

TRƯỜNG CAO ĐẲNG CÔNG NGHỆ THỦ ĐỨC
KHOA CÔNG NGHỆ THÔNG TIN



ĐỒ ÁN MÔN HỌC
TRUYỀN THÔNG KHÔNG DÂY

Đề Tài:

Thiết Kế Hệ Thống WiFi Marketing

Giáo viên hướng dẫn: CAO TRẦN THÁI ANH
Sinh viên thực hiện: NGUYỄN PHƯỚC BÌNH
NGUYỄN TRUNG THÀNH
NGUYỄN HOÀNG TUẤN
TRẦN MẠNH DUY

Lớp: CD22TM1

Khoa: 2022 – 2025

TP. HCM, tháng 4 năm 2024

Lời mở đầu

Trong thế giới kinh doanh ngày nay, sự kết nối và tiếp cận khách hàng đóng vai trò quan trọng trong việc xây dựng và phát triển một doanh nghiệp thành công. Trước sự thay đổi nhanh chóng của công nghệ, việc áp dụng các phương tiện tiếp thị hiệu quả là bước cần thiết để tạo ra một lợi thế cạnh tranh. Trong tập trung này, hệ thống WiFi Marketing đã nổi lên như một công cụ đặc biệt quan trọng, mang lại cho doanh nghiệp cơ hội tối ưu hóa việc tương tác với khách hàng.

Hệ thống này không chỉ là một phương tiện cung cấp dịch vụ internet, mà còn là một cầu nối tương tác giữa doanh nghiệp và khách hàng. Với sự tích hợp công nghệ WiFi, nó cho phép doanh nghiệp tạo ra một môi trường kết nối không dây, mở ra cơ hội để tương tác trực tiếp với khách hàng tại điểm bán hàng từ việc cung cấp thông tin quảng cáo, khuyến mãi đến việc thu thập dữ liệu và phản hồi từ khách hàng.

Trong phạm vi của đồ án “**Thiết kế hệ thống WiFi Marketing**” này, chúng em sẽ giới thiệu khái niệm và cách triển khai một hệ thống hoàn chỉnh giúp doanh nghiệp có được một chiến lược tiếp thị sáng tạo, khai thác mạng WiFi miễn phí như kênh truyền thông hiệu quả để thu hút và giữ chân khách hàng.

Nhóm chúng em xin chân thành cảm ơn thầy Cao Trần Thái Anh – trưởng bộ môn Truyền Thông và Mạng máy tính, khoa Công nghệ thông tin trường Cao Đẳng Công nghệ Thủ Đức – đã hướng dẫn nhiệt tình và giúp đỡ nhóm em hoàn thiện bài đồ án này. Do hạn chế về mặt kiến thức và tài liệu nên đồ án sẽ không tránh khỏi thiếu sót. Vì vậy nhóm em rất mong được sự góp ý chân thành từ phía thầy cô và các bạn thông qua email: 2221ITM0007@mail.tdc.edu.vn.

Chúng em xin chân thành cảm ơn!

MỤC LỤC

CHƯƠNG 1. TỔNG QUAN VỀ WIFI MARKETING.....	5
1.1. Giới thiệu về WiFi Marketing.....	5
1.1.1. WiFi Marketing là gì ?.....	5
1.1.2. WiFi Marketing hoạt động như thế nào?	5
1.1.3. Ưu điểm và nhược điểm của WiFi Marketing.....	6
1.2. Mô hình hoạt động	7
1.2.1. Radius Server.....	7
1.2.2. Captive Portal	8
1.2.3. pfSense.....	9
1.3. Lợi ích của WiFi Marketing.....	10
1.3.1. Đối với khách hàng.....	10
1.3.2. Đối với doanh nghiệp	11
1.3.3. Truyền tải thông điệp nhanh chóng	11
1.3.4. Thu hút khách hàng tìm hiểu sản phẩm.....	11
1.3.5. Hỗ trợ xây dựng cơ sở dữ liệu khách hàng.....	12
1.3.6. Tối ưu hóa các hoạt động Marketing khác	12
1.4. Các sản phẩm chuyên dụng.....	12
1.4.1. Mikrotik	12
1.4.2. DrayTek	13
1.4.3. Unifi	14
1.4.4. TP-Link.....	15
CHƯƠNG 2. TRIỂN KHAI MÔ HÌNH WIFI MARKETING	18
2.1. Mô Hình Thực Hiện.....	18
2.2. Cài Đặt Tường Lửa Pfsense	18

2.3. Cấu hình Captive Portal	32
2.4. Cấu hình RADIUS server	37
2.5. Cấu hình RADIUS	41

NỘI DUNG PHÂN CÔNG

Thành viên	Mô tả công việc
Nguyễn Phước Bình (nhóm trưởng)	<ul style="list-style-type: none"> - Tìm hiểu và demo Captive Portal trên pfSense. - Trình bày mô hình hoạt động của hệ thống WiFi Marketing.
Nguyễn Hoàng Tuấn	<ul style="list-style-type: none"> - Tìm hiểu khái niệm WiFi Marketing, giới thiệu ưu và nhược điểm. - Viết báo cáo Word phần giới thiệu mô hình.
Nguyễn Trung Thành	<ul style="list-style-type: none"> - Tìm hiểu và trình bày các sản phẩm chuyên dụng trong hệ thống. - Trình bày báo cáo Word phần giới thiệu sản phẩm.
Trần Mạnh Duy	<ul style="list-style-type: none"> - Tìm hiểu về lợi ích của WiFi Marketing đối với doanh nghiệp. - Tìm hiểu và kết nối RADIUS Server với Captive Portal.

CHƯƠNG 1. TỔNG QUAN VỀ WIFI MARKETING

1.1. Giới thiệu về WiFi Marketing

1.1.1. WiFi Marketing là gì ?

WiFi Marketing là một hình thức tiếp thị và quảng cáo thông qua mạng lưới sóng WiFi. Khi người dùng muốn truy cập Internet miễn phí tại một địa điểm nào đó, họ sẽ phải tương tác với nội dung quảng cáo của doanh nghiệp để có thể kết nối. WiFi Marketing giúp doanh nghiệp truyền tải thông điệp thương hiệu, sản phẩm, dịch vụ hoặc chương trình khuyến mãi đến khách hàng một cách trực tiếp và hiệu quả.

1.1.2. WiFi Marketing hoạt động như thế nào?



- Khách hàng đến địa điểm cung cấp WiFi miễn phí và chọn mạng WiFi của doanh nghiệp.
- Khách hàng được yêu cầu kết nối WiFi bằng cách truy cập trang đăng nhập.
- Trên trang đăng nhập, khách hàng sẽ thấy logo, slogan và thông tin về thương hiệu của doanh nghiệp.
- Khách hàng có thể được yêu cầu cung cấp thông tin cá nhân, bao gồm tên, email, số điện thoại, v.v. để đổi lấy kết nối WiFi miễn phí.
- Sau khi kết nối WiFi thành công, khách hàng có thể truy cập internet và sử dụng các dịch vụ online.
- Doanh nghiệp có thể hiển thị banner quảng cáo, voucher giảm giá hoặc các nội dung khuyến mãi khác trên trang chuyển hướng hoặc trong quá trình khách hàng sử dụng WiFi, thu hút sự chú ý và khuyến khích khách hàng tham gia vào các hoạt động marketing của doanh nghiệp.

1.1.3. Ưu điểm và nhược điểm của WiFi Marketing

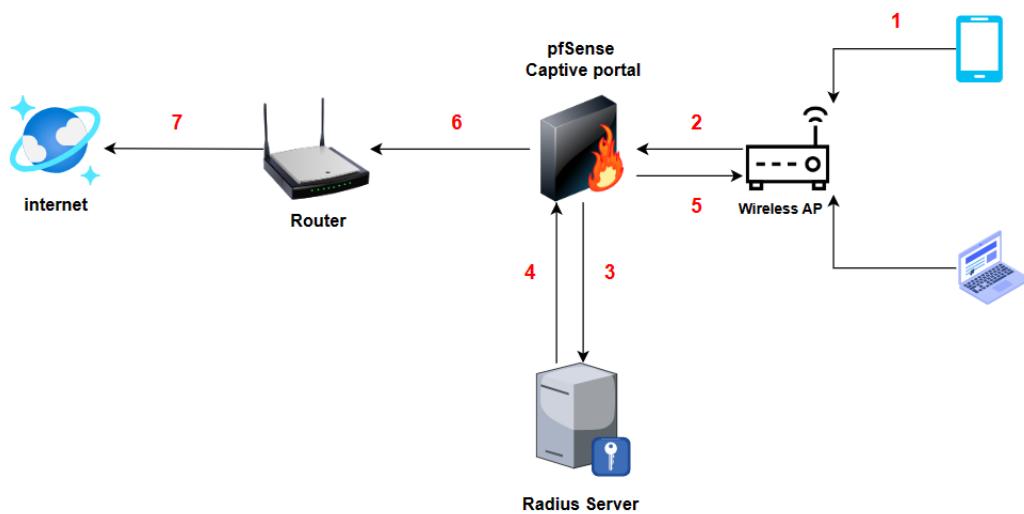
Ưu điểm:

- **Hiệu quả quảng cáo cao và tiết kiệm chi phí:** WiFi Marketing giúp doanh nghiệp truyền tải thông điệp thương hiệu hoặc nội dung trực tiếp đến khách hàng tiềm năng hoặc người dùng gần điểm phát WiFi. Khách hàng sẽ phải tương tác với quảng cáo để có thể truy cập Internet miễn phí, do đó tăng khả năng nhận biết và nhớ thương hiệu. Chi phí cho WiFi Marketing cũng thấp hơn so với các hình thức quảng cáo truyền thống khác.
- **Giúp doanh nghiệp giữ chân khách hàng và tăng doanh số:** WiFi Marketing tạo ra sự thuận tiện và hài lòng cho khách hàng khi sử dụng WiFi miễn phí tại các cơ sở kinh doanh. Đồng thời, doanh nghiệp có thể gửi các chương trình khuyến mãi, ưu đãi, sản phẩm mới... để kích thích khách hàng mua hàng hoặc tái sử dụng dịch vụ.
- **Hỗ trợ xây dựng dữ liệu khách hàng:** WiFi Marketing cho phép doanh nghiệp thu thập được các thông tin như email, số điện thoại, giới tính, tuổi... của khách hàng khi họ đăng nhập WiFi. Những dữ liệu này có thể giúp doanh nghiệp phân tích và phân loại khách hàng, từ đó đưa ra các chiến lược marketing phù hợp và hiệu quả hơn.

Nhược điểm:

- **Triển khai phức tạp và chi phí cao cho nhiều địa điểm:** WiFi Marketing đòi hỏi doanh nghiệp phải có thiết bị và phần mềm hỗ trợ, cũng như cấu hình và quản lý nội dung quảng cáo. Nếu doanh nghiệp muốn áp dụng WiFi Marketing cho nhiều địa điểm khác nhau, như các cửa hàng trong cùng một chuỗi, thì sẽ gặp nhiều khó khăn và tốn kém hơn.
- **Gây phiền nhiễu cho khách hàng:** Một số khách hàng có thể cảm thấy bị làm phiền hoặc khó chịu khi phải xem quảng cáo để truy cập WiFi. Họ có thể quyết định không sử dụng WiFi hoặc sử dụng các lựa chọn khác không yêu cầu xem quảng cáo.

1.2. Mô hình hoạt động



1.2.1. Radius Server

Radius Server (Remote Authentication Dial-In User Service Server) là một máy chủ sử dụng giao thức RADIUS để xác thực và ủy quyền cho người dùng truy cập vào mạng hoặc các dịch vụ khác.

Cách thức hoạt động:

1. Thiết bị mạng (như router, switch, VPN) gửi yêu cầu xác thực đến Radius Server.
2. Radius Server kiểm tra thông tin đăng nhập của người dùng (tên người dùng, mật khẩu) trong cơ sở dữ liệu của nó hoặc gửi yêu cầu đến một máy chủ khác (như LDAP, Active Directory).
3. Nếu thông tin đăng nhập hợp lệ, Radius Server sẽ gửi phản hồi ủy quyền cho thiết bị mạng.
4. Thiết bị mạng cho phép hoặc từ chối truy cập của người dùng dựa trên phản hồi từ Radius Server.

Lợi ích:

- **Quản lý tập trung:** Dễ dàng quản lý tài khoản người dùng từ một nơi.
- **Bảo mật:** Cung cấp xác thực và ủy quyền mạnh mẽ hơn so với các phương pháp truyền thống.
- **Khả năng mở rộng:** Hỗ trợ số lượng lớn người dùng và thiết bị.

- **Tính linh hoạt:** Hỗ trợ nhiều loại thiết bị và dịch vụ.

Ứng dụng:

- **Mạng WiFi công cộng / WiFi marketing:** Cung cấp truy cập WiFi cho khách hàng trong quán cà phê, nhà hàng, khách sạn, sân bay,...
- **Mạng doanh nghiệp:** Kiểm soát truy cập vào mạng nội bộ của công ty.
- **VPN:** Xác thực người dùng truy cập VPN.

1.2.2. Captive Portal

Captive Portal là một trang web bắt buộc người dùng phải đăng nhập hoặc thực hiện hành động cụ thể trước khi được phép truy cập internet. Nó hoạt động như một cổng kết nối thông minh, mang đến nhiều lợi ích cho việc quản lý và bảo mật mạng WiFi.

Cách hoạt động:

1. **Kết nối WiFi:** Khi người dùng kết nối với mạng WiFi được cài đặt Captive Portal, họ sẽ tự động được chuyển hướng đến trang web đăng nhập.
2. **Xác thực:** Người dùng cần nhập thông tin đăng nhập (tên người dùng, mật khẩu, voucher, mã PIN...) hoặc thực hiện hành động yêu cầu (xem quảng cáo, like fanpage...) để được phép truy cập internet.
3. **Chuyển hướng:** Sau khi xác thực thành công, người dùng sẽ được chuyển hướng đến trang web mong muốn hoặc được cấp quyền truy cập internet đầy đủ.

Lợi ích:

- **Kiểm soát truy cập:** Cho phép bạn hạn chế người dùng truy cập mạng WiFi, chỉ cho phép những người có quyền truy cập hợp lệ.
- **Bảo mật mạng:** Tăng cường bảo mật mạng WiFi bằng cách ngăn chặn truy cập trái phép và giảm nguy cơ tấn công mạng.
- **Marketing:** Hiển thị quảng cáo, thông tin marketing hoặc yêu cầu người dùng like fanpage để thu hút khách hàng tiềm năng.
- **Thu thập dữ liệu:** Thu thập thông tin về người dùng như địa chỉ IP, thời gian truy cập, trang web truy cập... để phục vụ cho mục đích marketing hoặc phân tích hành vi người dùng.

- **Quản lý băng thông:** Giới hạn băng thông cho từng người dùng hoặc nhóm người dùng để đảm bảo sự công bằng và hiệu quả trong việc sử dụng mạng WiFi.

Ứng dụng:

- **Mạng WiFi công cộng:** Captive Portal được sử dụng rộng rãi trong các mạng WiFi công cộng như quán cà phê, nhà hàng, khách sạn, sân bay... để kiểm soát truy cập, bảo mật mạng và thu thập dữ liệu.
- **Mạng doanh nghiệp:** Captive Portal có thể được sử dụng trong mạng WiFi của doanh nghiệp để tăng cường bảo mật, kiểm soát truy cập và quản lý băng thông.
- **Hội nghị, sự kiện:** Captive Portal có thể được sử dụng để cung cấp WiFi cho khách tham dự hội nghị hoặc sự kiện, đồng thời thu thập thông tin đăng ký hoặc hiển thị thông tin quảng cáo.

1.2.3. pfSense

pfSense là một hệ thống phần mềm mã nguồn mở được sử dụng để tạo tường lửa và bộ định tuyến cho mạng máy tính. Trong mô hình WiFi marketing, pfSense đóng vai trò quan trọng trong việc:

1.2.3.1. Cài đặt captive portal

Với pfSense, bạn có thể dễ dàng cài đặt captive portal với nhiều tùy chỉnh, bao gồm:

- **Giao diện đăng nhập:** Tùy chỉnh giao diện đăng nhập với logo, màu sắc và thông tin thương hiệu của bạn.
- **Phương thức xác thực:** Hỗ trợ nhiều phương thức xác thực như đăng nhập bằng mật khẩu, voucher, mạng xã hội, email, v.v.
- **Quyền truy cập:** Giới hạn băng thông, thời gian truy cập và các trang web mà người dùng có thể truy cập.
- **Quảng cáo:** Hiển thị quảng cáo, video hoặc thông tin marketing đến người dùng khi họ đăng nhập hoặc sử dụng WiFi.

1.2.3.2. Quản lý băng thông

pfSense cho phép bạn giới hạn băng thông cho từng người dùng hoặc nhóm người dùng, đảm bảo sự công bằng và hiệu quả trong việc sử dụng WiFi.

Bạn có thể đặt giới hạn băng thông tải lên và tải xuống, ưu tiên các ứng dụng quan trọng và hạn chế các hoạt động ngắn băng thông như tải file, xem video HD.

1.2.3.3. Theo dõi và phân tích dữ liệu

pfSense cung cấp các công cụ để theo dõi và phân tích dữ liệu sử dụng WiFi, bao gồm:

- **Số lượng người dùng:** Theo dõi số lượng người dùng truy cập WiFi theo thời gian.
- **Lượng truy cập:** Theo dõi lượng dữ liệu tải lên và tải xuống.
- **Sử dụng ứng dụng:** Theo dõi các ứng dụng nào được sử dụng nhiều nhất trên WiFi.

Dữ liệu này có thể được sử dụng để cải thiện hiệu quả chiến dịch marketing, hiểu rõ hơn về nhu cầu của khách hàng và tối ưu hóa trải nghiệm WiFi.

1.2.3.4. Bảo mật mạng

pfSense là một tường lửa mạnh mẽ giúp bảo vệ mạng WiFi của bạn khỏi các mối đe dọa an ninh mạng như tấn công truy cập trái phép, lừa đảo, mã độc...

Bạn có thể sử dụng các tính năng bảo mật nâng cao như VPN, lọc IP, tường lửa ứng dụng để tăng cường bảo mật cho mạng WiFi.

1.3. Lợi ích của WiFi Marketing

1.3.1. Đối với khách hàng

Lợi ích của WiFi Marketing là tạo sự thuận tiện của khách khi mua hàng. Phần lớn các khách hàng khi đến cửa hàng mua sắm đều có nhu cầu tìm kiếm sản phẩm. Do đó WiFi Marketing sẽ giúp khách tiết kiệm được việc sử dụng dữ liệu di động để truy cập, nhanh chóng trong việc mua sắm.

Ngoài ra để nâng cao trải nghiệm mua sắm và phục vụ khách hàng, WiFi Marketing còn giúp khách hàng cảm thấy thoải mái hơn khi không cần hỏi mật khẩu từ nhân viên. Theo thống kê, có gần 62% doanh nghiệp cho biết khi cửa hàng sử dụng WiFi Marketing khách hàng sẽ ở lại lâu hơn.

Ngày nay, việc sử dụng WiFi để truy cập Internet đã trở thành thói quen của nhiều người. Theo nghiên cứu của Social happiness, 84% người dùng cảm thấy hạnh phúc và thoải mái hơn với việc có WiFi miễn phí để sử dụng. Theo thống kê cho rằng,

việc có WiFi miễn phí khiến mọi người muốn lướt web và dạo quanh các trang thương mại điện tử nhiều hơn để mua hàng và trao đổi mọi thứ. Cho nên WiFi Marketing thực sự rất hữu ích đối với khách hàng và nhu cầu của mọi người.

1.3.2. Đối với doanh nghiệp

Việc sử dụng WiFi Marketing sẽ giúp doanh nghiệp tăng nhận diện thương hiệu với khách hàng. Bởi khi muốn truy cập vào WiFi khách hàng phải xem qua các thông tin từ quảng cáo. Doanh nghiệp sẽ dễ dàng gây ấn tượng hơn với khách hàng nếu khéo léo lồng ghép nội dung hấp dẫn.

Lợi ích tiếp theo từ việc sử dụng WiFi Marketing là thu thập được thông tin khách hàng. Với tâm lý chỉ cần bỏ ra vài giây để nhập thông tin là được sử dụng WiFi miễn phí. Doanh nghiệp có thể thu được tệp khách hàng tiềm năng để nuôi dưỡng và duy trì mối quan hệ với khách hàng.

Do đó, WiFi Marketing là một trong những loại WiFi được ưu tiên khi sử dụng. Có WiFi Marketing sẽ giúp cho khách hàng thoải mái truy cập mà không tốn phí. Hình thức này thường được lắp đặt trong các trung tâm thương mại lớn, quán cà phê...để giúp khách hàng sử dụng WiFi và tìm kiếm sản phẩm mong muốn.

1.3.3. Truyền tải thông điệp nhanh chóng

WiFi Marketing đã trở thành một vũ khí Marketing hiện đại và nhanh chóng với nhiều doanh nghiệp. Hầu hết các chiến dịch Marketing Online ngoài sử dụng các nền tảng như Google, Facebook..để quảng bá thì WiFi Marketing cũng đang là một xu hướng.

Có WiFi Marketing việc tiếp cận khách hàng trở nên dễ dàng và được thoải mái hơn. Thay vì phải sáng tạo nội dung liên tục và phân phối quảng cáo, bạn chỉ cần khách hàng truy cập và thu dữ liệu một cách dễ dàng. Cho nên việc truyền tải thông điệp truyền thông, promotion hay đơn giản là nhận diện thương hiệu cho nhãn hàng đã cực kỳ nhanh chóng.

1.3.4. Thu hút khách hàng tìm hiểu sản phẩm

Đối với doanh nghiệp, việc khiến khách hàng truy cập vào website hay bấm quan tâm là một vấn đề thách thức. Với WiFi Marketing, khi khách hàng truy cập vào để xem quảng cáo và ấn kết nối đây là một trong những bước quan trọng để tiếp cận khách hàng. Nếu thực sự có nhu cầu, khách hàng sẽ tìm hiểu sản phẩm trên các nền

tảng digital và mua hàng hoặc chia sẻ cho bạn bè là người đang có nhu cầu khi sử dụng WiFi.

1.3.5. Hỗ trợ xây dựng cơ sở dữ liệu khách hàng

Sau mỗi phiên truy cập và kết nối vào Internet, việc khách hàng để lại thông tin đã cho doanh nghiệp một kho dữ liệu khổng lồ. Nguồn dữ liệu này rất quan trọng để giúp cho doanh nghiệp khai thác và sử dụng sau này. Điểm mạnh của WiFi Marketing là thu thập dữ liệu, phân tích và khiến doanh nghiệp hiểu rõ hơn về khách hàng của mình.

1.3.6. Tối ưu hóa các hoạt động Marketing khác

Như đã chia sẻ, việc có được dữ liệu khách hàng là điều cực kỳ quan trọng. Khi cơ sở dữ liệu rõ ràng và đầy đủ sẽ khiến các hoạt động Marketing Online hoặc Offline trở nên tối ưu hơn. Lấy ví dụ về chiến dịch Marketing Online, khi có rõ chân dung khách hàng doanh nghiệp chỉ cần sản xuất nội dung đúng mục tiêu chiến dịch và phân bổ target phù hợp hoặc remarketing các khách hàng đã tương tác trước đó để tối ưu về mặc chi phí.

1.4. Các sản phẩm chuyên dụng

1.4.1. Mikrotik

MikroTik là một công ty công nghệ có trụ sở tại Latvia, chuyên thiết kế và sản xuất phần cứng mạng và phần mềm mạng. Công ty được biết đến nhiều nhất qua sản phẩm RouterOS – một hệ điều hành mạng linh hoạt – và dòng sản phẩm phần cứng RouterBOARD, bao gồm router, switch và thiết bị không dây. Các sản phẩm của MikroTik phổ biến trong các ứng dụng từ nhà cung cấp dịch vụ internet (ISP), doanh nghiệp nhỏ và trung bình (SMB), đến người tiêu dùng cuối cùng muốn có giải pháp mạng mạnh mẽ và linh hoạt.

Ưu điểm của MikroTik trong WiFi Marketing:

- **Cấu hình linh hoạt:** RouterOS cung cấp khả năng cấu hình linh hoạt, cho phép người dùng tạo ra các trang đăng nhập tùy chỉnh, thu thập dữ liệu khách hàng, và thực hiện các chiến dịch marketing thông qua mạng WiFi.
- **Chi phí hiệu quả:** So với các giải pháp chuyên biệt khác, MikroTik cung cấp một lựa chọn có chi phí hiệu quả với phần cứng và phần mềm mạnh mẽ, phù hợp cho cả doanh nghiệp vừa và nhỏ lẫn các nhà cung cấp dịch vụ lớn.

- **Phần cứng đa dạng:** Dòng sản phẩm RouterBOARD bao gồm nhiều loại thiết bị từ router, switch đến các giải pháp không dây, hỗ trợ mọi nhu cầu từ việc cung cấp WiFi trong nhà hàng, khách sạn, đến các khu phức hợp lớn.
- **Cộng đồng và hỗ trợ:** MikroTik có một cộng đồng lớn và đa dạng với nhiều tài liệu hỗ trợ, diễn đàn, và các khóa học chứng nhận, giúp người dùng dễ dàng tìm kiếm sự hỗ trợ và học hỏi.

Sự khác biệt so với các hãng khác:

- **Phần mềm và phần cứng tích hợp:** Một số hãng cung cấp giải pháp WiFi Marketing chủ yếu tập trung vào phần mềm hoặc là một dịch vụ đám mây. Trong khi đó, MikroTik cung cấp cả phần mềm (RouterOS) lẫn phần cứng (RouterBOARD), cho phép một sự tích hợp chặt chẽ và hiệu quả cao.
- **Tính năng mạng nâng cao:** RouterOS cung cấp một loạt các tính năng mạng nâng cao và linh hoạt hơn hầu hết các giải pháp chuyên biệt về WiFi Marketing, bao gồm định tuyến nâng cao, tường lửa, quản lý băng thông, VPN và nhiều hơn nữa.
- **Tự do cấu hình:** MikroTik cho phép người dùng có khả năng cấu hình hệ thống một cách tùy ý, điều này có thể là một lợi ích lớn cho những người có kỹ thuật và muốn tùy chỉnh hệ thống của mình một cách cụ thể.

1.4.2. DrayTek

DrayTek là một công ty công nghệ hàng đầu chuyên sản xuất và cung cấp các giải pháp mạng và viễn thông tiên tiến. DrayTek nổi tiếng với việc phát triển các sản phẩm mạng chất lượng cao, bao gồm bộ định tuyến (router), bộ điều hợp công truy cập (gateway), bộ chia sẻ tài nguyên mạng và các giải pháp mạng an toàn. Sản phẩm của DrayTek được thiết kế để đáp ứng nhu cầu của các doanh nghiệp và tổ chức với các tính năng mạnh mẽ như bảo mật mạng cao cấp, quản lý mạng linh hoạt, tốc độ truy cập cao và tích hợp nhiều công nghệ mới nhất như IPv6, VPN, VLAN, và nhiều tính năng khác.

Ưu điểm của DrayTek trong WiFi Marketing:

- **Bảo mật cao:** DrayTek nổi tiếng với việc tích hợp các tính năng bảo mật mạnh mẽ vào thiết bị của mình. Điều này bao gồm cả việc quản lý truy cập mạng và

bảo vệ dữ liệu, là điều cực kỳ quan trọng trong bất kỳ chiến dịch WiFi marketing nào để bảo vệ thông tin của khách hàng.

- **Quản lý băng thông:** Các sản phẩm của DrayTek cho phép doanh nghiệp kiểm soát mức độ sử dụng băng thông một cách chi tiết, đảm bảo rằng các dịch vụ quan trọng không bị ảnh hưởng bởi việc tải quá mức từ các hoạt động marketing.
- **Captive portal tùy chỉnh:** DrayTek cung cấp các tùy chọn để thiết lập captive portal, cho phép doanh nghiệp thu thập dữ liệu người dùng và tùy chỉnh trải nghiệm đăng nhập của khách hàng, một tính năng quan trọng cho WiFi marketing.
- **Đa SSID và VLAN hỗ trợ:** Với khả năng tạo ra nhiều SSID và hỗ trợ VLAN, các sản phẩm của DrayTek cho phép tạo các mạng riêng biệt cho khách hàng và hoạt động nội bộ, giúp triển khai các chiến dịch marketing một cách hiệu quả mà không làm ảnh hưởng đến hoạt động kinh doanh chính.

DrayTek so với các hãng khác:

- **Tập trung vào bảo mật và độ tin cậy:** So với các hãng sản xuất thiết bị mạng khác, DrayTek đặc biệt chú trọng vào bảo mật và độ tin cậy, làm cho sản phẩm của họ trở thành lựa chọn tốt cho các doanh nghiệp đặt bảo mật lên hàng đầu.
- **Phần cứng chất lượng cao:** DrayTek nổi tiếng với việc sử dụng các linh kiện chất lượng cao trong sản phẩm của mình, giúp tăng độ bền và độ ổn định trong môi trường doanh nghiệp.
- **Giá cả:** Mặc dù sản phẩm của DrayTek có thể có giá cao hơn so với một số đối thủ cạnh tranh như TP-Link hoặc D-Link, giá cả phản ánh chất lượng và tính năng nâng cao mà họ cung cấp, đặc biệt là trong các yêu cầu mạng doanh nghiệp phức tạp.

1.4.3. Unifi

UniFi là một thương hiệu nổi tiếng trong lĩnh vực thiết bị mạng và giải pháp Wi-Fi. UniFi tập trung vào việc cung cấp các giải pháp mạng tiên tiến cho doanh nghiệp, tổ chức và người dùng cá nhân, với sứ mệnh là tạo ra các sản phẩm mạng linh hoạt, dễ sử dụng và giá cả phải chăng. Các sản phẩm của UniFi bao gồm bộ định tuyến (router), bộ chia mạng (switch), bộ phát sóng Wi-Fi (access point), hệ thống giám sát mạng và các giải pháp mạng an ninh. UniFi nổi tiếng với việc thiết kế sản

phẩm đơn giản nhưng mạnh mẽ, cho phép người dùng dễ dàng triển khai và quản lý mạng một cách hiệu quả.

Ưu điểm của Unifi:

- **Quản lý tập trung:** Phần mềm UniFi Controller cho phép quản lý tập trung toàn bộ mạng WiFi từ một giao diện duy nhất. Điều này giúp dễ dàng triển khai, quản lý và theo dõi hiệu suất mạng, cũng như tùy chỉnh các trang đăng nhập WiFi, mà không cần đến kiến thức chuyên môn cao.
- **Tùy chỉnh trang đăng nhập cá nhân:** UniFi hỗ trợ tùy chỉnh trang đăng nhập hotspot, cho phép các doanh nghiệp tạo ra trải nghiệm đăng nhập WiFi độc đáo, thúc đẩy thương hiệu của họ, và thu thập dữ liệu quan trọng từ khách hàng.
- **Phân tích & báo cáo:** Phần mềm quản lý cung cấp thông tin phân tích sâu rộng và báo cáo về người dùng mạng, giúp doanh nghiệp hiểu rõ hơn về hành vi của khách hàng và tối ưu hóa các chiến dịch marketing của họ.

Unifi so với các hãng khác:

- **Giải pháp thống nhất:** So với các hãng như MikroTik hay Comfast, UniFi cung cấp một giải pháp mạng thống nhất rõ ràng, với phần mềm quản lý tập trung, làm cho việc triển khai và quản lý mạng trở nên dễ dàng và hiệu quả hơn.
- **Giao diện người dùng đồ họa:** UniFi Controller có giao diện đồ họa (GUI) trực quan và dễ sử dụng, giúp người dùng dễ dàng cài đặt và quản lý hệ thống mạng của mình mà không cần nhiều kiến thức chuyên môn. Điều này khác biệt với MikroTik, nơi mà RouterOS có thể cung cấp nhiều tính năng nâng cao hơn nhưng đòi hỏi người dùng phải có kiến thức kỹ thuật cao hơn.
- **Tích hợp dễ dàng:** UniFi dễ dàng tích hợp với các sản phẩm khác trong hệ sinh thái của Ubiquiti, cho phép một hệ thống mạng không dây mạnh mẽ và mở rộng dễ dàng, trong khi các hãng khác có thể không cung cấp một giải pháp thống nhất và tích hợp sâu đến mức này.

1.4.4. TP-Link

TP-Link là một trong những thương hiệu hàng đầu trong lĩnh vực thiết bị mạng và truy cập Internet. TP-Link nhanh chóng trở thành một trong những nhà sản xuất

hàng đầu về các sản phẩm mạng như bộ định tuyến (router), bộ chia mạng (switch), bộ phát sóng Wi-Fi (access point), và các sản phẩm khác liên quan đến mạng, nổi tiếng với việc cung cấp các sản phẩm chất lượng cao, đa dạng về mẫu mã và giá cả phải chăng, phù hợp với cả người dùng gia đình và doanh nghiệp. Các sản phẩm của TP-Link thường được đánh giá cao về độ ổn định, hiệu suất và tính năng tiên tiến.

Với sự cam kết về chất lượng và dịch vụ, TP-Link đã có mặt tại hơn 170 quốc gia và vùng lãnh thổ trên toàn thế giới. Điều này đã giúp TP-Link trở thành một trong những thương hiệu mạng được người tiêu dùng tin cậy và lựa chọn hàng đầu trên thị trường toàn cầu.

Ưu điểm của TP-Link:

- **Phổ cập và dễ tiếp cận:** TP-Link có mặt rộng rãi trên toàn cầu và sản phẩm của họ dễ tìm mua ở nhiều nơi, từ các cửa hàng điện tử đến các trang thương mại điện tử, làm cho việc triển khai giải pháp WiFi cho mục đích marketing trở nên dễ dàng và tiện lợi.
- **Giá cả cạnh tranh:** Các sản phẩm của TP-Link thường có mức giá cạnh tranh, giúp các doanh nghiệp, đặc biệt là các doanh nghiệp nhỏ và vừa, có thể triển khai hoặc mở rộng hệ thống WiFi của mình mà không cần phải đầu tư quá nhiều về mặt tài chính.
- **Dễ dàng cài đặt và quản lý:** TP-Link cung cấp các giải pháp mạng được thiết kế để dễ dàng cài đặt và quản lý, với giao diện người dùng trực quan và hướng dẫn cụ thể. Điều này giúp giảm thiểu rào cản kỹ thuật cho các doanh nghiệp muốn triển khai chiến dịch WiFi marketing.
- **Hỗ trợ Marketing qua WiFi:** Một số sản phẩm của TP-Link hỗ trợ tính năng captive portal, cho phép doanh nghiệp tùy chỉnh trang đăng nhập WiFi, thu thập dữ liệu người dùng và triển khai các chiến dịch marketing mục tiêu.

TP-Link so với các hãng khác:

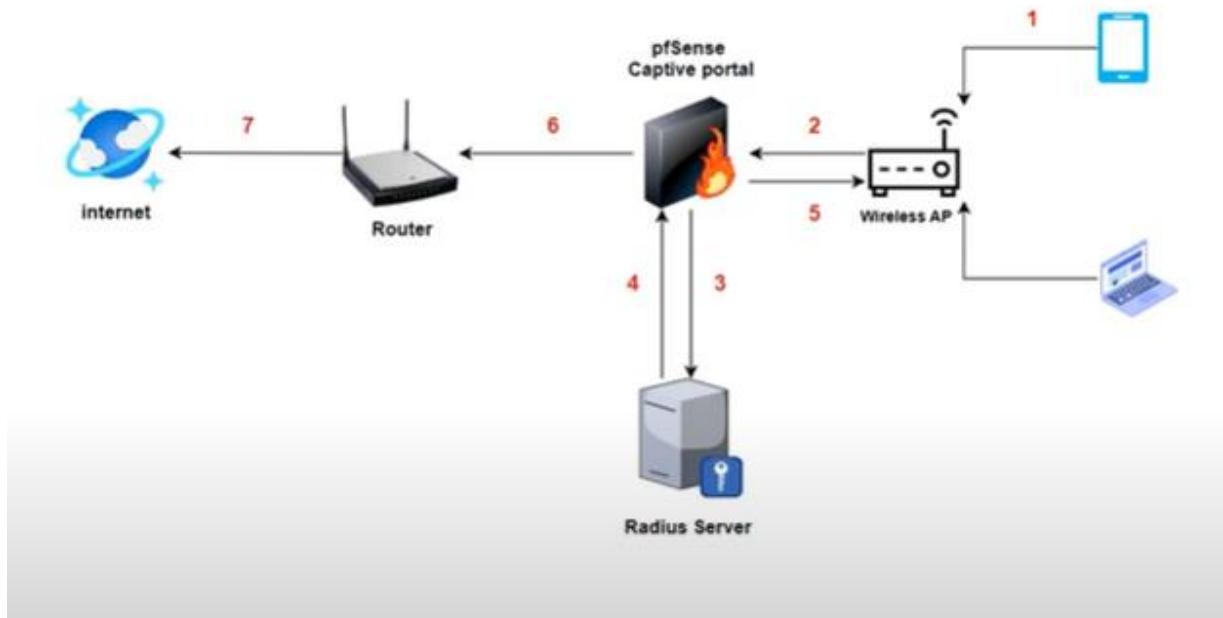
- **Phổ biến và tiếp cận:** So với các thương hiệu chuyên nghiệp như UniFi từ Ubiquiti, TP-Link có lợi thế về mức độ phổ biến và khả năng tiếp cận. Các sản phẩm của TP-Link thường dễ tìm mua hơn ở nhiều quốc gia.
- **Giá thành:** TP-Link thường hướng đến phân khúc giá thấp đến trung bình, làm cho nó trở thành lựa chọn tốt cho các doanh nghiệp với ngân sách hạn chế.

Trong khi đó, các hãng như UniFi có thể đặt hơn nhưng cung cấp giải pháp mạng toàn diện và nâng cao hơn.

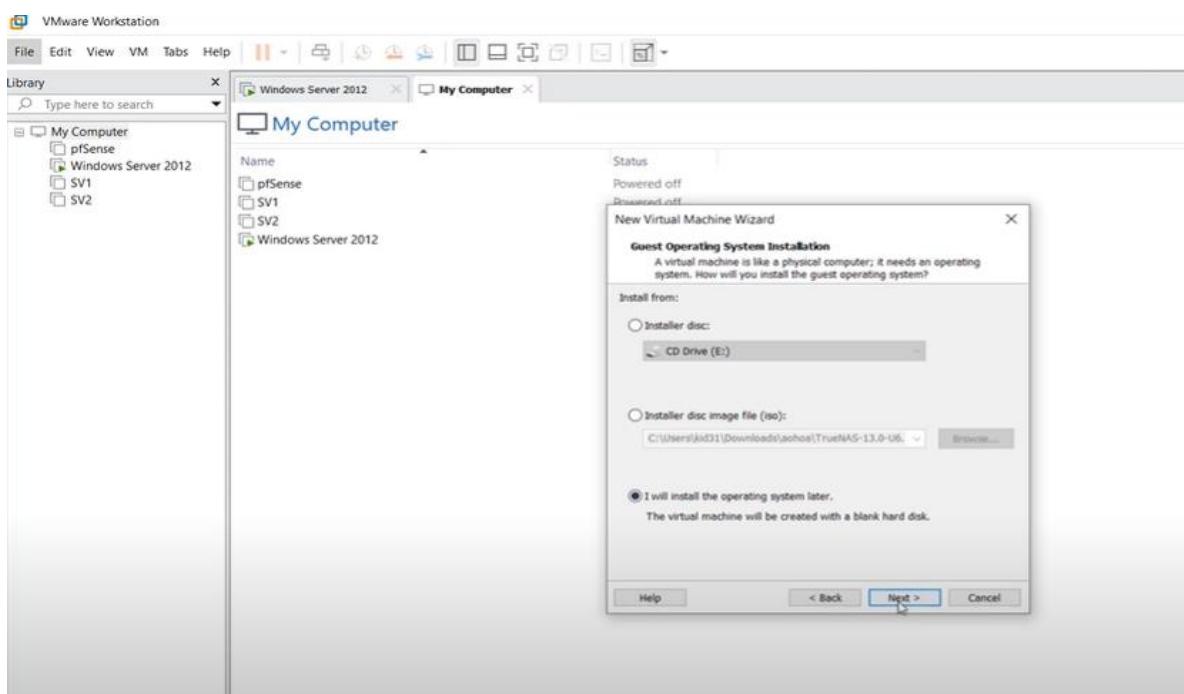
- **Tính năng và độ tin cậy:** Mặc dù TP-Link cung cấp giải pháp dễ dàng triển khai và quản lý, các thương hiệu chuyên nghiệp như UniFi và MikroTik có thể cung cấp nhiều tính năng nâng cao hơn và độ tin cậy cao hơn cho các ứng dụng doanh nghiệp và yêu cầu mạng phức tạp.
- **Hỗ trợ và cộng đồng:** Các hãng như UniFi và MikroTik có cộng đồng người dùng và hệ thống hỗ trợ mạnh mẽ, cung cấp tài nguyên phong phú cho việc giải quyết sự cố và tối ưu hóa hệ thống. TP-Link cũng cung cấp hỗ trợ tốt nhưng có thể không sâu rộng bằng các thương hiệu chuyên biệt khác.

CHƯƠNG 2. TRIỂN KHAI MÔ HÌNH WIFI MARKETING

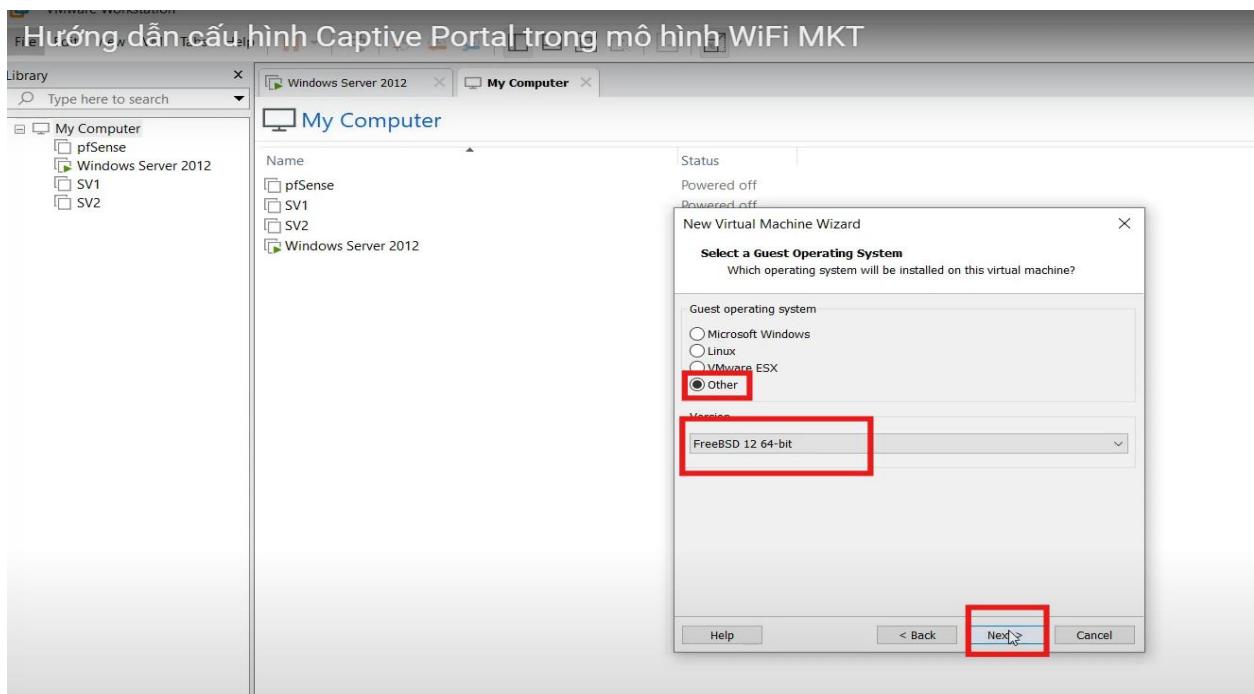
2.1. Mô Hình Thực Hiện



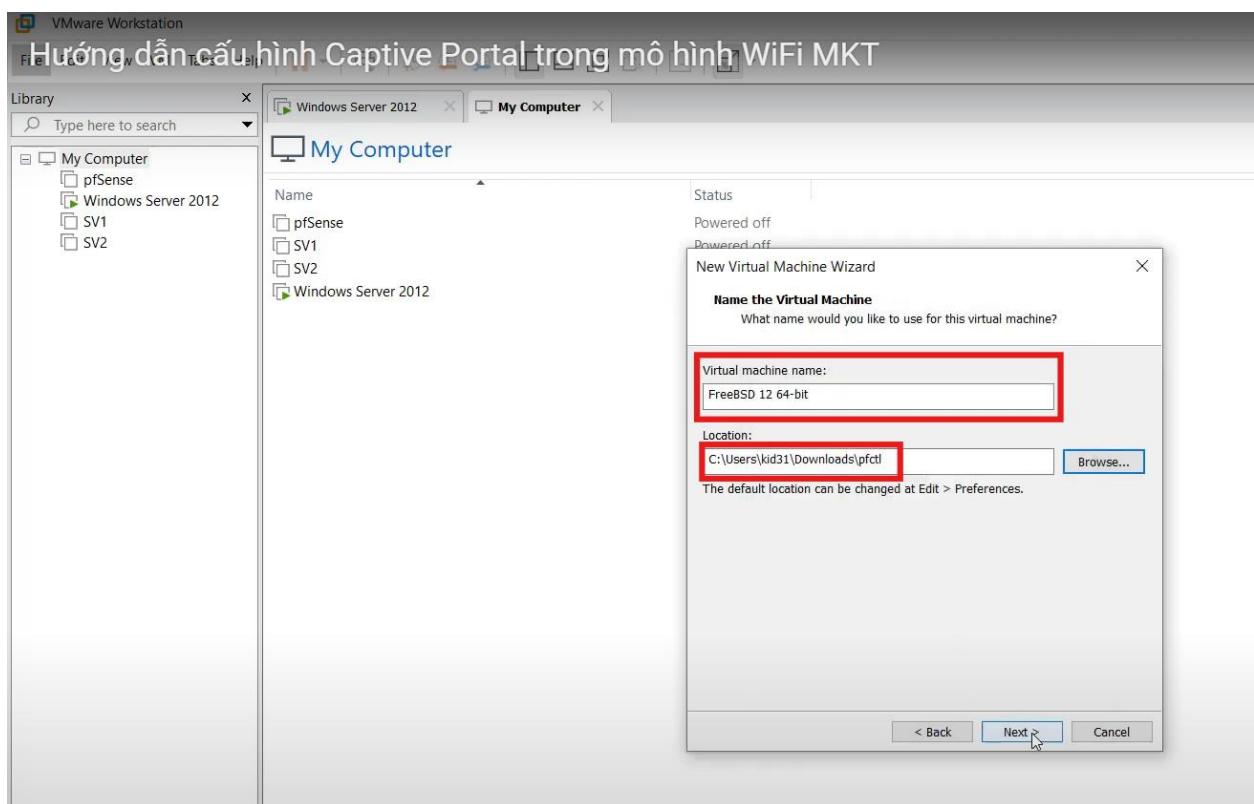
2.2. Cài Đặt Tường Lửa Pfsense



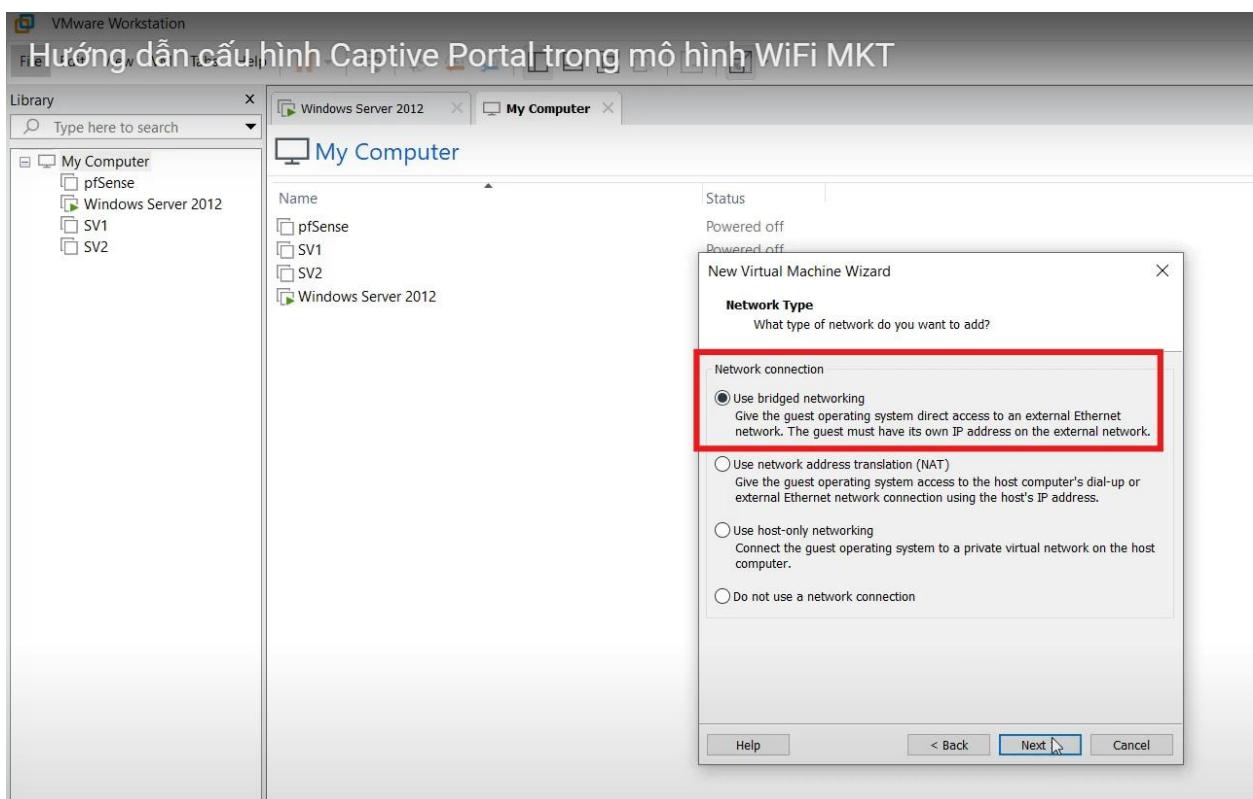
➤ Chọn other → FreeBSD



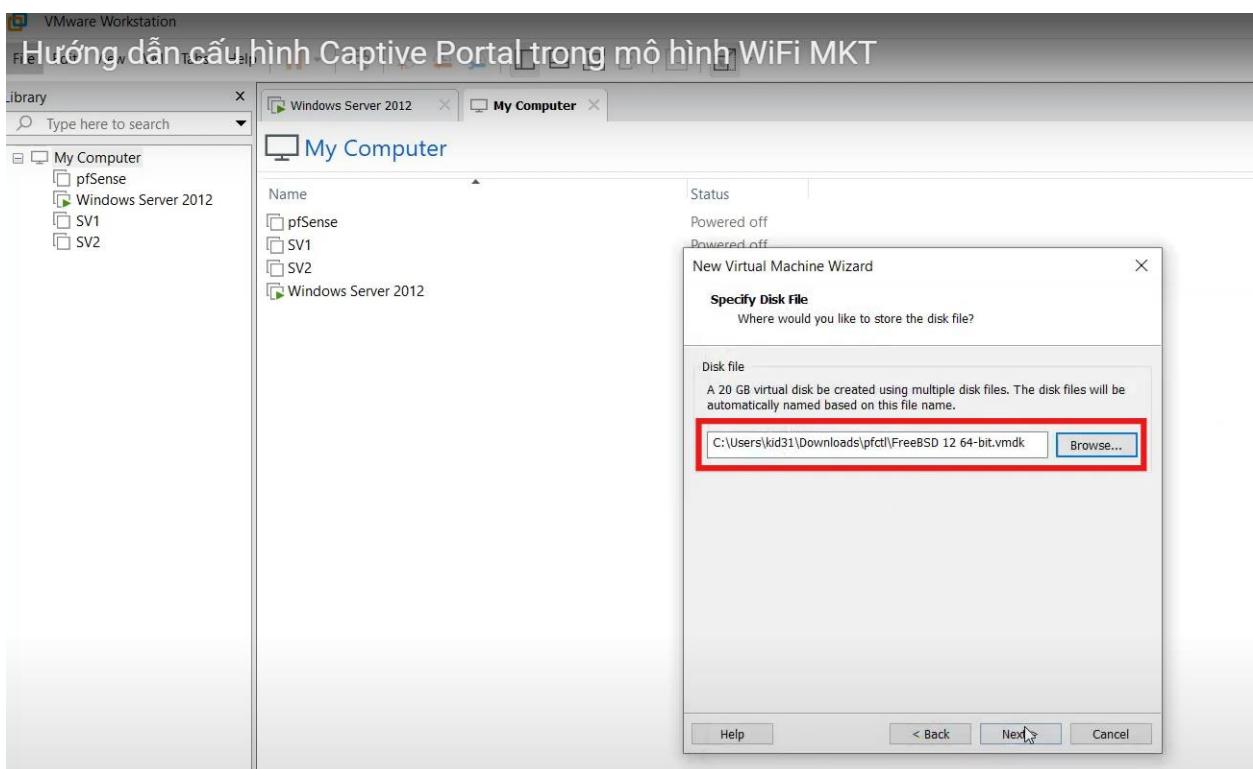
➤ Tạo thư mục và lưu vào



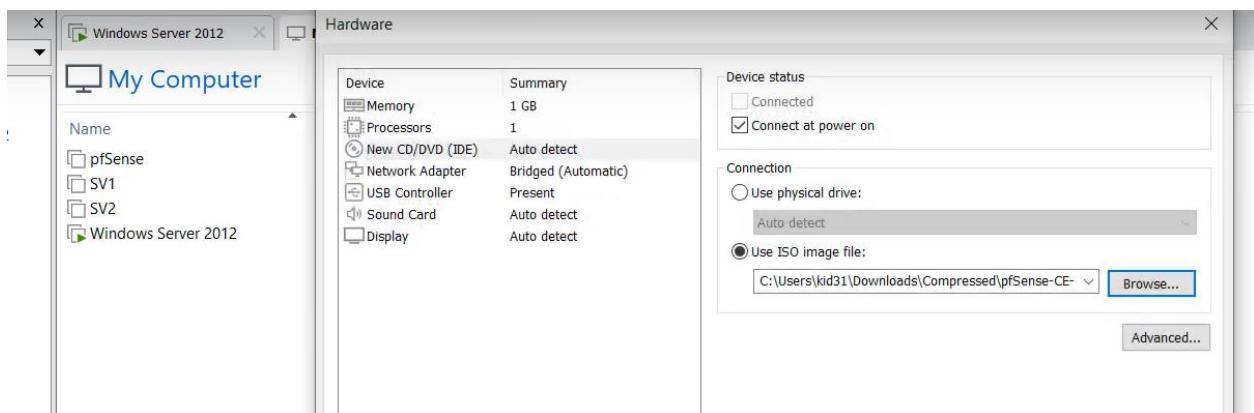
➤ Chọn Bridged



➤ Lưu file vào thư mục tạo ban đầu



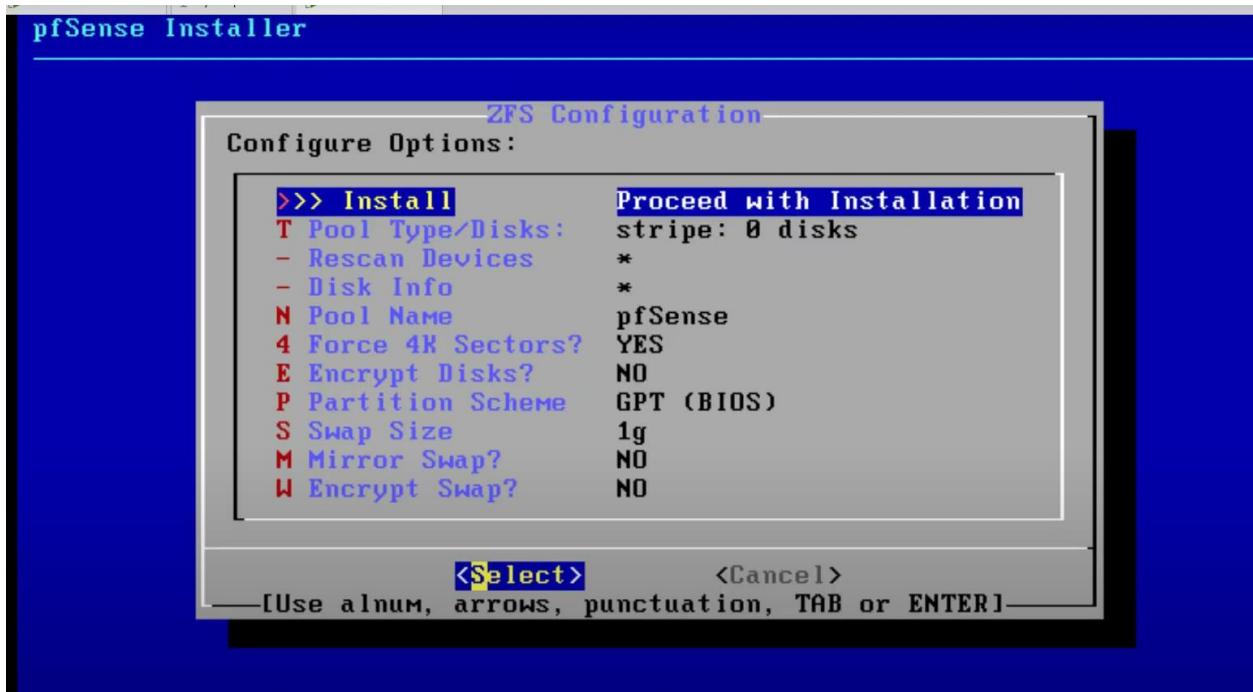
➤ Bỏ đĩa PFsense vào



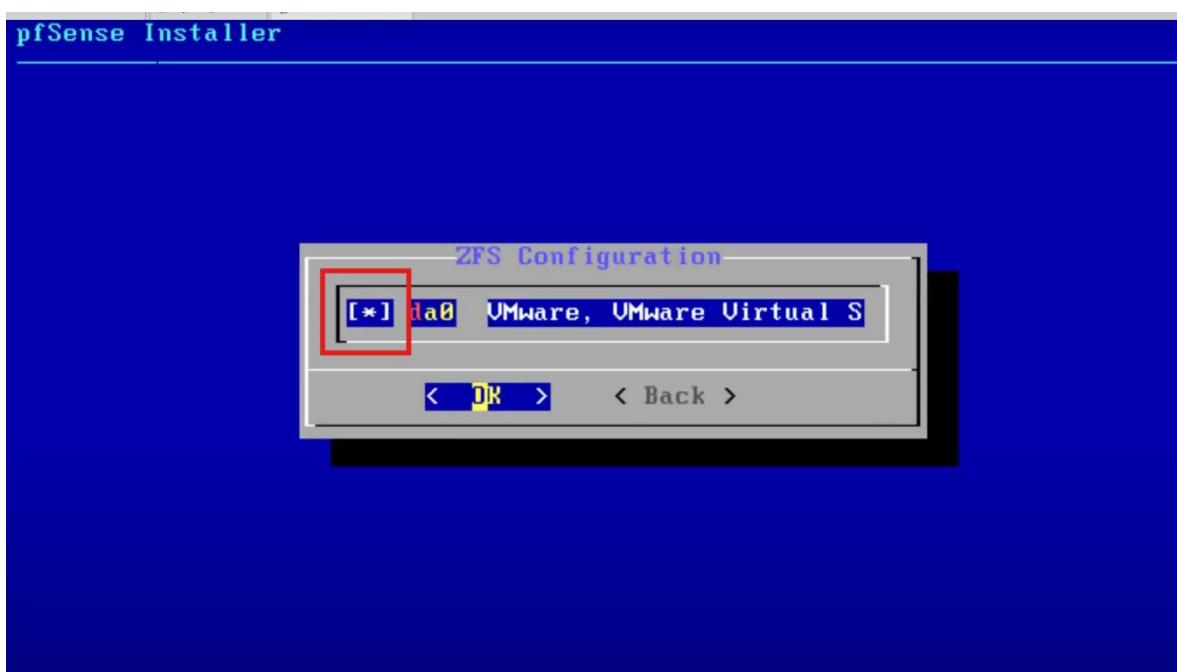
- Khởi động máy ảo và cài đặt



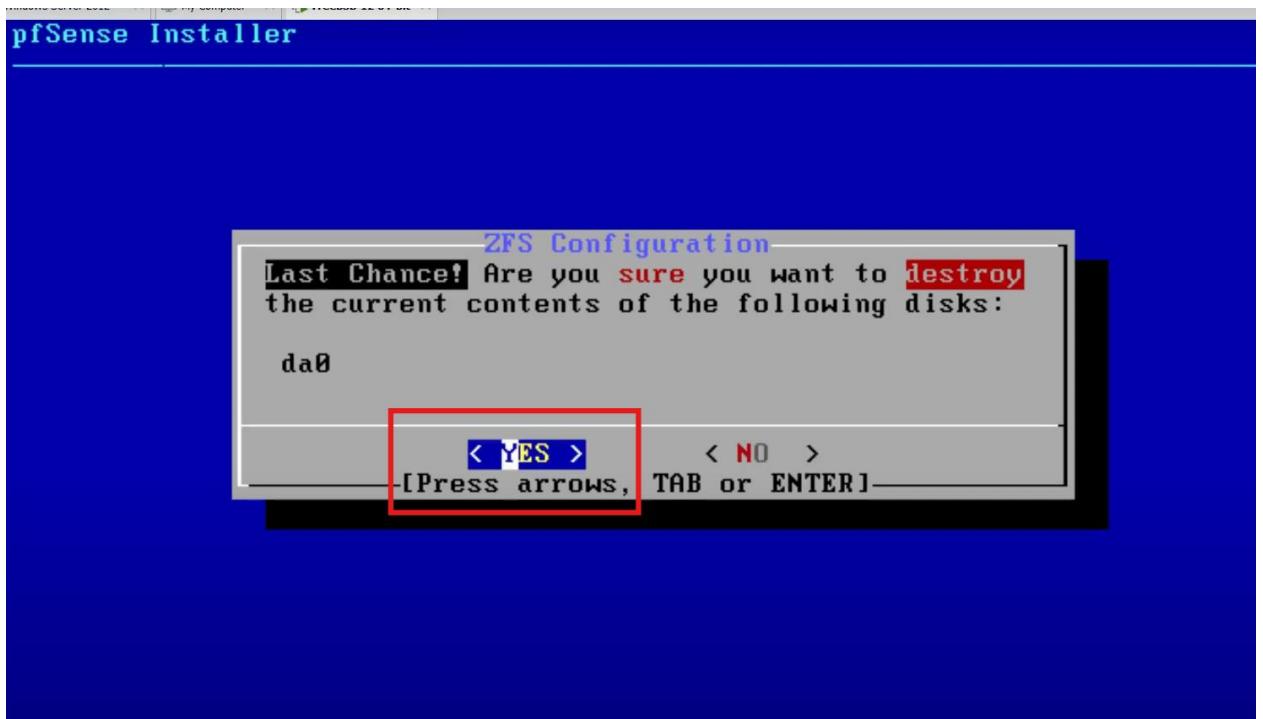
➤ Nhấn ENTER



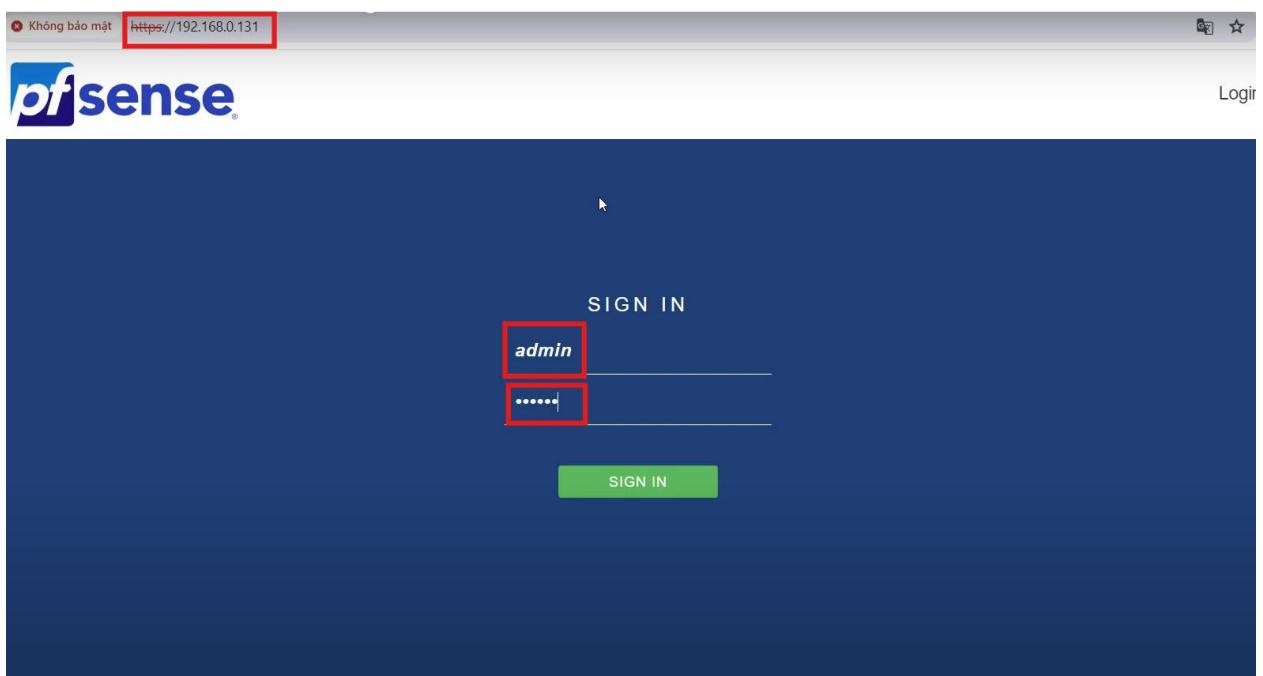
➤ Bấm phím Space (Khoảng trắng) để chọn rồi enter



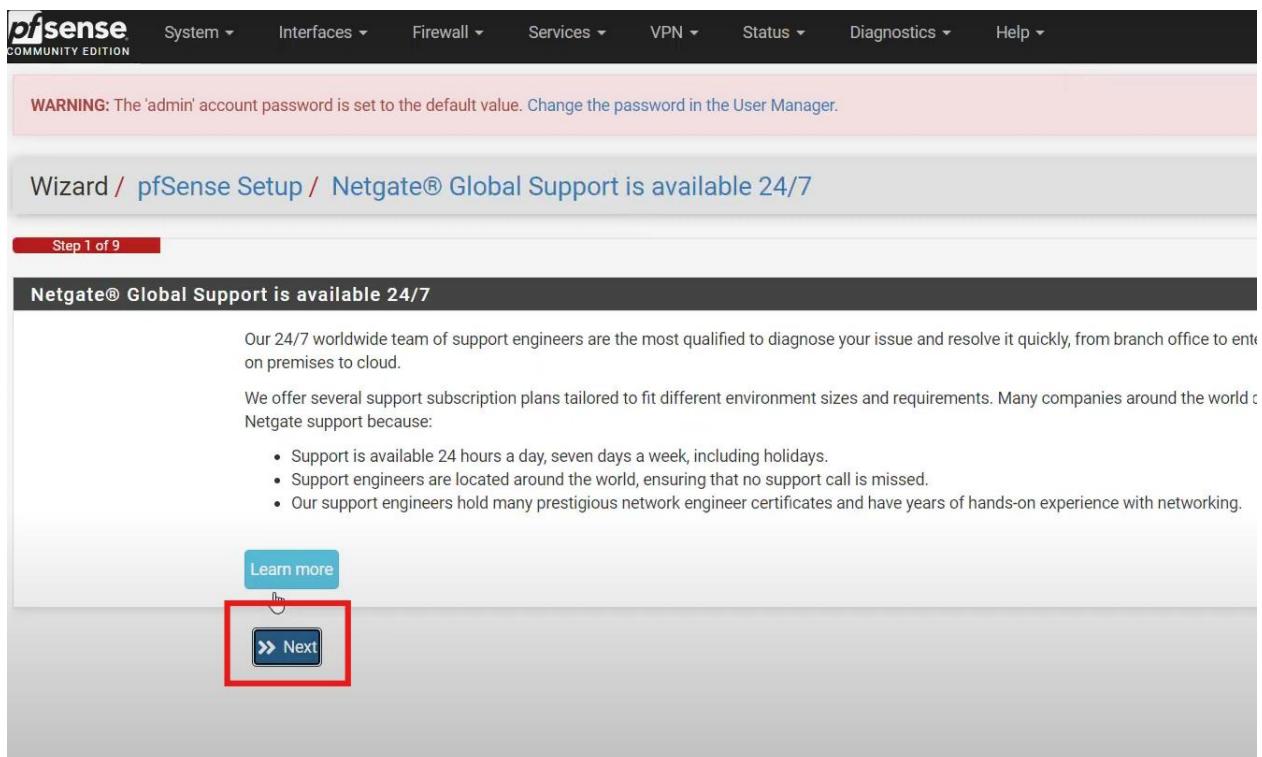
➤ ENTER



- Đăng nhập bằng tài khoản mặc định **admin/pfsense**



Đồ án Thiết kế hệ thống WiFi Marketing



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Netgate® Global Support is available 24/7

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

>> Next

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain: wifimkt.fit.tdc
Domain name for the firewall.
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server:

Secondary DNS Server:

Override DNS: Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

➤ Chọn mũi giờ +7

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname 2.pfsense.pool.http.org
Enter the hostname (FQDN) of the time server.

Timezone Etc/GMT+7

>> Next

PPTP Local IP Address

pptplocalsubnet 32

PPTP Remote IP Address

PPTP Dial on demand Enable Dial-On-Demand mode
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout

RFC1918 Networks

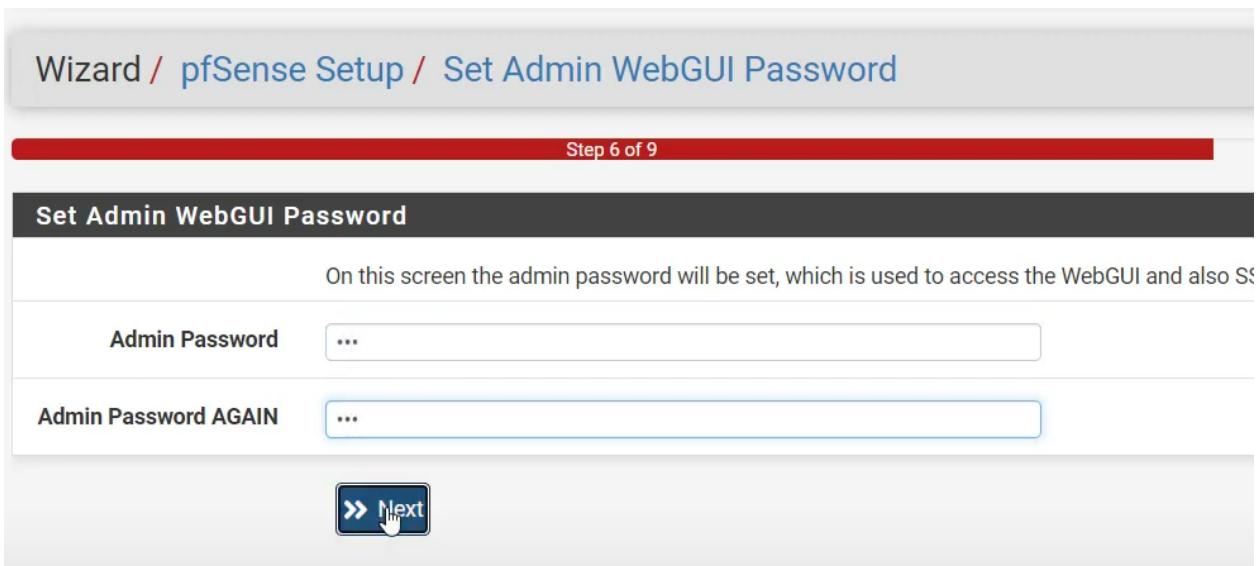
Block RFC1918 Private Networks Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

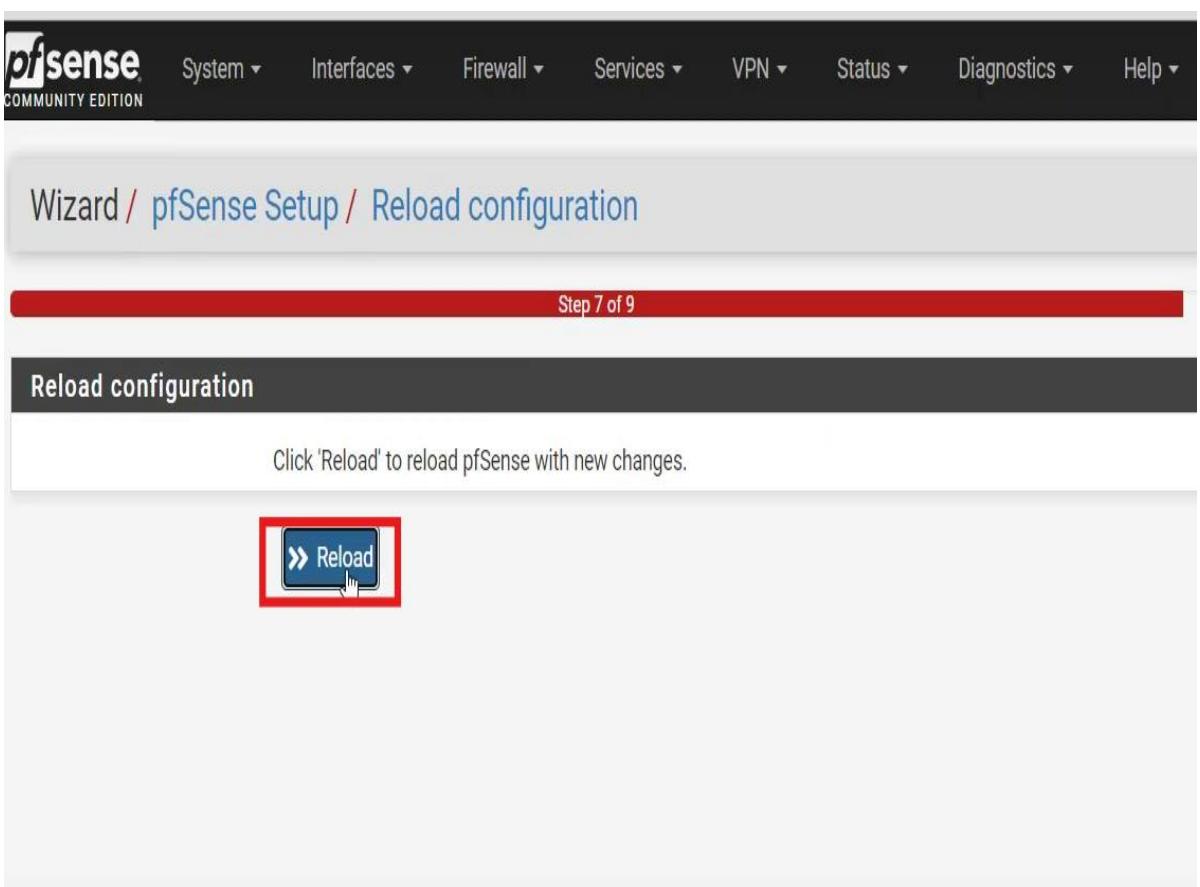
Block bogon networks Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

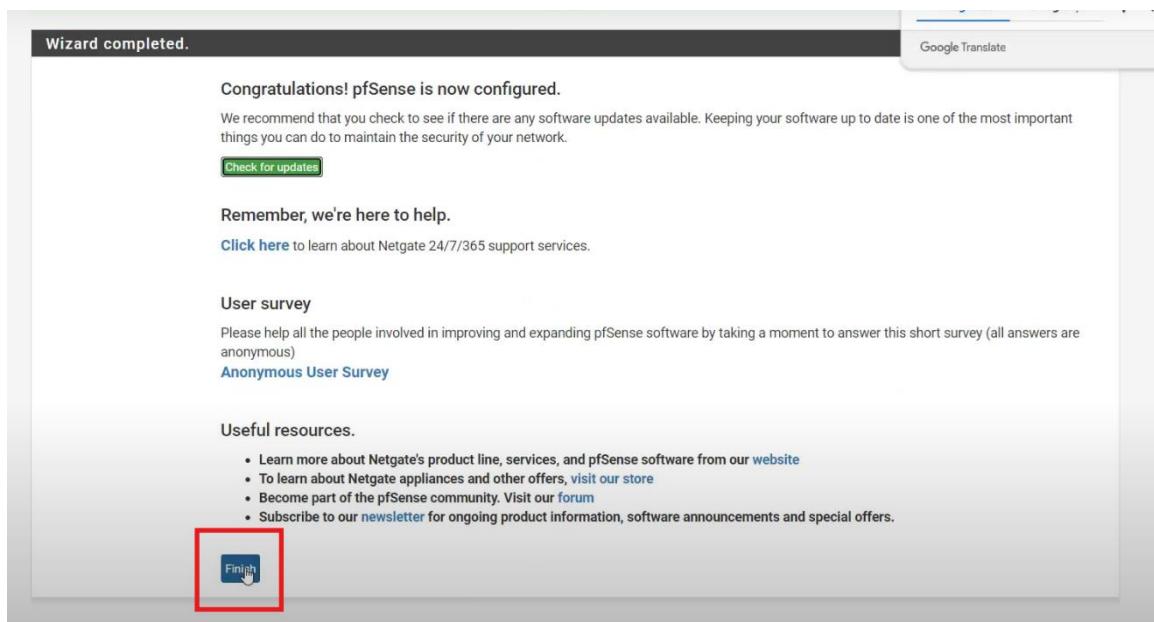
>> Next

➤ Đặt lại password

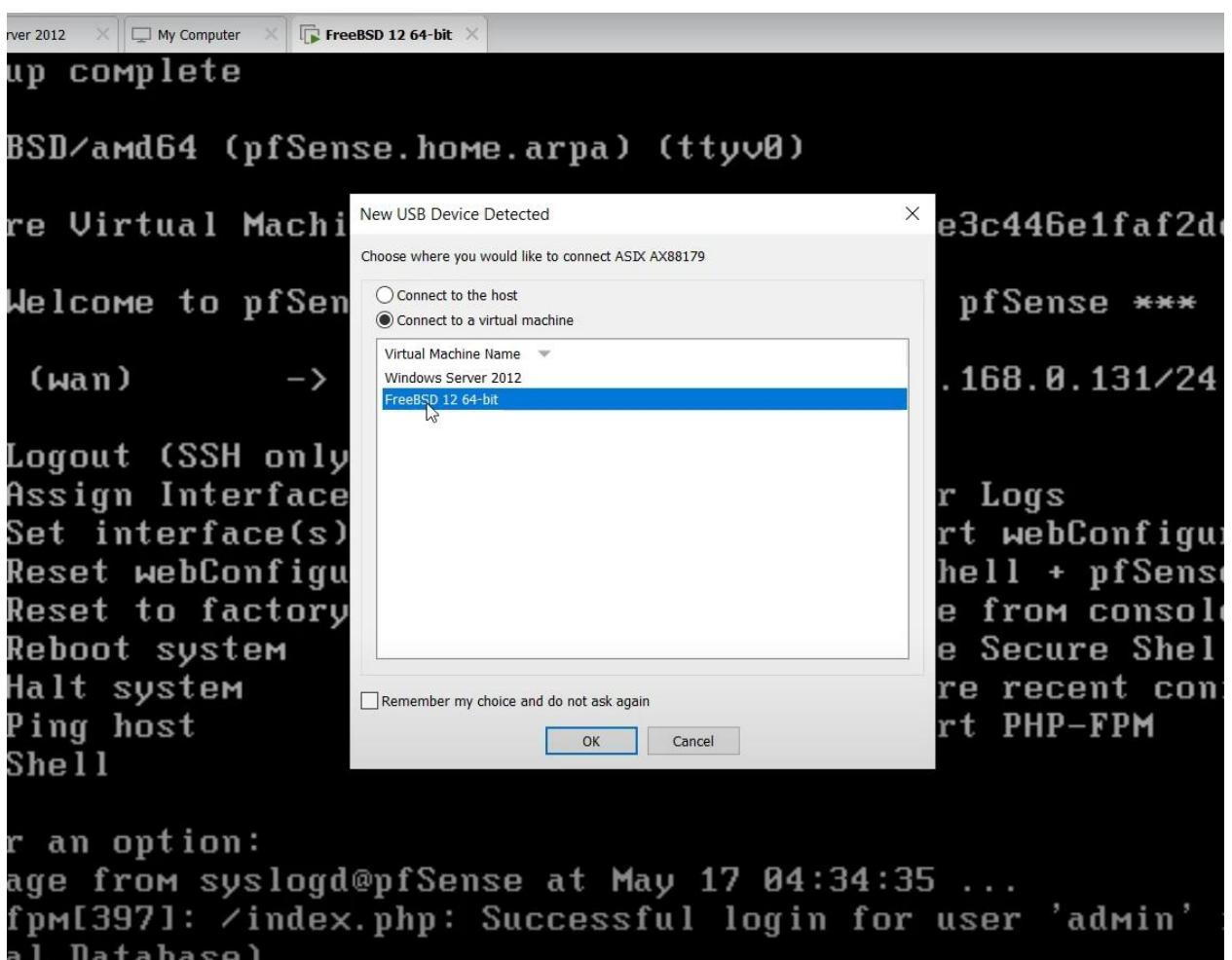


➤ Reload





- Thêm card mạng mới (gắn bộ chuyển đổi USB to RJ45 cho VM pfSense)



- Cấu hình card mạng

Đồ án Thiết kế hệ thống WiFi Marketing

The screenshot shows the pfSense interface under the 'Interfaces' tab. The 'Interface Assignments' sub-tab is selected. A red box highlights the 'Available network ports:' dropdown menu, which contains 'em0 (00:0c:29:99:00:03)' and 'ue0 (7c:c2:c6:42:a8:9d)'. A green 'Add' button with a plus sign is also highlighted with a red box. Below the interface list, there is a note: 'Interfaces that are configured as members of a lagg(4) interface will not be shown.' and 'Wireless interfaces must be created on the Wireless tab before they can be assigned.'

The screenshot shows the pfSense interface under the 'Interfaces' tab, specifically for the 'LAN (ue0)' configuration. The 'General Configuration' sub-tab is selected. The configuration fields include:

- Enable:** Enable interface
- Description:** LAN
Enter a description (name) for the interface here.
- IPv4 Configuration Type:** Static IPv4 (highlighted with a red box)
- IPv6 Configuration Type:** None
- MAC Address:** XX:XX:XX:XX:XX:XX
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.
- MTU:** (empty input field)
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
- MSS:** (empty input field)
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 head).

Static IPv4 Configuration

IPv4 Address / 24

IPv4 Upstream gateway None [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

➤ Cấu hình DHCP Server

System / Advanced / Networking

DHCP Options

Server Backend Kea DHCP ISC DHCP (Deprecated) Ignore Deprecation Warning
ISC DHCP has reached end-of-life and will be removed from a future version of pfSense. Kea DHCP is the newer, modern DHCP distribution from ISC that includes the most-requested features.

RADVD Debug Log all radvd log levels

DHCP6 Debug Start DHCP6 client in debug mode

Do not allow PD/Address release dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent

DHCP6 DUID Raw DUID: As stored in DUID file or seen in firewall logs
A DHCPv6 Unique Identifier (DUID) is used by the firewall when requesting an IPv6 address.
By default, the firewall automatically creates a dynamic DUID-LLT which is not saved in the firewall configuration. To ensure that the same DUID is retained by the firewall at all times, enter a DUID in this section. The new DUID will take effect after a reboot or when the WAN interface(s) are reconfigured by the firewall.

Network Interfaces

- Hardware Checksum Offloading**
 - Disable hardware checksum offload
Checking this option will disable hardware checksum offloading. Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading on some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
- Hardware TCP Segmentation Offloading**
 - Disable hardware TCP segmentation offload
Checking this option will disable hardware TCP segmentation offloading (TSO, TS04, TS06). This offloading is broken in some hardware drivers and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
- Hardware Large Receive Offloading**
 - Disable hardware large receive offload
Checking this option will disable hardware large receive offloading (LRO). This offloading is broken in some hardware drivers, and may impact performance with some specific NICs. This will take effect after a machine reboot or re-configure of each interface.
- hn ALTQ support**
 - Enable the ALTQ support for hn NICs.
Checking this option will enable the ALTQ support for hn NICs. The ALTQ support disables the multiqueue API and may reduce the system capability to handle traffic. This will take effect after a machine reboot.
- ARP Handling**
 - Suppress ARP messages
This option will suppress ARP log messages when multiple interfaces reside on the same broadcast domain.
- Reset All States**
 - Reset all states if WAN IP Address changes
This option resets all states when a WAN IP Address changes instead of only states associated with the previous IP Address.

Save

➤ Enable DHCP Server

Services / DHCP Server / LAN

General DHCP Options

DHCP Backend	Kea DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
Deny Unknown Clients	Allow all clients
When set to Allow all clients , any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface , any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface , only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.	
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet	172.16.1.0/24
--------	---------------

➤ Chọn khoản ip cần cấp

Đồ án Thiết kế hệ thống WiFi Marketing

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. server behavior violates the official DHCP specification.

Primary Address Pool	
Subnet	172.16.1.0/24
Subnet Range	172.16.1.1 - 172.16.1.254
Address Pool Range	<input type="text" value="172.16.1.50"/> From <input type="text" value="172.16.1.100"/> To
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	+ Add Address Pool
If additional pools of addresses are needed inside of this subnet outside of the above range, they may be specified here.	
Server Options	
WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>

➤ DNS server

Server Options	
WINS Servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="172.16.1.1"/> <input type="text" value="1.1.1.1"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>
Other DHCP Options	
Gateway	<input type="text" value="172.16.1.1"/>
The default is to use the IP address of this firewall interface as the gateway. Specify an network. Enter "none" for no gateway assignment.	
Domain Name	<input type="text" value="wifimkt.fit.tdc"/>

2.3. Cấu hình Captive Portal

Add Captive Portal Zone

Zone name Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description

A description may be entered here for administrative reference (not parsed).

Save & Continue

Captive Portal Configuration

Enable **Enable Captive Portal**

Description

A description may be entered here for administrative reference (not parsed).

Interfaces

Select the interface(s) to enable for captive portal.

Maximum concurrent connections

Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can connect to the portal, but rather how many connections a single IP can establish to the portal web server.

- Thêm trang web .html

HTML Page Contents

Portal page contents Chọn tệp portal.html

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL_REDIRURL\$". Include "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail.

Example code for the form:

```
<form method="post" action="$PORTAL_ACTION$">
<input name="auth_user" type="text">
<input name="auth_pass" type="password">
<input name="auth_voucher" type="text">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
<input name="zone" type="hidden" value="$PORTAL_ZONE$">
<input name="accept" type="submit" value="Continue">
</form>
```

Auth error page contents Chọn tệp error.html

The contents of the HTML/PHP file that is uploaded here are displayed when an authentication error occurs. It may include which will be replaced by the error or reply messages from the RADIUS server, if any.

Logout page contents Chọn tệp logout.html

➤ Chọn loại xác thực

Authentication

Authentication Method None, don't authenticate users

Select an Authentication Method to use for this zone. One method must be selected.
 - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
 - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
 - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

HTTPS Options

Login Enable HTTPS login
 When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

Save

Sau khi mình áp dụng thì rules của tường lửa không cho phép ta truy cập vào PFsense nữa . Vì vậy ta cần tắt tạm thời PFsense và tạo thêm rules cho phép truy cập để có thể tiếp tục thực hiện cấu hình tiếp.

```

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

Enter an option: 8

[2.7.2-RELEASE][root@pfSense.wifimkt.fit.tdc]#root: pfctl -d
pf disabled

```

- Thêm rules cho phép truy cập

Sau khi cấp quyền ta tiếp tục cấu hình

- Thêm các file cần thiết cho Captive portal

The screenshot shows the pfSense web interface under the 'File Manager' tab. A red box highlights the breadcrumb navigation: Services / Captive Portal / captiveportal / File Manager. Below the navigation, there are tabs for Configuration, MACs, Allowed IP Addresses, Allowed Hostnames, Vouchers, High Availability, and File Manager (which is selected). A table titled 'Installed Files' lists three files: 'captiveportal-background.jpg', 'captiveportal-logo.svg', and 'captiveportal-style.css'. The total size is 551 KiB. A red box highlights the file names in the list.

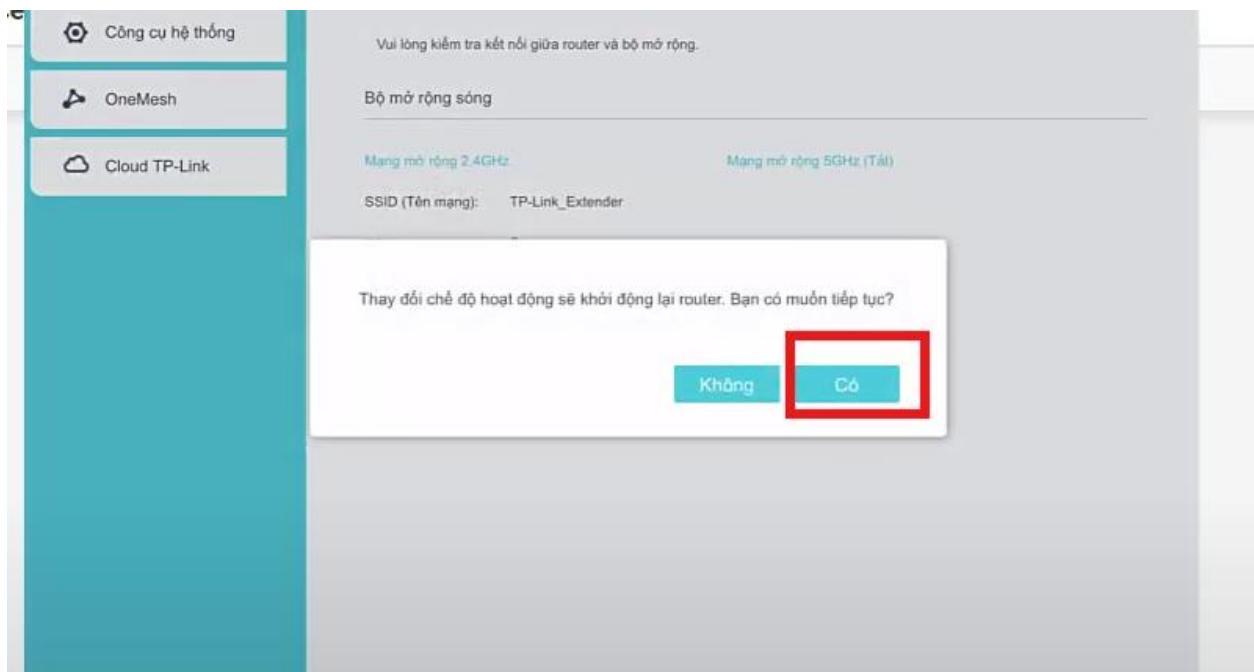
➤ Cấu hình ban đầu access point và cấu hình nhận DHCP

The screenshot shows the TP-Link app interface. On the left, a sidebar has icons for Trạng thái, Không dây, Mạng, Cài đặt nâng cao, Công cụ hệ thống, OneMesh, and Cloud TP-Link. The main area shows a network diagram with icons for Internet, Router, RE200, and Khách hàng. A message says 'Vui lòng kiểm tra kết nối giữa router và bộ mở rộng.' Below it, a section for 'Bộ mở rộng sóng' is shown. A modal window titled 'Chuyển chế độ' is open, with a red box highlighting the 'Điểm truy cập' (Access Point) option. It says 'Chuyển đổi mạng dây sang không dây' (Change from wired to wireless). There are two radio buttons: 'Lắp sóng' (Install antenna) and 'Mở rộng vùng phủ sóng mạng không dây của bạn' (Expand your wireless network coverage). At the bottom are 'Hủy' (Cancel) and 'Lưu' (Save) buttons.

➤ Tắt chế độ DHCP server để có thể nhận ip DHCP từ PFSENSE cấp xuống

The screenshot shows the pfSense 'Máy chủ DHCP' (DHCP Server) configuration page. A red box highlights the 'Tự động' (Automatic) radio button under 'Máy chủ DHCP:'. Other options are 'Mới' (New) and 'Tắt' (Disabled), which is selected. The configuration fields include: Đầu địa chỉ IP: 192.168.0.100 - 192.168.0.199; Thời gian thuê địa chỉ: 2 phút (1-2880, Giá trị mặc định là 1); Gateway mặc định: 192.168.0.254 (Tùy chọn); DNS thứ nhất: 192.168.0.254 (Tùy chọn); and DNS thứ hai: 0.0.0.0 (Tùy chọn). A 'Lưu' (Save) button is at the bottom right.

- Tiến hành khởi động lại.



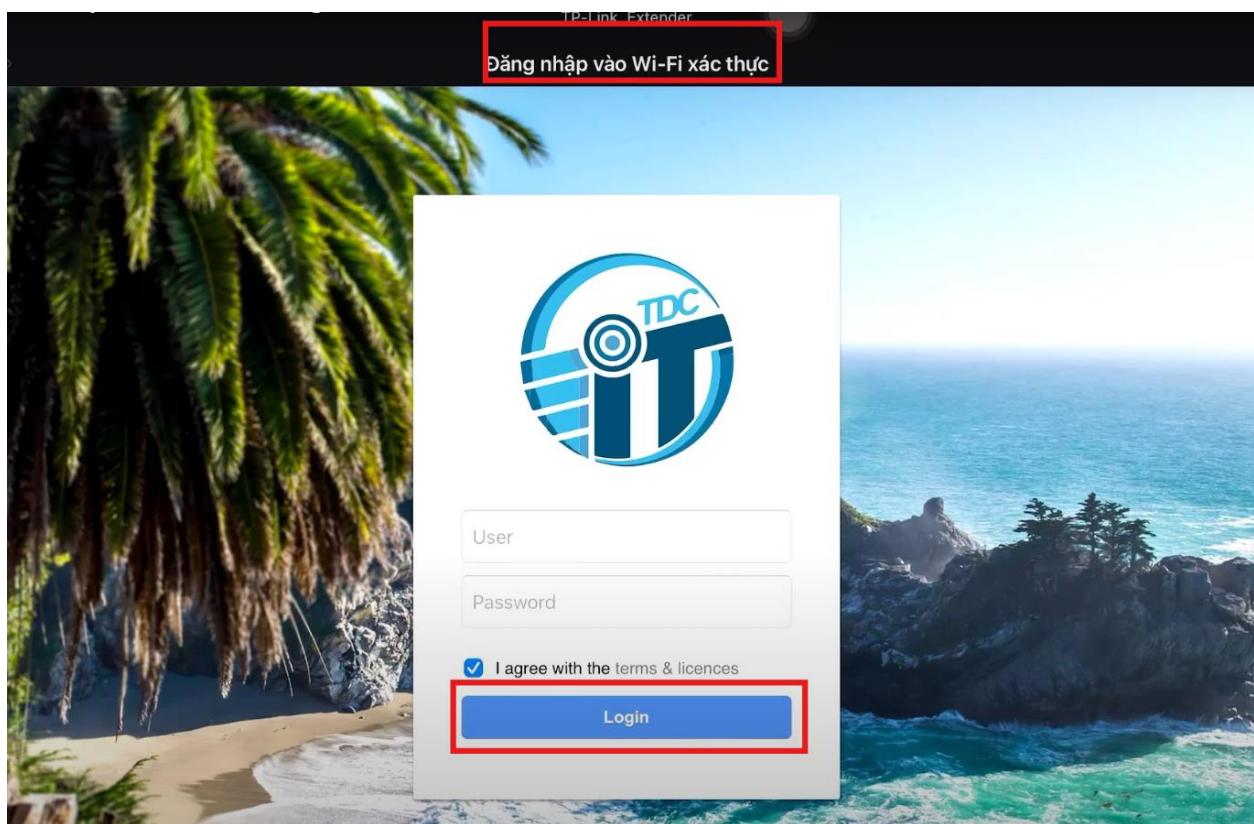
- Kiểm tra xem DHCP đã được cấp chưa

IP Address	MAC Address	Hostname	Description	Start	End	Actions
172.16.1.50	b0:95:75:69:11:ea	re200		2024/05/16 21:58:59	2024/05/16 23:58:59	[Edit] [Delete] [Release]
172.16.1.51	34:f6:4b:a4:10:46	hyperv.		2024/05/16 22:00:07	2024/05/17 00:00:07	[Edit] [Delete] [Release]

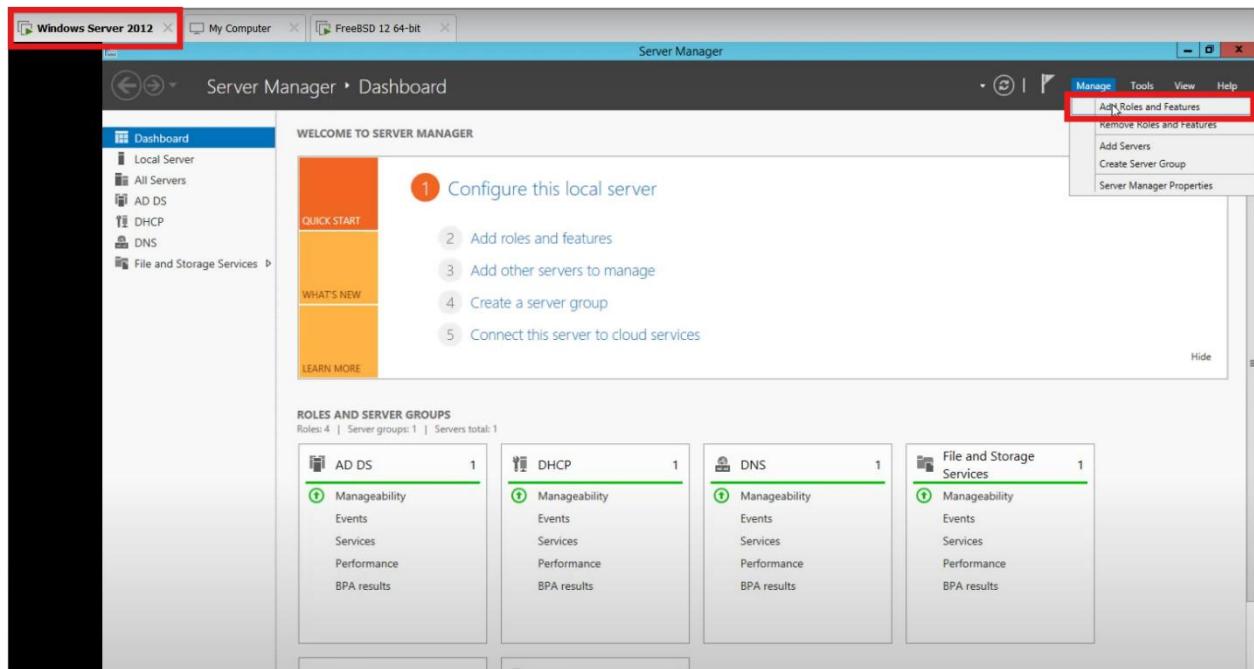
Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	172.16.1.50	172.16.1.100	2	51	3% of 51

Lúc này ta có thể truy cập wifi từ **Access Point**

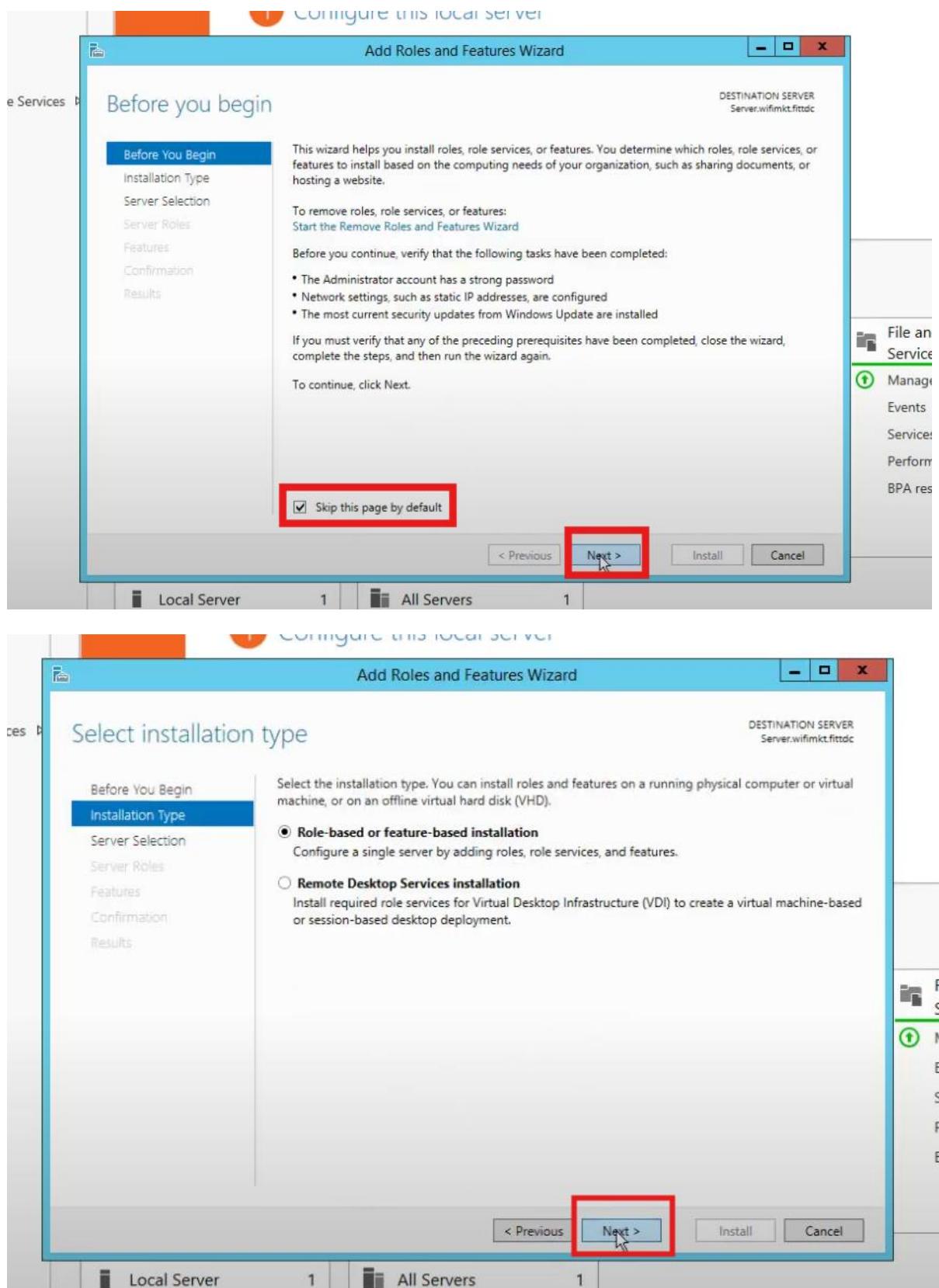
Nhưng ta chưa cấu hình xác thực RADIUS nên chỉ cần nhấn login là có thể truy cập được internet:



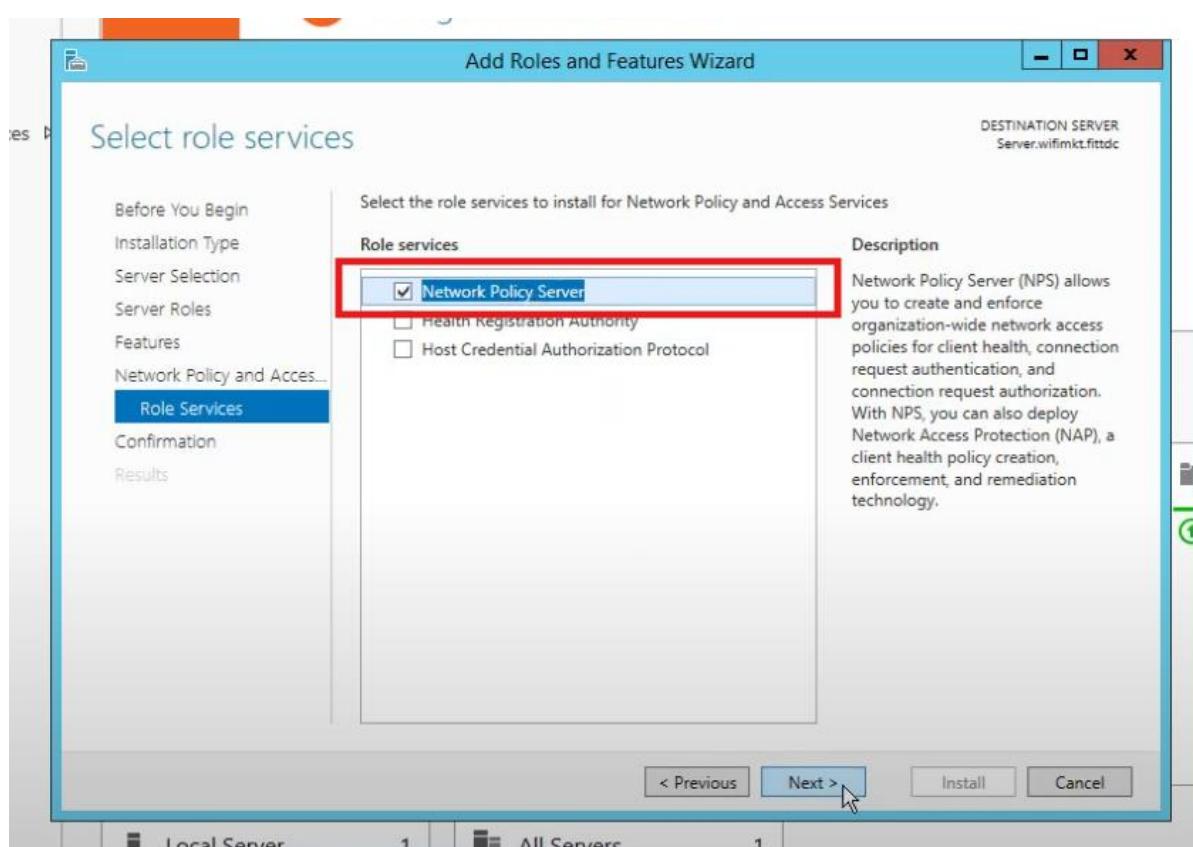
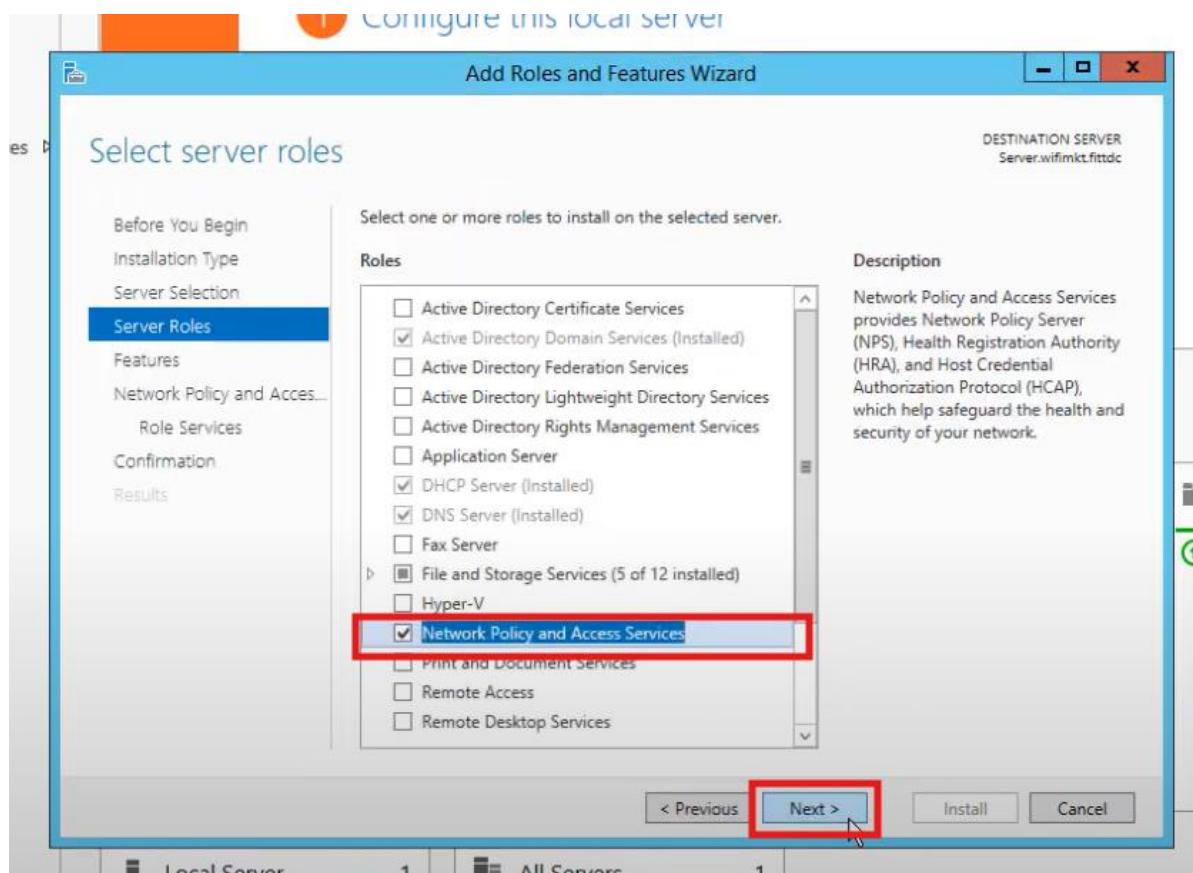
2.4. Cấu hình RADIUS server



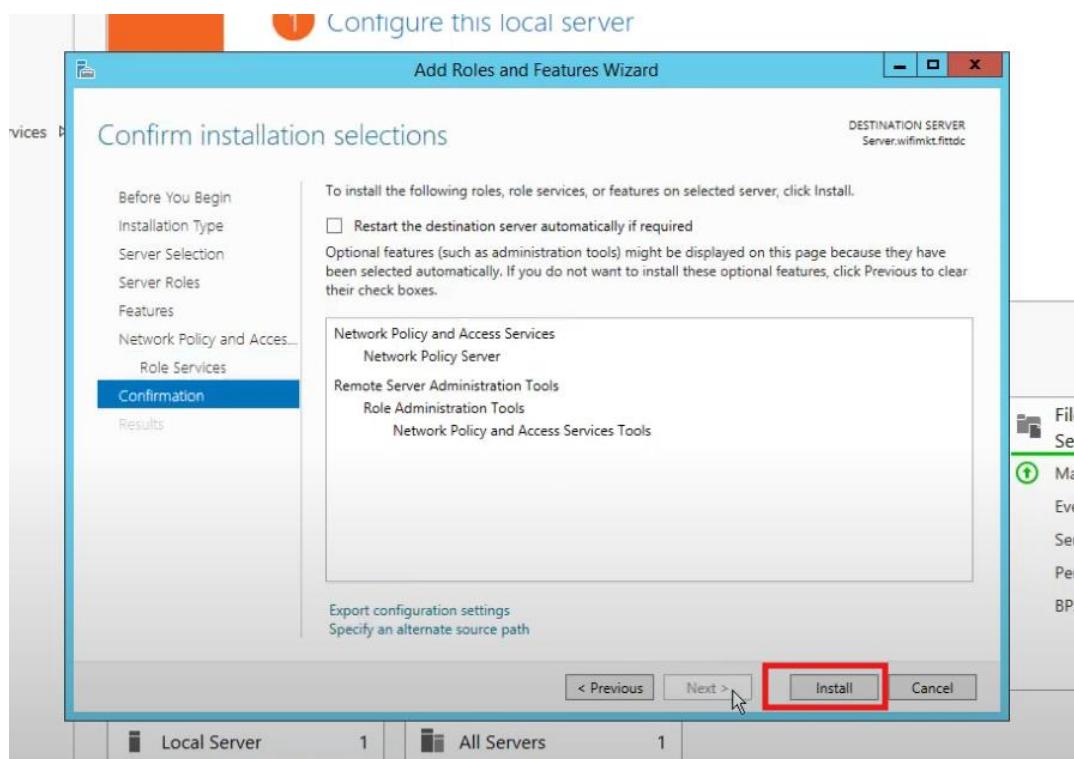
➤ ADD ROLES



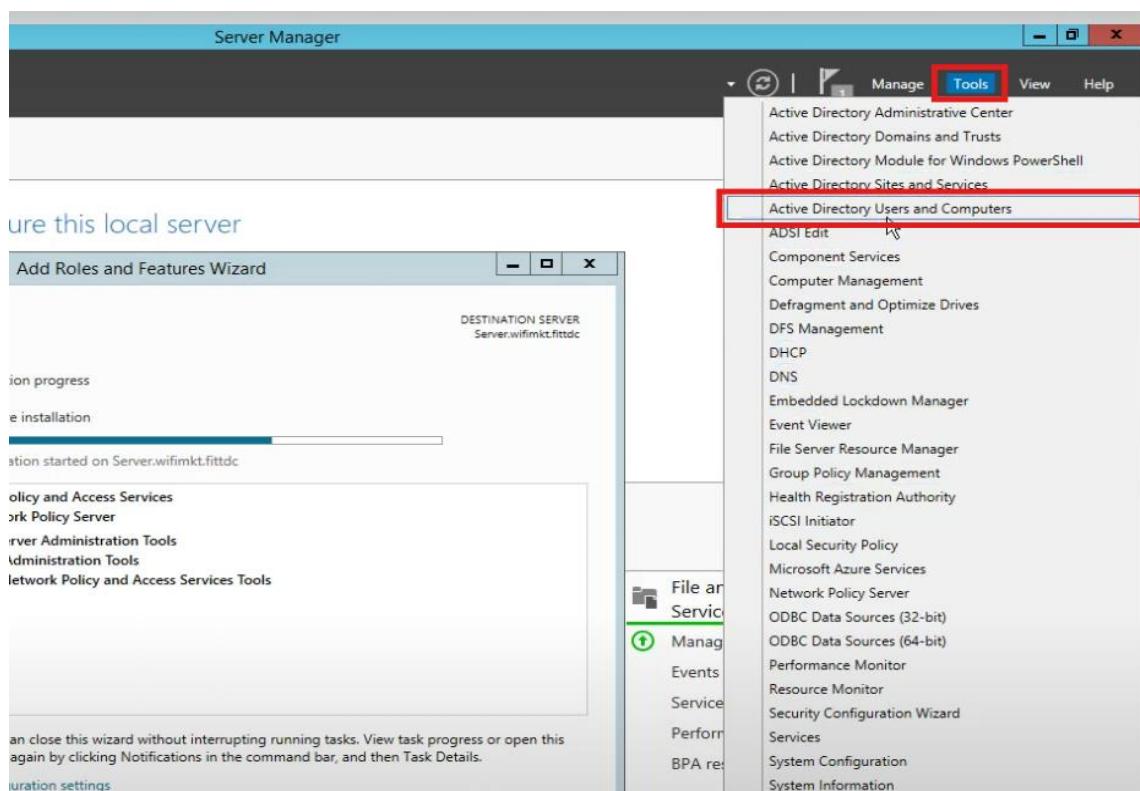
➤ Chọn Network Policy and Access Services



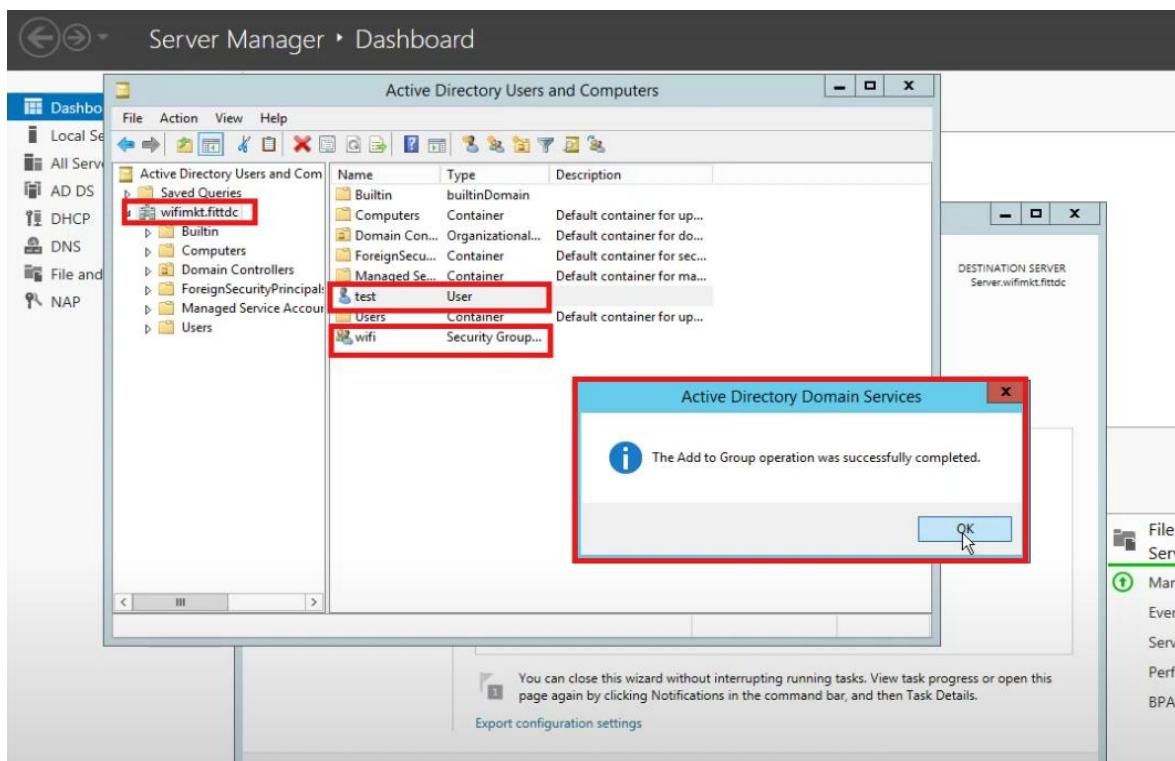
➤ Cài đặt roles



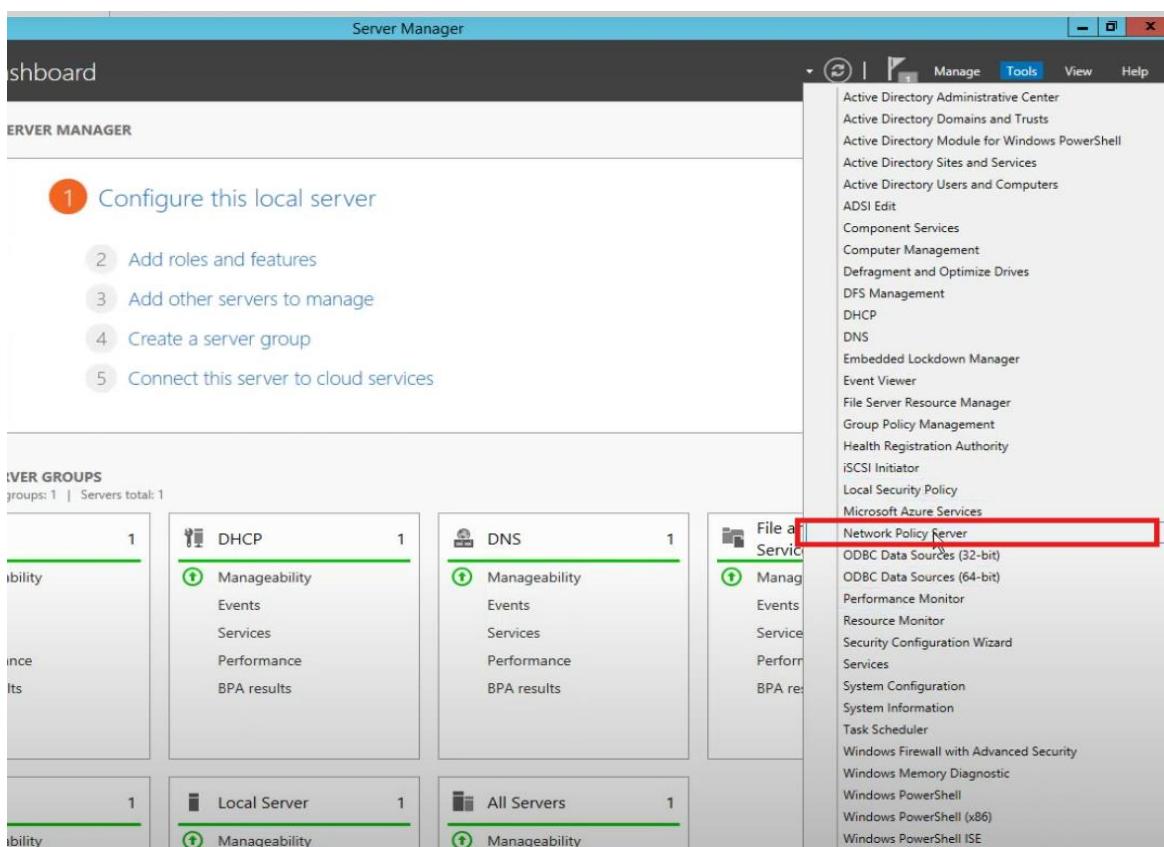
➤ Tạo group và user



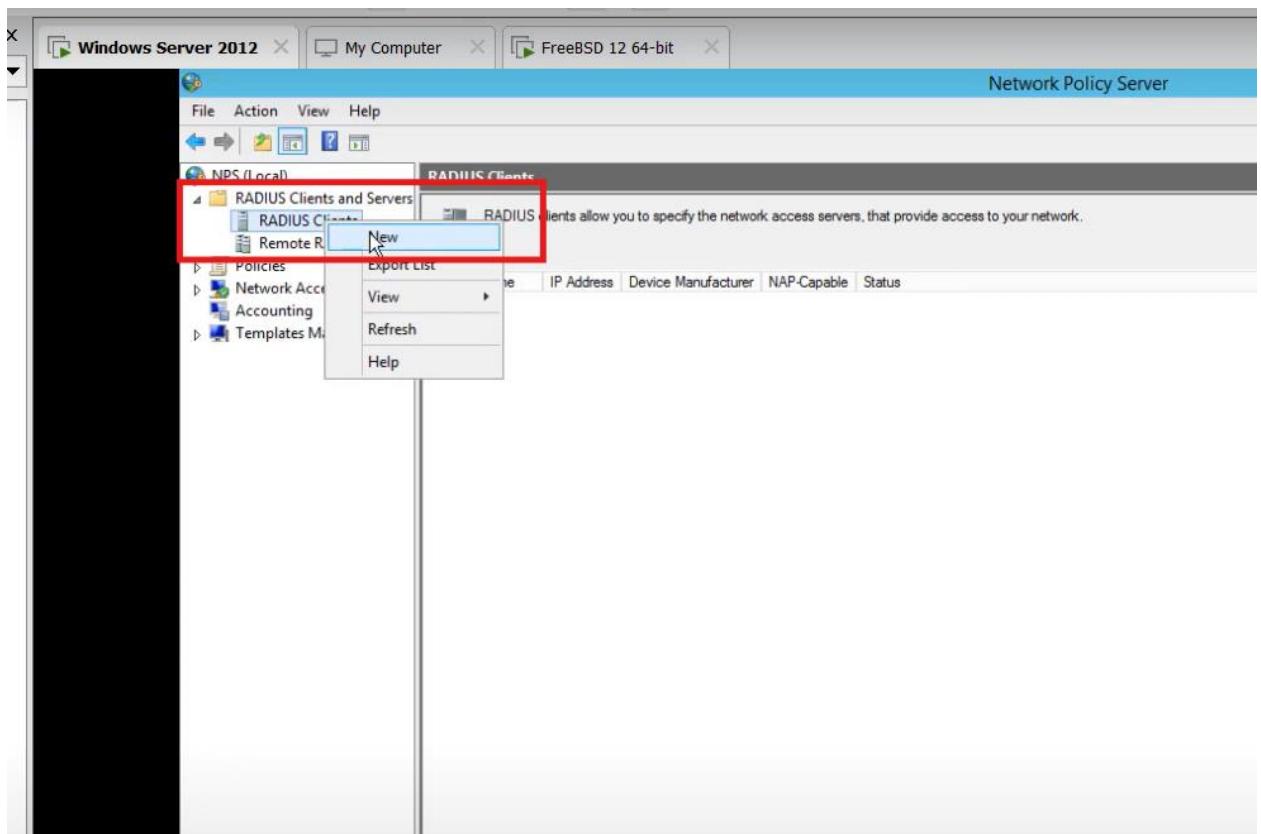
➤ Add user vào group



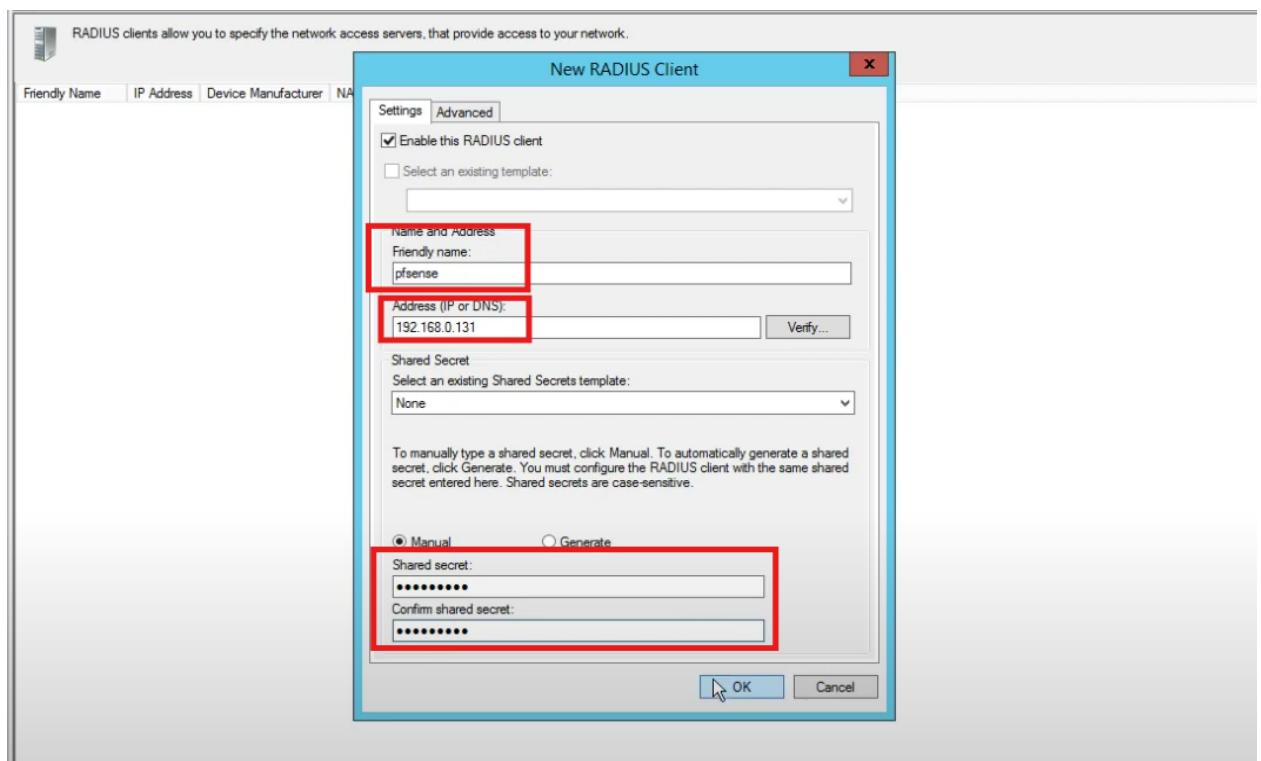
2.5. Cấu hình RADIUS



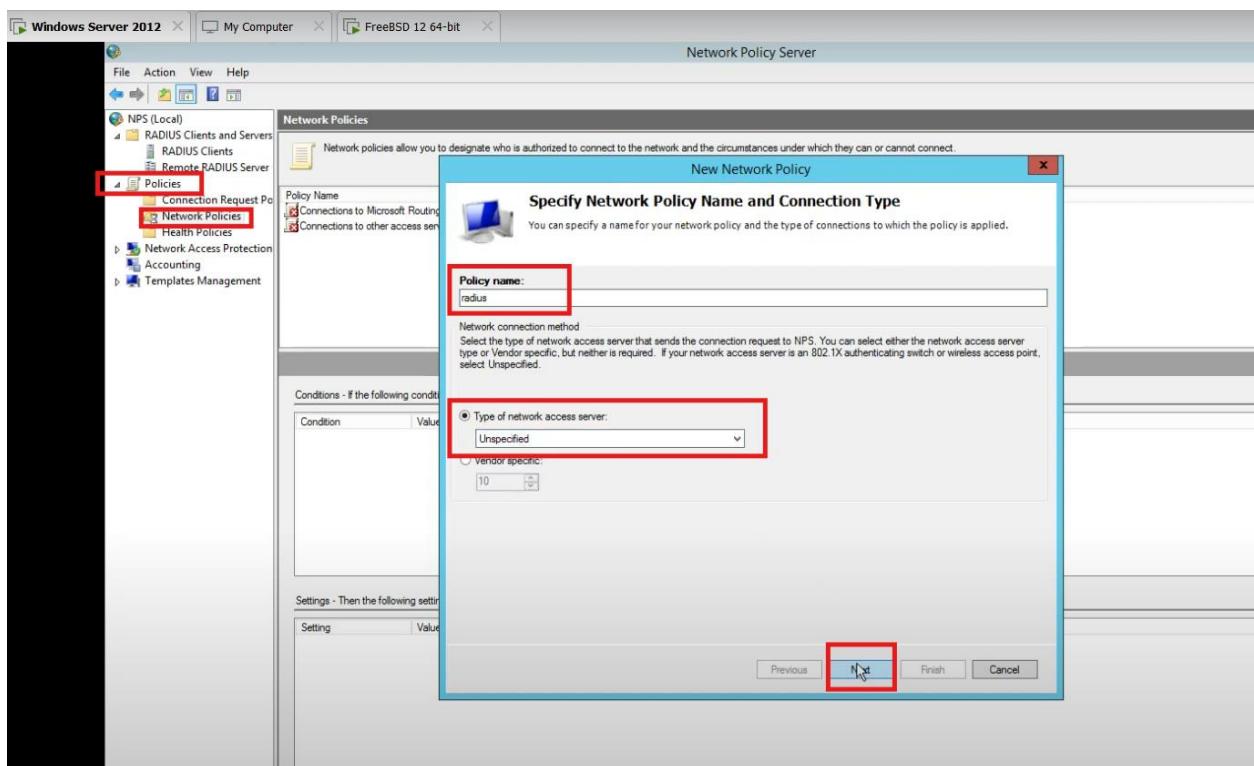
➤ Tạo RADIUS client



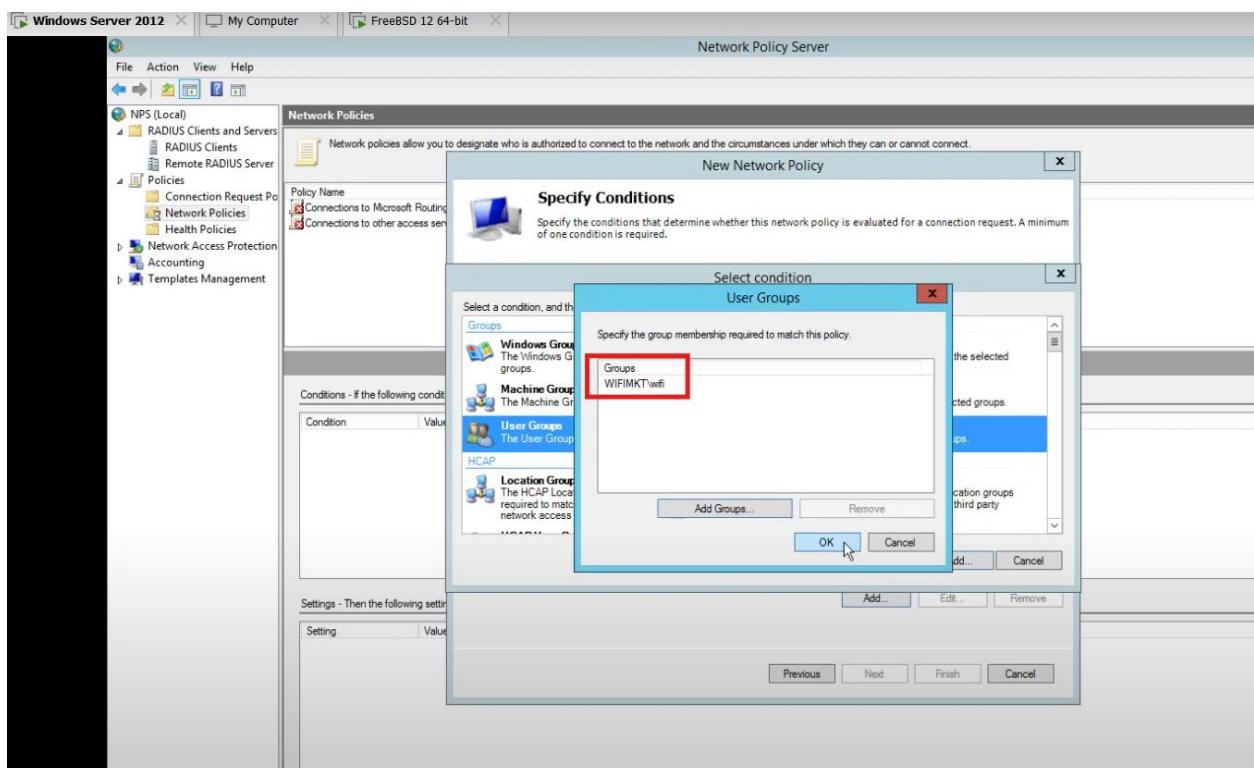
➤ Đặt ip và mật khẩu xác thực



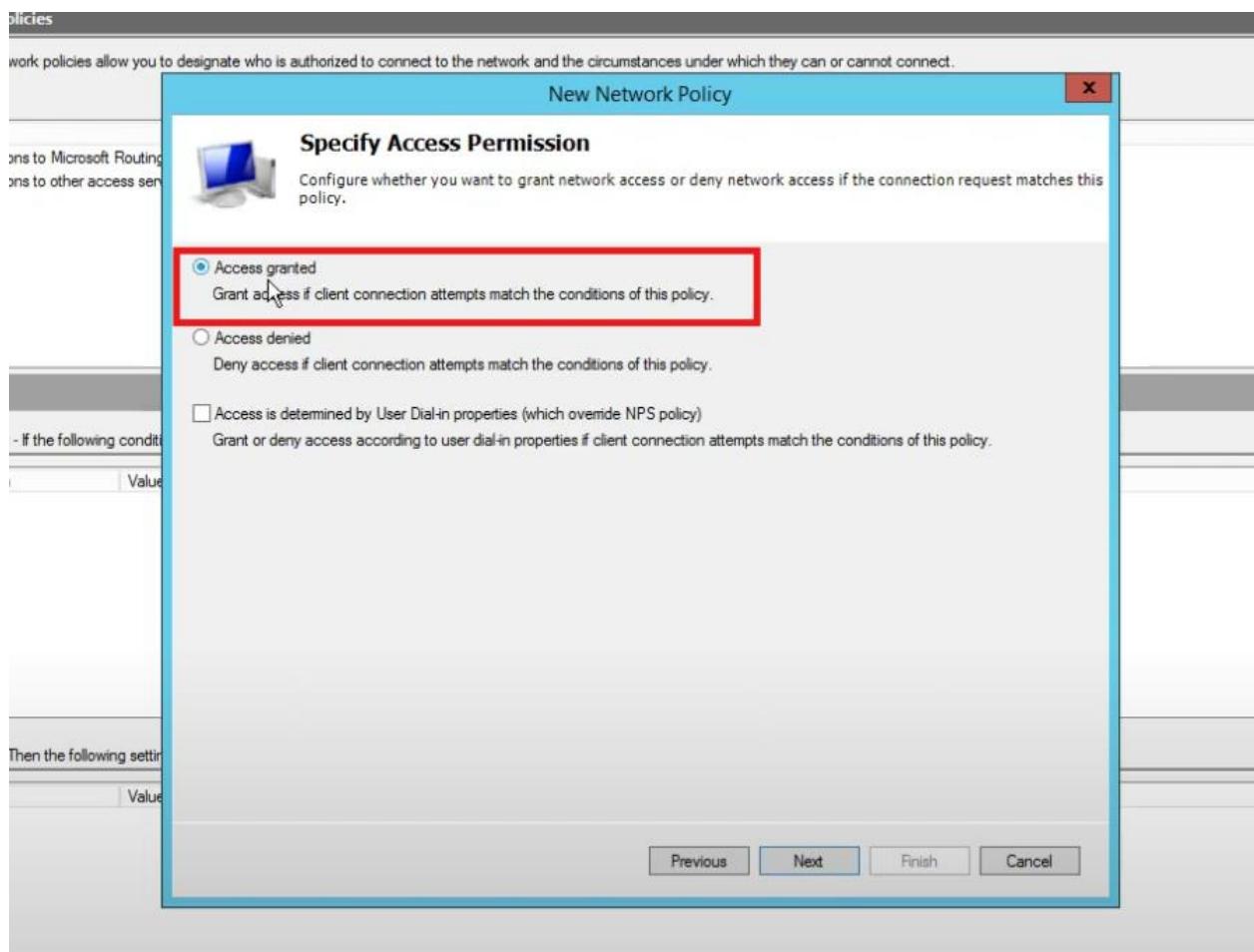
➤ Tạo Policy



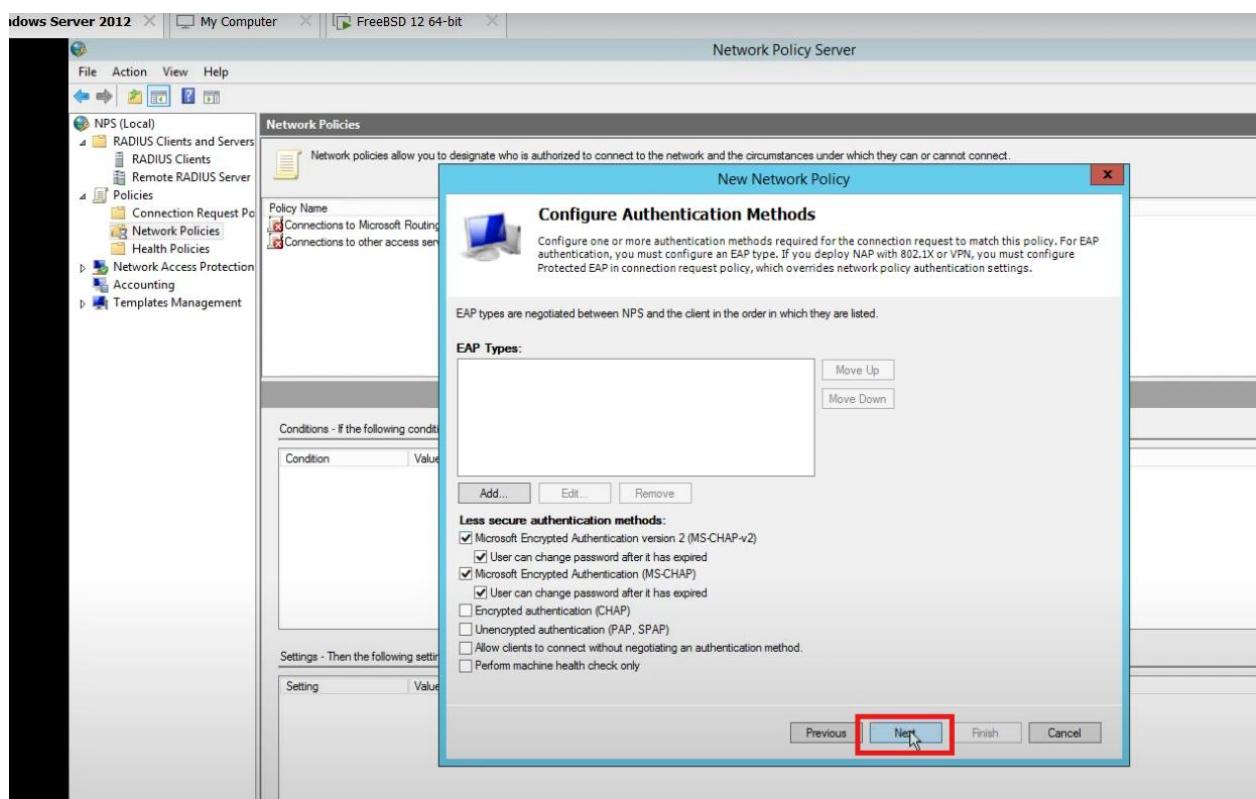
➤ Add group vào



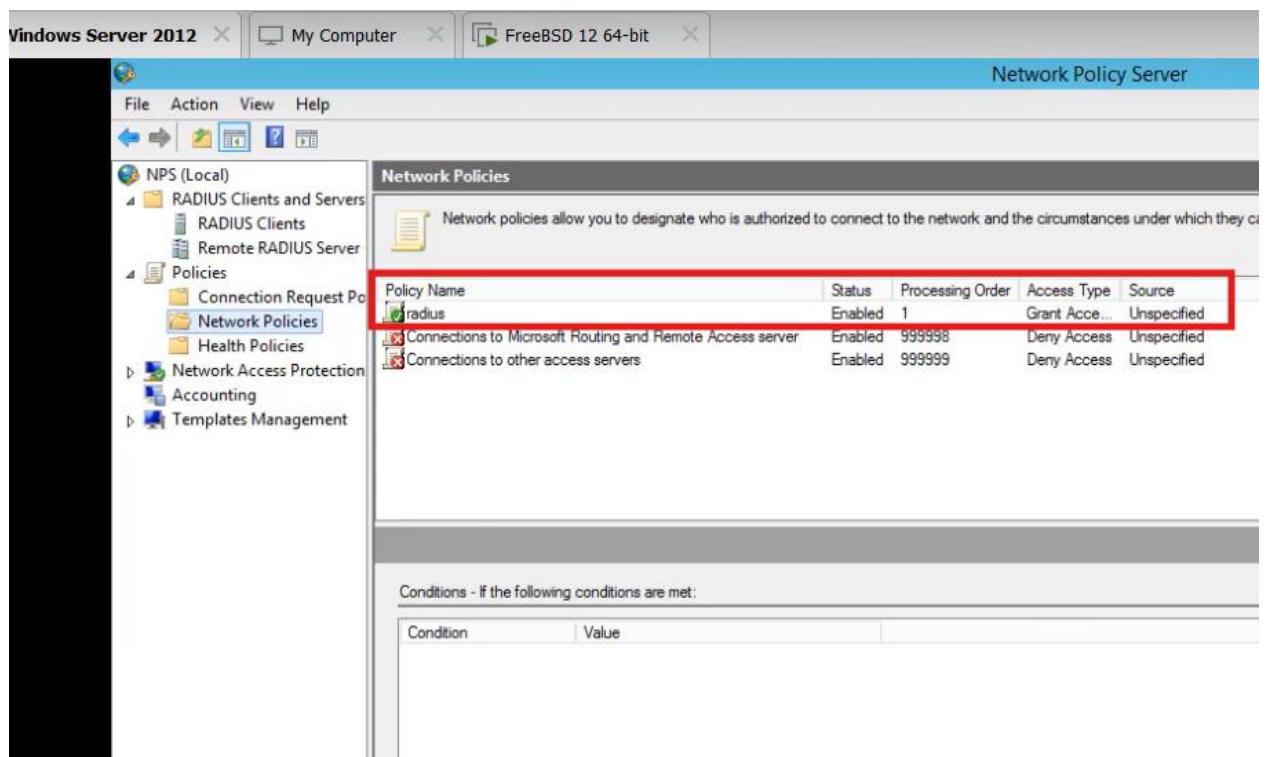
Đồ án Thiết kế hệ thống WiFi Marketing



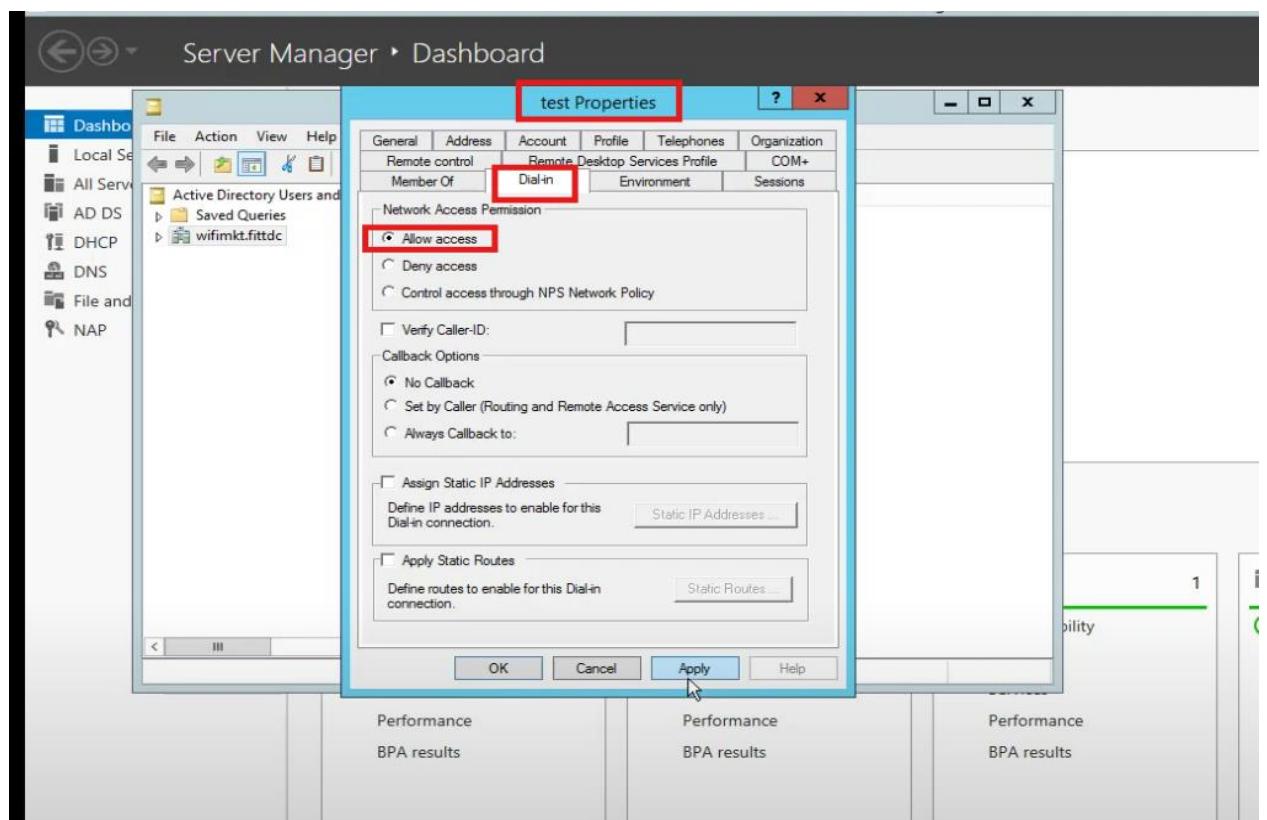
➤ Next



➤ Sau khi tạo policy



➤ Bật chế độ Allow access cho user



➤ Cài đặt xác thực

Không bảo mật https://192.168.0.131/system_authservers.php?act=new

System / User Manager / Authentication Servers / Edit

Users Groups Settings Authentication Servers

Server Settings

Descriptive name NPS

Type RADIUS

RADIUS Server Settings

Protocol MS-CHAPv2

Hostname or IP address I

Shared Secret

Services offered Authentication and Accounting

Type RADIUS

RADIUS Server Settings

Protocol MS-CHAPv2

Hostname or IP address 192.168.0.254

Shared Secret *****

Services offered Authentication and Accounting

Authentication port 1812

Accounting port 1813

Authentication Timeout

This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take and enter a token.

RADIUS NAS IP Attribute WAN - 192.168.0.131

Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

Save

➤ Ta quay trở lại chỉnh sửa dịch vụ CAPTIVE PORTAL bật chế độ xác thực

Authentication

Authentication Method

Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying a login page.

Authentication Server

NPS
Local Database

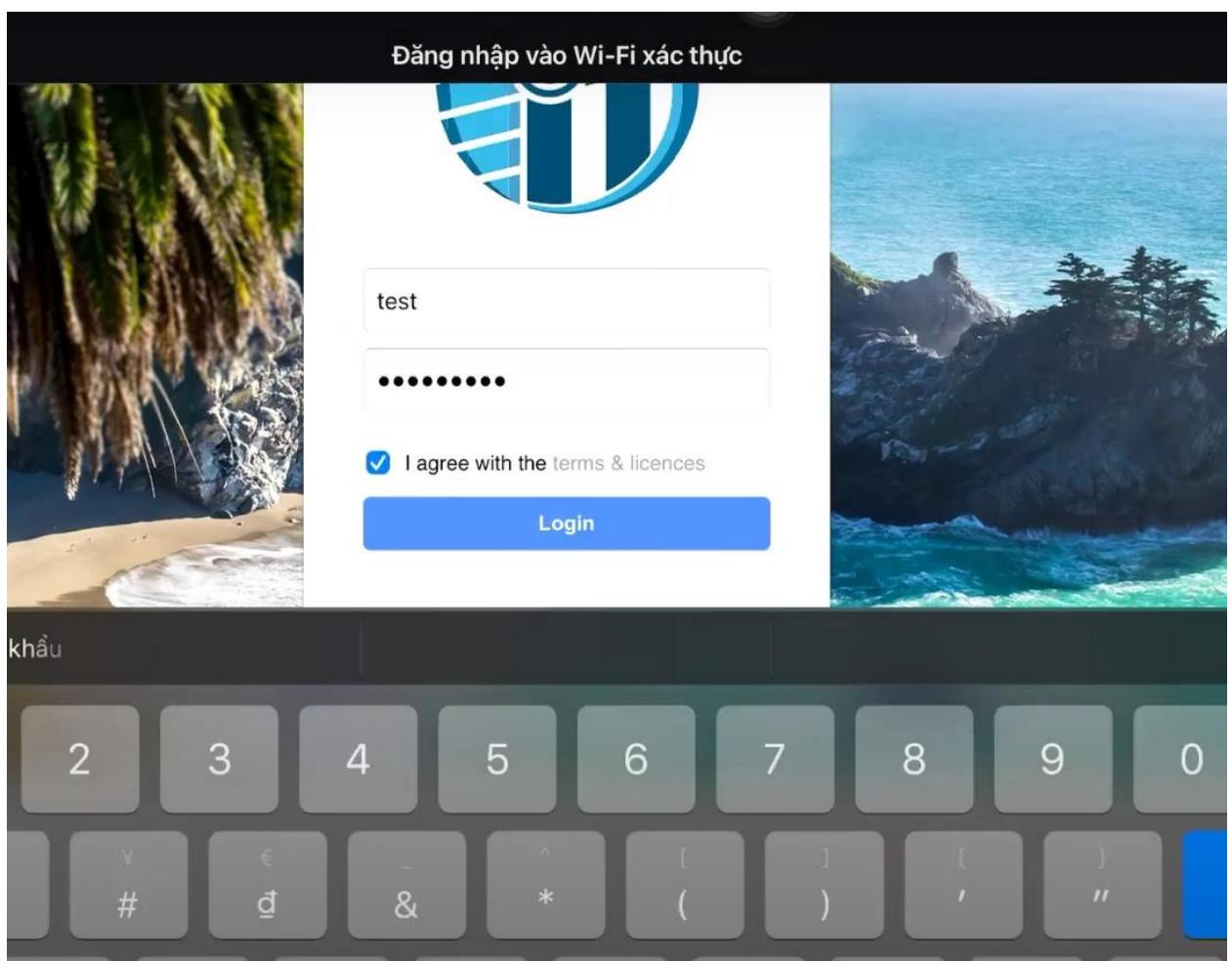
You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.

Secondary authentication Server

NPS
Local Database

You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated logins. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication, leave this setting empty.

- Lúc này ta quay lại client để kiểm tra xem RADIUS đã hoạt động chưa
Bằng cách kết nối WIFI. Nếu bắt nhập tài khoản thì RADIUS là hoạt động



BẤM VÀO ĐÂY ĐỂ XEM VIDEO HƯỚNG DẪN!!!

TÀI LIỆU THAM KHẢO

[1] ***Captive Portal / PfSense Documentation.***

<https://docs.netgate.com/pfsense/en/latest/captiveportal/index.html>.

[2] ***Services — DHCPV4 Server / PfSense Documentation.***

<https://docs.netgate.com/pfsense/en/latest/services/dhcp/ipv4.html>.

[3] ***pfSense® software Configuration Recipes — Authenticating from Active Directory using RADIUS/NPS / pfSense Documentation.***

<https://docs.netgate.com/pfsense/en/latest/recipes/radius-windows.html>.