|  |
| --- |
| **ĐỒ ÁN AN TOÀN MÁY CHỦ WINDOWS**  **Đề tài: TÌM HIỂU VÀ CÀI ĐẶT HỆ THỐNG FIREWALL PFSENSE**  **Ngành: CÔNG NGHỆ THÔNG TIN**  **Chuyên ngành:**    **Giảng viên hướng dẫn :**  **Sinh viên thực hiện:**    **TP. Hồ Chí Minh, 2022**  **ĐỒ ÁN AN TOÀN MÁY CHỦ WINDOWS**  **Đề tài: TÌM HIỂU VÀ CÀI ĐẶT HỆ THỐNG FIREWALL PFSENSE**  **Ngành: CÔNG NGHỆ THÔNG TIN**  **Chuyên ngành:**    **Giảng viên hướng dẫn :**  **Sinh viên thực hiện:**  **TP. Hồ Chí Minh, 2022** |

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

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

TP.HCM,ngày…tháng …năm 2022

**Giảng viên hướng dẫn**

**LỜI MỞ ĐẦU**

Trong nhưng năm gần đây, công nghệ thông tin của đất nước ta đã có nhưng bước tiến vượt bậc. Đi đôi cùng với sự phát triển về công nghệ, mạng lưới cơ sở hạ tầng cũng được nâng cấp, tạo điều kiện cho các dịch vụ gia tăng, trao đổi thông qua mạng bùng nổ. Nhưng cùng với sự phát triển về hệ thống mạng, đặc biệt là sự phát triển rộng khắp của hệ thống mạng toàn cầu (Internet), các vụ tấn công phá hoại trên mạng diễn ra ngày càng nhiều và ngày càng nghiêm trọng hơn. Chúng xuất phát từ nhiều mục đích, như là đê khẳng định bản thân, để thỏa mãn lợi ích cá nhân, hay vì những mâu thuẫn, cạnh tranh,… nhưng tựu chung lại đã gây ra một hậu quả rất nghiêm trọng cả về vật chất và úy tín của doanh nghiệp, tổ chức.

Đối với các doanh nghiệp, vai trò của Internet là không thể phủ nhận, ứng dụng thương mại điện tử vào công việc kinh doanh giúp cho các doanh nghiệp không những giảm đi các chi phí thông thường mà còn mở rộng đối tác, quảng bá sản phẩm cũng như liên kết với khách hàng. Nhưng chấp nhận điều đó cũng có nghĩa là doanh nghiệp đang đúng trước nguy cơ đổi mặt với các rủi ro và nguy hiểm từ Internet. Chính vì lý do đó vấn đề an ninh mạng đàng trở nên nóng bỏng hơn bao giờ hết, các doanh nghiệp cũng đã dẫn nhận thức được điều này và có những quan tâm đặc biệt hơn tới hạ tầng an ninh mạng. Một trong những thành phần căn bản và hữu ích nhất có thể kể tới trong hạ tầng đó là hệ thống FireWall - công nghệ đang ngày càng được cải tiến và phát triển đa dạng, phong phú. Xuất phát từ nhu cầu thực tế, khi các doanh nghiệp rất cần một Ưhệ thống FireWall để bảo vệ họ, đồ án ra đời với hy vọng có thể tìm kiếm một giải pháp nào đó cho vấn đề này.

**LỜI CẢM ƠN**

Đầu tiên, em xin gửi lời cảm ơn chân thành đến Trường Đại Học đã đưa môn học An Toàn Máy Chủ Windows vào trương trình giảng dạy. Đặc biệt, em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn - thầy đã dạy dỗ, truyền đạt những kiến thức quý báu cho em trong suốt thời gian học tập vừa qua. Trong thời gian tham gia lớp học của thầy, em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập hiệu quả, nghiêm túc. Đây chắc chắn sẽ là những kiến thức quý báu, là hành trang để em có thể vững bước sau này.

Bộ môn An Toàn Máy Chủ Windows là môn học thú vị, vô cùng bổ ích và có tính thực tế cao, cung cấp rất nhiều kiến thức về mạng cũng như mọi thứ liên quan về mạng. Đảm bảo cung cấp đủ kiến thức, gắn liền với nhu cầu thực tiễn của sinh viên. Tuy nhiên, do vốn kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ.

Do chưa có nhiều kinh nghiệm nghiên cứu, thực hành nên đề tài thực hiện còn nhiều thiếu sót, chúng em mong nhận được đóng góp ý kiến của thầy để đề tài được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

**Sinh viên thực hiện**

**MỤC LỤC**

[CHƯƠNG 1: FIREWALL 1](#_Toc106919845)

[1.1 Định nghĩa về FireWall 1](#_Toc106919846)

[1.2 Chức năng của FireWall 1](#_Toc106919847)

[CHƯƠNG 2: PFSENSE 2](#_Toc106919848)

[2.1 Định nghĩa về PfSense 2](#_Toc106919849)

[2.2 Phần mềm mã nguồn mở FireWall PfSense 2](#_Toc106919850)

[2.3 Chức năng của PfSense. 4](#_Toc106919851)

[2.3.1 Aliases 4](#_Toc106919852)

[2.3.2 Rules 5](#_Toc106919853)

[2.3.3 Virtual IPs 5](#_Toc106919854)

[2.3.4 CARP 6](#_Toc106919855)

[2.3.5 Other 6](#_Toc106919856)

[2.3.6 NAT 6](#_Toc106919857)

[2.3.7 Routing 7](#_Toc106919858)

[2.3.8 Virtual Lans (Vlans) 7](#_Toc106919859)

[2.3.9 Multi-Wan 7](#_Toc106919860)

[2.3.10 VPN 8](#_Toc106919861)

[2.3.11 Ipsec (Ip Security) 8](#_Toc106919862)

[2.3.12 PPTP VPN 9](#_Toc106919863)

[2.3.13 OpenVPN 9](#_Toc106919864)

[2.3.14 Traffic Shaper (Quản Lý Băng Thông) 10](#_Toc106919865)

[2.3.15 Server Load Balancing 10](#_Toc106919866)

[2.3.16 Wireless 10](#_Toc106919867)

[2.3.17 Captive Portal 10](#_Toc106919868)

[2.3.18 Firewall Redundancy / High Availability 12](#_Toc106919869)

[2.3.19 WOL (Wake On Lan) 12](#_Toc106919870)

[2.3.20 PPPoE Server 13](#_Toc106919871)

[2.3.21 Một Số Chức Năng Khác 13](#_Toc106919872)

[2.4 Tóm lược của PfSense 14](#_Toc106919873)

[CHƯƠNG 3: CÀI ĐẶT FIREWALL PFSENSE TRÊN VMWARE 14](#_Toc106919874)

[3.1 Sơ đồ kịch bản 14](#_Toc106919875)

[3.2 Công cụ 14](#_Toc106919876)

[3.3 Cách thức thực hiện 15](#_Toc106919877)

[CHƯƠNG 4: TỔNG KẾT 32](#_Toc106919878)

[4.1 Kết quả đạt được 32](#_Toc106919879)

[4.2 Kết quả chưa đạt được 32](#_Toc106919880)

[TÀI LIỆU THAM KHẢO 33](#_Toc106919881)

# CHƯƠNG 1: FIREWALL

## 1.1 Định nghĩa về FireWall

FireWall là một hệ thống bảo mật mạng giám sát và kiểm soát lưu lượng mạng đến và đi dựa trên các quy tắc bảo mật được xác định trước. Một tường lửa thường thiết lập một rào cản giữa một mạng nội bộ đáng tin cậy và mạng bên ngoài không tin cậy, chẳng hạn như Internet.

Về cơ bản thì FireWall là tấm lá chắn giữa máy tính của bạn giữa Internet, giống như một nhân viên bảo vệ giúp bạn thoát khỏi những kẻ thù đang muốn tấn công bạn. Khi Firewall hoạt động thì có thể từ chối hoặc cho phép lưu lượng mạng giữa các thiết bị dựa trên các nguyên tắc mà nó đã được cấu hình hoặc cài đặt bởi một người quản trị tường lửa đưa ra.

## 1.2 Chức năng của FireWall

FireWall dùng để bảo vệ chống lại sự tần công bên ngoài như:

* Tấn công trực tiếp.
* Nghe trộm.
* Giả mạo địa chỉ IP.
* Vô hiệu hóa chức năng của hệ thống (deny service).
* Lỗi người quản trị hệ thống.

# CHƯƠNG 2: PFSENSE

## 2.1 Định nghĩa về PfSense

PfSense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này sẽ cho phép bạn mở rộng mạng của mình mà không bị thỏa hiệp về sự bảo mật. Bẳt 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 bạn 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 P3, Ram 128 MB ,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 Phần mềm mã nguồn mở FireWall PfSense

Là một trong số các sản phẩm FireWall nguồn mở được đánh giá cao nhất hiện nay, nó hoàn toàn miễn phí. Được tách ra từ dự án xây dựng sản phẩm m0n0wall cho các hệ thống nhúng, PfSense được tập trung hướng tới việc cài đặt và chạy ổn định trên cái máy tính thông thường. Bản thân PfSense là một phần mềm đọc lập riêng biệt với hệ điều hành FreeBSD nhỏ gọn được thiết kế riêng và đóng gói cùng, điều này cho phép PfSense cài đặt và chạy trực tiếp lên các máy tính thông thường mà không cần phải cài đặt trước một hệ điều hành nền nào khác. Kế thừa các tính năng từ m0n0wall, PfSense đã phát triển để trở thành một FireWall mạnh mẽ với đầy đủ với các tính năng đáp ứng được nhu cầu từ nhà mạng gia đình, doanh nghiệp nhỏ cho đến hệ thống lớn với hàng ngàn thiết bị kết nối mạng. Để có được thành công đó là sự phát triển vượt trội khi chỉ từ nền tảng lọc gói và định tuyến thuần túy, một danh sách dài các tính năng liên quan và các gói cài đặt hữu ích được bổ sung tạo nên một hệ thống linh hoạt và vững chắc.

* 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.

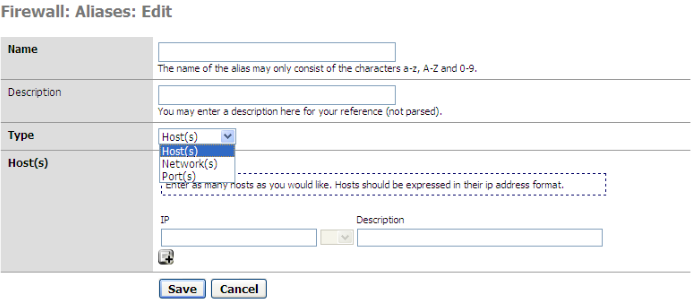
Sau đây là danh sách một số đặc trưng và tính năng nổi bật của FireWall PfSense:

* Chức năng tường lửa lọc gói.
* Công nghệ stateful.
* Dịch địa chỉ mạng (NAT).
* Khả năng dự phòng (redundency).
* Mạng riêng ảo: SSL, VPN, IPSec Site-to-site VPN, PPTP VPN.
* Giám sát và thống kê.
* Dynamics DNS.
* DHCP Server and Reply.
* PPPoE Server.
* DNS forwander.

## 2.3 Chức năng của PfSense.

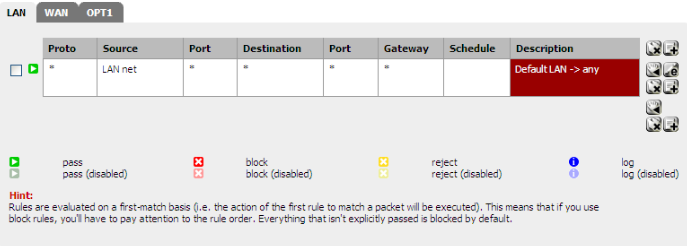
### 2.3.1 Aliases

* 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.
* 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



### 2.3.2 Rules

* Nơi lưu các rules (luật) của Firewall  
  Mặc định pfSense cho phép mọi lưu thông ra/vào hệ thống  
  Bạn phải tạo các rules để quản lý mạng bên trong Firewall  
  Một số lựa chọn trong Destination và Source
* Any: bất kì , 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 PPT
* PPPoE clients: Các clients thực hiện kết nối VPN   
  sử dụng giao thức PPPoE



### 2.3.3 Virtual IPs

* Pfsense cho phép sử dụng nhiều địa chỉ IP công cộng kết hợp với cơ chế NAT thông qua IP ảo. Có ba loại IP ảo có sẵn trên pfSense: Proxy ARP, CARP và một loại khác.  
  Mỗi loại đều rất hữu ích trong các tình huống khác nhau.  
  Trong hầu hết các trường hợp, pfSense sẽ cung cấp ARP trên IPs, do đó cần phải sử dụng Proxy ARP hoặc CARP.  
  Trong tình huống mà ARP không cần thiết, chẳng hạn như khi các IP công cộng bổ sung được định tuyến bởi nhà cung cấp dịch vụ mạng, sẽ sử dụng IP ảo loại khác.Virtual IP được sử dụng để cho phép pfSense đúng cách chuyển tiếp lưu lượng cho những việc như chuyển tiếp cổng NAT, NAT Outbound và NAT 1:1.  
  Họ cũng cho phép các tính năng như failover, và có thể cho phép dịch vụ trên router để gắn kết với địa chỉ IP khác nhau.

### 2.3.4 CARP

* Có thể được sử dụng bởi các tường lửa chính nó để chạy các dịch vụ hoặc được chuyển tiếp.
* Tạo ra lớp 2 lưu lượng cho các VIP (Virtual IP)
* Có thể được sử dụng cho clustering (tường lửa và tường lửa chủ failover chế độ chờ)
* Các VIP đã được trong cùng một subnet IP của giao diện thực.
* Sẽ trả lời ICMP ping nếu được phép theo các quy tắc tường lửa.
* Proxy ARP.
* Không thể được sử dụng bởi các bức tường lửa chính nó, nhưng có thể được chuyển tiếp
* Tạo ra lớp 2 lưu lượng cho các VIP
* Các VIP có thể được trong một subnet khác với IP của giao diện thực.
* Không trả lời gói tin ICMP ping

### 2.3.5 Other

* Có thể được sử dụng nếu các tuyến đường cung cấp cho bạn VIP của bạn dù sao mà không cần thông báo lớp 2.
* Không thể được sử dụng bởi các bức tường lửa chính nó, nhưng có thể được chuyển tiếp
* Các VIP có thể được trong một subnet khác với các giao diện IP
* Không trả lời ICMP ping

### 2.3.6 NAT

* Trong Firewall bạn cũng có thể cấu hình các thiết lập NAT nếu cần sử dụng cổng chuyển tiếp cho các dịch vụ hoặc cấu hình NAT tĩnh (1:1) cho các host cụ thể.  
  Thiết lập mặc định của NAT cho các kết nối outbound là Automatic outbound NAT…, tuy nhiên bạn có thể thay đổi kiểu Manual outbound NAT nếu cần.

### 2.3.7 Routing

* Một trong những tính năng chính của một Firewall ngoài việc lọc và thực hiện NAT là định tuyến được lưu thông trong mạng. Nó bao gồm các tuyến tĩnh, các giao thức định tuyến, định tuyến IP công cộng và hiển thị các thông tin định tuyến.Bridging  
  Thông thường mỗi interface trên pfSense sẽ đại diện cho một miền riêng với một subnet IP duy nhất, giống như một vùng riêng biệt. Trong một số trường hợp cần kết hợp nhiều interfaces thành một miền mới, lúc đó chức năng này sẽ kết hợp hai cổng trên tường lửa sẽ hoạt động giống như nó đang trên cùng một miền, ngoại trừ lưu lượng giữa các interface được kiểm soát bởi các quy luật (rule) đã được cấu hình.

### 2.3.8 Virtual Lans (Vlans)

* VLAN cung cấp một phương tiện để phân đoạn mạng miền thành nhiều mạng con, mỗi mạng con hoạt động độc lập với nhau. Nhưng vấn đề bảo mật cần phải đưa vào account khi thiết kế và thực thi một giải pháp liên quan đến VLAN. VLAN không đảm bảo an toàn nên sai có thể dẫn đến tổn thương cho mạng của bạn.

### 2.3.9 Multi-Wan

* Multi-WAN của pfSense cho phép sử dụng nhiều kết nối Internet để đạt được thời gian hoạt động cao hơn và băng thông lớn. Trước khi cầu hình Multi-WAN cần phải cấu hình hai interfaces (LAN và WAN) hoạt động. Pfsense có khả năng xử lý nhiều WAN interface, triển khai sử dụng khoảng 10-12 WANs. WAN interface bổ sung được gọi là OPT WAN.

### 2.3.10 VPN

* VPN (Virtual Private Network) là một kiểu kết nối cho phép các máy tính truyền thông với nhau thông qua một môi trường chia sẻ như mạng Internet nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu. Để cung cấp kết nối giữa các máy tính, các gói thông tin được bao bọc bằng một header có chứa những thông tin định tuyến, cho phép dữ liệu có thể gửi từ máy truyền qua môi trường mạng chia sẻ và đến được máy nhận, như truyền trên các đường ống riêng được gọi là tunnel. Để bảo đảm tính riêng tư và bảo mật trên môi trường chia sẻ này, các gói tin được mã hoá và chỉ có thể giải mã với những khóa thích hợp, ngăn ngừa trường hợp “trộm” gói tin trên đường truyền. Chức năng này của pfSense được đánh giá là rất tốt.



### 2.3.11 Ipsec (Ip Security)

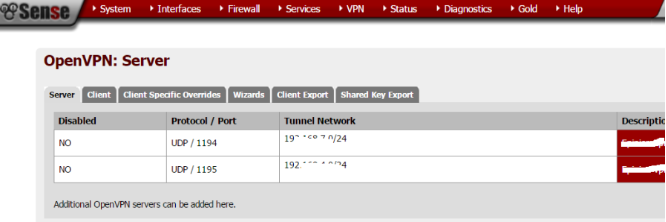
* IPSec có vai trò rất quan trọng trong việc giải quyết các vấn đề mà chúng ta cố giải quyết nó với firewall. IPSec (IP Security) đề ra một tập các chuẩn được phát triển bởi Internet Engineering Tast Force (IETF). IPSec giải quyết hai vấn đề gây hại cho bộ giao thức IP: Sự xác thực host-to-host (cho các host biết là chúng đang nói chuyện với nhau mà không phải là sự giả mạo) và việc mã hóa (ngăn chặn những kẻ tấn công xem dữ liệu trong luồng lưu lượng giữa hai máy). Đây là các vấn đề mà firewall cần giải quyết. Mặc dù firewall có thể làm giảm nguy cơ tấn công trên Internet mà không cần sự xác thực và mã hóa, nhưng vẫn còn hai vấn đề lớn ở đây: tính toàn vẹn và sự riêng tư của thông tin đang truyền giữa hai host và sự giới hạn trong việc đặt ra các loại kết nối giữa các mạng khác nhau. IPSec giúp giải quyết các vấn đề này. Có vài khả năng đặc biệt khi chúng ta xem xét sự kết hợp giữa các firewall với các host cho phép IPSec. Cụ thể là, VPN, việc lọc gói tốt hơn (lọc những gói mà có tiêu đề xác thực IPSec), và các firewall lớp ứng dụng sẽ cung cấp sự xác minh host tốt hơn bằng cách sử dụng tiêu đề xác thực IPSec thay cho “just trusting” địa chỉ IP hiện tại.

### 2.3.12 PPTP VPN

* Pfsense có thể hoạt động như một máy chủ PPTP VPN, là một trong ba tùy chọn của VPN, là lựa chọn phổ biến nhất vì hầu hết các hệ điều hành đã được xây dựng trong PPTP client. Bao gồm tất cả các phiên bản Windows từ Windows 95. Tuy nhiên nó không được đảm bảo an toàn, không nên sử dụng

### 2.3.13 OpenVPN

* OPENVPN là một giải pháp SSL VPN mã nguồn mở có thể được sử dụng cho cả client truy cập từ xa và kết nối kiểu site-to-site. Nó hỗ trợ client trên phạm vi rộng của các hệ điều hành bao gồm tất cả BSD, Linux, Mac OS X, Windows 2000 trở đi. Chức năng này tương đường với cấu hình trực diện. Địa điểm chính được cấu hình như client đang kết nối với máy chủ tại địa điểm từ xa đó.



### 2.3.14 Traffic Shaper (Quản Lý Băng Thông)

* Pfsense cung cấp tính năng Traffic Shaper giúp bạn theo dõi và quản lí băng thông mạng dễ dàng và hiệu quả hơn.

### 2.3.15 Server Load Balancing

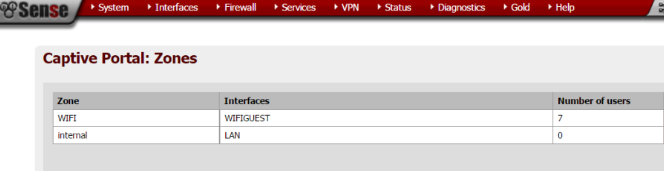
* Với chức năng này bạn có thể điều phối mạng hay còn gọi là cân bằng tải.
* Có 2 loại load balancing trên pfSense:
  + Gateway load balancing: được dùng khi có nhiều kết nối WAN. Client bên trong LAN khi muốn kết nối ra ngoài Internet thì pfSense lựa chọn card WAN để chuyển packet ra card đó giúp cho việc cân bằng tải cho đường truyền
  + Server load balancing: cho phép cân bằng tải cho các server của mình. Được dùng phổ biến cho các web server, mail server và server không hoạt động nữa thì sẽ bị xóa

### 2.3.16 Wireless

* Pfsense có khả năng cho phép xây dựng mạng không dây, sử dụng kết nối không dây như là một kết nối WAN.

### 2.3.17 Captive Portal

* Captive portal cho phép admin có thể chuyển hướng client tới một trang web khác, từ trang web này client có thể phải chứng thực trước khi kết nối tới internet.
* Captive portal: các chức năng của Captive Portal:
* Enable captive portal: Đánh dấu chọn nếu muốn sử dụng captive portal.
* Maximum concurrent connections: Giới hạn các connection trên mỗi ip/user/mac.
* Idle timeout: Nếu mỗi ip không còn truy cập mạng trong 1 thời gian xác định thì sẽ ngắt kết nối của ip/user/mac.
* Hard timeout: Giới hạn thời gian kết nối của mỗi ip/users/mac
* Logout popup windows: Xuất hiện 1 popup thông báo cho ip / user / mac
* Redirect URL: Địa chỉ URL mà người dùng sẽ được direct tới sau khi đăng nhập
* Pass-through MAC: Các MAC address được cấu hình trong mục này sẽ được bỏ qua không authentication
* Allowed IP address: Các IP address được cấu hình sẽ không authentication
* Users: Tạo local user để dùng kiểu authentication: local user
* ile Manager: Upload trang quản lý của Captive portal lên pfSense.
* Có 3 kiểu chứng thực client:
  + No authentication: pfSense sẽ điều hướng người dùng tới 1 trang nhất định mà không chứng thực
  + Local user manager: pfSense hỗ trợ tạo user để chứng thực.
  + Radius authentication: Chứng thực bằng radius server (Cần chỉ ra địa chỉ IP của radius, port, …)



### 2.3.18 Firewall Redundancy / High Availability

* Pfsense là một trong rất ít các giải pháp mã nguồn mở cung cấp khả năng sẳn sàng cao với trạng thái dự phòng. Cho phép loại bỏ các bức tường lửa bị lỗi.Firewall Schedules  
  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 lý nhân viên sử dụng internet trong giờ hành chính.Các Dịch Vụ Của Firewall Pfsense  
  DHCP ServerDịch vụ này cho phép pfSense cấp địa chỉ IP và các thông tin cấu hình cho client trong mạng LAN.DHCP Relay  
  Dịch vụ này cho phép pfSense forward yêu cầu cấp IP của client nằm trong một subnet nào đó tới một DHCP server cho trước.  
  Chỉ được phép chạy một trong hai dịch vụ DHCP server và DHCP relay.Dynamic DNS  
  Pfsense cho phép đăng ký địa chỉ IP của WAN interface của nhiều nhà cung cấp DNS động. Nó rất hữu ích khi muốn điều khiển từ xa.SNMP (Simple Network Management Protocol)  
  Chức năng SNMP của pfSense sẽ cho phép giám sát từ xa các thông số hệ thống pfSense. Tùy thuộc vào các tùy chọn cho phép mà có thể theo dõi như: lưu lượng mạng, hàng đợi, thông tin chung hệ thống(CPU, bộ nhớ….).

### 2.3.19 WOL (Wake On Lan)

* Được dùng để đánh thức máy tính đã tắt bằng cách gửi gói tin đặc biệt “Magic packet”. Các NIC trong máy tính phải được hỗ trợ WOL và phải được cấu hình đúng. Thông thường thiết lập WOL của NIC ở BIOS.

### 2.3.20 PPPoE Server

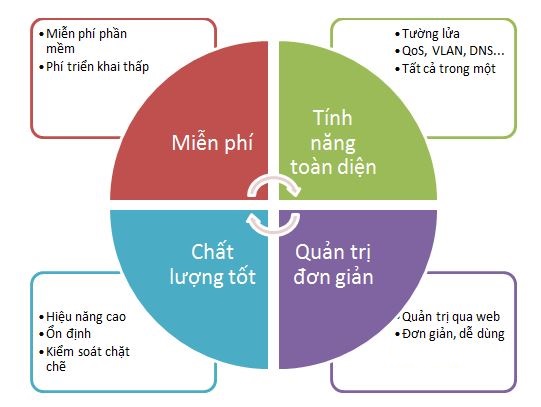
* Pfsense có thể hoạt động như một máy chủ PPPoE, chấp nhận hoặc xác thực kết nối từ client PPPoE trên interface cục bộ. Nó được dùng để bắt buộc người dùng xác thực trước khi được quyền truy cập mạng hoặc kiểm soát hoạt động đăng nhập của họ.

### 2.3.21 Một Số Chức Năng Khác

* System log: theo dõi hoạt động của hệ thống pfSense và các dịch vụ mà pfSense cung cấp. Mọi hoạt động của hệ thống và dịch vụ đều được ghi lại.
* System Status: Liệt kê các thông tin và tình trạng của hệ thống.
* Service Status: Hiển thị trạng thái của tất cả các service có trong hệ thống. Mỗi service có hai trạng thái là: running, stopped.
* Interface Status: Hiển thị thông tin của tất cả card mạng.
* RRD Graph: Hiển thị các thông tin dưới dạng đồ thị. Các thông tin mà RRD Graph sẽ thể hiện là: System, Traffic, Packet, Quality, Queues.
* Pfsense khá linh hoạt với các hệ thống khác để hỗ trợ tốt hơn cho việc vận hành của pfSense như: kết hợp chứng thực người dùng thông qua hệ thống RADIUS…

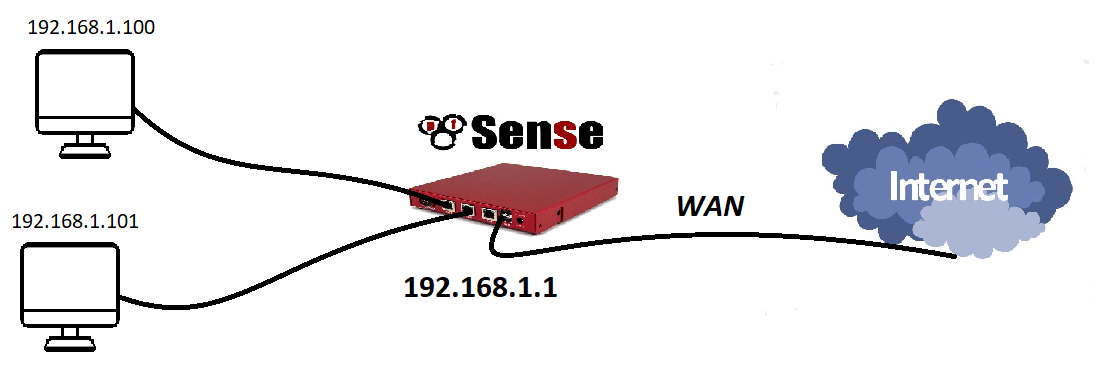
Ngoài ra pfSense còn có thể kết nối với mạng 3G, 4G thông qua thiết bị 3G, 4G. Trường hợp này phòng bị cho sự cố bất khả kháng khi tất cả các đường truyền internet bằng cáp bị hư hỏng.

## 2.4 Tóm lược của PfSense



# CHƯƠNG 3: CÀI ĐẶT FIREWALL PFSENSE TRÊN VMWARE

## 3.1 Sơ đồ kịch bản



## 3.2 Công cụ

Laptop

VMWare Workstation Pro

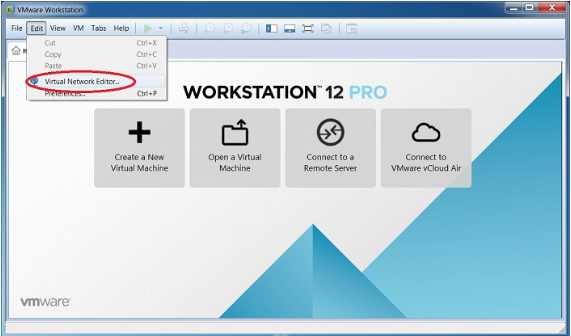
[pfSense-CE-2.5.1-RELEASE-amd64.iso](https://sgpfiles.netgate.com/mirror/downloads/pfSense-CE-2.5.1-RELEASE-amd64.iso.gz)

Trình duyệt web Chrome, Opera,…

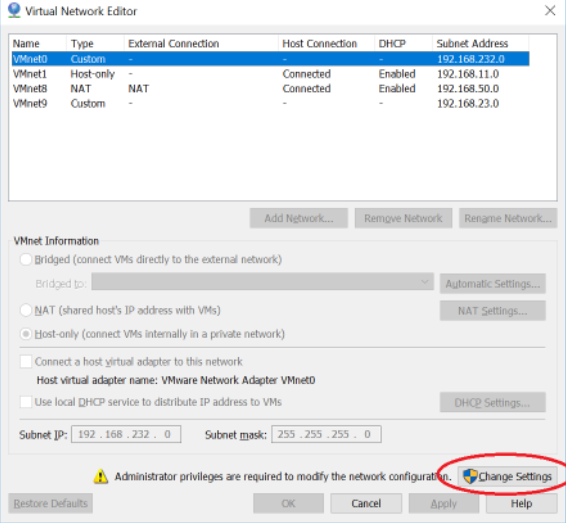
## 3.3 Cách thức thực hiện

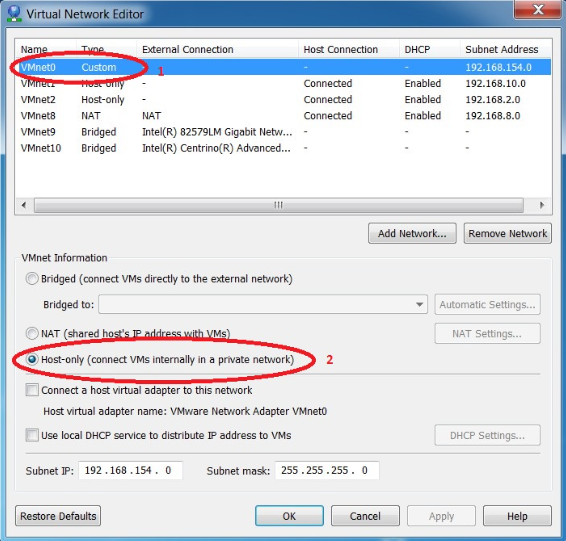
Bước 1: Download file ISO từ trang chủ [https://www.pfsense.org](https://www.pfsense.org/)

Bước 2: Khởi động **VMWare** chọn **Edit -> Virtual Network Editor**

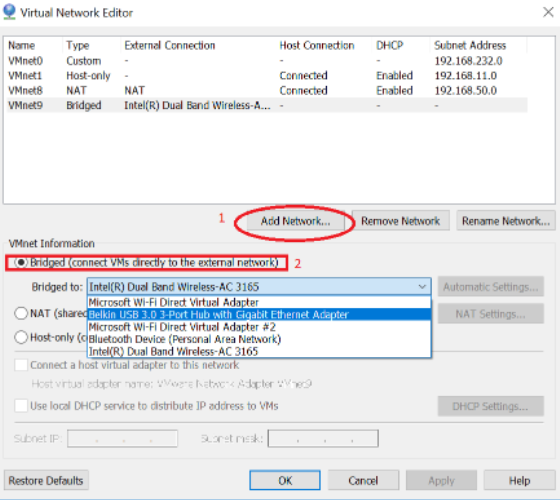


 Chỉnh lại **VMnet0** từ “**Bridged**” thành “Host-only” ( bấm Change Settings nếu đòi quyền administrator)

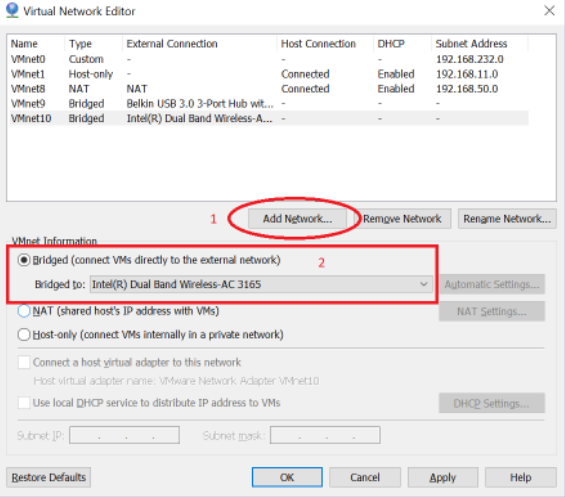




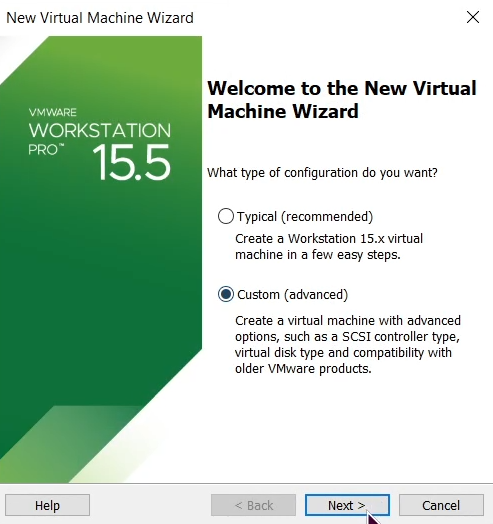
Thêm **VMnet9**và thiết lập ở chế độ “**Bridged**” với card mạng **ethernet (LAN)** của Laptop thật



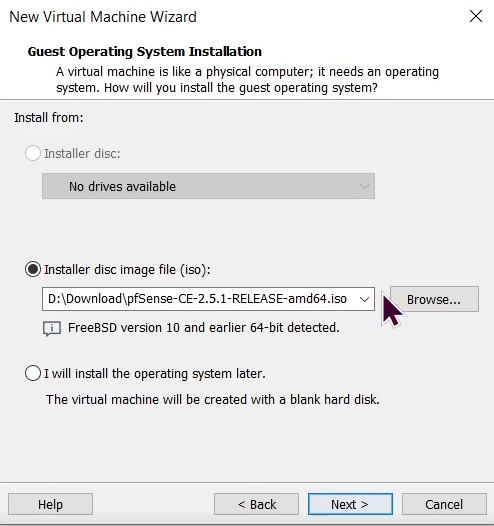
 Thêm **VMnet10** và thiết lập ở chế độ “**Bridged**” với card mạng **“Wireless”** của Laptop thật



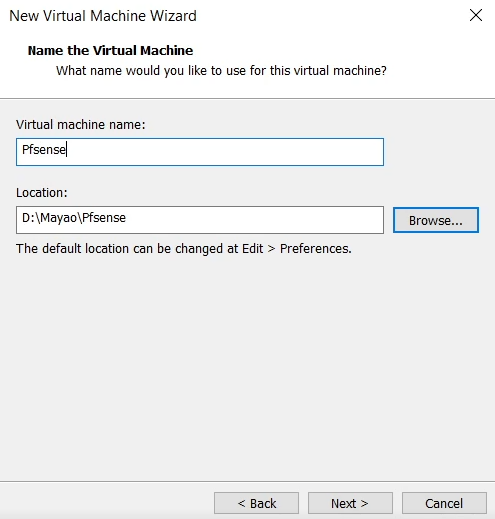
Bước 3: Tạo 1 máy ảo mới ( New Virtual Machine Wizard (Ctrl+N) ). Chọn “**Custom**” -> “**Next**”



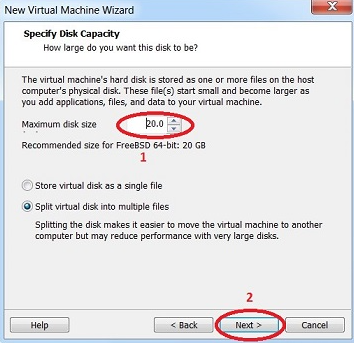
**Browse** tới file pfSense.iso download ở trên -> click “**Next**”



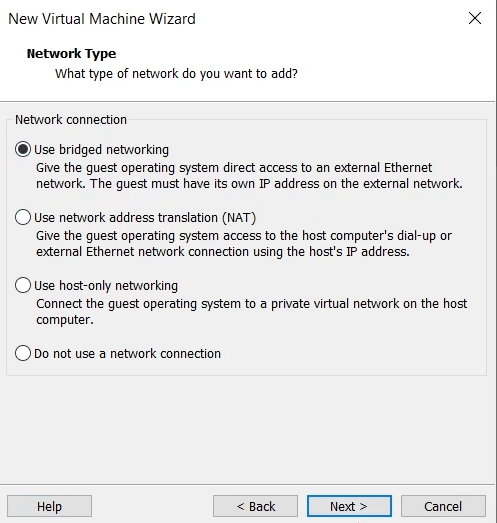
Tạo thư mục chứa máy ảo pfSense -> chọn “Next”



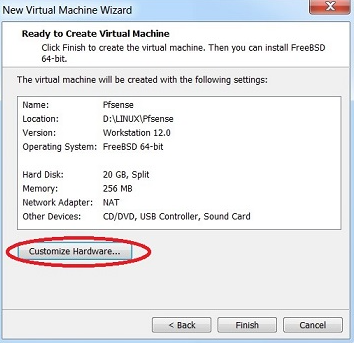
Chọn dung lượng cho máy ảo pfSense -> click **“Next”**



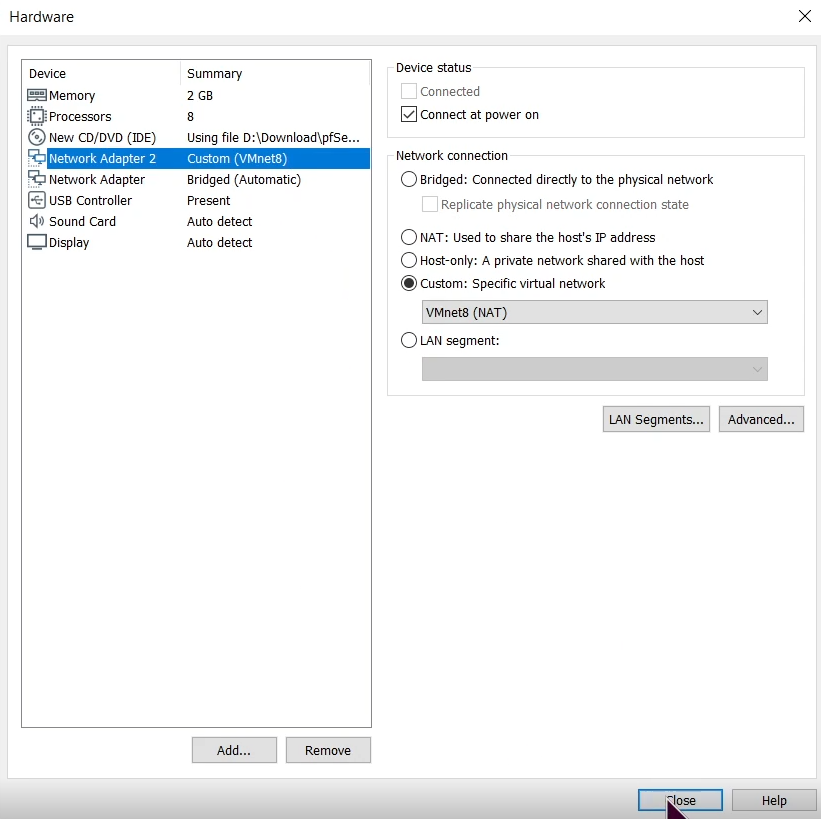
Chọn “**Use bridged networking**” -> Next



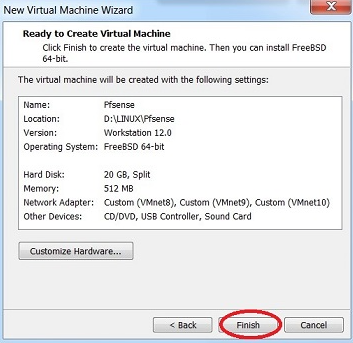
Tiếp tục Next. Chọn “**Customize Hardware**” để thêm card mạng cho máy ảo pfSense



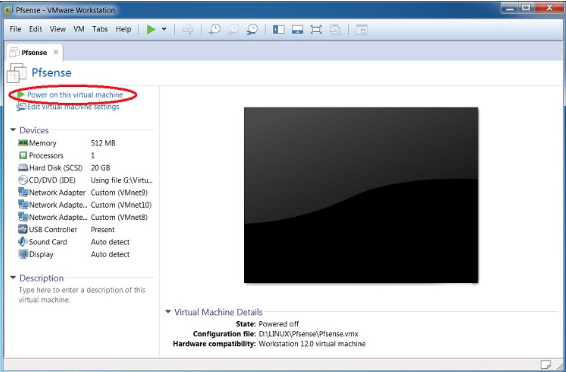
Chọn “Add” và thêm 1 card mạng “VMnet8” cho máy ảo pfSense -> chọn**“Close”**



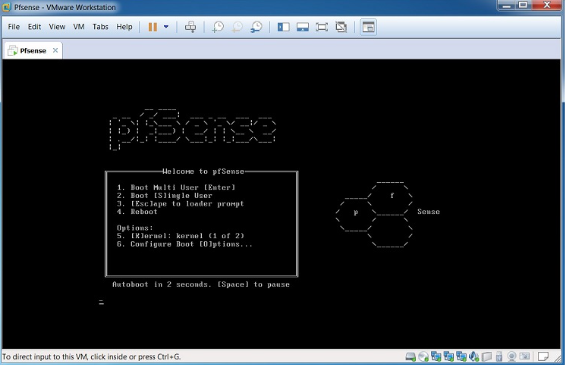
Chọn “**Finished**” để kết thúc quá trình cài đặt pfSense



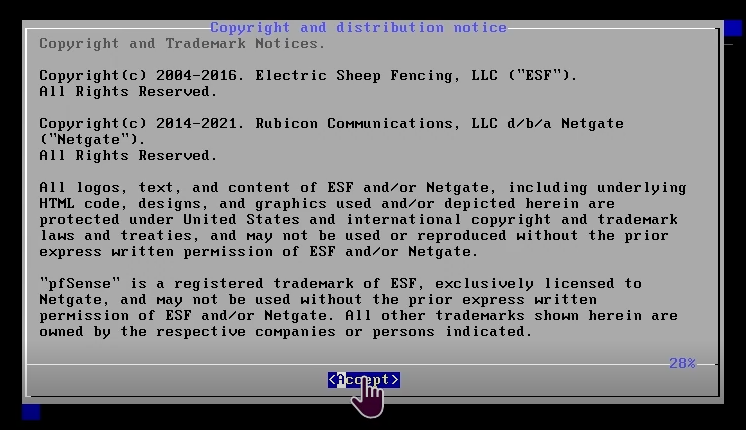
Khởi động để cài đặt máy ảo pfSense



pfSense sẽ tự chọn mode khởi động



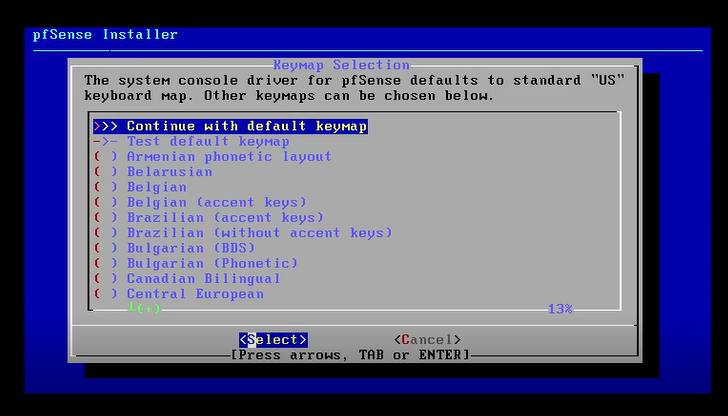
Bấm **Accept**



Bấm OK để Install pfSense



Bấm Select



Bước tiếp theo bấm OK để pfSense cài đặt

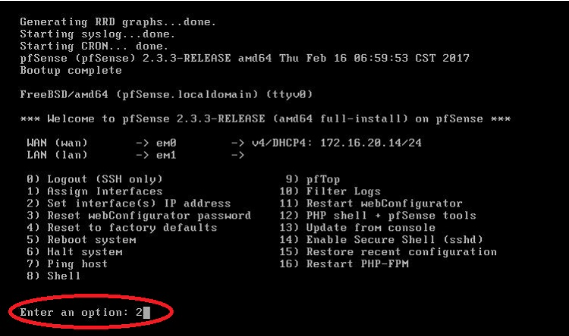


Bước cuối bấm No rồi Reboot lại hệ thống

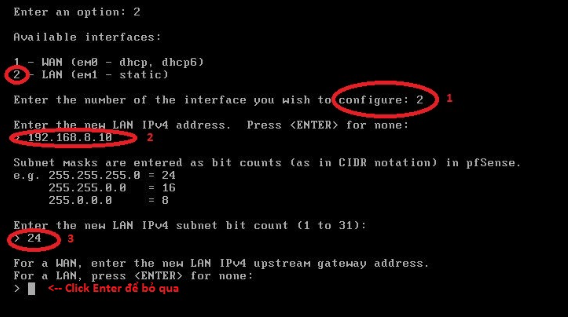




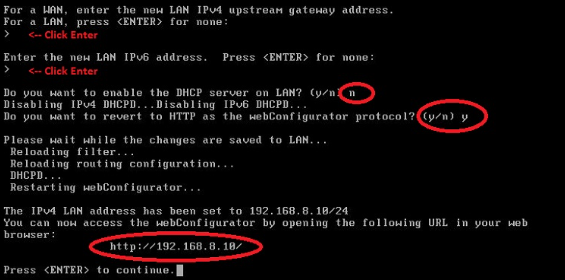
Khởi động lại pfSense. Tại mục menu chọn “**option : 2**” để thiết lập IP address cho interface LAN



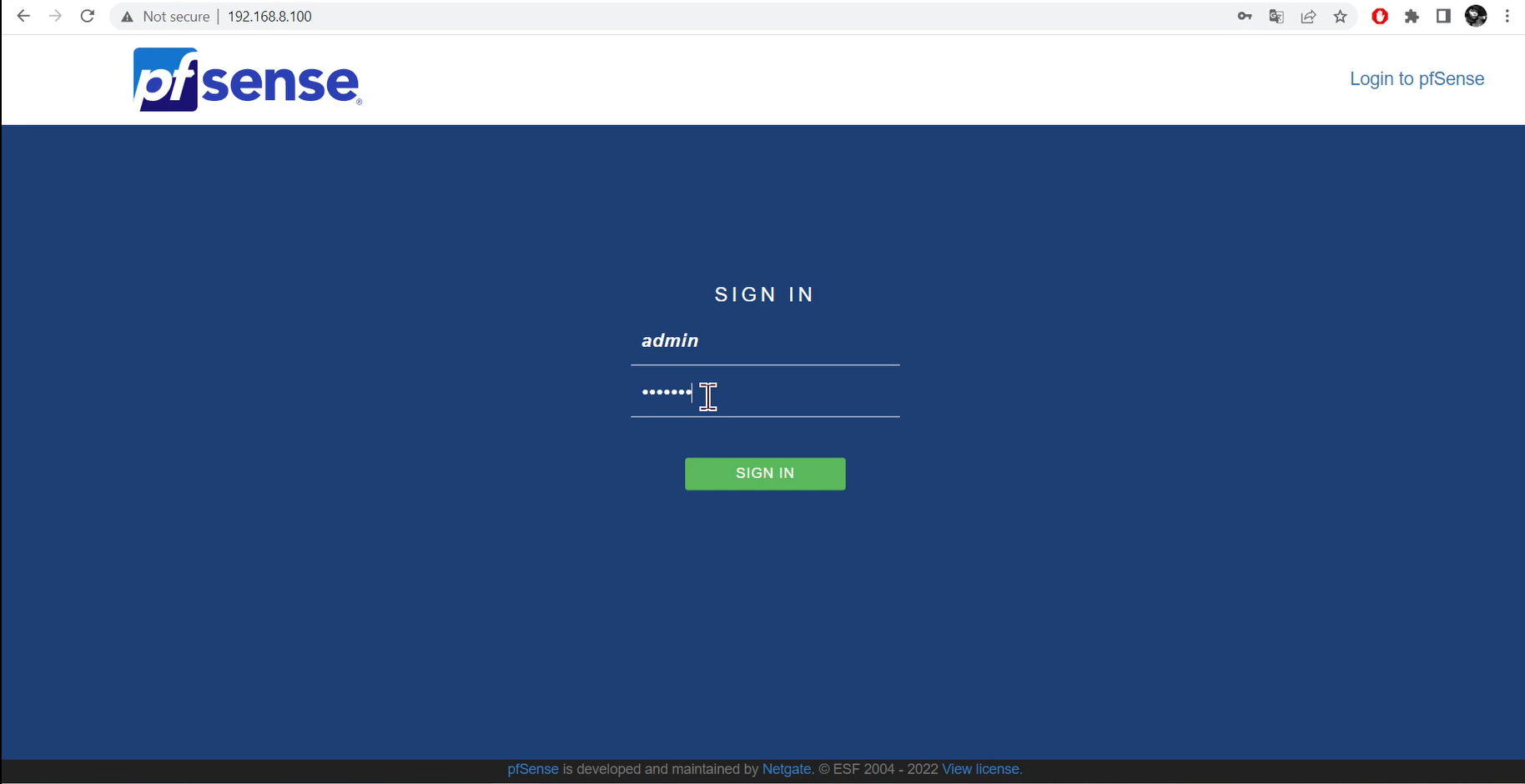
Chọn “**2 – LAN interface**” -> thiết lập ip address: **192.168.8.100** -> subnetmask:**24** -> và **Click Enter**



Phần IPv6 “**Click Ente**r ” 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://192.168.8.10**](http://192.168.8.10)**0**

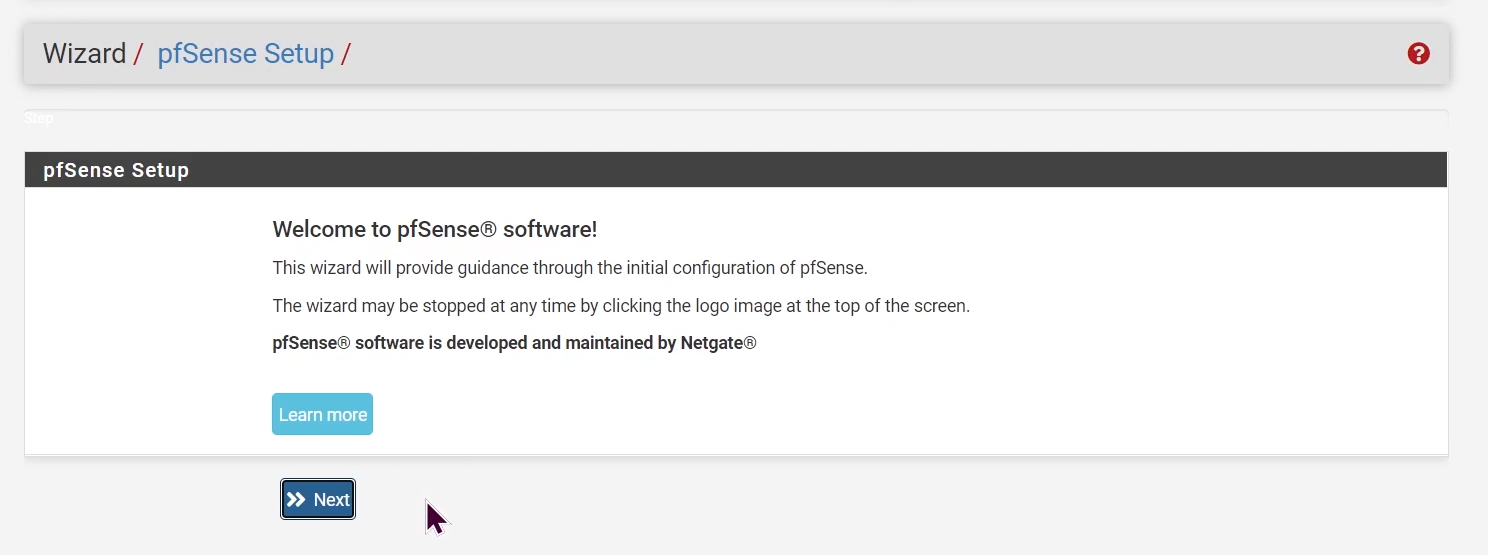


Truy cập pfSense trên trình duyệt web**http://192.168.8.100** . Đăng nhập với username: **admin**& password: **pfsense**

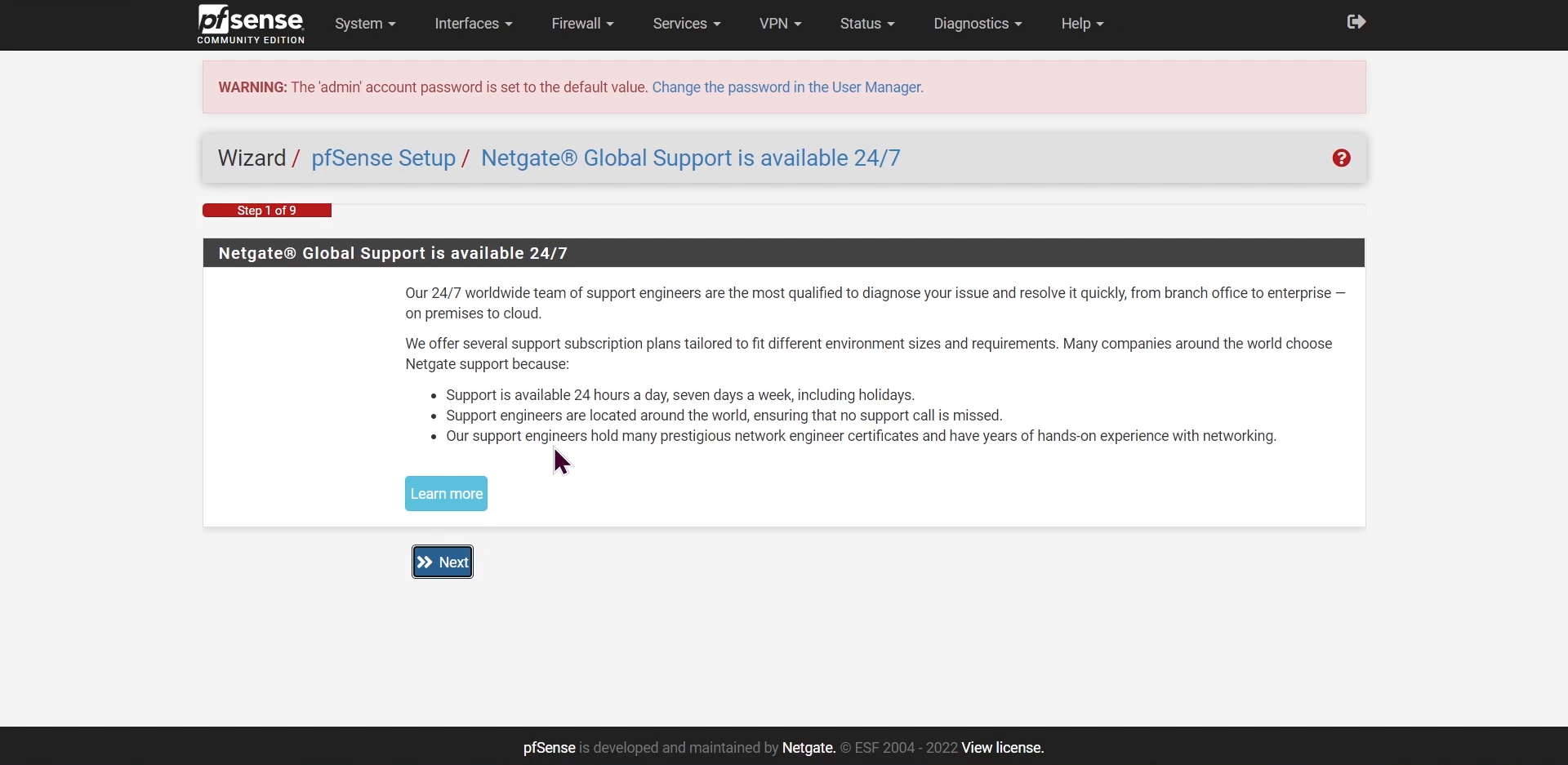


Cài đặt các thông số cơ bản Hostname, Domain, DNS Server, Disable DNS Forwarder, timezone… cho pfSense -> “**Save**”

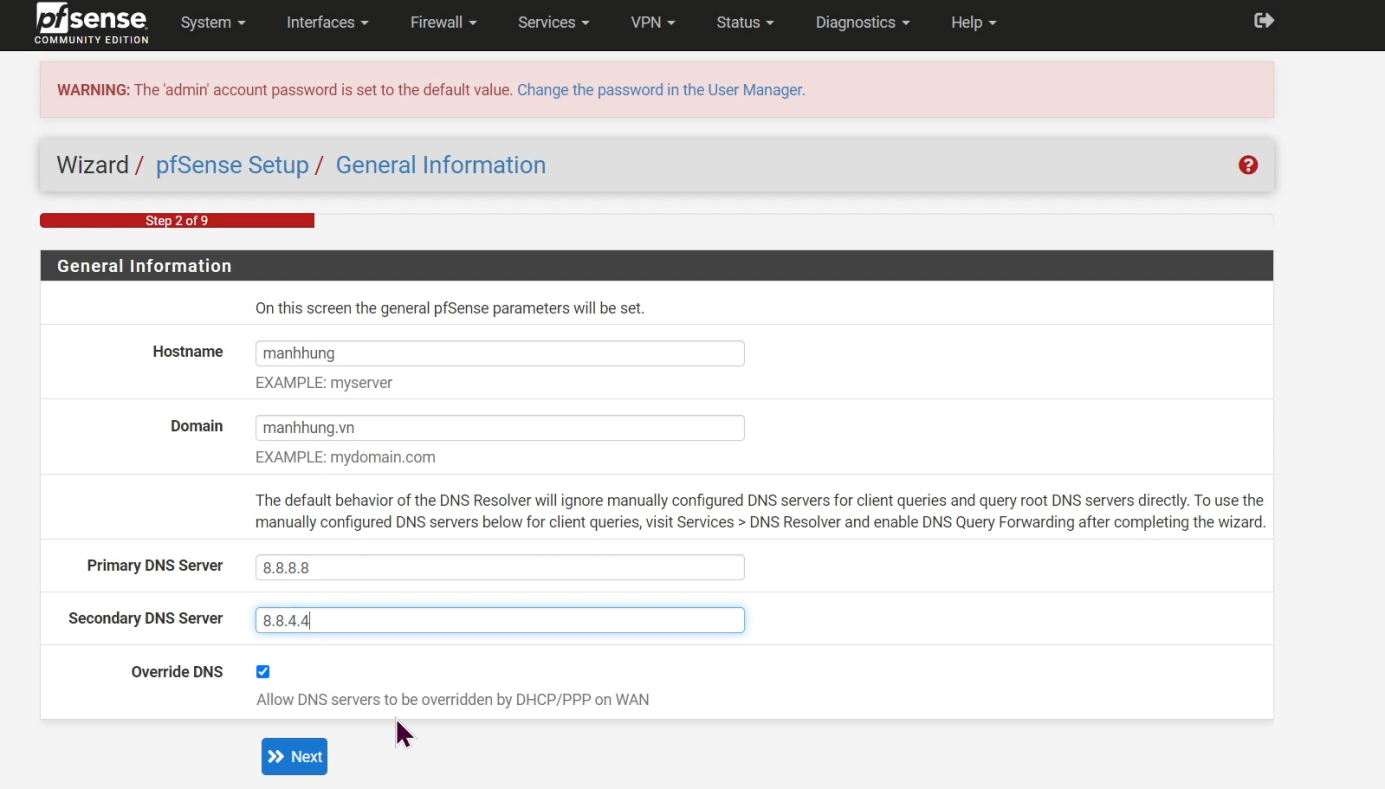
Bấm Next tại màn hình Wizard đầu tiên sau khi đăng nhập



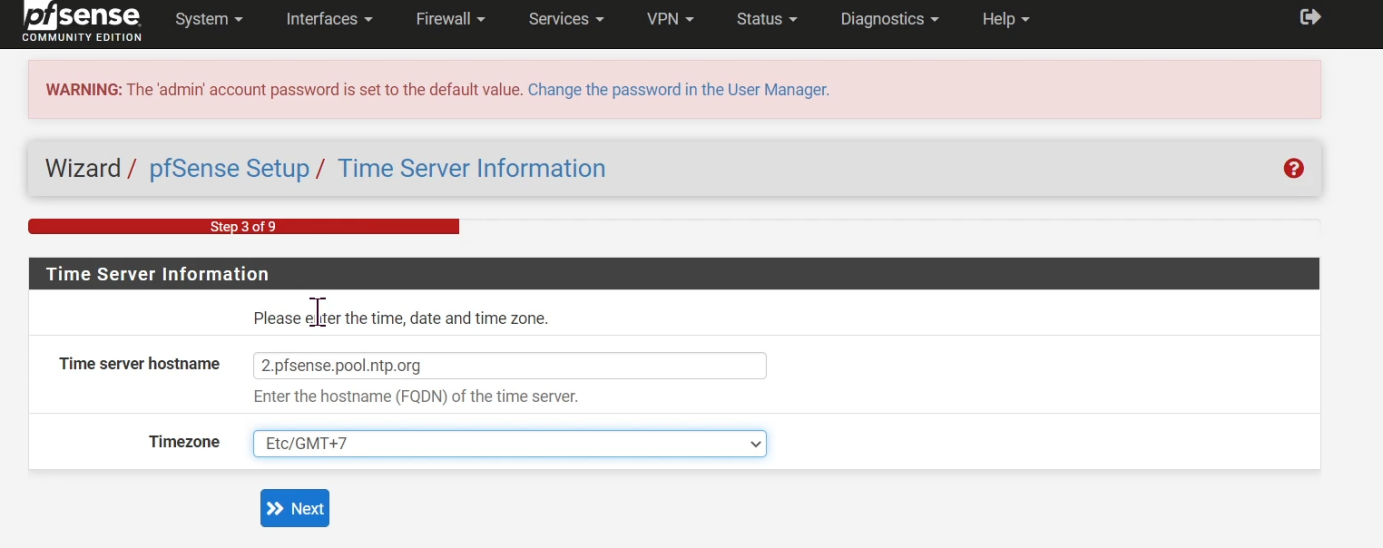
Step 1 of 9 : Bấm Next



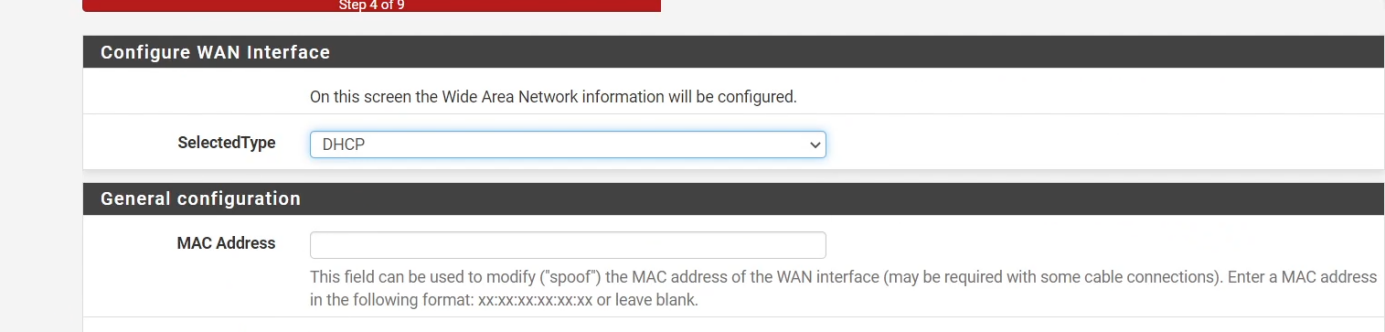
Khai báo Hostname , domain … rồi bấm Next



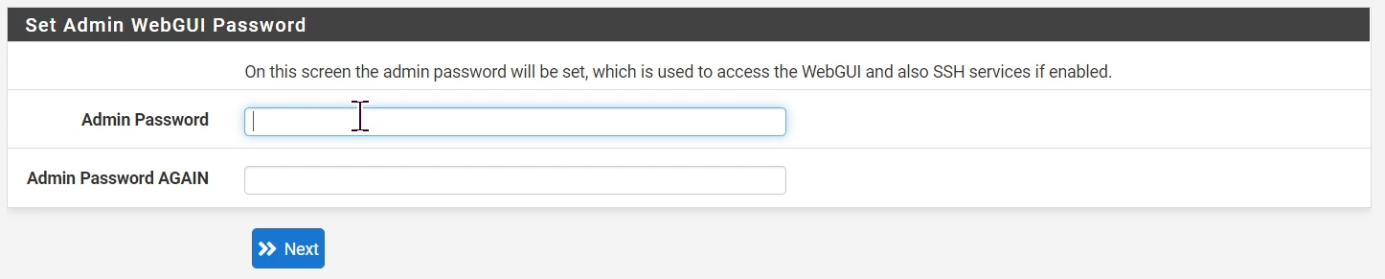
TimeZone là GMT+7



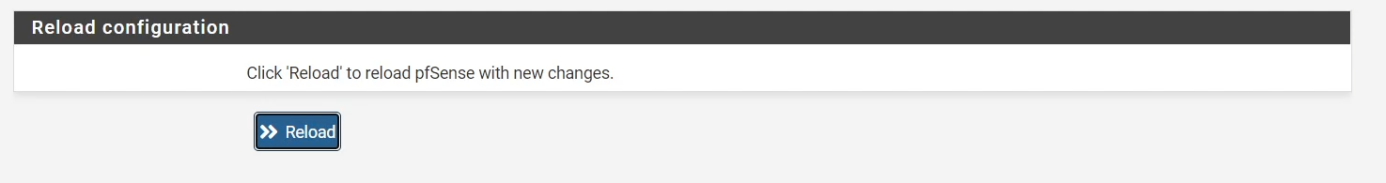
Chọn DHCP tại phần này -> Next



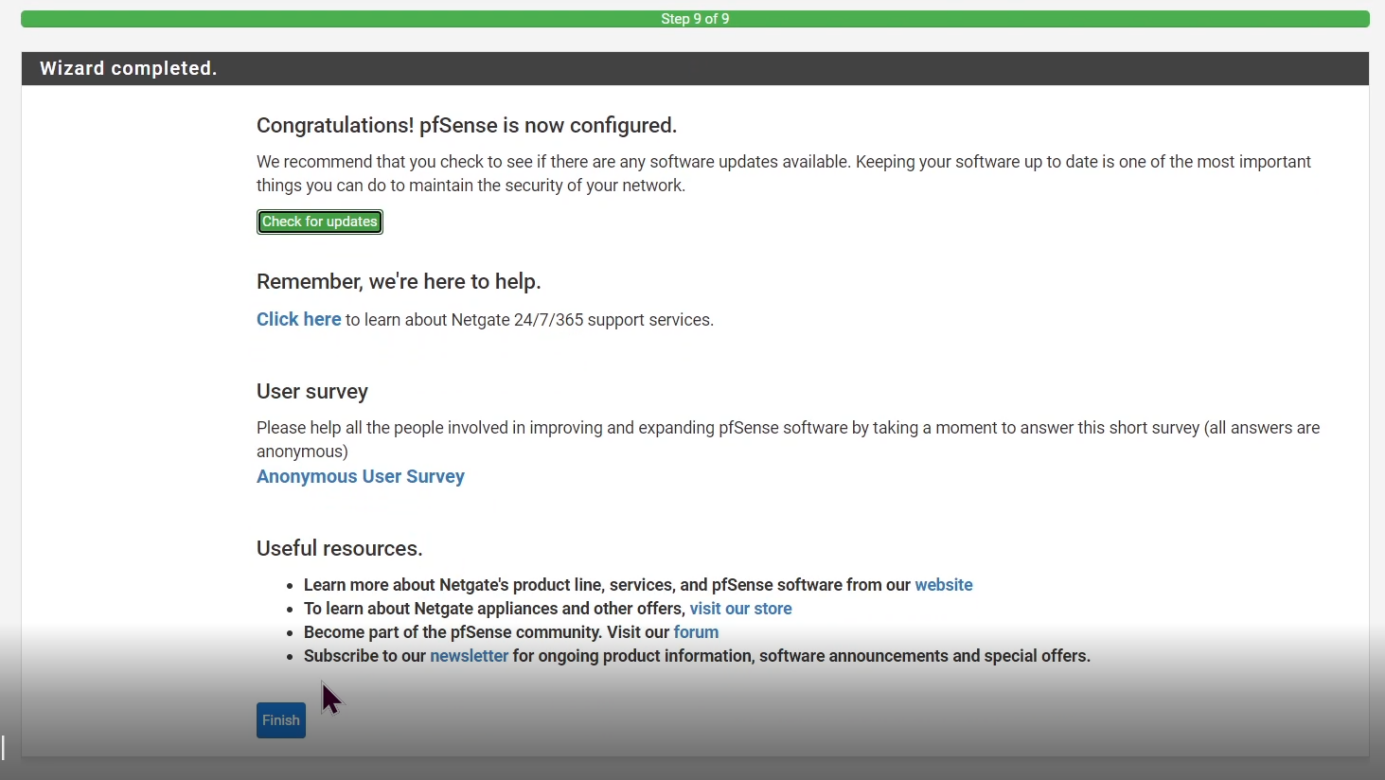
Đặt lại password cho admin -> Next



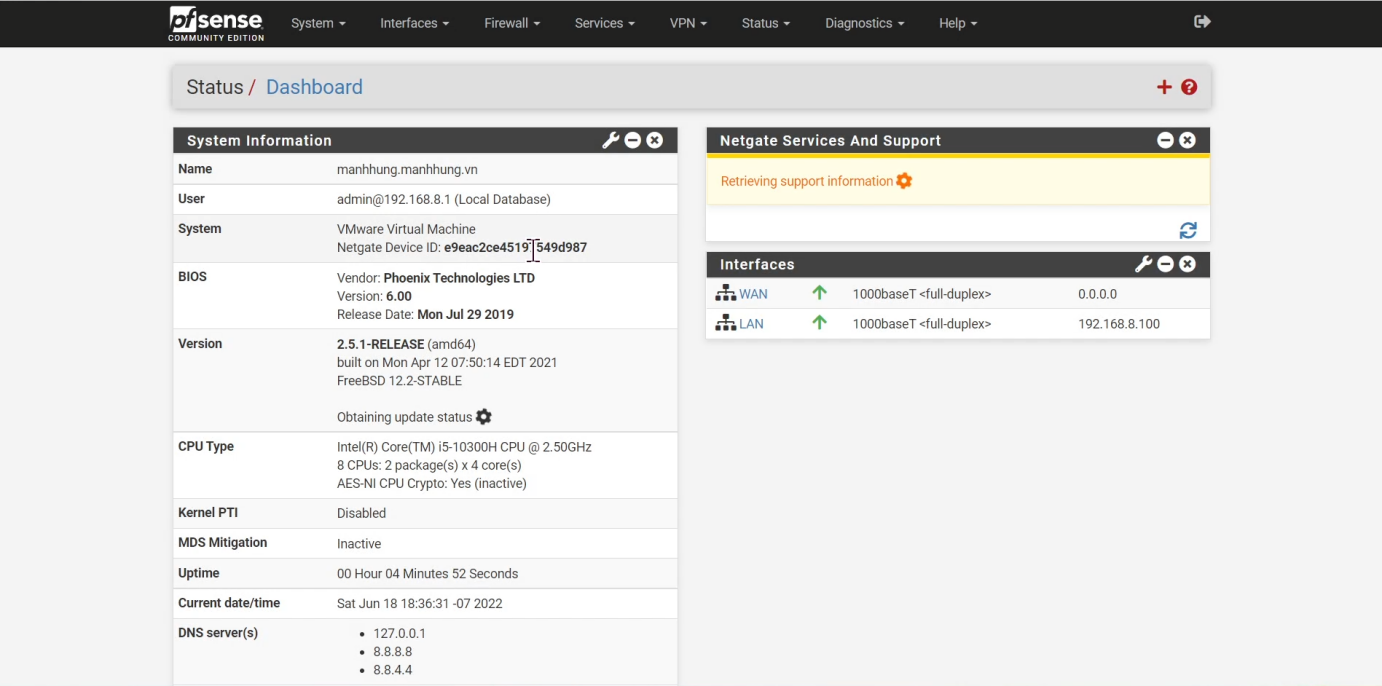
Chọn Reload



Chọn Finish



Sau khi vào được Dasboard là đã cài đặt thành công FireWall PfSense



# CHƯƠNG 4: TỔNG KẾT

## 4.1 Kết quả đạt được

- Hiểu được cách hoạt động của FireWall.

- Đã cài đặt được thành công PfSense trên máy ảo VMWare.

- Tìm hiểu được các chức năng cơ bản của PfSense.

## 4.2 Kết quả chưa đạt được

- Chưa cài đặt được các chức năng khác của PfSense.

- Chưa tìm hiểu sâu được các chức năng khác của PfSense.

# TÀI LIỆU THAM KHẢO

[1] <https://mdungblog.wordpress.com/2018/07/23/huong-dan-cai-dat-pfsense-tren-vmware-part-i/>

[2] <https://mdungblog.wordpress.com/2018/07/23/huong-dan-cai-dat-pfsense-tren-vmware-part-ii/>

[3] <https://www.youtube.com/watch?v=MtrgYptwS7M>

[4] https://www.pfsense.org/download/