. báo cáo thực tập tốt nghiệp

Toán cao cấp (Trường Đại học Kinh tế Thành phố Hồ Chí Minh)

BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

THỰC TẬP TỐT NGHIỆP

BÁO CÁO THỰC TẬP TỐT NGHIỆP

TRIỂN KHAI TƯỜNG LỬA PFSENSE CHO K&H

Ngành: An toàn thông tin

Mã số: 7.48.02.02

Sinh viên thực hiện:

Phan Văn Thế

Lớp: AT14E

Đơn vị thực tập:

CÔNG TY TNHH DỊCH VỤ VÀ GIẢI TRÍ K&H

Người quản lý thực tập:

ThS. Hoàng Thanh Nam

Khoa ATTT – Học viện KTMM

Hà Nội - 2021

MỤC LỤC

LỜI MỞ ĐẦU.....4

CHƯƠNG 1: GIỚI THIỆU VỀ CƠ SỞ THỰC TẬP.....5

1. Loại hình doanh nghiệp......5

2. **Khái quát quá trình hình thành và phát triển.**.....5

3. Cơ cấu tổ chức, chức năng của từng bộ phận, cơ cấu nguồn lực......5

3.1. Cơ cấu tổ chức......5

3.2. Chức năng, nhiệm vụ từng bộ phận......6

a. Ban giám đốc của công ty.....6

b. Khối nghiệp vụ.....6

c. Phòng kinh doanh.....6

d. Phòng công nghệ.....7

e. Các lĩnh vực kinh doanh......7

4. Chiến lược, định hướng phát triển trong thời gian tới......8

CHƯƠNG 2: PHÂN TÍCH CÁC NGUY CƠ MẤT AN TOÀN THÔNG TIN VÀ ĐỀ XUẤT GIẢI PHÁP KHẮC PHỤC.....9

1. Khảo sát hiện trạng hạ tầng công nghệ thông tin và an toàn thông tin......9

2. Phân tích làm rõ các nguy cơ mất an toàn thông tin đối với hạ tầng công nghệ thông tin hiện có......10

3. Phân tích, đánh giá các giải pháp an toàn thông tin hiện có......11

4. Đề xuất các giải pháp nhằm khắc phục hạn chế, giúp nâng cao mức độ an toàn......11

5. Thử nghiệm triển khai tường lửa PfSense.....12

5.1.Triển khai.....12

5.2. Cài đặt tường lửa PfSense.....12

5.3. Cấu hình tường lửa cơ bản.....13

5.4. Quản trị tường lửa bằng đồ họa.....16

5.5. Tạo tập luật theo Thử nghiệm.....18

Kết luận......23

LỜI MỞ ĐẦU

Thực tập là một nội dung quan trọng trong chương trình đào tạo của nhà trường. Quá trình thực tập tốt nghiệp đã giúp em:

- Được rèn luyện kỹ năng
- Củng cố, nâng cao trau dồi kiến kiến thức đã được học tại nhà trường , vận dụng kiến thức vào thực tiễn tại cơ sở thực tập.
- Quá trình học tập tại trường em chỉ mới nắm được phần lý thuyết và chưa có kinh nghiệm thực tế, vì vậy, quá trình thực tập khi tiếp cận với thực tiễn em cần phải chủ động tư duy giữa lý thuyết và thực tế. Trên cơ sở đó nâng cao kiến thức và vận dụng kiến thức đã học vào giải quyết những vấn đề thực tiễn đặt ra.

- Thông qua đợt thực tập này, em có điều kiện tiếp xúc với cán bộ, công nhân viên, với lãnh đạo của đơn vị thực tập để học hỏi kinh nghiệm về mọi mặt,nâng cao được khả năng làm việc nhóm, khả năng giao tiếp xã hội . Trên cơ sở đó xác định cho mình một quan điểm về nghề nghiệp, xây dựng, bổ sung vun đắp cho mình lòng yêu nghề .

CHƯƠNG 1: GIỚI THIỆU VỀ CƠ SỞ THỰC TẬP

1. Loại hình doanh nghiệp.

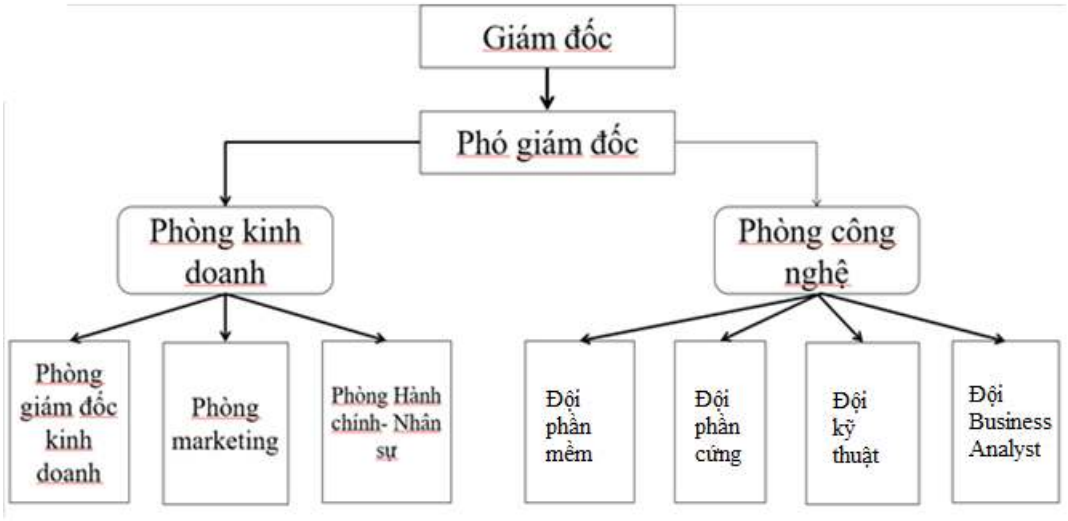
CÔNG TY TNHH DỊCH VỤ VÀ GIẢI TRÍ K&H là công ti cung cấp các dịch vụ giải trí , các phần mềm , thiết bị điện tử , hệ thống máy chơi game thông minh cho các khu vui chơi công nghệ cao , các trung tâm thương mại và cách khu vui chơi giải trí , với toàn thể nhân viên công ty luôn nỗ lực không ngừng phấn đấu để mang đến khách hàng những sản phẩm chuyên nghiệp, hiện đại, phù hợp yêu cầu của khách hàng.

2. Khái quát quá trình hình thành và phát triển.

Công ty được thành lập vào ngày 05 tháng 8 năm 2020 bởi anh Nguyễn Văn Kiên . Công ty có địa chỉ: Thôn Mai Nội - Xã Mai Đình - Huyện Sóc Sơn - Thành phố Hà Nội. Văn phòng giao dịch: Khu giao thương 365, đường Tô Hiệu, P Hà Cầu, Quận Hà Đông, Hà Nội. Công ty có các chi nhánh tại Đà Nẵng, Hải Phòng và Bình Dương

3. Cơ cấu tổ chức, chức năng của từng bộ phận, cơ cấu nguồn lực.

3.1. Cơ cấu tổ chức.



1. Cơ cấu tổ chức công ty

- Được thành lập vào năm 2015 , công ty K&H đã có một bộ máy điều hành gồm hơn 40 thành viên làm việc trong các phòng ban khác nhau, bao gồm phòng kinh doanh và phòng công nghệ

3.2. Chức năng, nhiệm vụ từng bộ phận.

a. Ban giám đốc của công ty

- Giám đốc điều hành, là người phụ trách công tác quản lý và chỉ đạo hành chính của tổ chức. Giám đốc điều hành là người đứng đầu chuỗi. CEO cũng là người sáng lập và định hướng mục đích, tầm nhìn và sứ mệnh của công ty. Chịu trách nhiệm kết nối doanh nghiệp với thị trường, có tiếng nói cuối cùng trong việc lập ngân sách, quyết định đầu tư và chỉ đạo các chiến lược của công ty để công ty đạt được mục tiêu, cung cấp hướng dẫn và nguồn lực cho nhóm, đồng thời tháo gỡ các trở ngại.

- Phó giám đốc còn là người chịu trách nhiệm chính và hoạt động của doanh nghiệp. Phó giám đốc là cánh tay phải của ban giám đốc, giúp ban giám đốc có thể quan sát, nắm rõ tình hình thực tế của công ty qua từng ngày.

b. Khối nghiệp vụ

- Thực hiện công tác cán bộ, Đảng, Đoàn viên, quản lý xuất nhập cảnh, xây dựng kế hoạch lao động. Tiền lương, chính sách người lao động, đào tạo đánh giá sắp xếp nhân sự sẽ do bộ phận tài chính – nhân sự thực hiện.

- Bộ phận tài chính – nhân sự có trách nhiệm thực hiện công tác văn thư bảo mật, quản lý thiết bị văn phòng, thực hiện các hoạt động đối ngoại.

- Thực hiện công tác xây dựng kế hoạch, đánh giá tình hình thực hiện kế hoạch của các đơn vị, quản lý tiến trình dự án đầu tư.

- Đảm bảo các hoạt động của công ty tuân thủ đúng pháp luật, là đầu mối liên hệ giữa các cổ đông.

- Bộ phân nhân sự, hành chính nhân sự thực hiện công tác tìm hiểu thị trường mới, triển khai các hoạt động tại các thị trường.

c. Phòng kinh doanh

- Phòng kinh doanh có trách nhiệm tiếp nhận và xử lý các đơn hàng, các dự án của công ty.

- Tổng hợp phân tích đánh giá tình hình kinh doanh của công ty và các thị trường trong/ngoài nước đưa ra.

- Truyền thông nội bộ, bên ngoài. Xây dựng thương hiệu tổ chức các sự kiện của công ty để giới thiệu sản phẩm, đưa ra chiến lược quảng bá công ty đến thị trường trong và ngoài nước.

d. Phòng công nghệ

- Phòng công nghệ gồm các đội chịu trách nhiệm chính trong thiết kế , phát triển các hệ thống phần mềm, phần cứng, triển khai và lắp đặt .

- Đứng đầu là giám đốc công nghệ, chịu trách nhiệm chính về các sản phẩm công nghệ của công ty. Là người phân chia các công việc phù hợp với từng người.

- Đội Phần mềm là đội chịu trách nhiệm tạo ,phát triển và quản lý, kiểm thử và đảm bảo chất lượng đầu ra của các sản phẩm phần mềm.

- Đội Phần cứng chịu trách nhiệm quản lý , phát triển, và đảm bảo hoạt động chất lượng liên quan đến các thiết bị giải trí, điện tử , máy game , VR

- Đội Kỹ Thuật bao gồm một số thành viên vủa đội phần cứng và phần mềm cũng với đội ngũ kỹ thuật có trách nhiệm triển khai, lắp đặp các hệ thống phần mềm cùng với các hệ thống thiết thiết bị và bảo trì khắc phục sự cố sau khi triển khai.

- Đội Business Analys có nhiệm vụ đi gặp khách hàng, đối tác và các bên liên quan đến dự án của công ty để có thể nắm được yêu cầu của khách hàng về chuyển giao thông tin về cho công ty.

e. Các lĩnh vực kinh doanh.

K&H cung cấp các dịch vụ sau:

- Tư vấn , Thiết kế và Triển khai mô hình khu giải trí

- Cung cấp phần mềm game
- Cung cấp các thiết bị vui chơi giải trí
- Cung cấp hệ thống máy điện tử , hệ thống game công nghệ cao
- Triển khai , lắp đặt hệ thống VR

4. Chiến lược, định hướng phát triển trong thời gian tới.

- Đa dạng hóa sản phẩm.
- Phát triển thêm các công nghê
- Mở rộng quy mô thị trường
- Kêu gọi đầu tư vốn từ các nguồn quỹ mở.
- Áp dụng AI vào quản trị hệ thống.

CHƯƠNG 2: PHÂN TÍCH CÁC NGUY CƠ MẤT AN TOÀN THÔNG TIN VÀ ĐỀ XUẤT GIẢI PHÁP KHẮC PHỤC

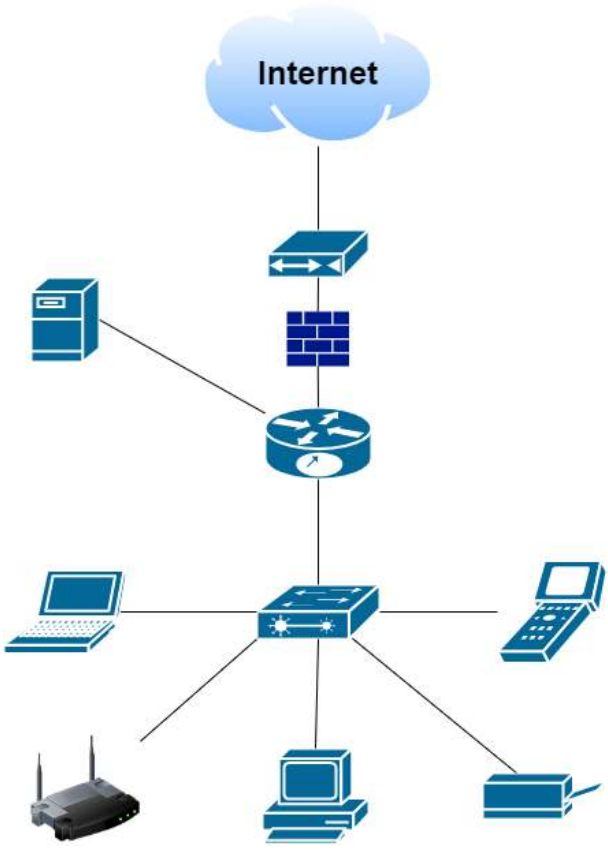
1. Khảo sát hiện trạng hạ tầng công nghệ thông tin và an toàn thông tin.

- An toàn thông tin đóng vai trò quan trọng trong việc bảo vệ dữ liệu của người dùng trong hệ thống công ty TNHH Dịch vụ và Giải trí K&H

- Nhìn chung, hệ thống mạng của công ty được thiết kế khá đơn giản nhưng vẫn đáp ứng đủ nhu cầu của người dùng trong hệ thống công ty.

- Các máy trạm, máy tính cá nhân đều được cài đặt những phần mềm diệt virus.

- Vì nguồn lực cho việc phát triển, nghiên cứu an toàn thông tin còn hạn hẹp, nên trang thiết bị phần cứng còn hạn chế, phần mềm bảo mật mới dừng ở các sản phẩm phổ thông.



Mô hình mạng hệ thống công ty K&H

2. **Phân tích làm rõ các nguy cơ mất an toàn thông tin đối với hạ tầng công nghệ thông tin hiện có.**

- Tuy hệ thống của công ty hoạt động khá ổn định nhưng cũng không thể tránh khỏi những rủi ro từ bên ngoài.

- Việc dùng một con server để cho nhiều mục đích khác nhau như chia sẻ tài nguyên,quản lý người dùng… ta thấy được nguy cơ tiềm ẩn mất an toàn là khá cao nếu hacker chiếm quyền điều khiển của toàn bộ hệ thống.

- Đi tiếp vào trong hệ thống mạng từng phòng ban, ta thấy các phòng ban vẫn đang sử dụng chung một hệ thống mạng mà chưa chia thành các VLAN cụ thể, điều này dẫn tới việc các phòng ban có thể vô tình làm lộ dữ liệu nhạy cảm bên trong công ty.

- Những chính sách an toàn trong K&H còn khá "lỏng lẻo" ví dụ như đặt password cho máy tính cá nhân, hoặc đặt password đơn giản, tắt máy trước khi về,download những file không có bản quyền, file không có nguồn gốc… Tuy đây là những việc làm nhỏ và mất ít thời gian, nhưng lại rất cần thiết đối với việc an toàn trong một hệ thống.

- Vẫn chưa thường xuyên kiểm thử, kiểm tra định kì hệ thống mạng trong công ty như rà soát log firewall, rà soat log server,… Điều này có thể dẫn tới nguy cơ tiềm ẩn trong hệ thống mạng công ty.

- Những phần mềm như quét lỗ hổng, quét mạng không dây, nhận dạng cổng và dịch vụ mạng còn thiếu sót nhiều.

- Nhiều nhân viên trong công ty tắt cập nhật cho những phiên bản hệ điều hành mới. Điều này tuy sẽ không gây mất thời gian cho nhân viên, nhưng lại là 1 nguy cơ cao gây mất an toàn thông tin. Đó là việc những phần mềm Antivirus, anti malware sẽ không được cập nhật thường xuyên dẫn tới việc sẽ khó có thể phát hiện được những trình, những tệp tin độc hại.

- Dữ liệu trên máy chủ, máy tính cá nhân của K&H hiện chưa an toàn vì không được mã hóa nội dung kể cả khi đi trên đường truyền.

3. **Phân tích, đánh giá các giải pháp an toàn thông tin hiện có.**
    - Triển khai them lớp bảo mật Firewall
    - Triển khai hệ thống VPN
    - Xây dựng chính sách an toàn thông tin toàn diện cho công ty
    - Hiện nay, công ty đã và đang tuyên truyền về an toàn thông tin cũng như tầm quan trọng của nó đối với dữ liệu bảo mật của công ty nhằm nâng cao ý thức của mỗi thành viên trong công ty.
    - Bổ sung thêm những chính sách an toàn thông tin như đặt mật khẩu phức tạp hoặc thường xuyên trong việc rà soát các file nhật ký trong hệ thống.
4. **Đề xuất các giải pháp nhằm khắc phục hạn chế, giúp nâng cao mức độ an toàn.**

- Trong hệ thống mạng trong công ty, có thể coi là còn khá đơn giản nhưng cũng còn phải phụ thuộc vào nhu cầu, ngân sách cũng như nguồn lực phía công ty. Việc đưa ra những giải pháp tốn nhiều chi phí trong thời điểm hiện tại là chưa cần thiết vì có thể chia thành nhiều giai đoạn hoàn thiện theo thời gian.

- Nếu kinh phí cho phép thì nên bổ sung thêm 1 server để tránh việc đầy tài nguyên và sẵn sàng sao lưu dự phòng nếu cần thiết.

- Chia VLAN ứng với các phòng bạn

- Cập nhật phiên bản hệ điều hành

- Bổ sung các luật trong tường lửa để có thể phòng tránh tối đa rủi ro đến an toàn thông tin của công ty.

- Việc cần thiết là rà soát định kì các file nhật ký trong hệ thống, như server, firewall,…

- Thường xuyên kiểm tra, giám sát về việc tuân thủ những chính sách an toàn thông tin của nhân viên đối với công ty.

- Tại hệ thống máy chủ và máy tính có dữ liệu nhạy cảm, có dữ liệu cần được chia sẻ; tại các thiết bị lưu trữ cần phải tiến hành mã hóa nội dung.

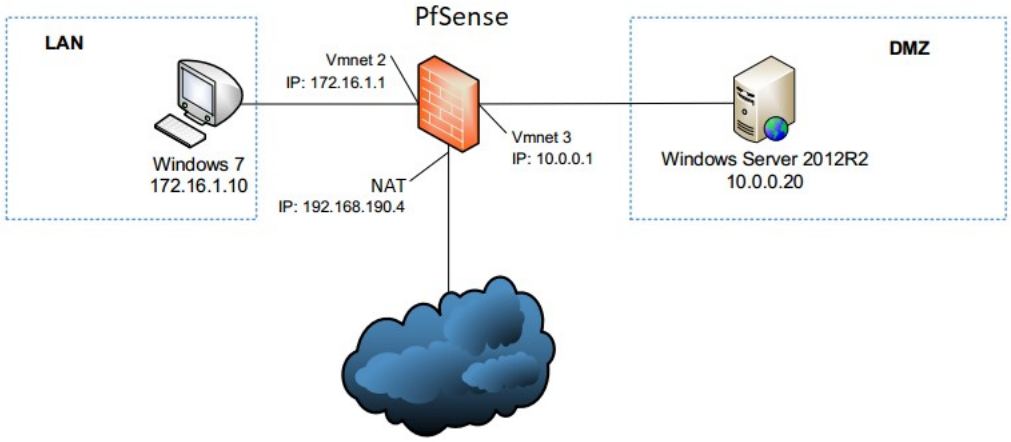
5. Thử nghiệm triển khai tường lửa PfSense

5.1.Triển khai

Cài đặt thử nghiệm hệ thống với tường lửa PfSense (mô phỏng trên Vmware)

− 01 máy ảo hệ điều hành Windows 7: Cài đặt ứng dụng Google Chrome − 01 máy ảo hệ điều hành Windows Server 2012. (tương tự như máy tại công ty K&H)

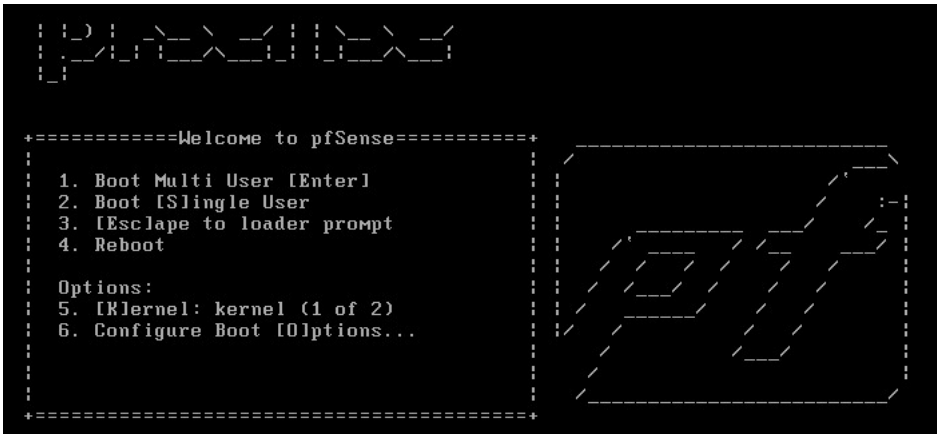
− 01 máy ảo gốc



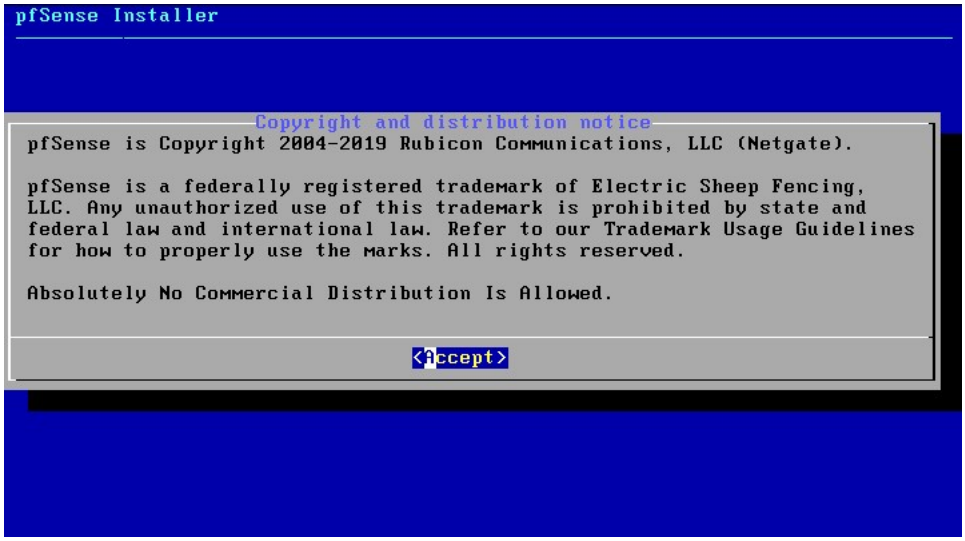
5.2. Cài đặt tường lửa PfSense

Sau khi cấu hình phần cứng cho máy ảo PfSense xong, khởi động máy ảo.

Quá trình cài đặt bắt đầu

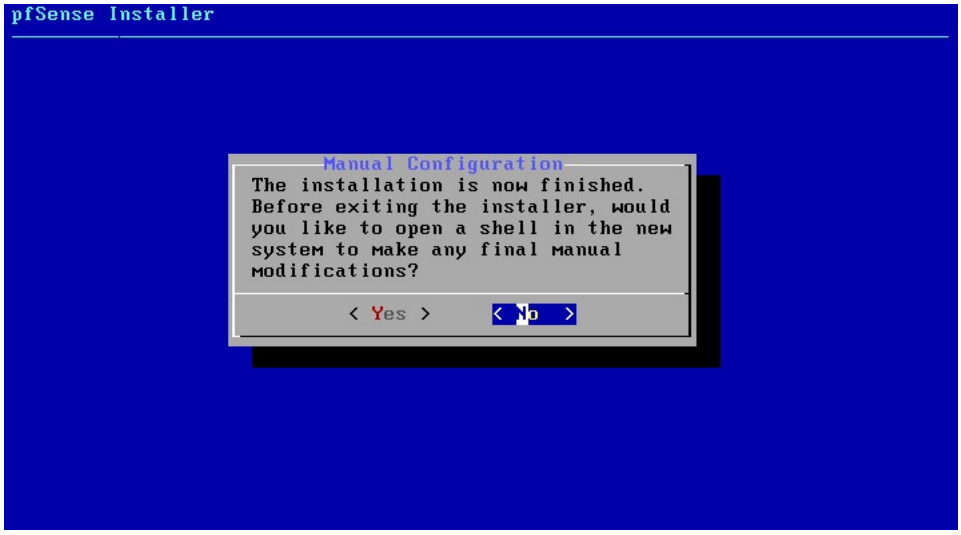


Quá trình diễn ra mặc định



Quá trình tiếp theo để mặc định và nhấn Enter để cài đặt.

Giao diện cuối cùng chọn

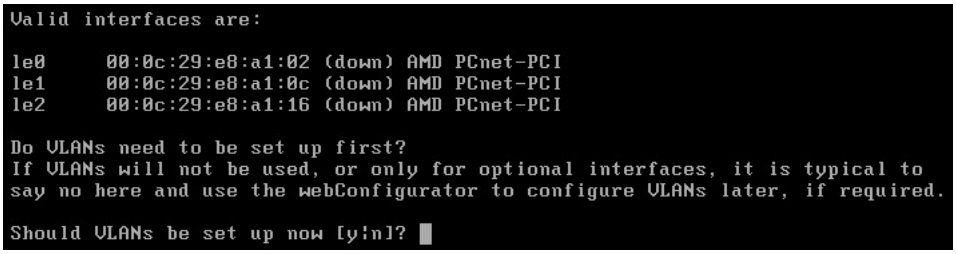


Chọn No để bỏ qua chế độ kiểm tra.

Chọn Reboot để khởi động lại tường lửa sau khi đã cài đặt xong.

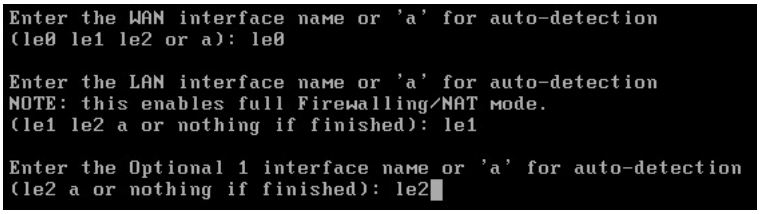
5.3. Cấu hình tường lửa cơ bản

Sau khi khởi động lại tường lửa, bắt đầu cấu hình cơ bản:



Cấu hình mạng LAN ảo, chọn n để bỏ qua.

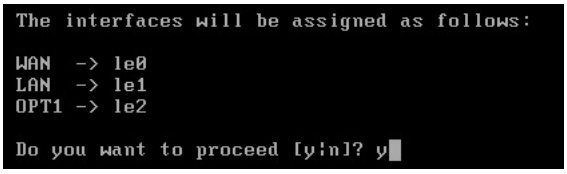
Lựa chọn cổng mạng tương ứng với các phân vùng mạng



Le0: Cổng mạng kết nối Internet

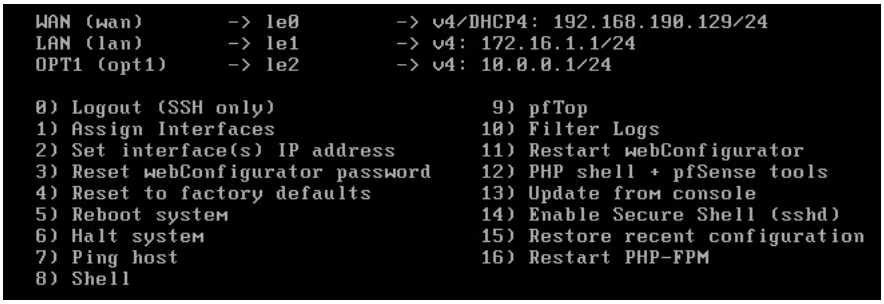
Le1: Cổng mạng kết nối LAN

Le2: Cổng mạng kết nối DMZ



Chọn y để thực hiện xử lý.

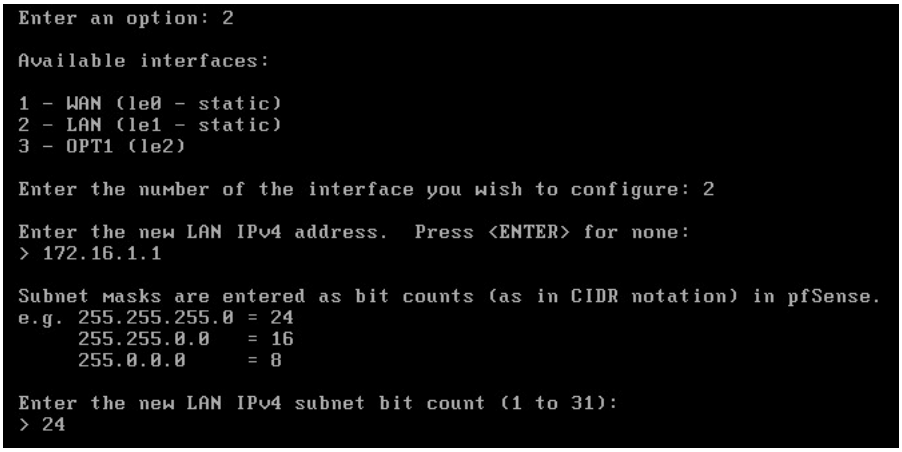
Tiếp tục cấu hình địa chỉ IP cho mỗi cổng mạng tương ứng với mô hình đã cho.



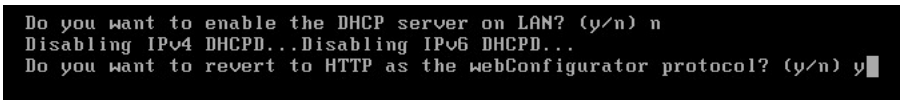
Chọn 2 để cấu hình

Chú ý: ở trong môi trường ảo hóa này IP cổng WAN nên để mặc định.

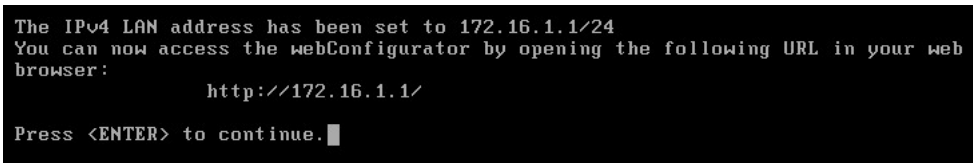
Tiếp tục cấu hình cho cổng LAN



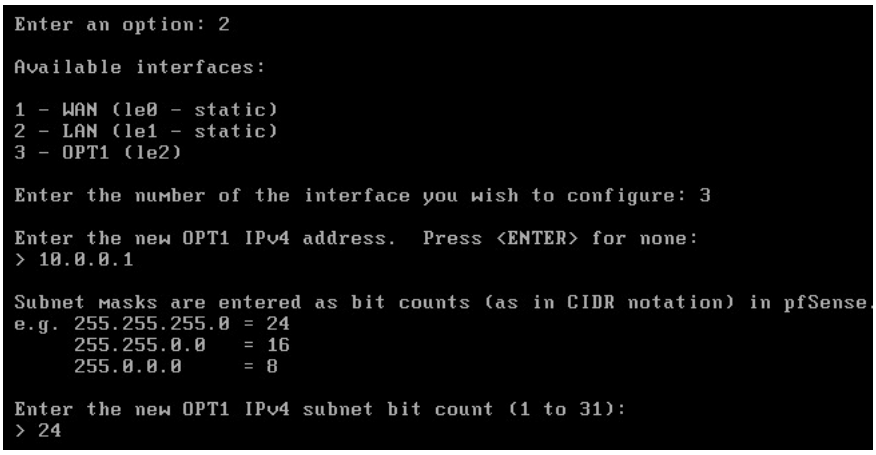
Chú ý muốn quản trị tường lửa PfSense qua giao diện web thì phải thực hiện bước sau đây:



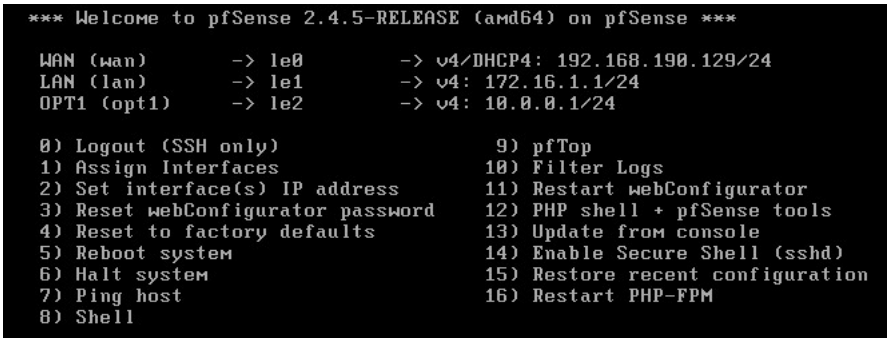
Kết quả:



Tương tự cấu hình IP cho cổng mạng DMZ qua OPT1

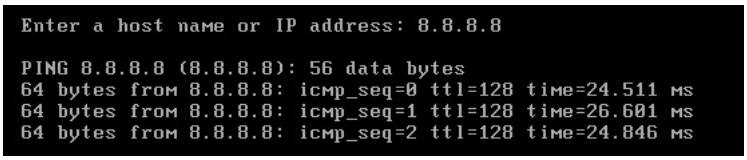


Kết quả cuối cùng sau khi cấu hình cơ bản:

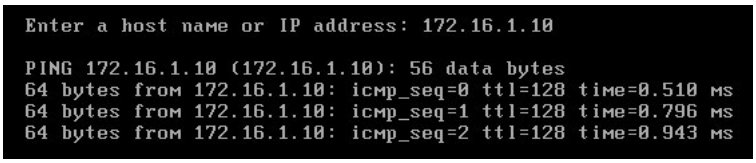


Kiểm tra kết nối tới các máy:

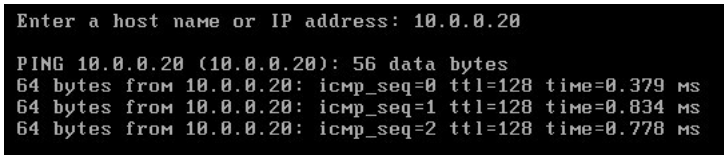
Ping ra Internet



Ping tới máy Windows 7



Ping tới Server 2012



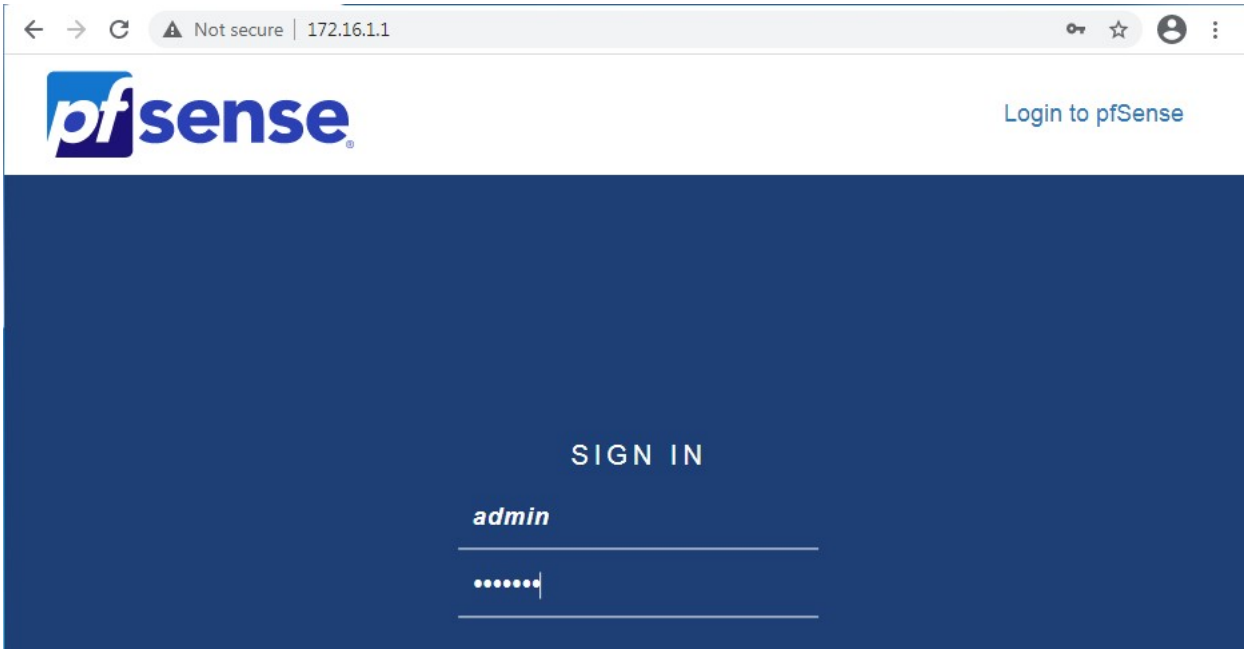
Kết quả cấu hình mạng thành công.

5.4. Quản trị tường lửa bằng đồ họa

Sau khi kết thúc quá trình cấu hình cơ bản xong, lúc này sử dụng trình duyệt web trên máy tính Windows 7 để truy cập và quản trị tường lửa qua giao diện đồ họa.

Tại máy Windows 7 sử dụng trình duyệt Google Chrome đã cài đặt truy cập theo đường dẫn:

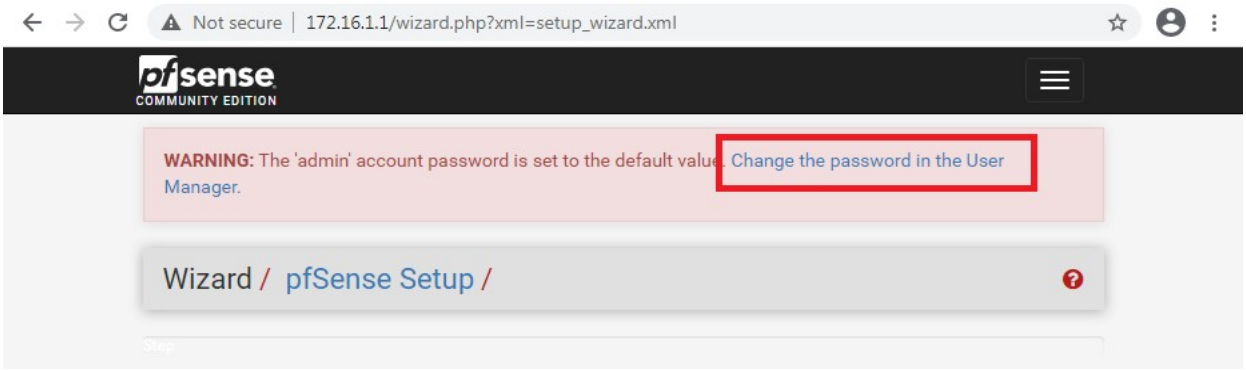
http://172.16.1.1

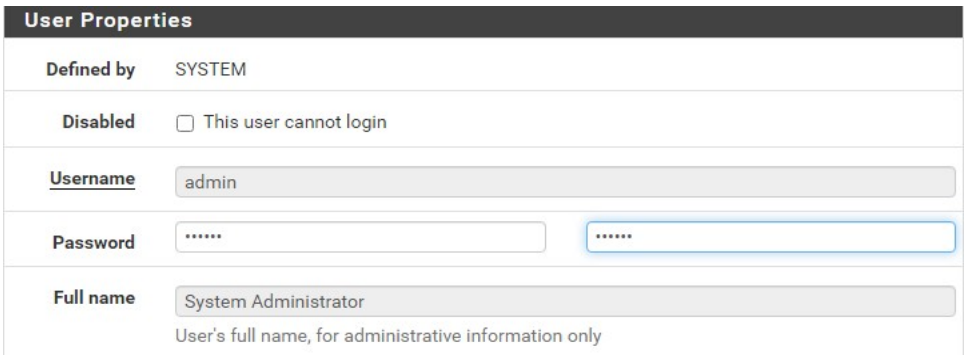


User: admin

Pass: pfsense

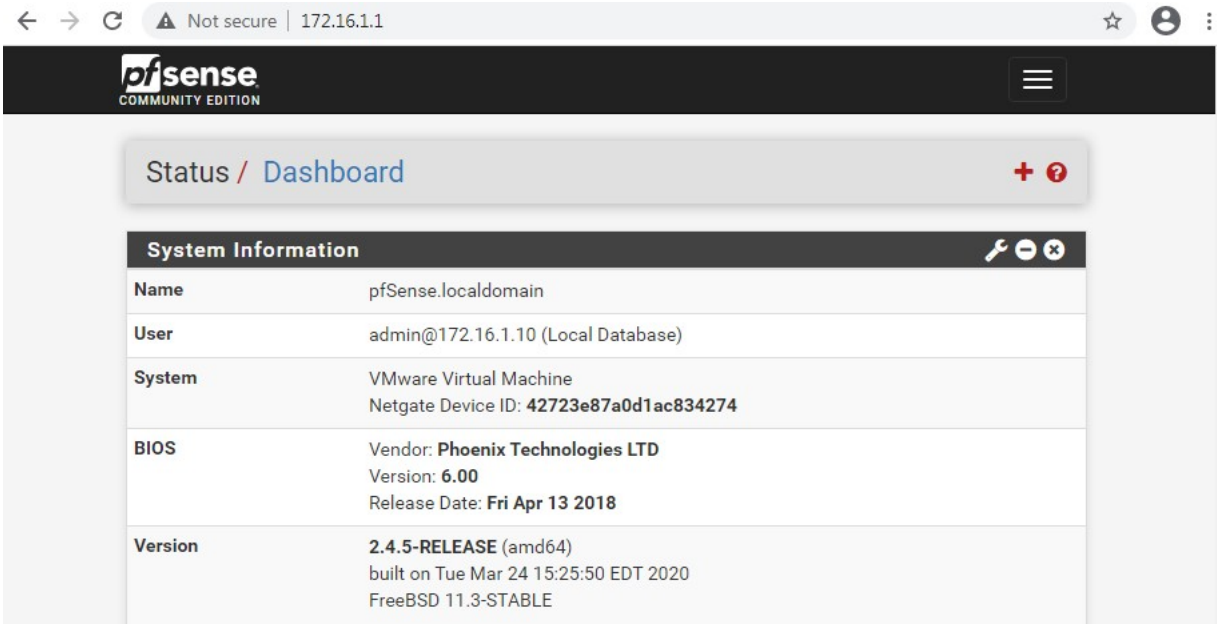
Công việc đầu tiên cần thay đổi mật khẩu cho tài khoản admin



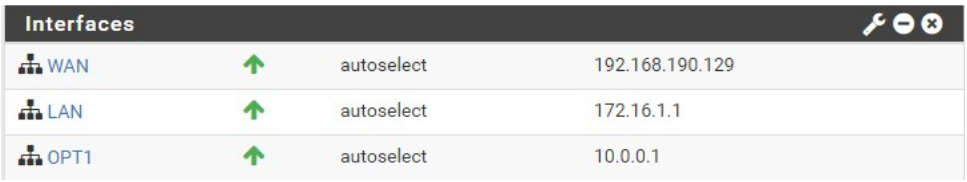


Nhấn Save ở phía cuối trang để lưu và trở về giao diện quản trị.

Giao diện quản trị chung



Thông tin về cổng mạng



Chú ý: IP cổng WAN khác với IP trong mô hình đã cho vì để chế độ DHCP, trong môi trường máy ảo phải để chế độ này mới truy cập được Internet.

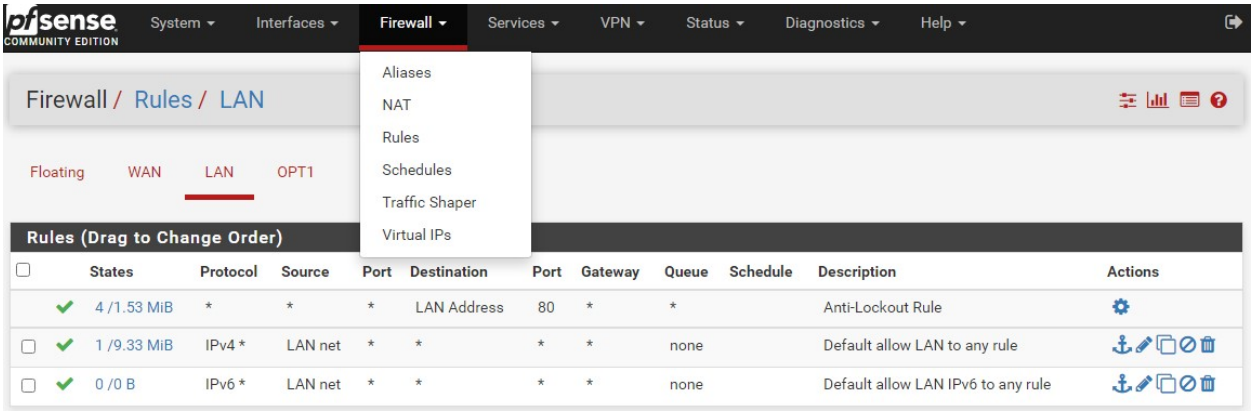
Trong thực tế IP cổng này là IP public là địa chỉ tĩnh.

5.5. Tạo tập luật theo Thử nghiệm

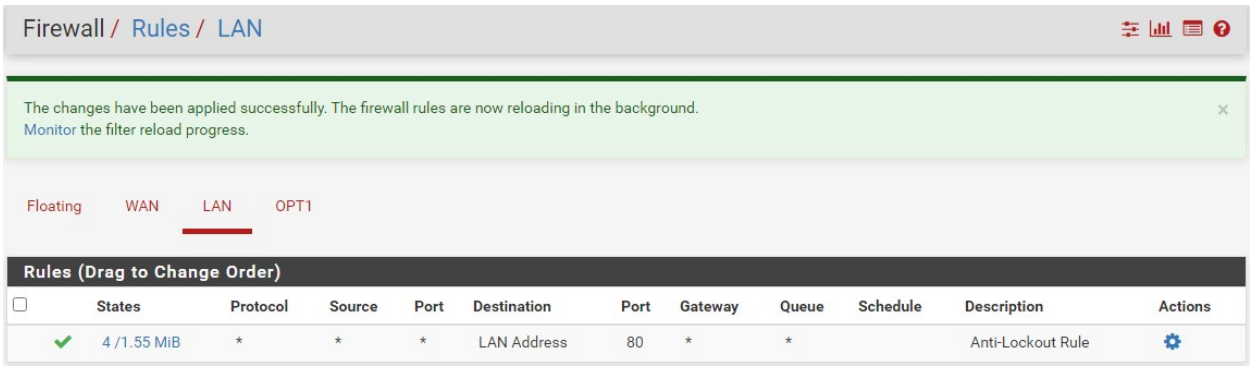
- Thử nghiệm 0: Xóa các luật mặc định.

Mặc định khi cài đặt xong tường lửa sẽ có các luật mặc định tạo sẵn, những luật này chưa đảm bảo an toàn vì thế cần thiết lập lại từ đầu.

Truy cập theo đường dẫn: Firewall → Rules → LAN



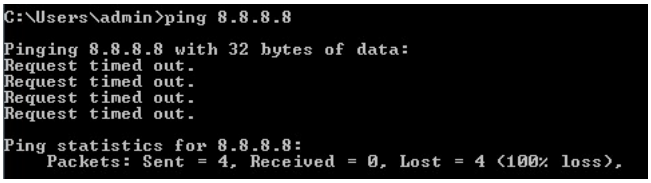
Xóa các luật mặc định, kích vào tùy chọn Apply changes, kết quả.



Lúc này chỉ còn 1 luật mặc định, luật này không thể xóa được vì đây là luật cho quản trị tường lửa.

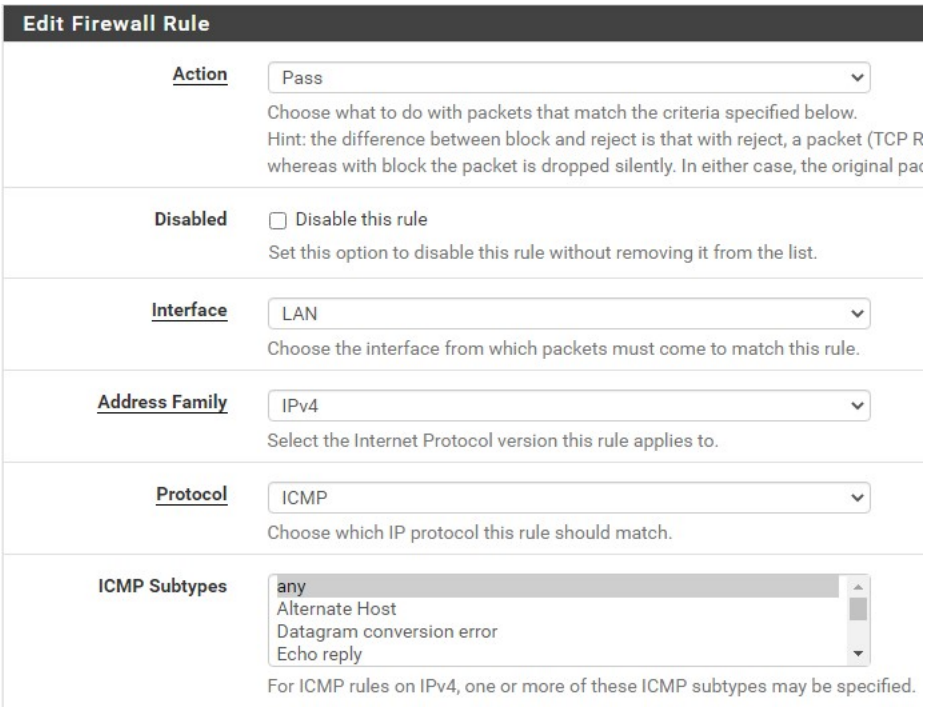
5.5.1. ***Thử nghiệm 1:*** *Cho phép máy trạm trong mạng LAN Ping ra Internet*

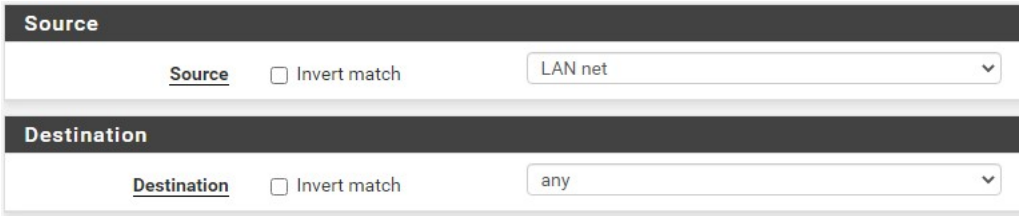
Trước khi thiết lập luật, kiểm tra Ping:



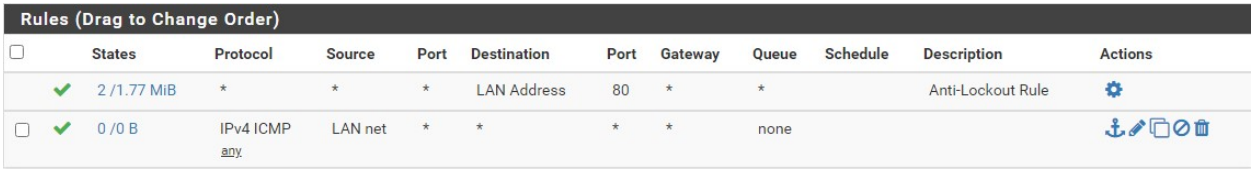
Kết quả đang bị chặn bởi tường lửa.

Chọn Add, giao diện cấu hình luật xuất hiện lựa chọn các thông tin sau:

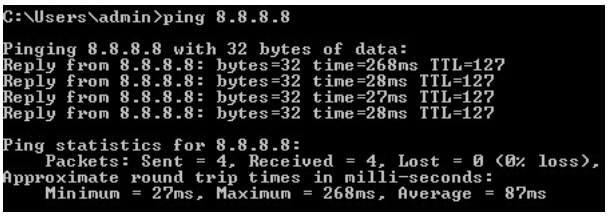




Chọn Save để lưu cấu hình. Kết quả



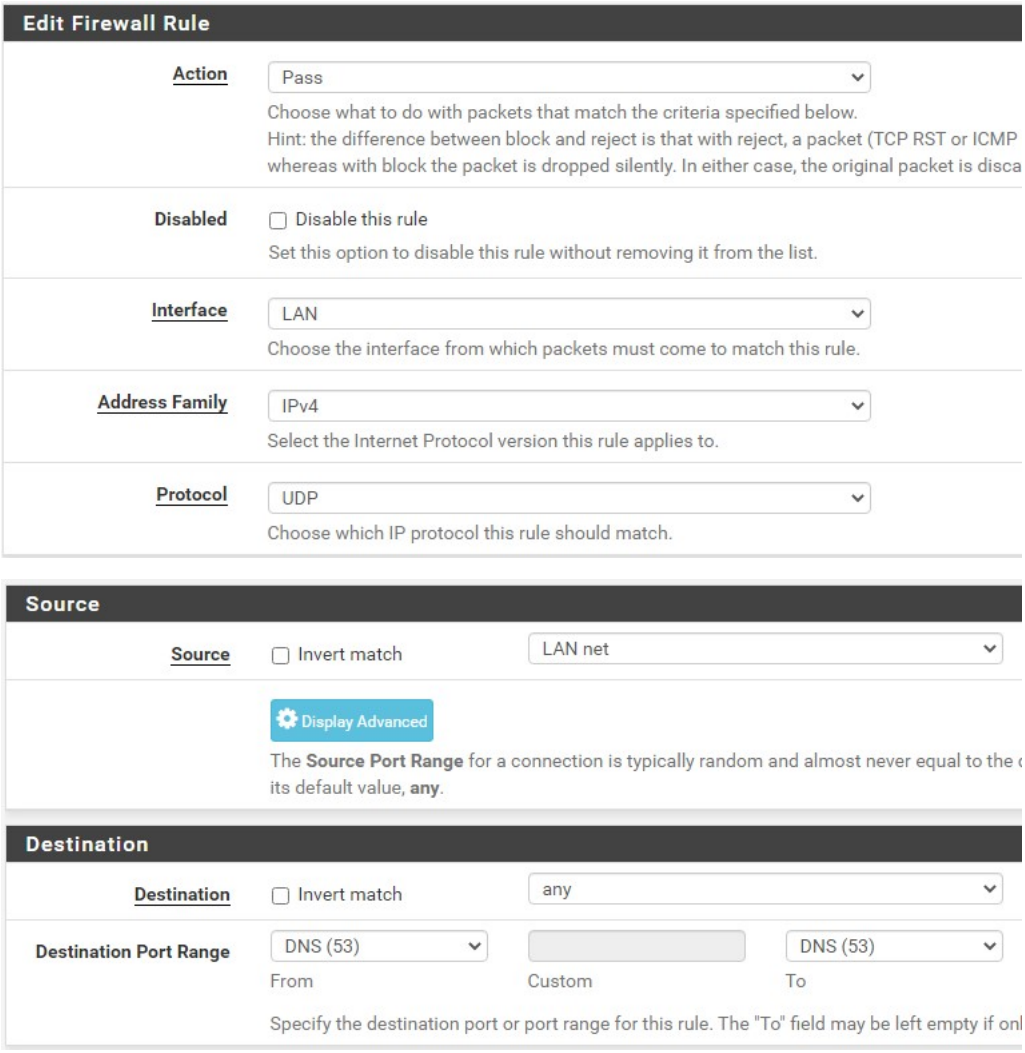
Ping kiểm tra lại, kết quả:



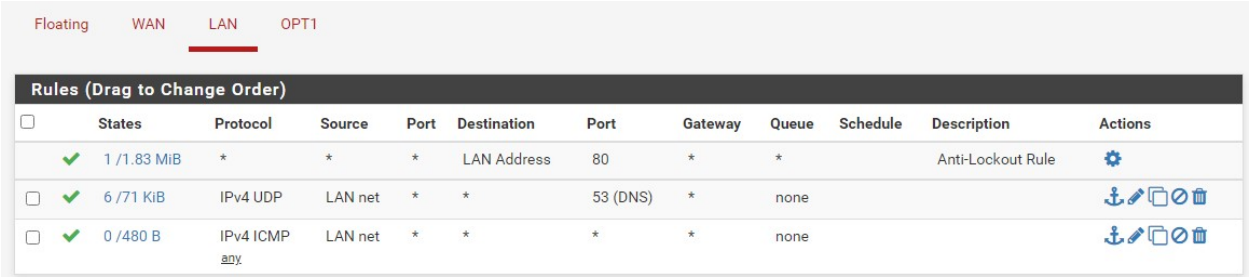
Như vậy sau khi thiết lập luật cho tường lửa, thì lúc này các gói tin ICMP đi qua tường lửa đều cho phép.

5.5.2. ***Thử nghiệm 2:*** *Cho phép máy tính trong mạng LAN truy vấn DNS ra Internet*

Chọn Add, cấu hình luật với thông tin như sau;



Nhấn Save để lưu, và Apply Changes để chạy luật.



Kiểm tra kết quả, sử dụng giao diện dòng lệnh DOS, chạy lệnh: nslookup để kiểm tra:

```
C:\Users\admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> facebook.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    facebook.com
Addresses:  2a03:2880:f109:81:face:b00c:0:25de
          31.13.75.35
```

Có kết quả trả về địa chỉ IP tương ứng với tên miền.

5.5.3. ***Thử nghiệm 3:*** *Cho phép máy tính trong mạng LAN truy cập website qua cổng 80, 443.*

Luật đã tạo như sau:

Floating | WAN | LAN | OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	2 /1.91 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
✓	0 /0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none			
✓	68 /2.92 MiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none			
✓	0 /82 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none			
✓	0 /480 B	IPv4 ICMP any	LAN net	*	*	*	*	none			

Kiểm tra kết quả truy cập website trên Windows 7:

Kết luận.

Tường lửa PfSense là loại tường lửa mềm, miễn phí có chức năng kiểm soát lưu lượng mạng, thực hiện các hành động để bảo vệ an toàn cho mạng máy tính.

PfSense là tường lửa cấu hình cơ bản dựa trên dòng lệnh. Quản trị dựa trên chế độ đồ họa cho nên dễ dàng cho người quản trị có thể cấu hình, theo dõi hoạt động của mạng, đảm bảo an toàn cho mạng máy tính.

Nhờ sự giúp đỡ tận tình mọi người trong công ty, cùng với kiến thức đã được học, em đã triển khai và báo cáo các bước để áp dụng tường lửa PfSense vào thực tế. Tuy nhiên vẫn cần phải có sự thông qua của ban lãnh đạo để thực hiện với toàn bộ các máy tính trong công ty và sau đó mới có kế hoạch triển khai cụ thể.