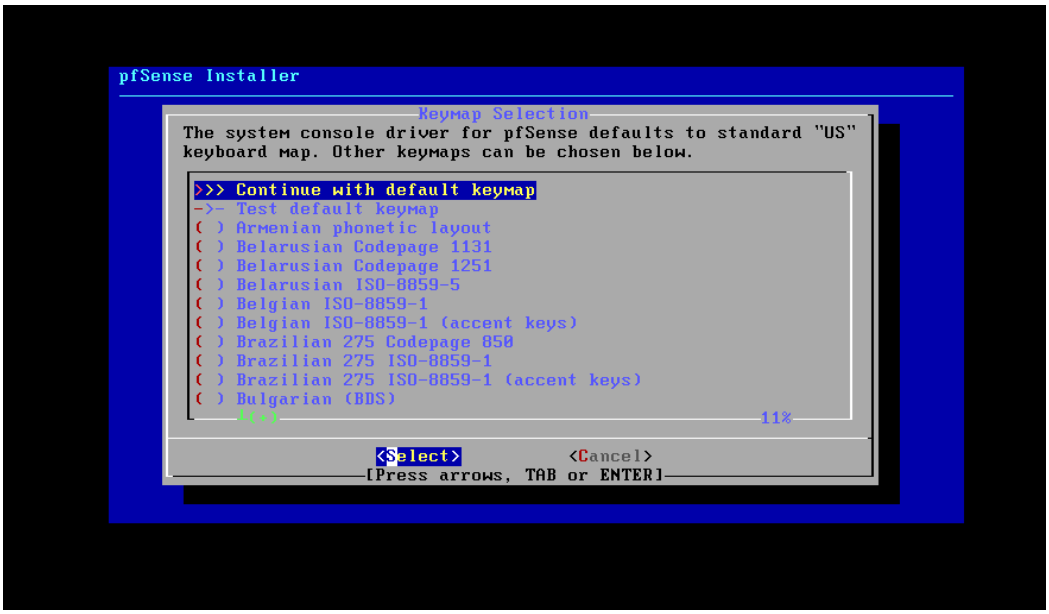
Hình 2-16 Giao diện khởi động

Bấm OK để Install pfSense



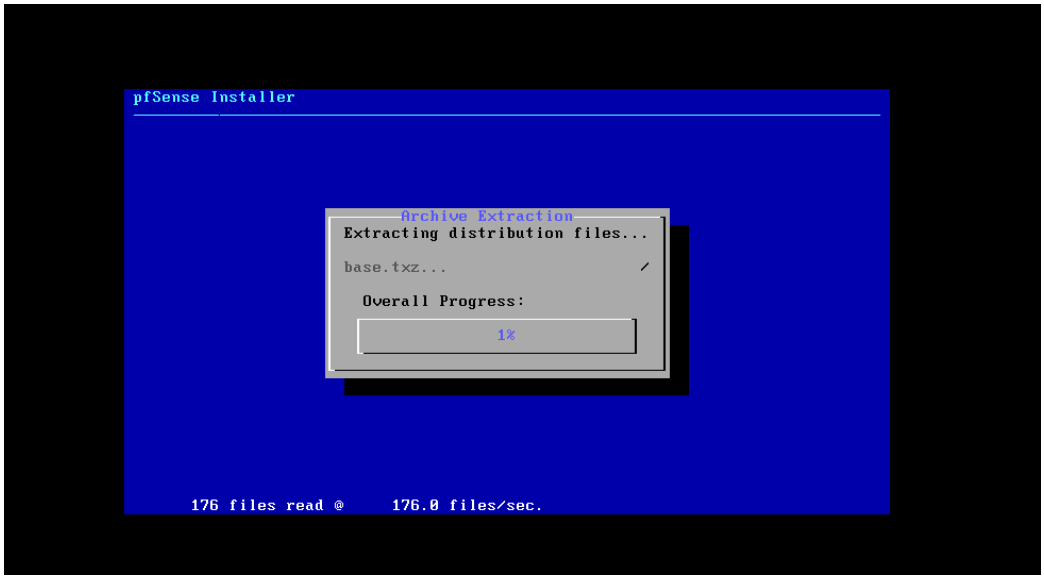
Hình 2-17 Cài đặt PFSENSE

Chọn Select



Hình 2-18 Chọn kiểu bàn phím

Bước tiếp theo bấm OK để pfSense cài đặt

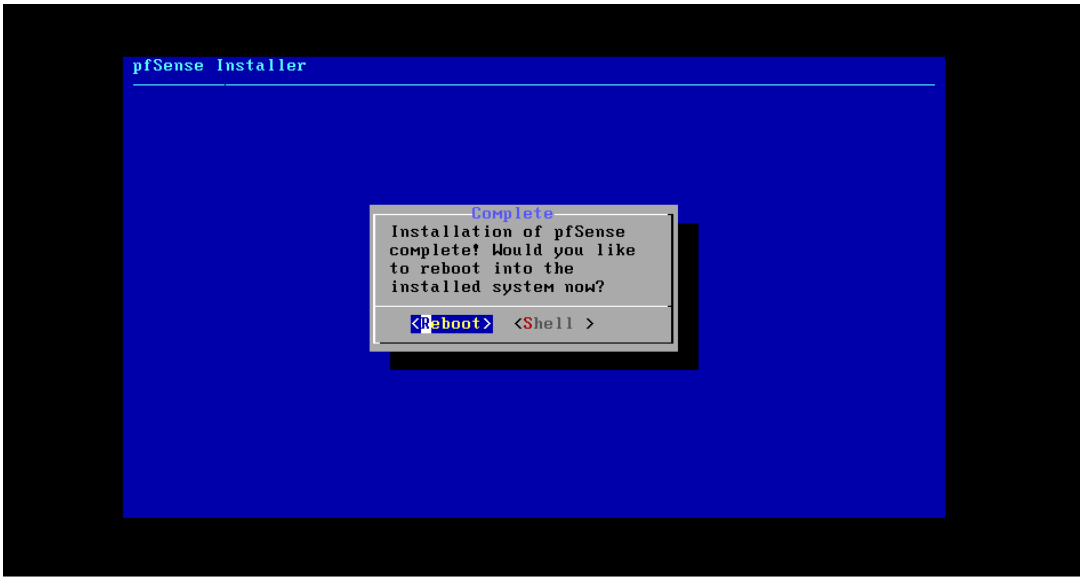


Hình 2-19 Quá trình cài đặt

Chọn No

Hình 2-20 Xác nhận cài đặt

Cuối cùng chọn Reboot



Hình 2-21 Khởi động máy chủ

CHƯƠNG 3: THỰC NGHIỆM FIREWALL TRÊN PFSENSE

3.1 Phát biểu bài toán

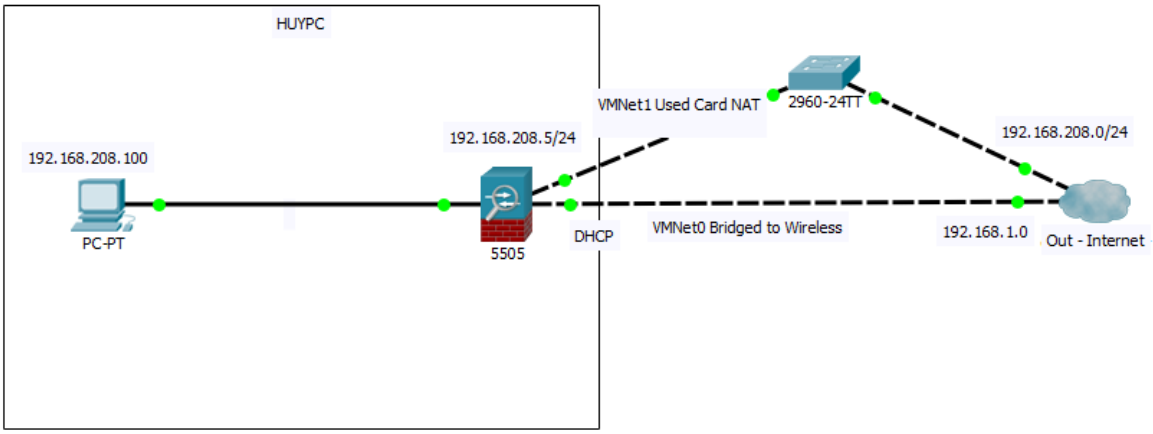
Hiện nay các doanh nghiệp vừa và nhỏ được thành lập rất nhiều để giúp nền kinh tế nước nhà phát. Doanh nghiệp phát triển kéo theo nhu cầu về công nghệ phát triển rất mạnh, kéo theo đó là nhu cầu về an ninh mạng càng được thúc đẩy.

Bài toán đặt ra là doanh nghiệp vừa và nhỏ kinh tế còn rất hạn chế, quản trị không tốt dẫn đến người dùng có thể truy cập tới bất cứ trang web nào, hoặc nhân viên sử dụng mạng nội bộ mạng của công ty xem phim, nghe nhạc, chơi game. Hệ quả để lại có thể dẫn đến năng suất làm việc không hiệu quả.

Giải quyết vấn đề trên đồ án đã sử dụng Squid & SquidGuard trên Pfsense. Với mô hình này giải quyết được tất cả những vấn đề nêu trên và đặc biệt giảm chi phí một cách tối đa cho doanh nghiệp.

3.2 Mô hình thực nghiệm

Mô hình trên được triển khai gồm có một Firewall Pfsense sử dụng card Vmnet0 được kết nối với card vật lí của máy tính đóng vai trò là card WAN và card Vmnet1 đóng vai trò là card LAN. Pfsense được cấu hình dịch vụ Squid Proxy để xử lí lọc, ngăn chặn các website dựa theo danh sách tên miền người quản trị đã thống kế. Một máy tính Win7 đóng vai trò làm client trên Pfsense.



Hình 3-1 Mô hình triển khai

3.3 Cấu hình Pfsense

3.3.1 Phần cứng yêu cầu

CPU Pentium II trở lên

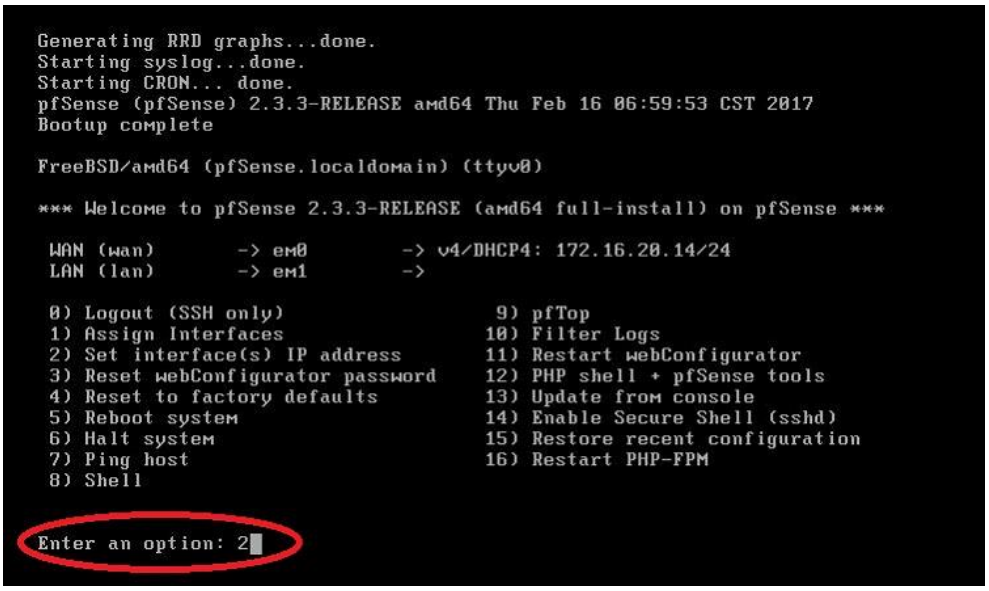
Ram: 256MB

2 Card mạng gồm: Lan và WAN

Lưu ý: Vì Pfsense yêu cầu bắt buộc phải sử dụng 2 Card mạng, một dùng cho Wan và một dùng cho Lan.

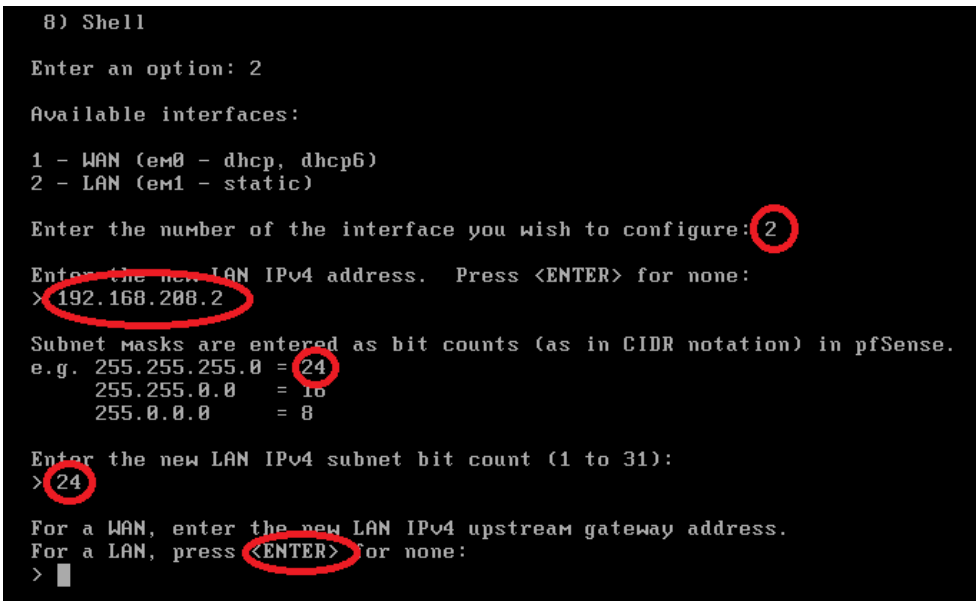
3.3.2 Cấu hình cơ bản Pfsense

Sau khi khởi động lại pfSense. Tại mục menu chọn "**Enter an option: 2**" để thiết lập IP address cho interface LAN



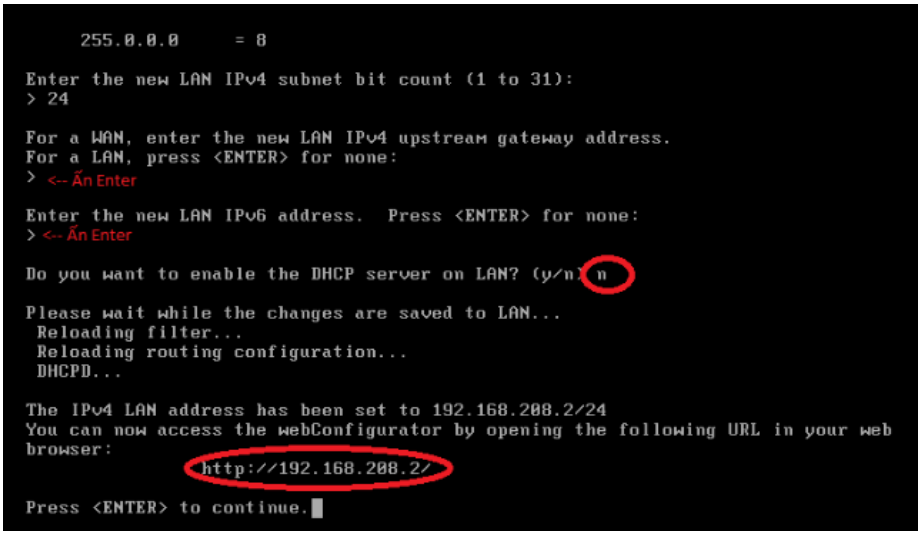
Hình 3-2 Thiết lập IP

Chọn "**2 – LAN interface**" -> thiết lập ip address: **192.168.208.5** -> subnetmask: **24** -> và **Click Enter**



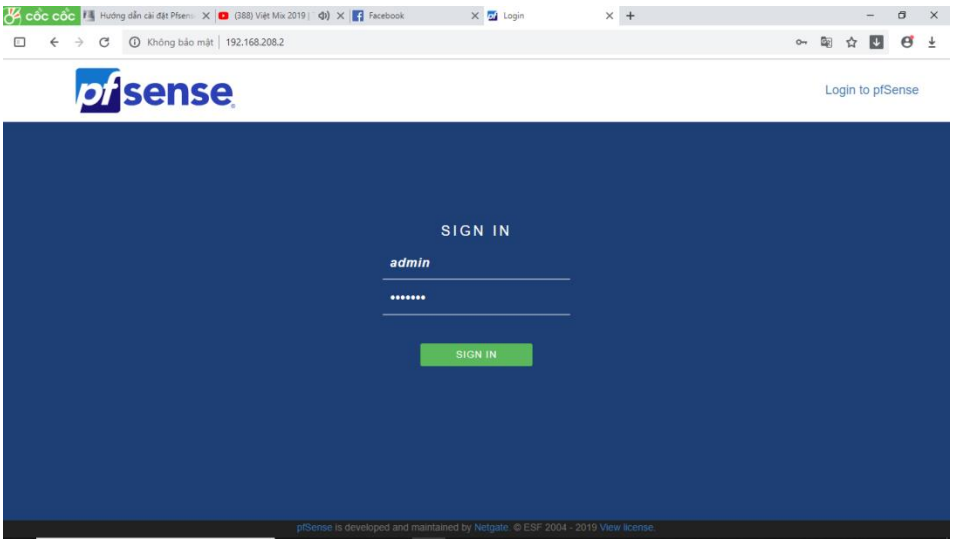
Hình 3-3 Đặt địa chỉ và subnetmask

Phần IPv6 "**Click Enter** " để bỏ qua -> Chọn **"n"** không thiết lập DHCP cho LAN -> Chọn **"y"** (revert to HTTP) -> Sau đó truy cập pfSense tại địa chỉ http://192.168.208.5



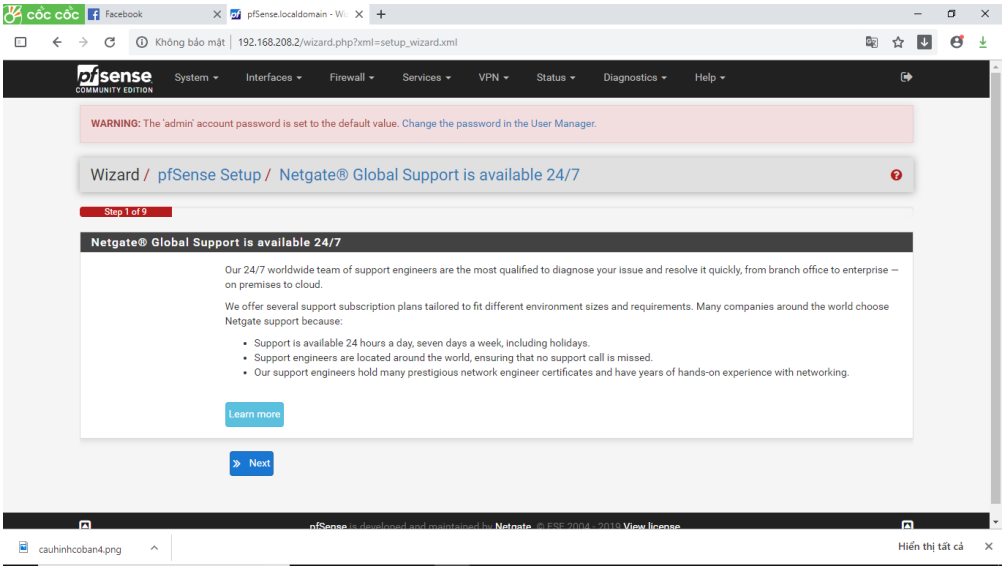
Hình 3-4 Thiết lập DHCP

Truy cập pfSense trên trình duyệt web **http://192.168.208.5**. Đăng nhập với username: **admin** & password: **pfsense**



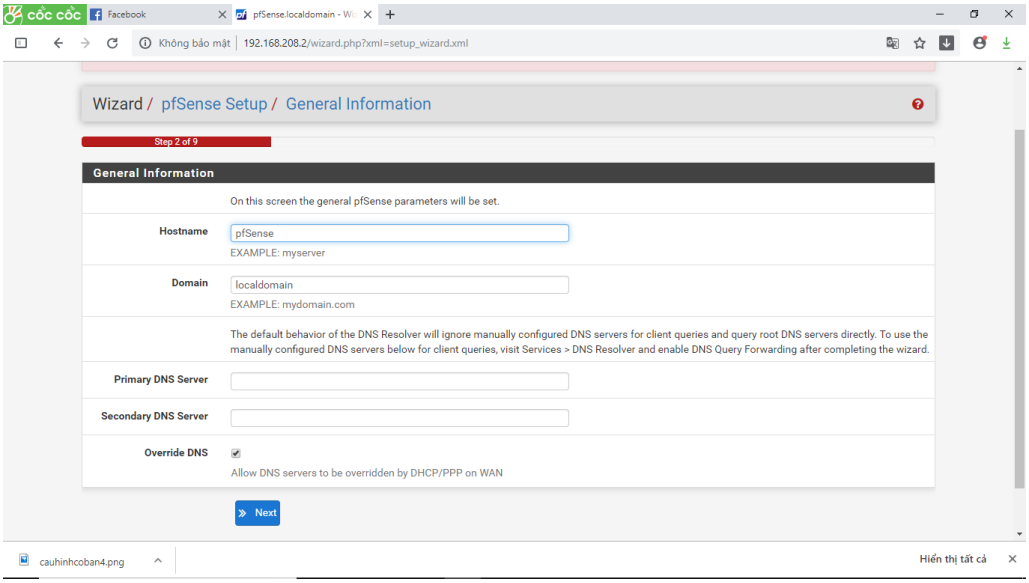
Hình 3-5 Cấu hình trên giao diện Web

Bước 1: Bấm Next



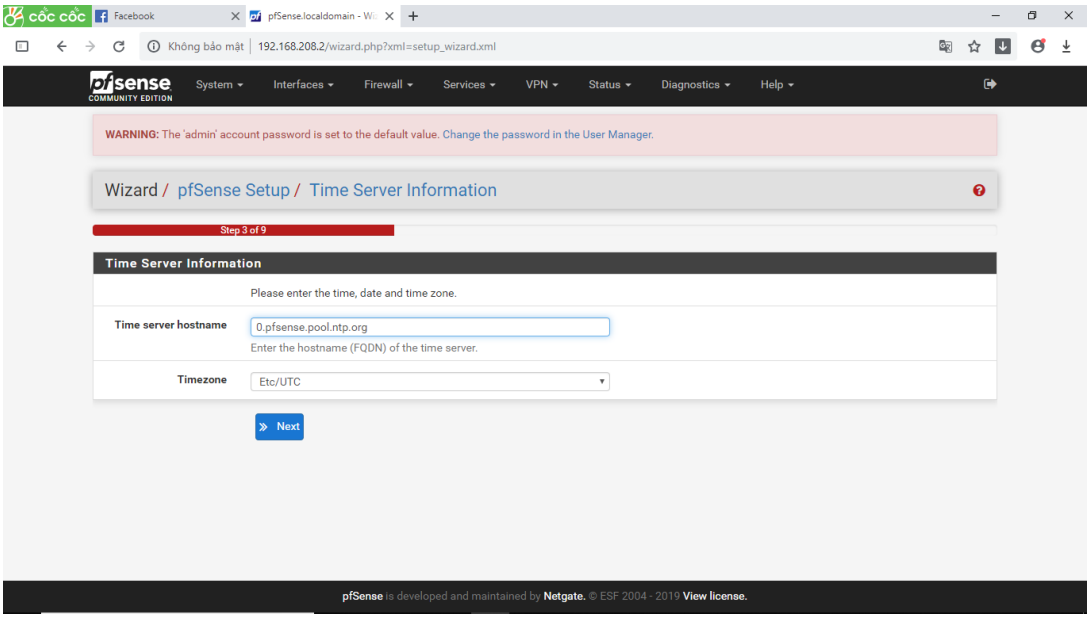
Hình 3-6 Bắt đầu cấu hình trên Web

Bước 2: Khai báo Hostname, domain … rồi bấm Next



Hình 3-7 Khai báo thông số cơ bản

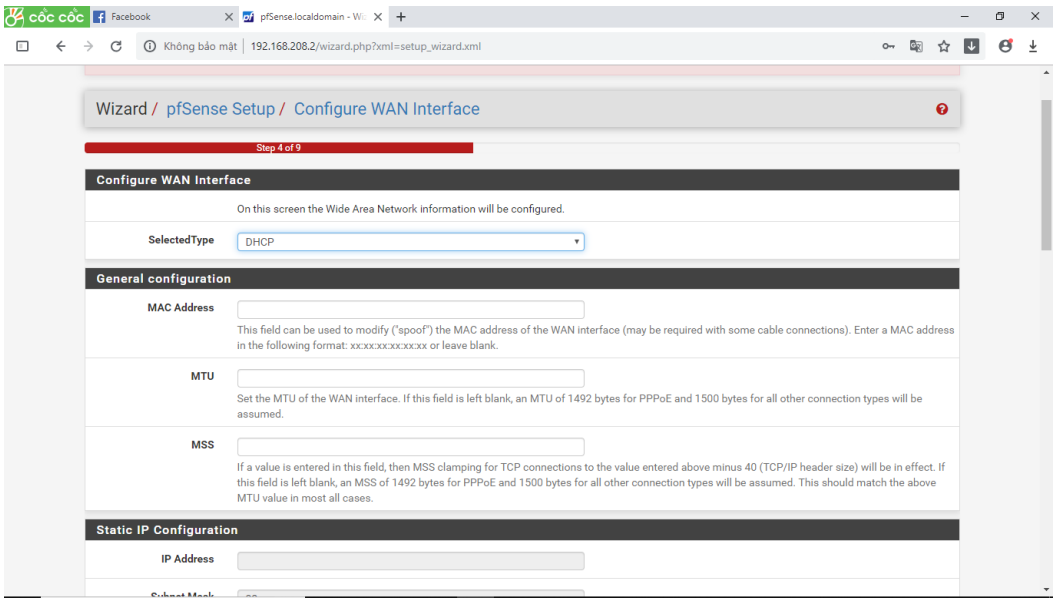
Bước 3: chọn Time Zone GMT+7 bấm Next



Hình 3-8 Cấu hình múi giờ

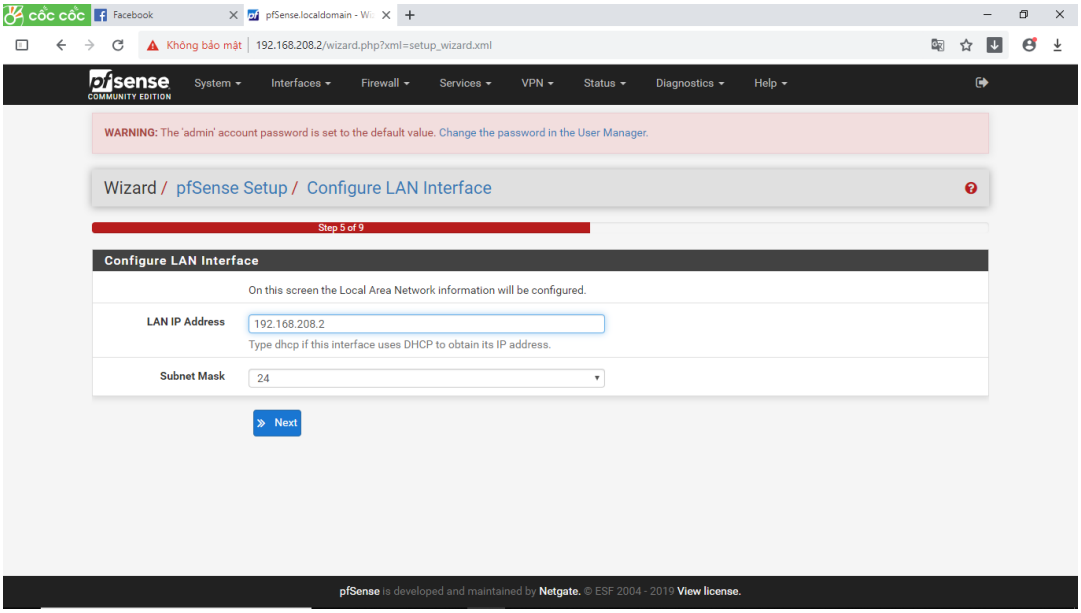
Bước 4: Cấu hình WAN interface:

Tại bước này pfsense cung cấp nhiều phương thức cấu hình mạng WAN khác nhau – static / dhcp / pppoe



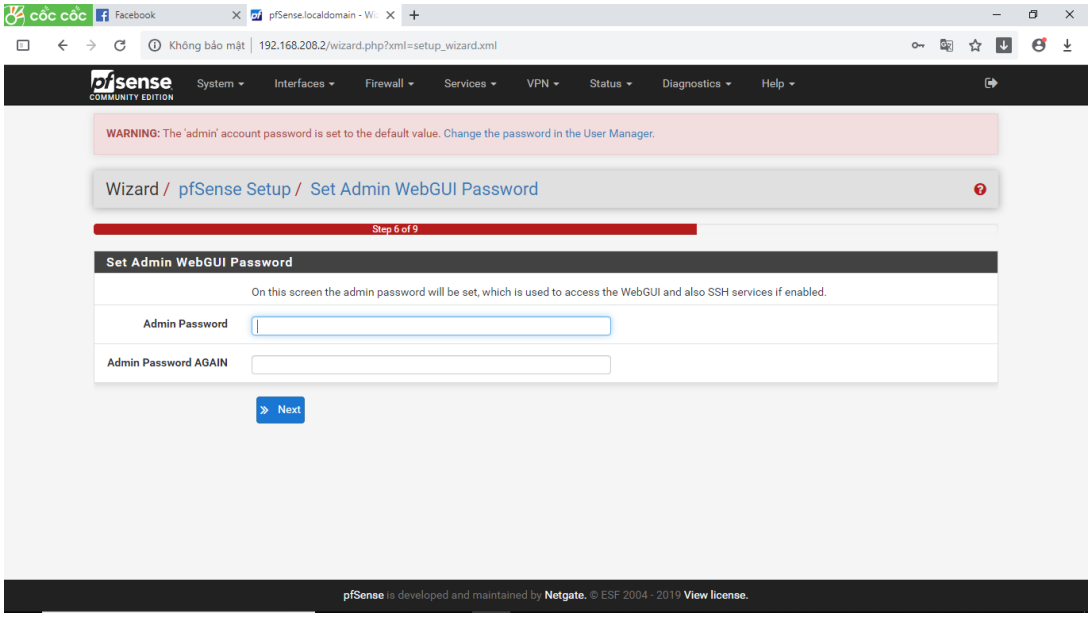
Hình 3-9 Cấu hình card WAN

Bước5: cấu hình cổng LAN – IP là 192.168.208.5



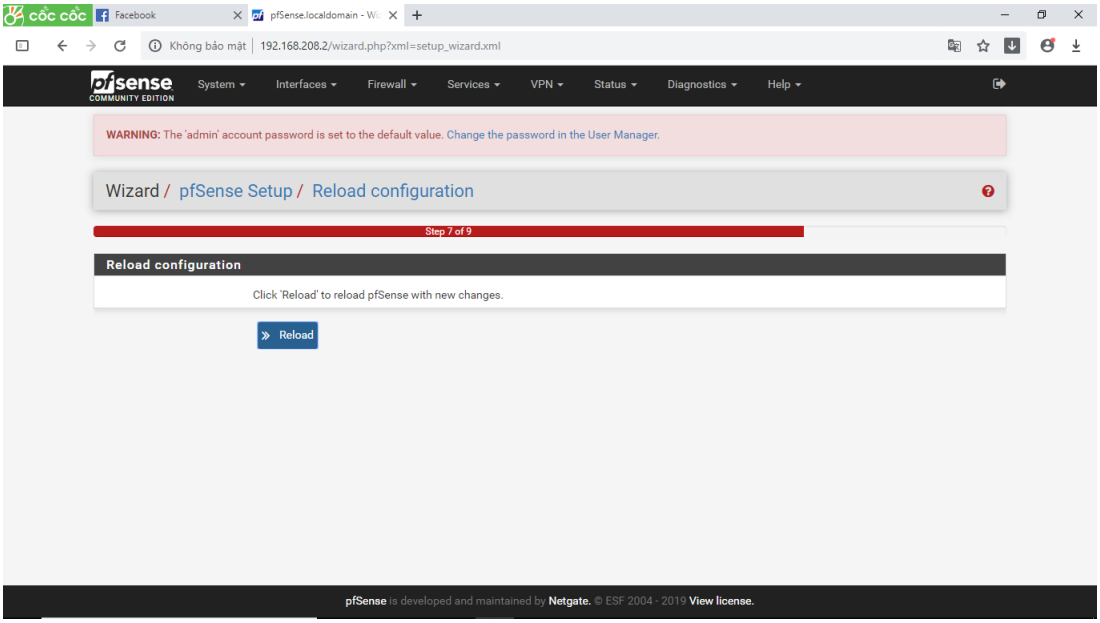
Hình 3-10 Cấu hình Card LAN

Bước 6: Thay đổi mật khẩu tài khoản admin



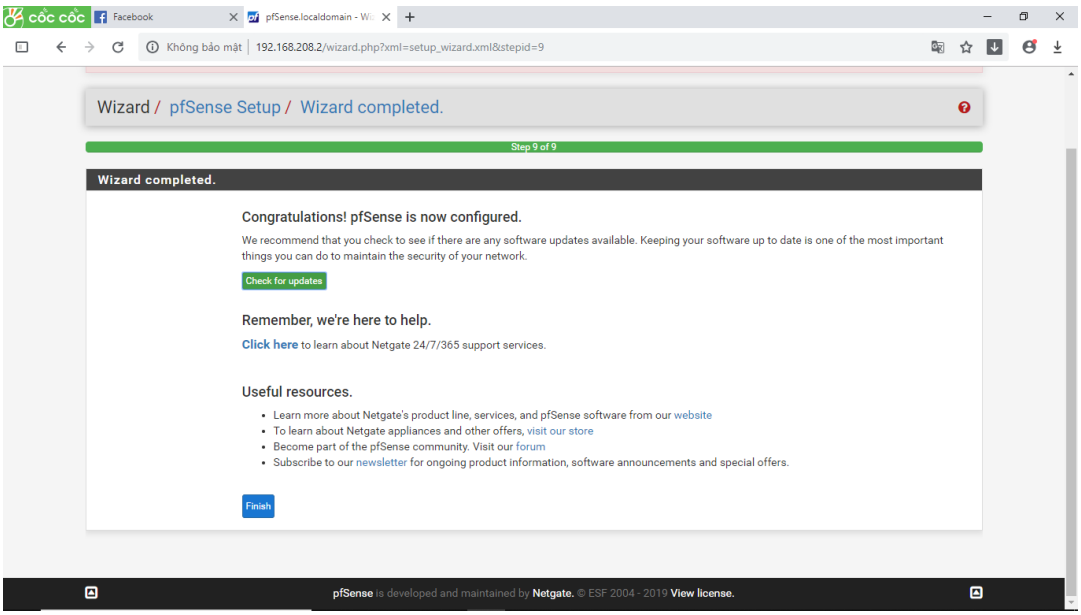
Hình 3-11 Đặt lại mật khẩu

Bước 7 bấm Reload



Hình 3-12 Xác nhận cấu hình

Bước cuối sau khi Reload xong sẽ vào giao diện Dashboard của Pfsense



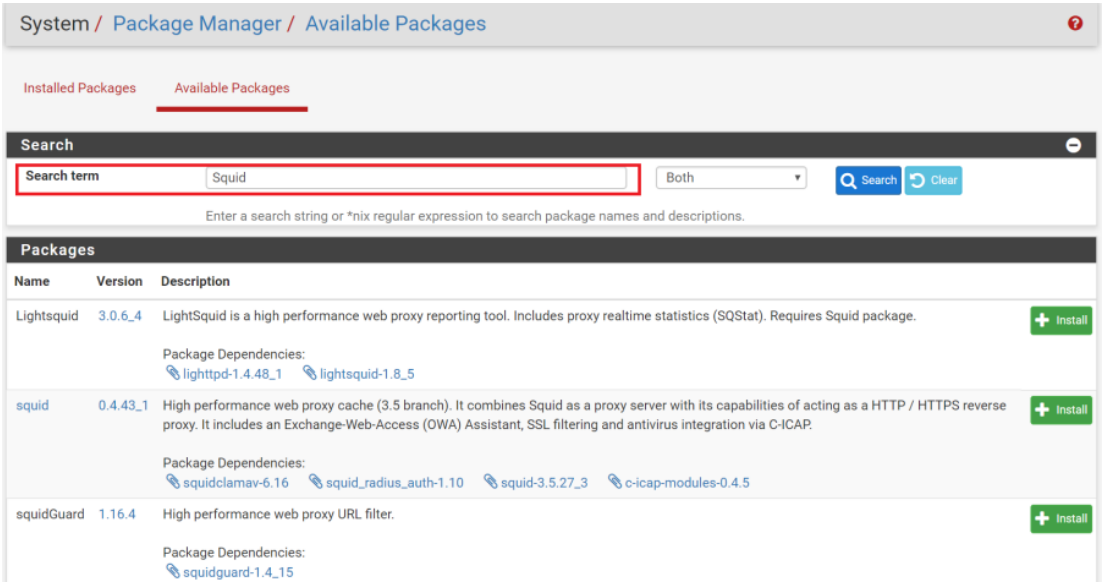
Hình 3-13 Kết quả cấu hình

3.4 Cấu hình Squid và SquidGuard trên Pfsense

Đảm bảo Pfsense kết nối được tới internet

Cài Squid và SquidGuard trên Pfsense

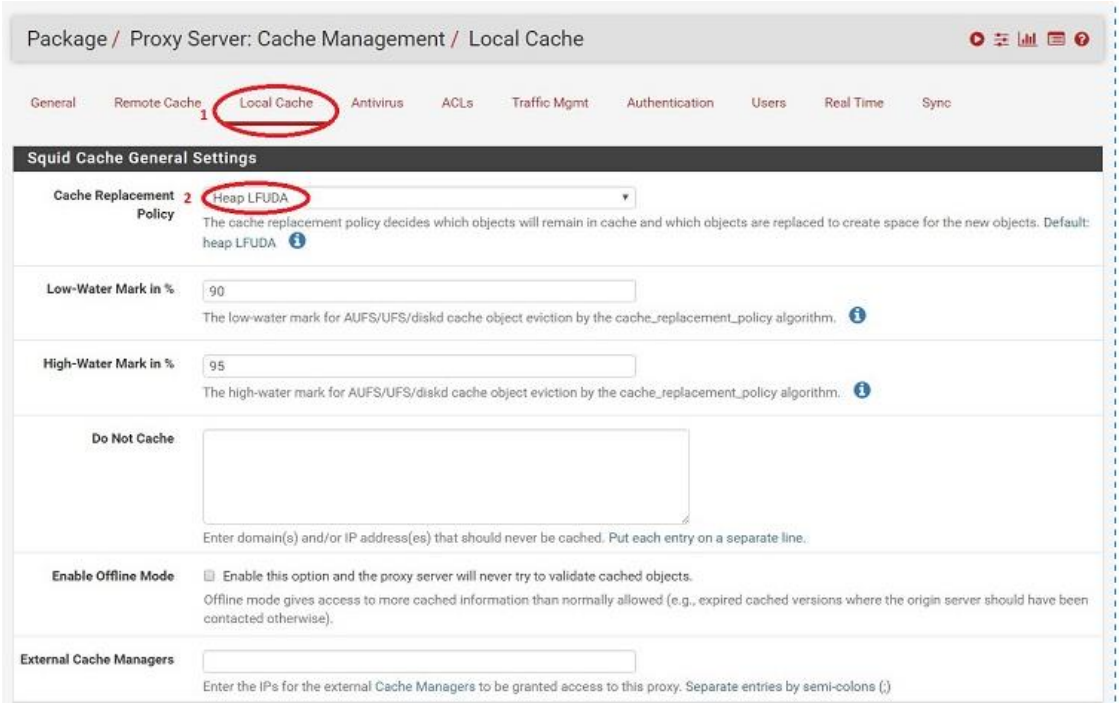
Chọn "**System** > **Package Manager** > chọn Tab **Available Packages**", gõ "squid" vào ô tìm kiếm -> Nhấn "**Install**" để cài đặt "squid & squidGuard"



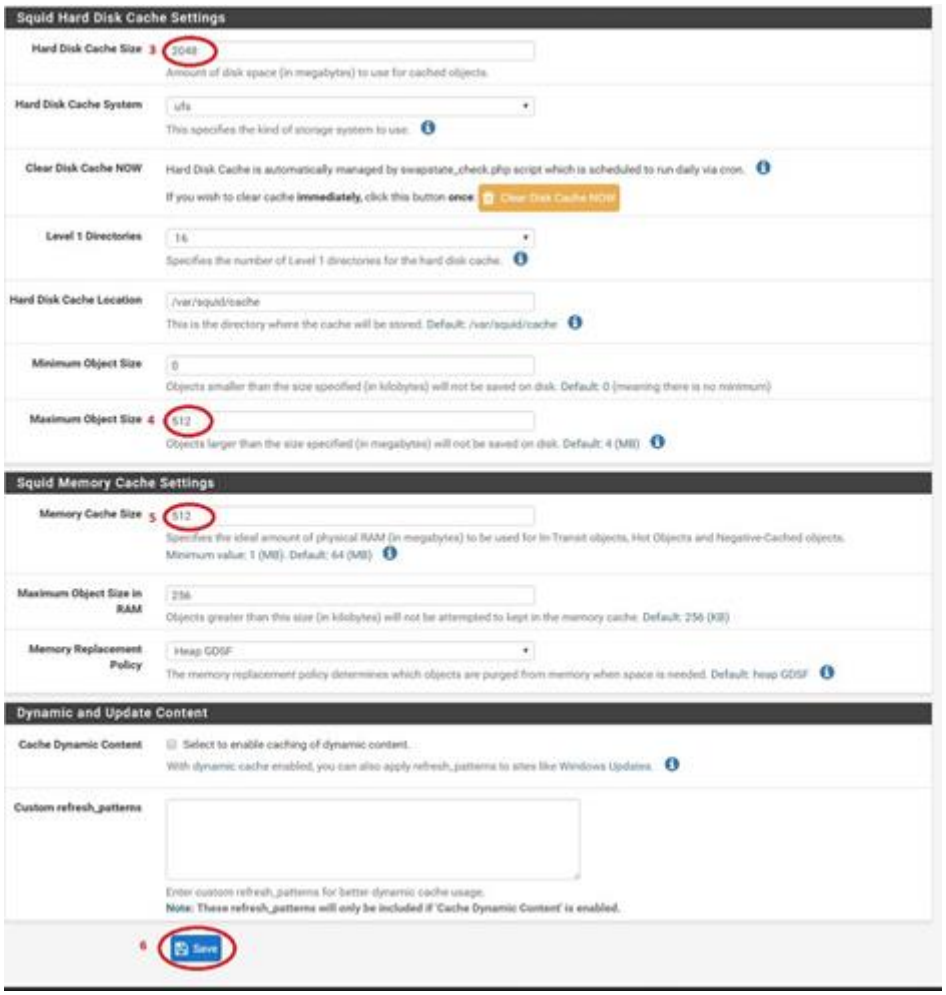
Hình 3-14 Cài đặt Squid và SquidGuard

3.4.1.1 **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

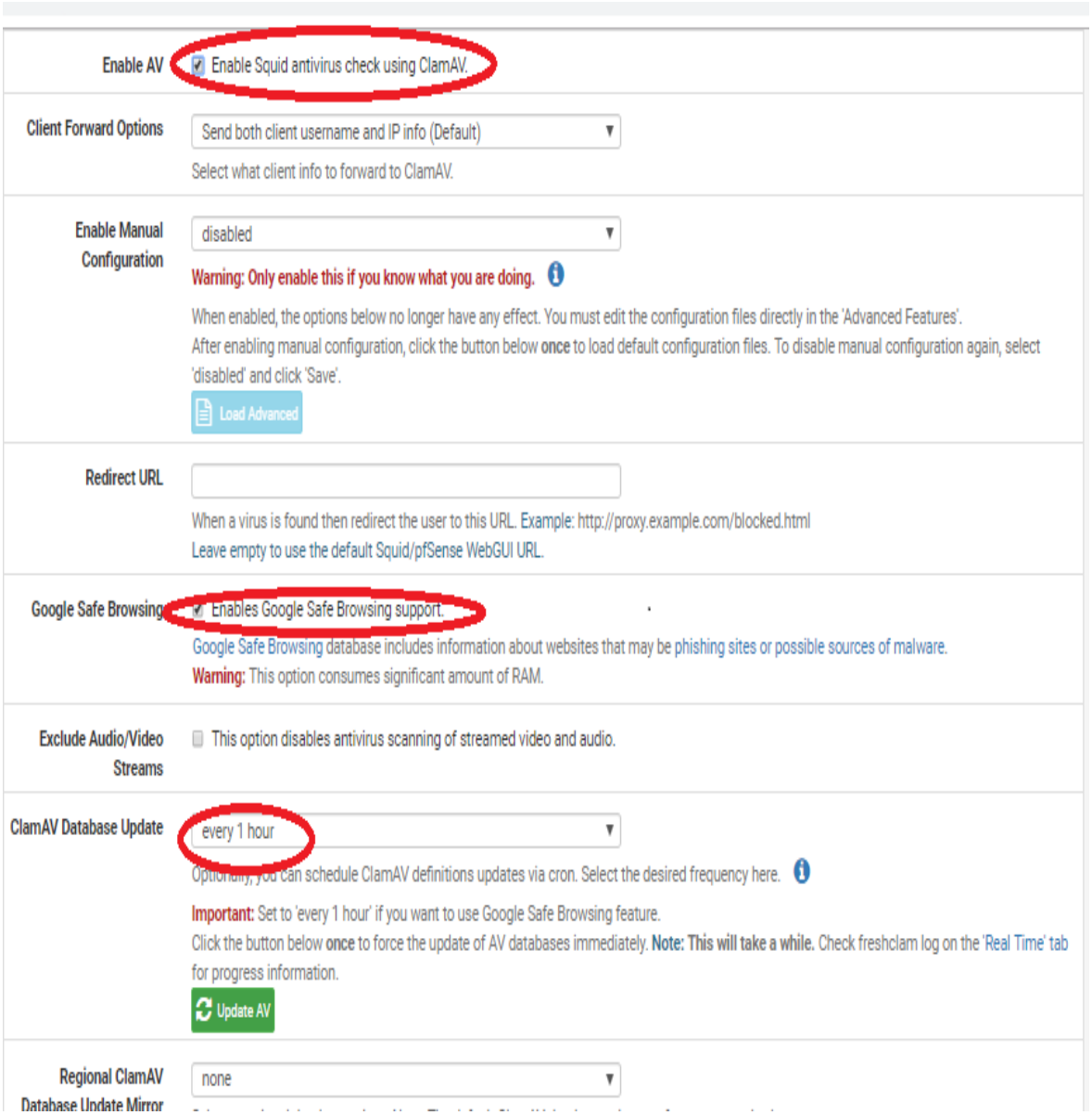


Hình 3-15 Cấu hình Squid Proxy



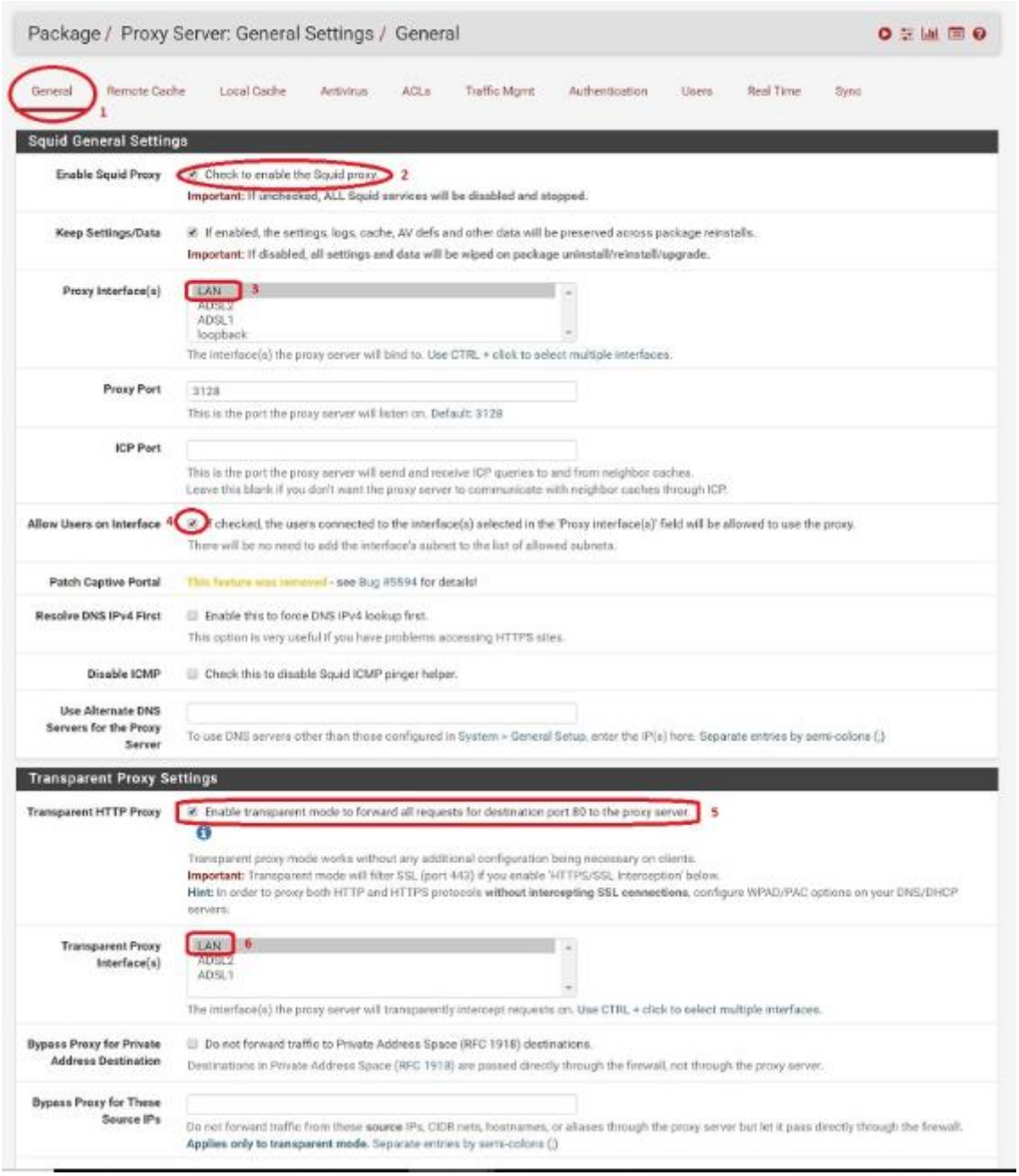
Hình 3-16 Cấu hình Squid Proxy

Tiếp theo 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

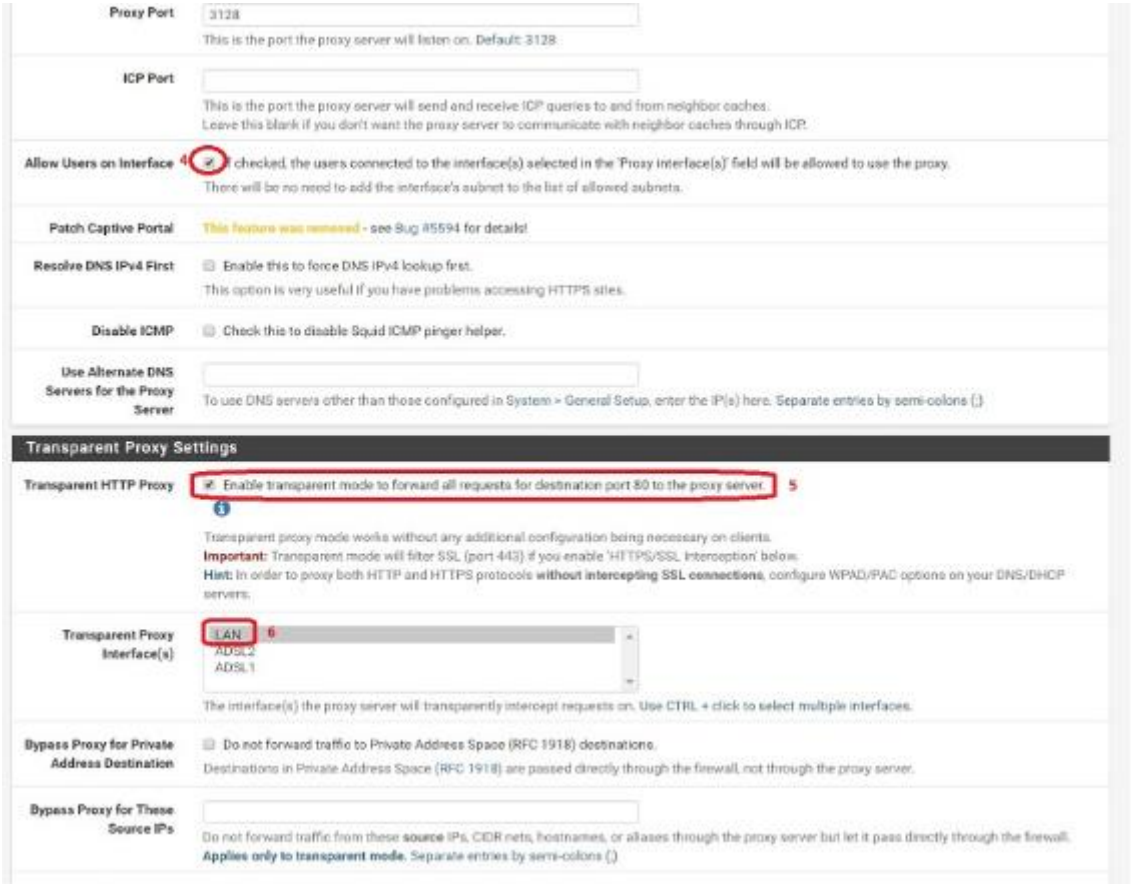


Hình 3-17 Cấu hình diệt virus

Tiếp theo Enable Squid Proxy. Chọn "**Services > Squid Proxy > General** Tab" .Tích vào "**Check to enable the Squid Proxy", Proxy interface(s): LAN**, Tích vào "**Allow Users on Interface**", Tích vào "**Transparent HTTP Proxy**", **Transparent Proxy Interface(s): LAN**, Tích "**Enable Access Logging**", **Log Store Directory: /var/squid/log**s -> Click "**Save**" để lưu cấu hình



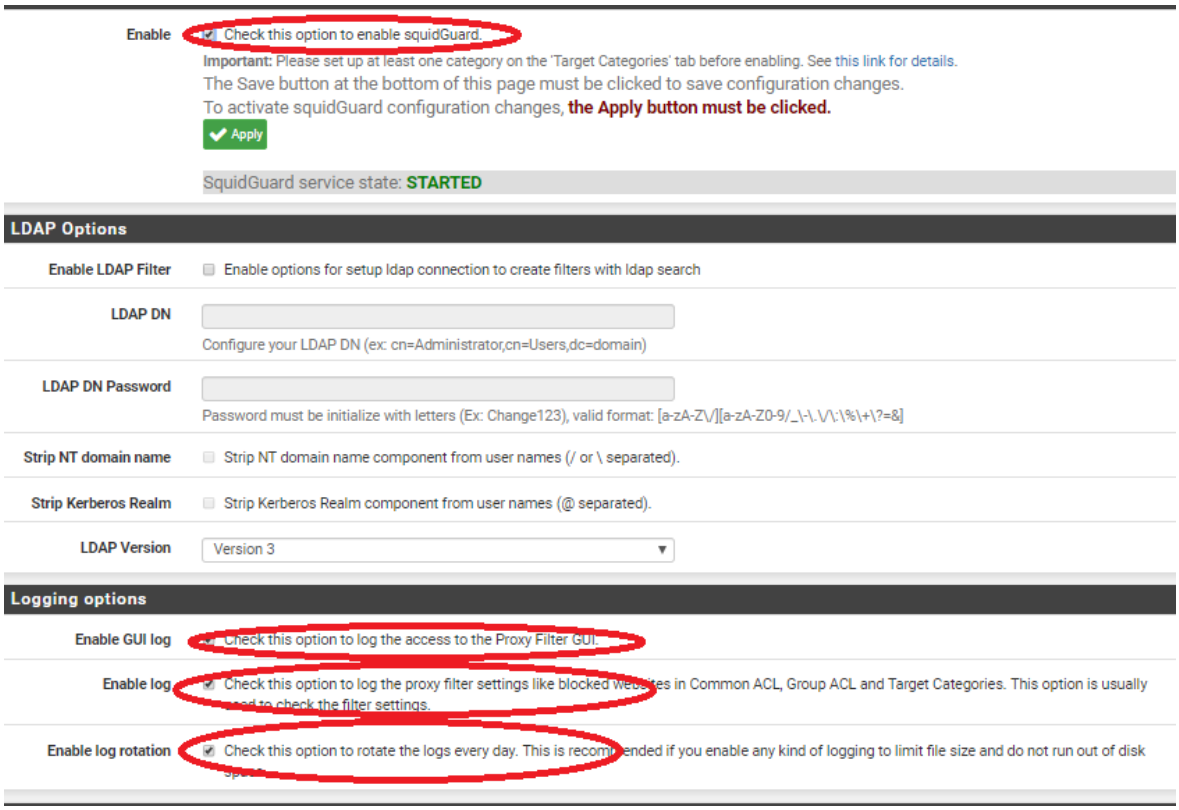
Hình 3-18 Kích hoạt dịch vụ Squid Proxy



Hình 3-19 Kích hoạt quét port 80

3.4.1.2 **Cấu hình SquidGuard**

Truy cấp Services> SquidGuard Proxy Filter> General Setting bật Enable> Apply

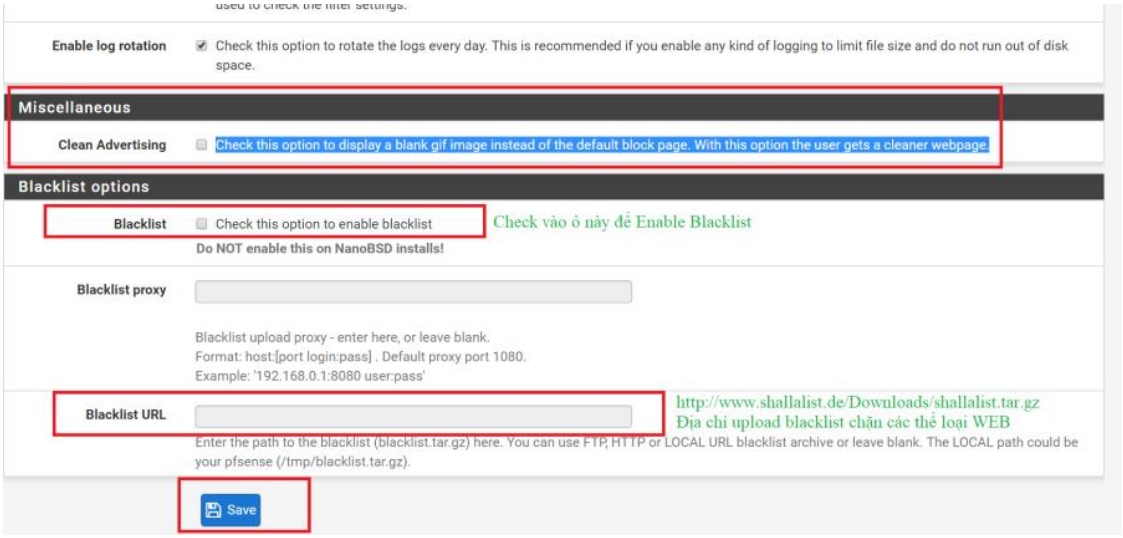


Hình 3-20 Kích hoạt SquidGuard

Enable BlackList và nhập địa chỉ:

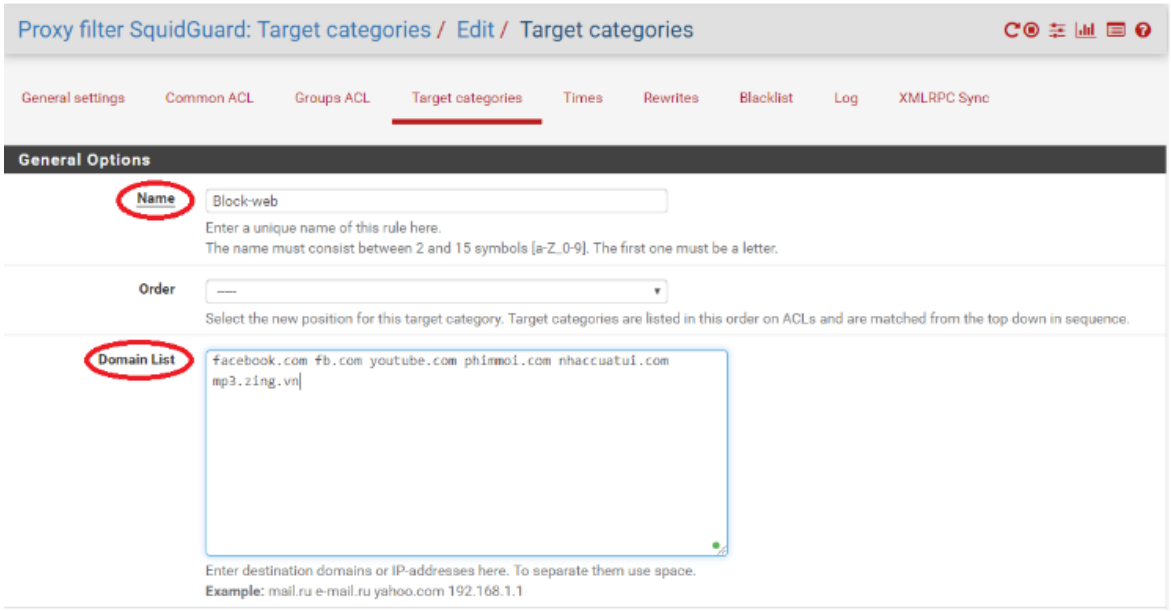
http://www.shallalist.de/Downloads/shallalist.tar.gz

vào ô Blacklist URL. Đây là địa update cái list web khiêu dâm, bạo lực, nhạc, dowload ….

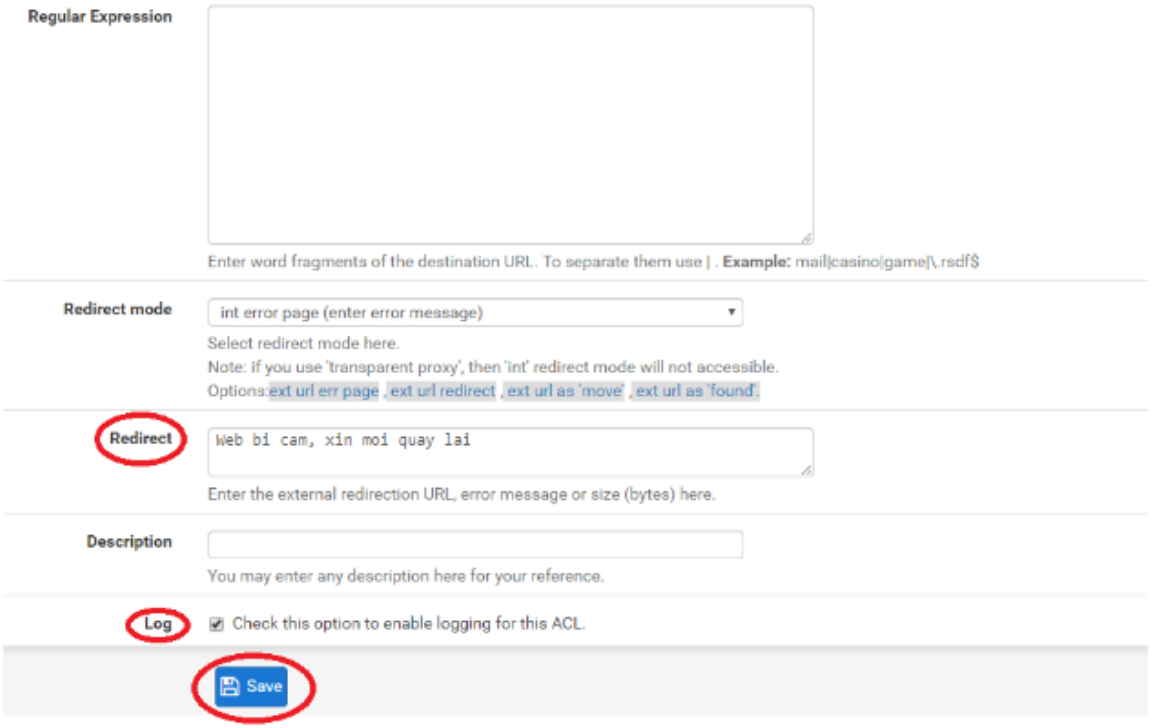


Hình 3-21 Nhập địa chỉ đường dẫn

Tiếp theo **Services -> SquidGuard Proxy Filter -> Target categories->ADD.** Tại đây thêm tên miền muốn chặn



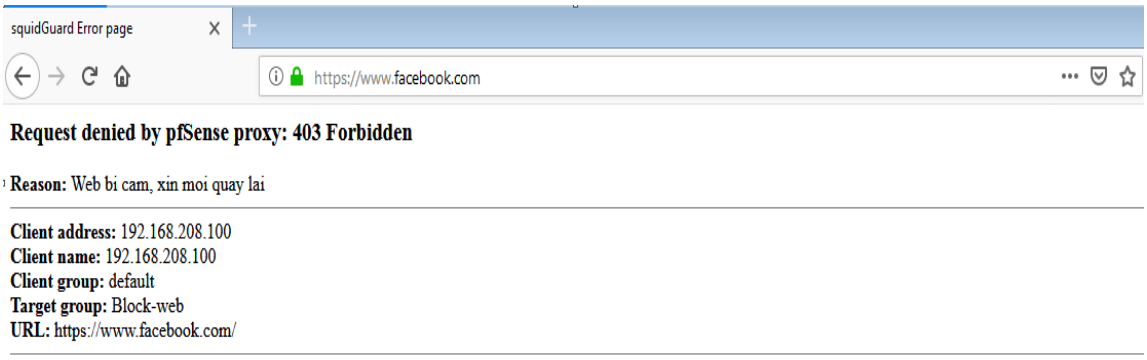
Hình 3-22 Thêm web chặn



Hình 3-23 Kết thúc

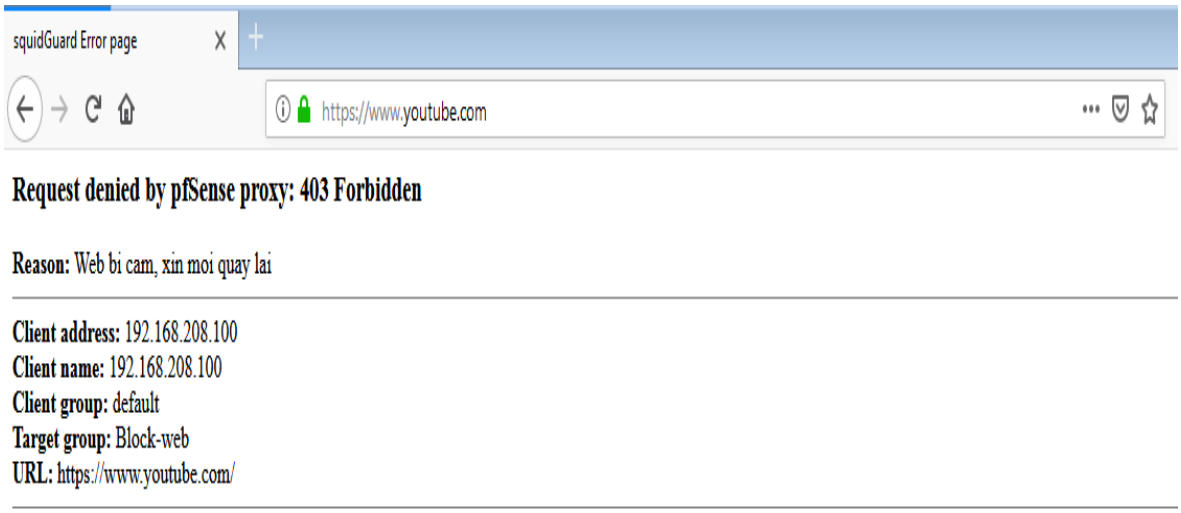
3.4.1.3 **Kết quả bài thực nhiệm**

Facebook đã bị chặn



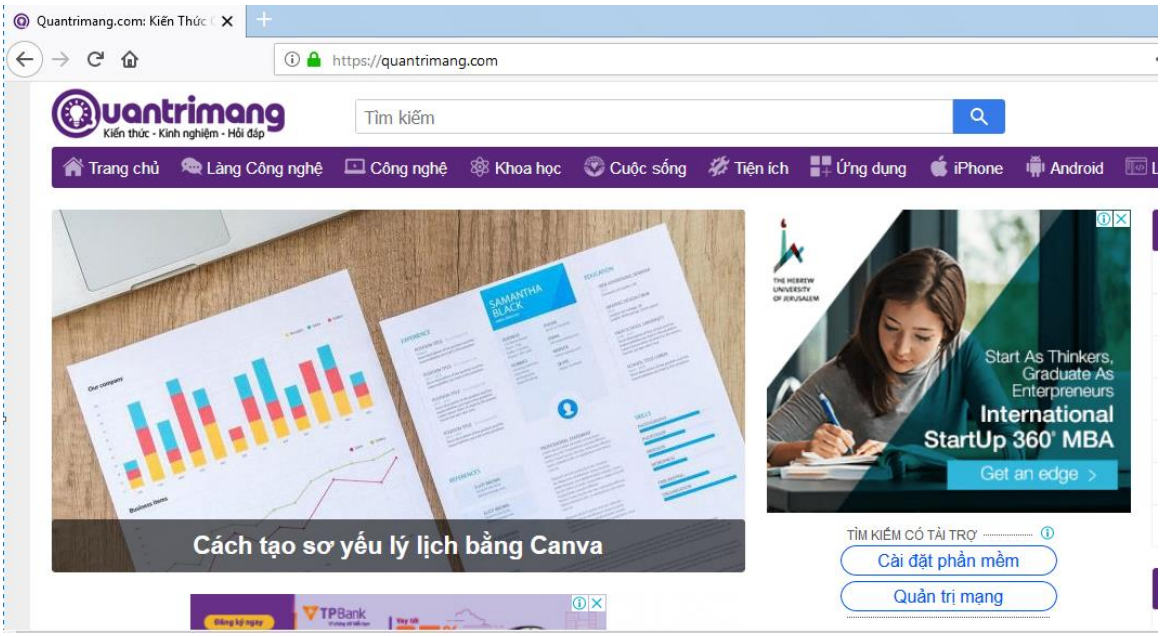
Hình 3-24 Chặn các web phim

Trang xem phim youtube cũng đã bị chặn



Hình 3-25 Chặn các web ca nhạc

Đối với những nhu cầu về tìm kiếm, đọc tài liệu để phục vụ cho công việc vẫn luôn được mở cho nhân viên



Hình 3-26 Trang web cho phép đi qua

KẾT LUẬN

Đồ án "Tìm kiểu giải pháp an ninh mạng với FireWall" 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.
- Trình bày được Firewall là gì, chức năng của Firewall đối với mạng máy tính….
- Nêu lên một số giải pháp về Firewall hiện nay

Về thực thi, đồ án tiến hành:

- Triển khai thực thi điều tiết mục đích sử dụng lưu lượng mạng của doanh nghiệp nhỏ một cách hợp lí

Tuy nhiên trong quá trình thực hiện, do năng lực còn nhiều hạn chế, cùng những nguyên nhân khách quan khác như, cơ sở vật chất, khả năng dịch hiểu tiếng Anh trong quá trình trao đổi trên các diễn đàn công nghệ nên chắc chắn trong đồ án còn nhiều sai sót. Em rất mong nhận được sự đóng góp ý kiến của các Thầy Cô và các bạn để em có thêm kiến thức và kinh nghiệm tiếp tục hoàn thiện nội dung nghiên cứu trong đề tài. Em xin chân thành Cảm ơn!

TÀI LIỆU THAM KHẢO

[1].https://quantrimang.com/

[2].https://lib.hpu.edu.vn/

[3].https://pfsense.org/

[4].https://tailieu.vn/