

## MỤC LỤC

<b>1. NHU CẦU THỰC TẾ.....</b>	<b>2</b>
<b>2. GIỚI THIỆU GIẢI PHÁP VỀ CAPTIVE PORTAL.....</b>	<b>3</b>
2.1. Captive portal.....	3
2.2. Cơ chế hoạt động.....	4
2.3. Giải pháp PFsense.....	4
2.4. Mô hình giải pháp.....	5
<b>3. TRIỂN KHAI CAPTIVE PORTAL.....</b>	<b>7</b>
3.1. Giới thiệu.....	7
3.1.1. Máy Laptop.....	8
3.1.2. Máy pfSense.....	8
3.1.3. Internet.....	9
3.1.4. Radius server.....	9
3.1.5. Laptop or mobile other.....	9
3.2. Cấu hình PFsense.....	9
3.2.1. Cài đặt pfSense.....	9
3.2.2. Cấu hình các cổng giao diện.....	12
3.2.3. Cấu hình DHCP server.....	13
3.2.4. Cấu hình Firewall.....	14
3.2.5. Cấu hình Captive Portal.....	17
3.2.6. Cấu hình Radius.....	18
3.2.7. Kiểm tra hoạt động.....	30

## 1. NHU CẦU THỰC TẾ

Trong thời buổi hiện nay, nhu cầu kết nối mạng không dây cho các thiết bị cầm tay hay di động ngày càng tăng cao. Do sự phổ biến của nó ngày càng rộng rãi nên độ tin cậy giảm xuống. Lấy một ví dụ đơn giản ở các khu vực như trường học, quán cafe hay khách sạn chẳng hạn. Khi một người muốn kết nối vào mạng không dây ở một trong các khu vực đó, công việc của họ là đơn giản đi hỏi những người xung quanh đã truy cập vào mạng đó để lấy thông tin về khóa đăng nhập, sau đó họ có thể dễ dàng truy cập vào mạng không dây đó.

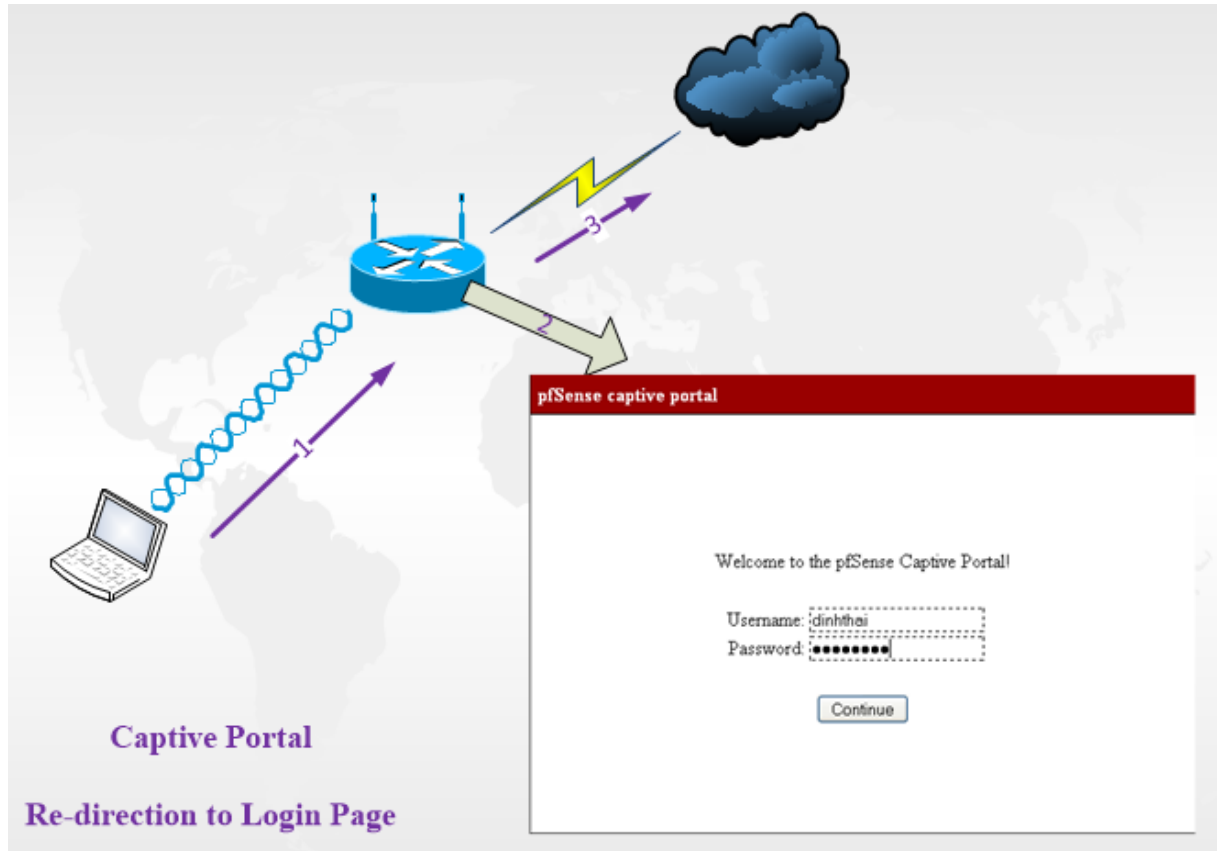
Nếu như có người truy cập vào hệ thống mạng vì mục đích xấu thì họ chỉ cần một vài công cụ hoặc phần mềm chuyên dụng thì họ có thể lấy các thông tin nhạy cảm của những người khác đang cùng kết nối vào khu vực đó một cách dễ dàng như thông tin username và password. Theo như trên thì rõ ràng độ tin cậy của mạng không dây đó đã giảm xuống đáng kể.

Để khắc phục, ta có một giải pháp chung để giải quyết vấn đề trên bằng cách là sẽ cho người dùng truy cập vào mạng không dây của tổ chức một cách tự do. Sau đó khi một người dùng muốn duyệt web (vì các thông tin nhạy cảm thường các là các số thẻ ngân hàng dùng để mua bán online hoặc username và password cho một tổ chức nào đó ở trên mạng Internet), họ sẽ mở trình duyệt web (firefox, chrome) gõ vào thanh địa chỉ tên miền muốn vào. Ngay lập tức trình duyệt sẽ tự động chuyển hướng sang một trang web tạm thời khác yêu cầu phải có username và password đặc biệt nhận được từ tổ chức phát ra mạng không dây đó mới có thể truy cập vào Internet.

Điều này làm giảm độ rủi ro về việc mất mát thông tin nhạy cảm cũng như giảm thiểu việc mất mát bằng thông cho những người truy cập không minh bạch và đặc biệt là tránh những người dùng có mục đích xấu.

## 2. GIỚI THIỆU GIẢI PHÁP VỀ CAPTIVE PORTAL

### 2.1. Captive portal



Captive portal là một kỹ thuật buộc người dùng web phải chuyển hướng tới một trang web đặc biệt (thường sử dụng cho mục đích chứng thực) trước khi được truy cập Internet. Kỹ thuật Captive portal biến Web browser trở thành một công cụ chứng thực hiệu quả. Việc này được thực hiện thông qua việc ngăn chặn tất cả các gói tin (bất kể địa chỉ IP và port) cho đến khi nào người dùng mở web browser lên và thử truy cập vào Internet. Trong thời gian đó, web browser sẽ tự động chuyển hướng sang một trang web đặc biệt sử dụng cho việc chứng thực, trả tiền cho việc truy cập internet theo thông tin đưa ra hoặc có thể đơn giản hơn chỉ là thông tin nội quy về việc sử dụng Internet. Captive portal được sử dụng nhiều trong các ứng dụng wifi hotspot.

## 2.2. Cơ chế hoạt động

### Redirection by HTTP

Nếu một người dùng chưa xác thực yêu cầu liên kết tới 1 trang web bất kì (bằng cách gõ tên miền trang web và sử dụng địa chỉ IP truy vấn được từ tên miền đó). Lúc này, web browser sẽ gửi một gói HTTP request với địa chỉ đích là địa chỉ IP của trang web đó. Tuy nhiên, gói tin request này bị chặn bởi firewall và sau đó được chuyển tiếp đến một redirect server. Redirect server này sẽ trả lời lại bằng một gói HTTP response chứa status code 302 để chuyển hướng người dùng tới Captive portal. Về phía người dùng thì tiến trình này hoàn toàn trong suốt.

## 2.3. Giải pháp PfSense



PfSense là một FreeBSD mã nguồn mở được sử dụng như một tường lửa và bộ định tuyến. Ưu điểm của pfSense là sự mạnh mẽ, cùng với sự linh hoạt và đơn giản trong việc thiết lập tường lửa và định tuyến, nó bao gồm luôn một dải các tính năng và các gói cài đặt thêm, giúp cho việc mở rộng thêm các chính sách bảo mật khác trong khi vẫn giữ nguyên các thiết lập tường lửa của hệ thống.

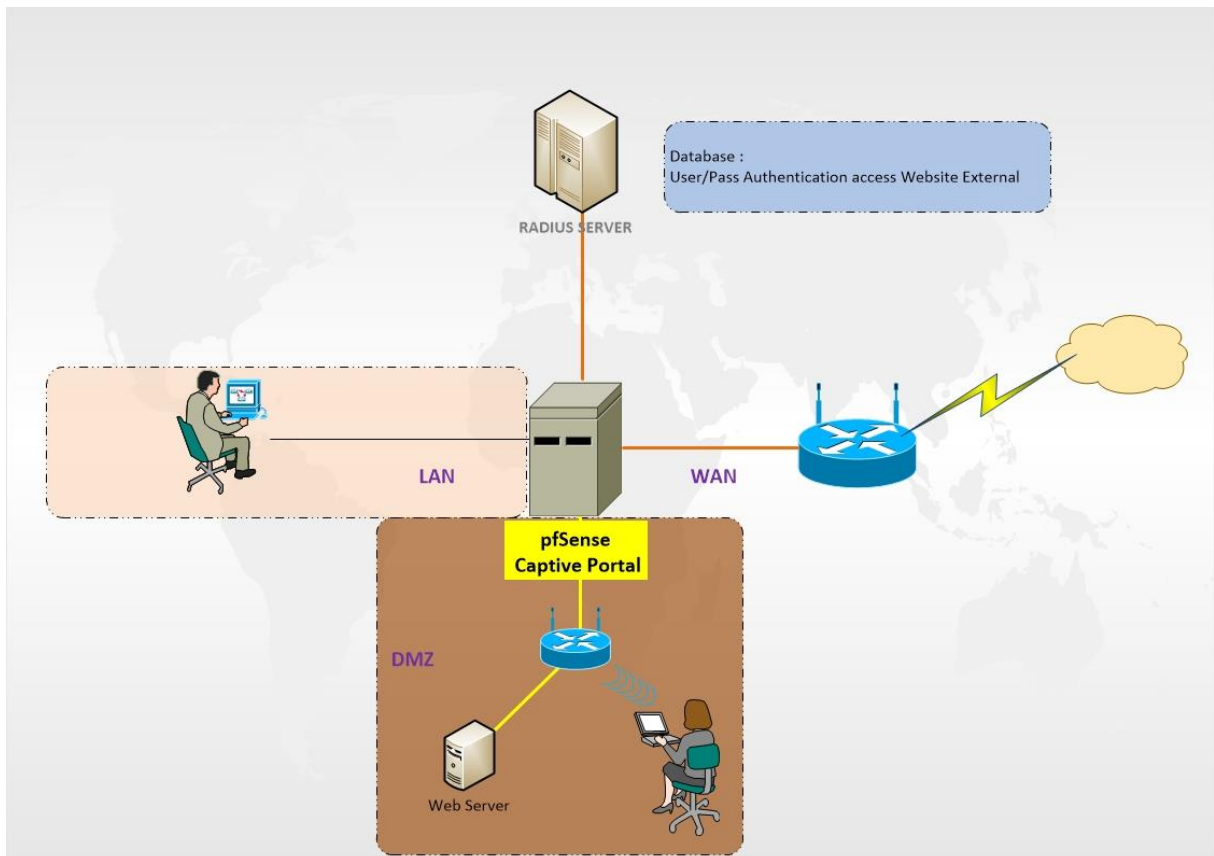
PfSense cung cấp cơ chế Captive portal cùng với việc sử dụng các tính năng tường lửa mạnh mẽ. Giúp cho hệ thống được bảo mật tốt hơn. pfSense sử dụng cơ chế Redirection by HTTP cho Captive portal. Tức các gói tin HTTP request được gửi từ các nguồn chưa được xác thực đến interface của pfSense, thì các nguồn này đều được chuyển hướng đến một trang web đặc biệt yêu cầu chứng thực trước khi có thể đi ra Internet.

PfSense khuyến khích người quản trị triển khai Captive portal trên interface kết nối với khu vực DMZ. DMZ là viết tắt của Demilitarized Zone (vùng phi quân sự), là một khu vực mạng nhỏ nằm trong một tổ chức (xem hình 1). Thường chứa các dịch vụ

không tin cậy như web server nhằm phục vụ cho các người dùng bên ngoài Internet. Khu vực này tách biệt hoàn toàn với mạng LAN và được kiểm duyệt không nghiêm ngặt bởi các thiết lập tường lửa khi có dữ liệu muốn đi vào. Việc triển khai mạng không dây nằm trong vùng DMZ và được kiểm duyệt xác thực bởi Captive portal khi có người dùng muốn đi vào Internet sẽ tăng cường độ bảo mật của hệ thống mạng đáng kể.

## 2.4. Mô hình giải pháp

Mô hình:



Mô hình giải pháp bao gồm:

- 1 Access Point hoặc 1 Wireless Modem thiết lập ở chế độ Access Point Mode.
- Dùng để cung cấp mạng không dây cho các thiết bị di động không dây.

- 1 Máy chủ cài đặt pfSense làm tường lửa, DHCP server cho 2 cổng LAN, DMZ và cài đặt dịch vụ Captive portal trên cổng DMZ nhằm mục đích xác thực người dùng trong khu vực này khi họ muốn ra ngoài Internet.

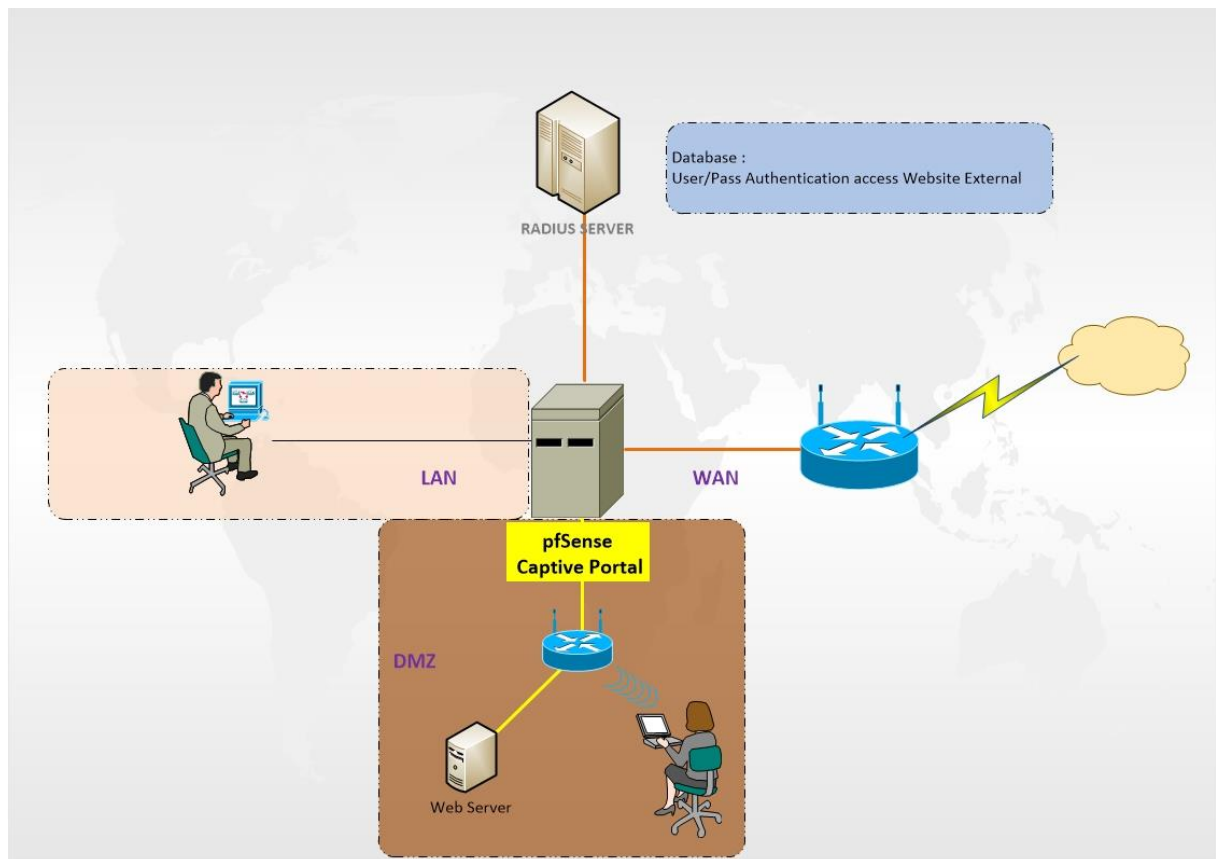
- 1 Máy client nằm trong LAN. Nhận địa chỉ IP động từ DHCP server của pfSense, dùng web browser truy cập vào địa chỉ gateway nhận được để giám sát, cấu hình pfSense thông qua giao diện web.

### 3. TRIỂN KHAI CAPTIVE PORTAL

#### 3.1. Giới thiệu

Bây giờ ta giả sử sẽ xây dựng một mạng không dây cho một khách sạn vừa. Với yêu cầu là mọi khách hàng thuê phòng nếu muốn lướt Internet thì đều phải liên hệ với quầy tiếp tân, đóng tiền để nhận được một account đăng nhập dùng để xác thực khi mở trình duyệt web lên. Các khách hàng khác nếu không liên hệ với tiếp tân và đóng tiền thì không thể truy cập Internet.

Sau đây ta sẽ thực hiện 1 bài LAB ảo mô tả việc trên một cách đơn giản nhằm mục đích hiểu thêm về giải pháp. Sau đây là mô hình của bài LAB:

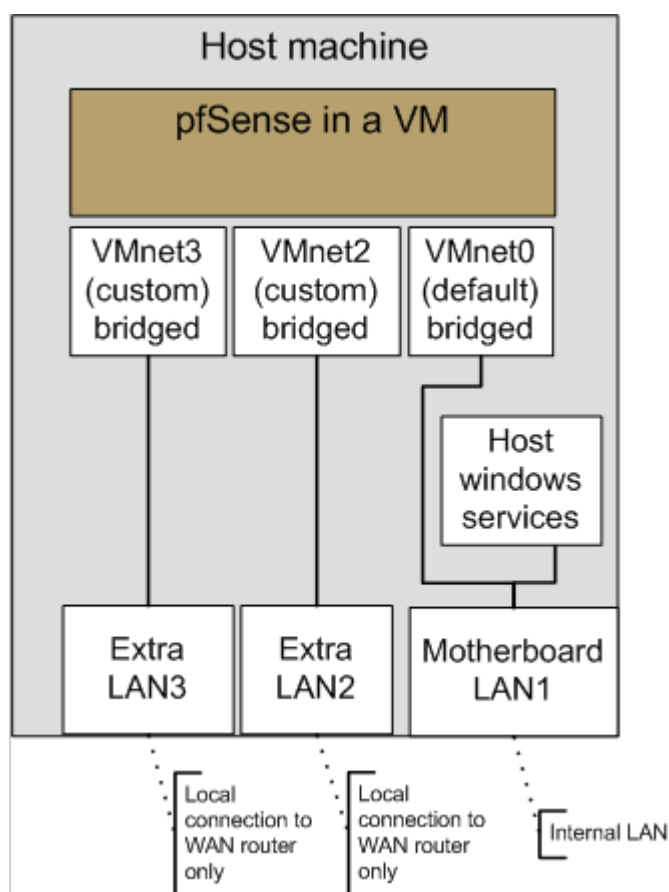


Theo mô hình này ta sẽ sử dụng 1 Laptop, 1 Access point và 1 thiết bị di động để thực hiện bài LAB. Sau đây là các mô tả thêm cho bài LAB:

### 3.1.1. Máy Laptop

Trên mô hình là máy thật. Được dùng như là client trong hệ thống mạng LAN của khách sạn. Mục đích chính là sử dụng trình duyệt web để cấu hình cho pfSense thông qua giao diện web. Là máy cung cấp phần mềm ảo hóa VMware để cài đặt 2 máy pfSense và Web Server. Sử dụng 1 card mạng ảo VMnet 1 để giao tiếp với máy pfSense và không dùng card thật của chính máy này để giả sử rằng máy Laptop chỉ là client trong mạng LAN của pfSense.

### 3.1.2. Máy pfSense



Là máy ảo được tạo ra bởi phần mềm VMware ở máy Laptop. Sử dụng 4 card mạng là 4 card ảo là Vmnet0 (bridged: card Wireless), VMnet 1 (Host only) LAN, Vmnet2 (Host only) RADIUS, VMnet 3 (Host only) DMZ, của máy Laptop nhằm mục đích cung cấp dịch vụ Captive portal cho cổng giao diện đó. Ngoài ra máy pfSense server sẽ cung cấp thêm tường lửa cùng với DHCP Server để gán địa chỉ động của cho các máy client.



**3.1.3. Internet**

Là mạng thật. Sử dụng 1 card mạng duy nhất là VMnet 0 để giao tiếp với cổng WAN của máy pfSense.

**3.1.4. Radius server**

Là máy ảo sử dụng card VMnet 2 dùng làm Server cung cấp user và password cho Client thông qua chứng thực Radius.

**3.1.5. Laptop or mobile other**

Là máy wireless client truy cập vào mạng không dây và vào Internet bằng cách gõ địa chỉ bất kì vào trình duyệt.

**3.2. Cấu hình PFsense****3.2.1. Cài đặt pfSense**

Như khi này ta đã tạo ra 1 máy ảo pfSense. Bây giờ ta sẽ tiến hành cấu hình từng bước. Đây là menu lúc khởi động. Ta sẽ chờ hết thời gian mặc định hoặc chọn tùy chọn số 1 để tiến hành boot pfSense.

pfSense sẽ cấp địa chỉ IP động ở cổng WAN, và 3 cổng còn lại chưa cấu hình sẽ không có IP (NONE).

Nhưng cấu hình pfSense, ta phải dùng đến cổng LAN để cấu hình, ta tiến hành đặt IP cho cổng LAN như sau:

- Ở menu ta chọn số 2, và tiến hành đặt IP, subnet. Mình sẽ đặt IP cho cổng LAN là 10.0.0.65 subnet 255.255.255.0 và không cấp DHCP.

```
Please wait while the changes are saved to WAN... Reloading filter...
DHCPD...

The IPv4 WAN address has been set to dhcp
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://dhcp/

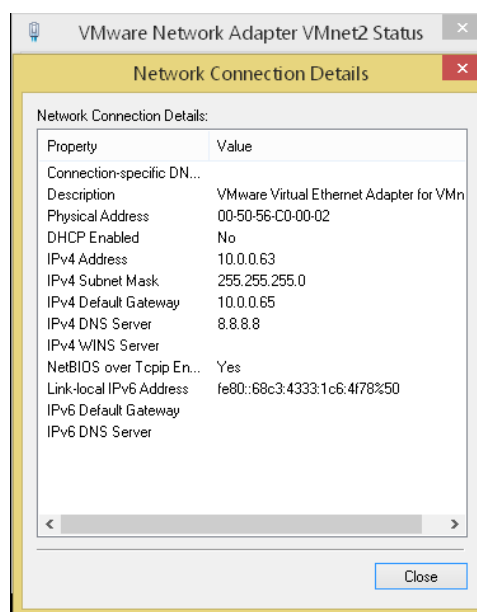
Press <ENTER> to continue.
*** Welcome to pfSense 2.0.1-RELEASE-cdrom (i386) on pfSense ***

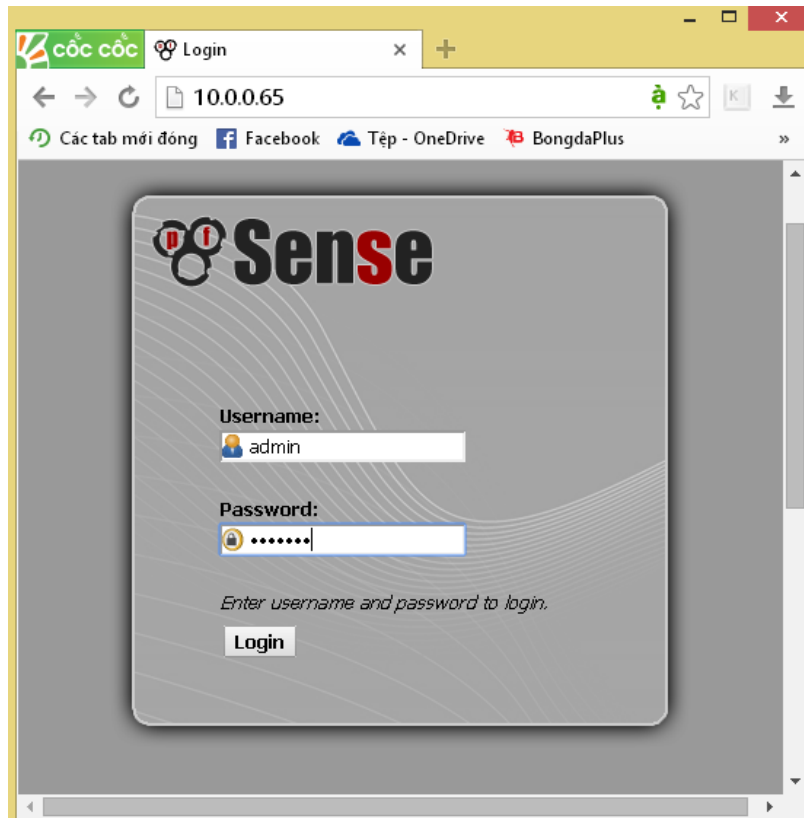
WAN (wan)          -> em0          -> NONE (DHCP)
LAN (lan)          -> em1          -> 10.0.0.65

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults    12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                14) Enable Secure Shell (sshd)
7) Ping host
99) Install pfSense to a hard drive, etc.

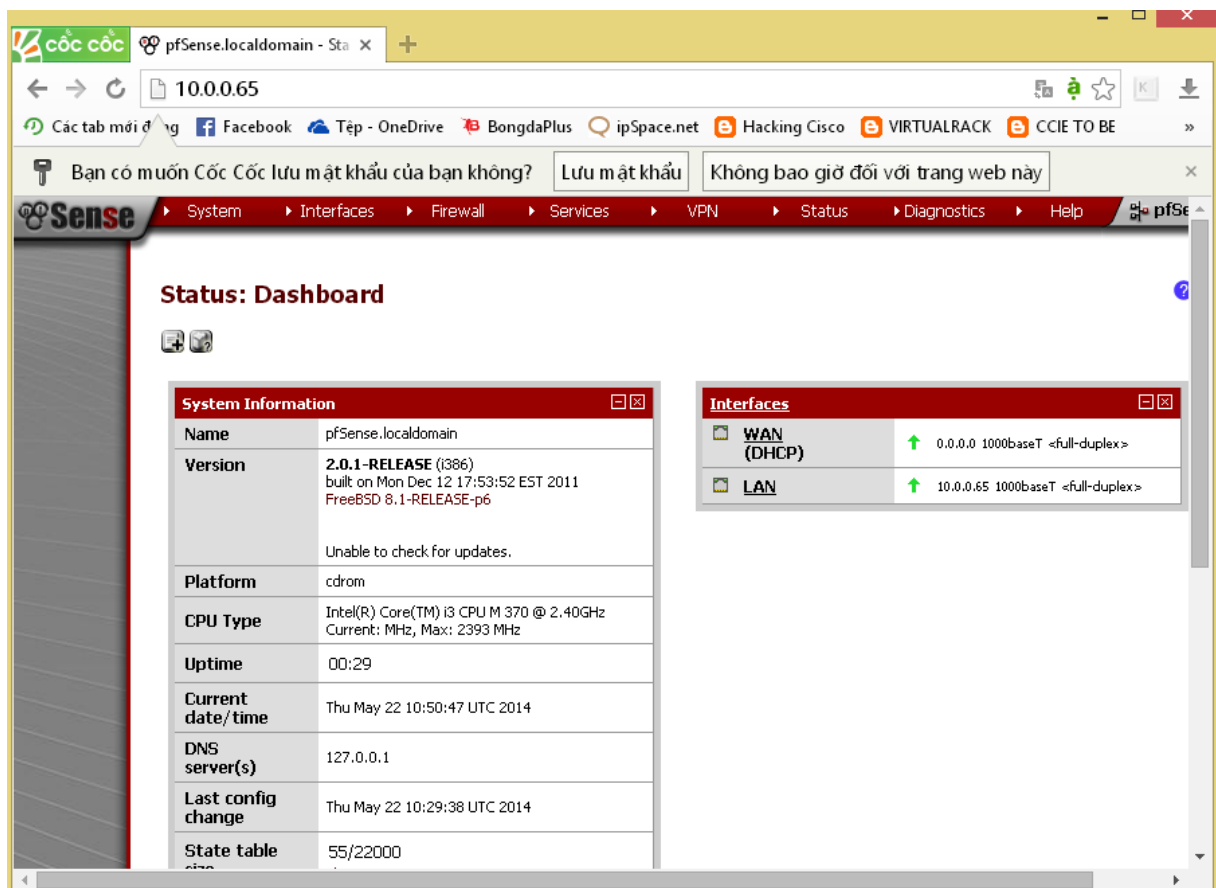
Enter an option: █
```

Tiếp tục ta sẽ dùng máy Laptop vào card Vmnet1 đặt IP là 10.0.0.63 để cấu hình pfSense thông qua giao diện web mà pfSense đã cung cấp bằng cách mở 1 trình duyệt web bất kì lên và gõ “https://10.0.0.65” đúng với địa chỉ gateway mà pfSense đã gán cho cổng đó với username và password mặc định lần lượt là “admin” và “pfsense”.





Giao diện pfSense hiện ra :



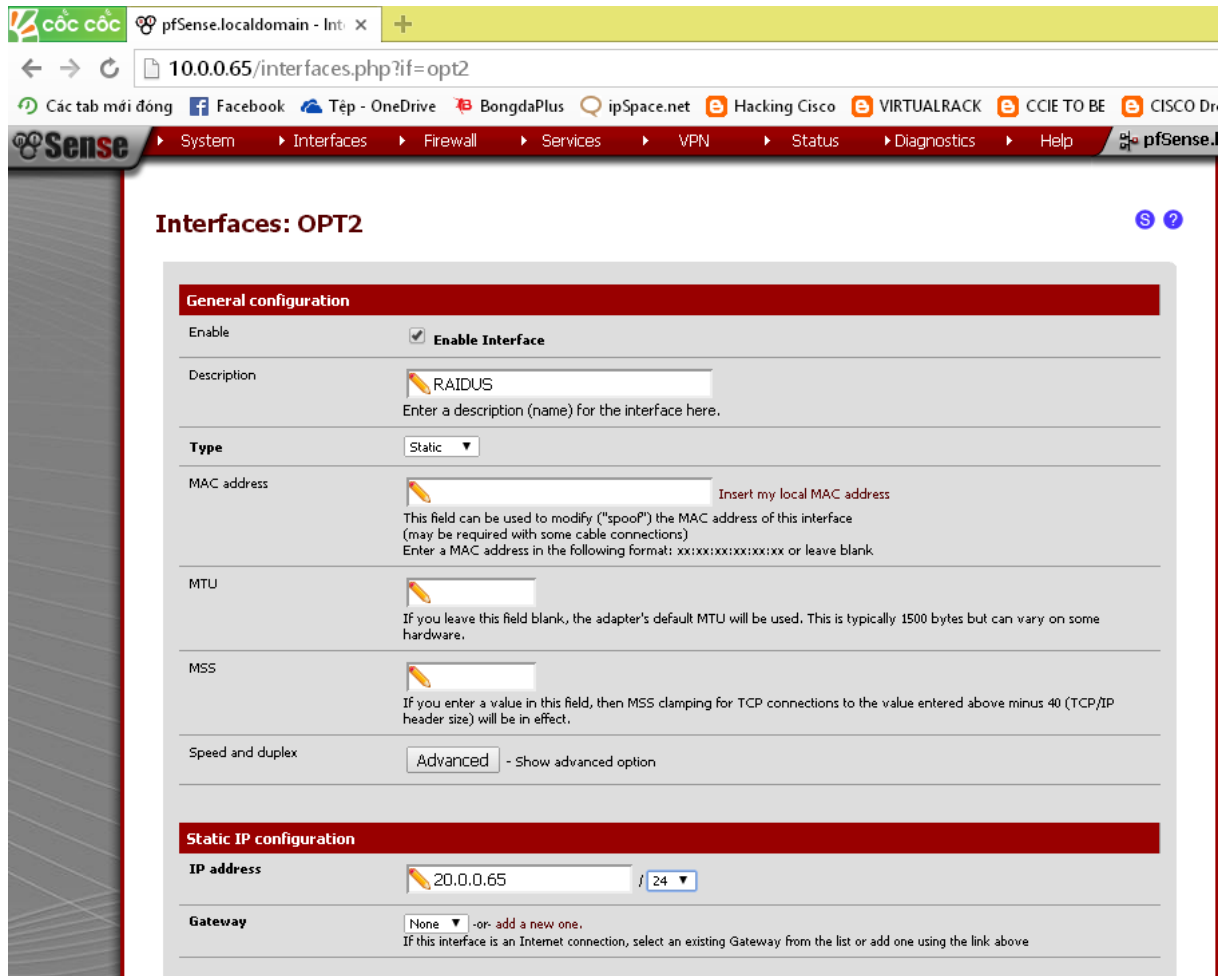
### 3.2.2. Cấu hình các cổng giao diện

- Cổng WAN và LAN đều đã có IP, nên tiếp theo ta sẽ thiết lập cổng Interfaces -> OPT1. Enable Interface -> Description là DMZ, type: Static, IP address là 192.168.0.65/24 như trên mô hình. Sau đó Save thiết lập lại.

The screenshot shows the pfSense web interface for configuring interface OPT1. The browser address bar shows '10.0.0.65/interfaces.php?if=opt1'. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'Interfaces: OPT1' page is displayed with the following configuration:

- General configuration**
  - Enable: ☒ **Enable Interface**
  - Description:  (Enter a description (name) for the interface here.)
  - Type: **Static**
  - MAC address:  (Insert my local MAC address. This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.)
  - MTU:  (If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.)
  - MSS:  (If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.)
  - Speed and duplex: **Advanced** - Show advanced option
- Static IP configuration**
  - IP address:  / **24**
  - Gateway: **None** -or- add a new one. (If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above)

- Tương tự ta cũng sẽ thiết lập Interfaces -> OPT2. Enable Interface -> Description là RADIUS và IP address là 20.0.0.65/24 và cổng này sẽ nối với RADIUS Server

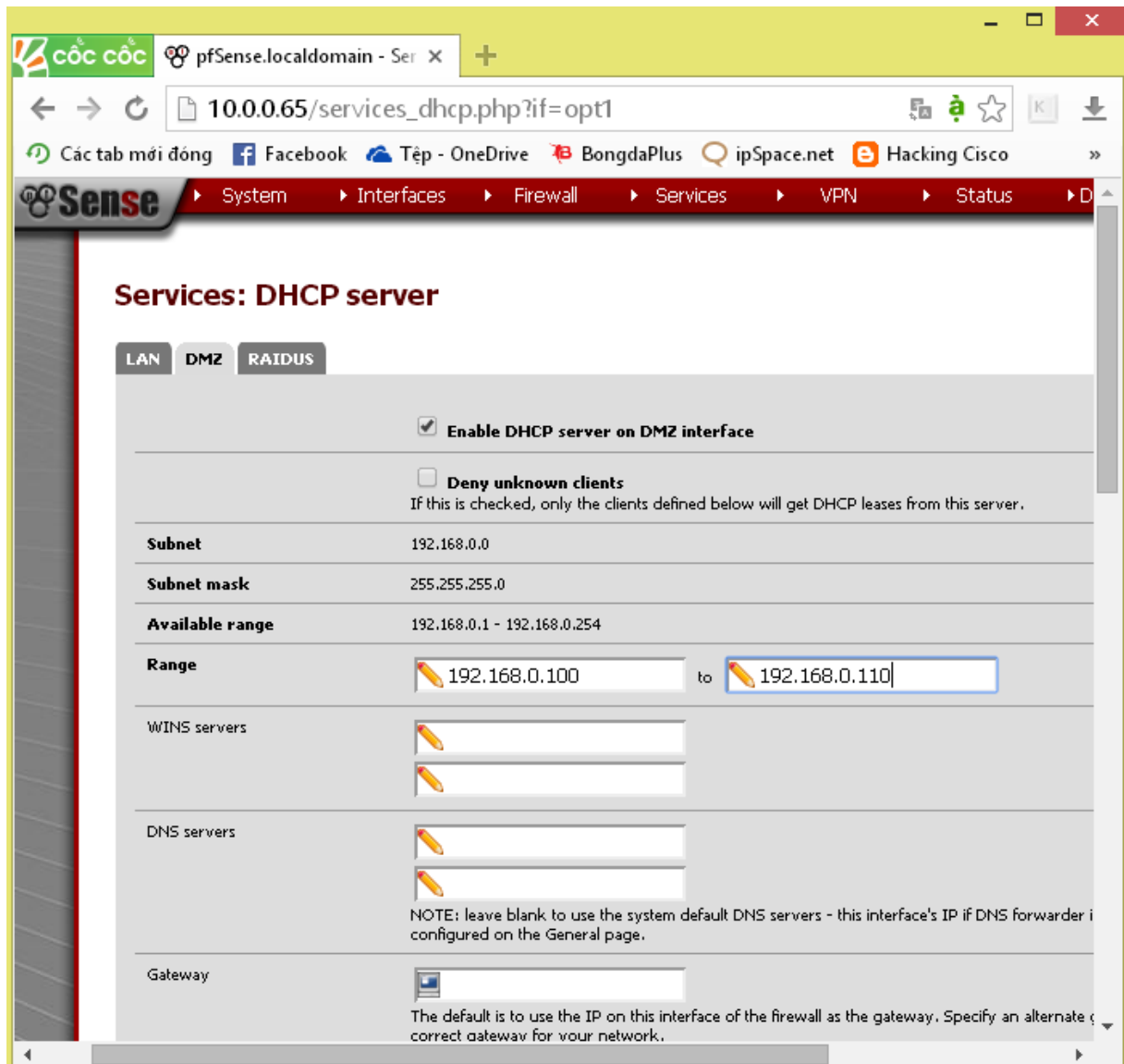


### 3.2.3. Cấu hình DHCP server

Mặc định chỉ có cổng LAN cấp địa chỉ IP động cho client trong vùng. Bước này ta sẽ cấu hình địa chỉ IP động cho cổng DMZ nơi mà các wireless client kết nối vào access point có thể nhận được địa chỉ để giao tiếp với các client khác.

Cấu hình DHCP Server bằng cách click vào tab Services -> DHCP server. Sau đó chọn tiếp qua tab con DMZ và thiết lập như sau:

1. Enable DHCP server on DMZ interface
2. Subnet, Subnet mask và Available Range là thông tin về đường mạng của DMZ interface
3. Range – Nhập vào dải IP muốn cấp dựa trên thông tin Available range
4. Do trong bài LAB không đề cập gì đến DNS và Domain nên ta sẽ bỏ trống

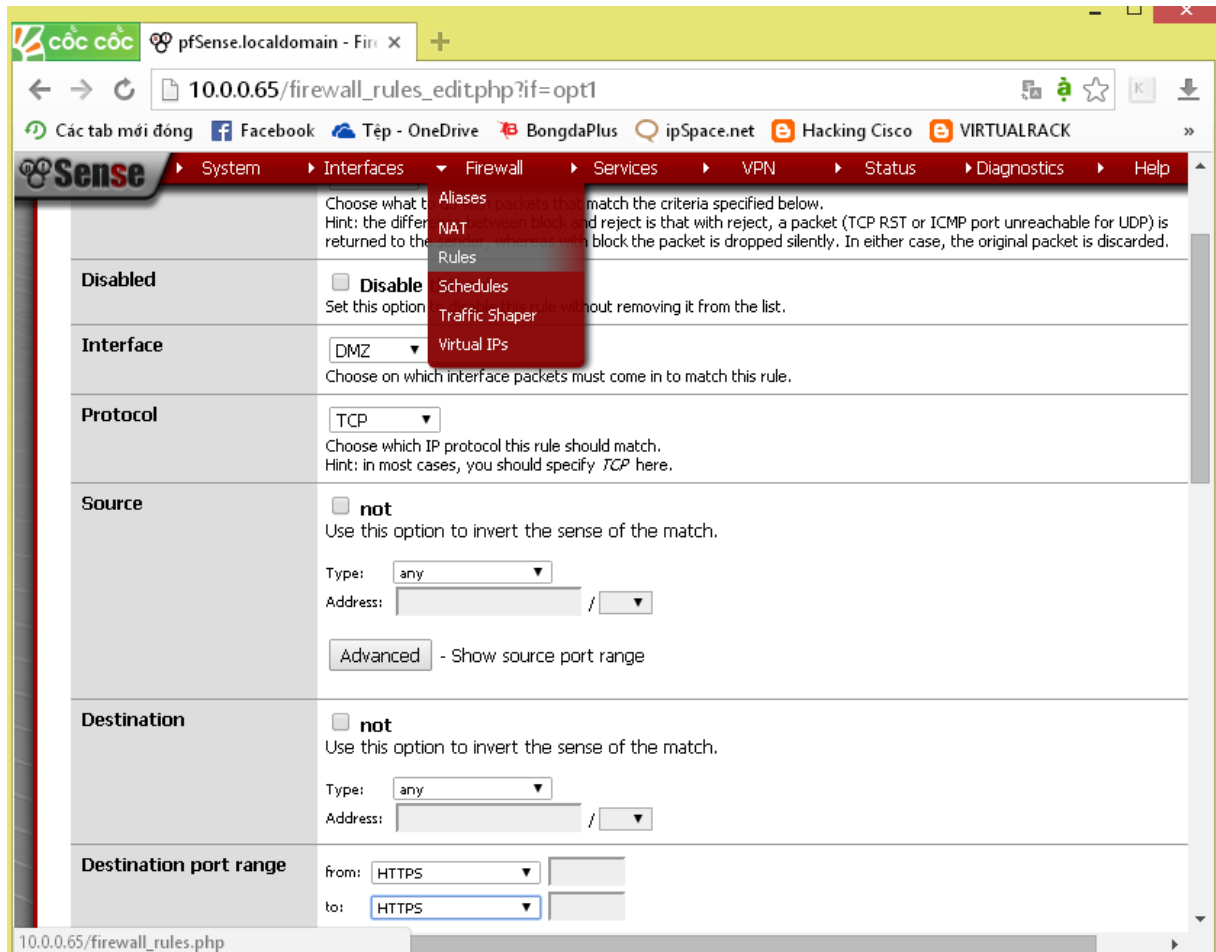


### 3.2.4. Cấu hình Firewall

Mặc định cổng WAN và LAN cũng đã có những firewall rules thích hợp cho mỗi cổng. Riêng cổng DMZ thì vẫn chưa thiết lập bất cứ thông số nào. Do mục đích của bài LAB là triển khai Captive portal trên cổng DMZ nên ta sẽ cấu hình firewall đơn giản trên cổng DMZ và không thiết lập thêm bất cứ chính sách nào trên chuỗi firewall của 2 cổng LAN và WAN nữa.

Do cổng DMZ của ta mặc định là cổng optional (tùy chọn) nên firewall không hề cho phép bất cứ lưu lượng nào đi qua cổng này. Mục đích của ta là cấu hình Captive portal, mà captive portal dựa trên cơ chế Redirection by HTTP khi người dùng gõ 1 tên miền

trang web nào đó lên web browser. Vậy ta sẽ cấu hình firewall cho phép các lưu lượng HTTP và HTTPS đi qua cổng này.



Sau khi tạo 2 firewall rules

**Firewall: Rules**

The settings have been applied. The firewall rules are now reloading in the background. You can also monitor the reload progress.

Floating WAN LAN DMZ RAIDUS

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	TCP	*	*	*	443 (HTTPS)	*	none		
<input type="checkbox"/>	TCP	*	*	*	80 (HTTP)	*	none		

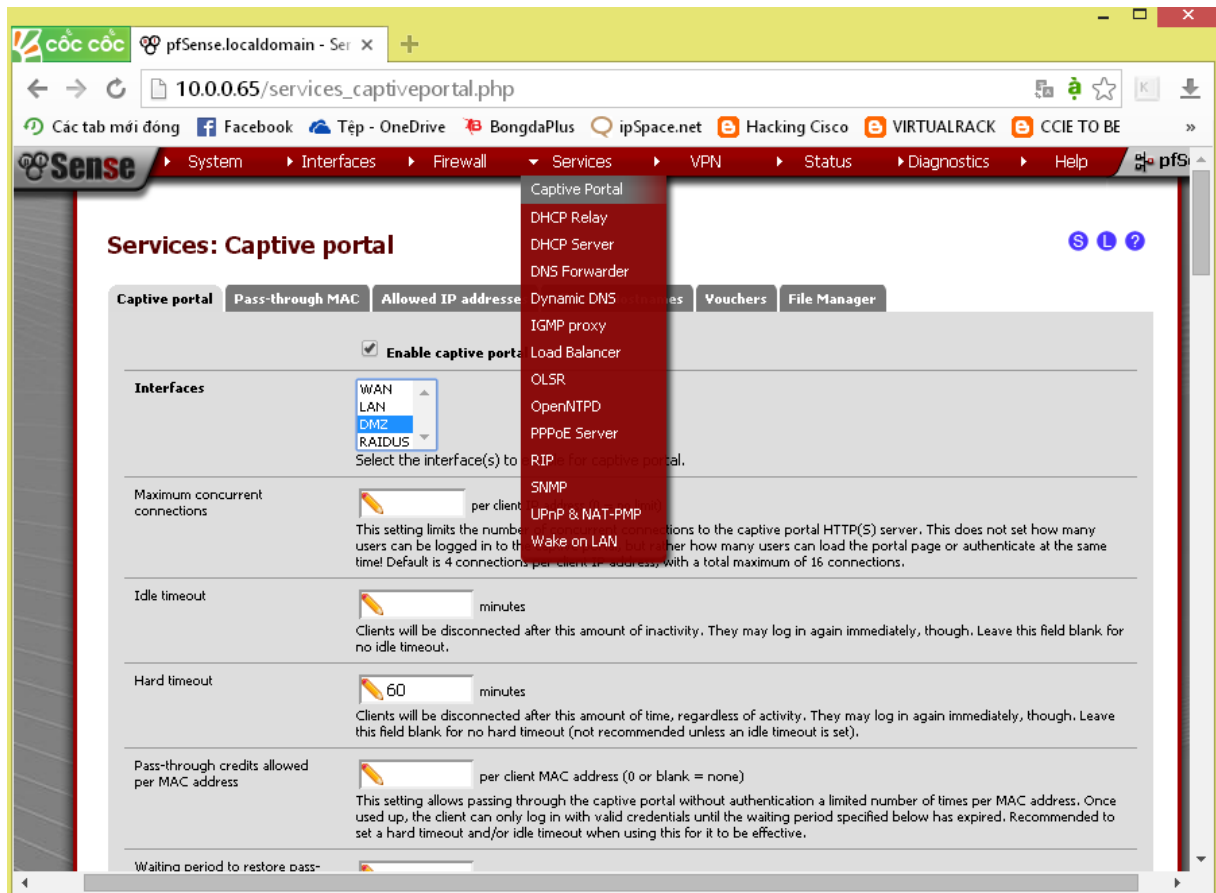
☒ pass  
☐ pass (disabled)
 ☒ block  
☐ block (disabled)
 ☒ reject  
☐ reject (disabled)
 ☒ log  
☐ log (disabled)

**Hint:**  
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

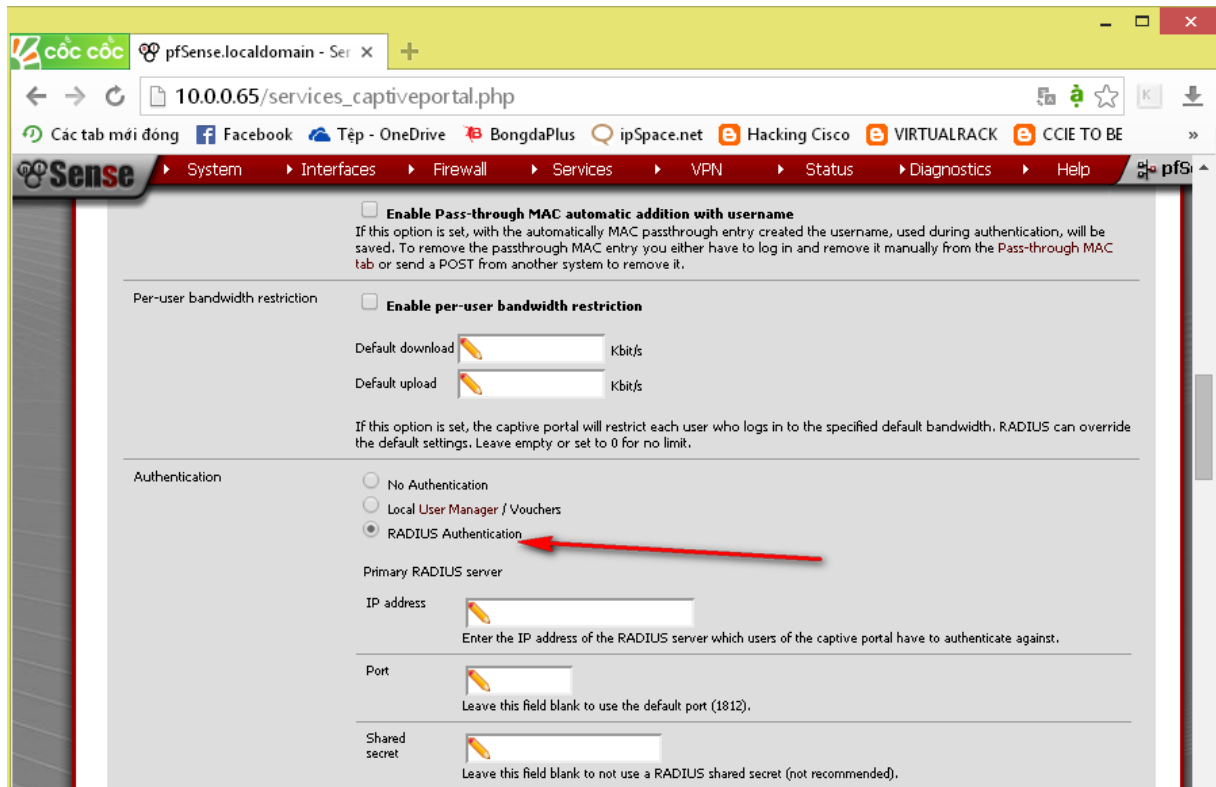


### 3.2.5. Cấu hình Captive Portal

Như đã giới thiệu ở trên, Captive portal sử dụng cơ chế Redirection by HTTP để điều hướng người dùng đến một trang web đặc biệt thông qua việc bắt nhận gói tin HTTP request. Để cấu hình Captive portal. Ta chọn tab Services -> Captive portal:



Phần Authentication ta sẽ chọn loại: chứng thực bằng Radius :



### 3.2.6. Cấu hình Radius.

Khi 1 Client truy cập đến 1 địa chỉ bất kì, lập tức Redirection HTTP sẽ chuyển hướng đến pfSense Firewall yêu cầu nhập users và password.

Lúc này Client cần 1 Account để đăng nhập, và ta sẽ cấu hình Radius quản lý users và cấp users cho các

Client có nhu cầu truy cập web.

Ta dùng win server 2k8 làm Radius server. Và sau đây là các bước cấu hình Radius server quản lý user:

1. Đầu tiên ta cài Domain cho server: Start -> cmd -> dcpromo bằng quyền Admin

**Active Directory Domain Services Installation Wizard**

**Name the Forest Root Domain**

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain:

Example: corp.contoso.com

< Back   Next >   Cancel

**Active Directory Domain Services Installation Wizard**

**Set Forest Functional Level**

Select the forest functional level.


Forest functional level:

Details:

The Windows Server 2008 R2 forest functional level provides all the features that are available in the Windows Server 2008 forest functional level, plus the following additional feature:

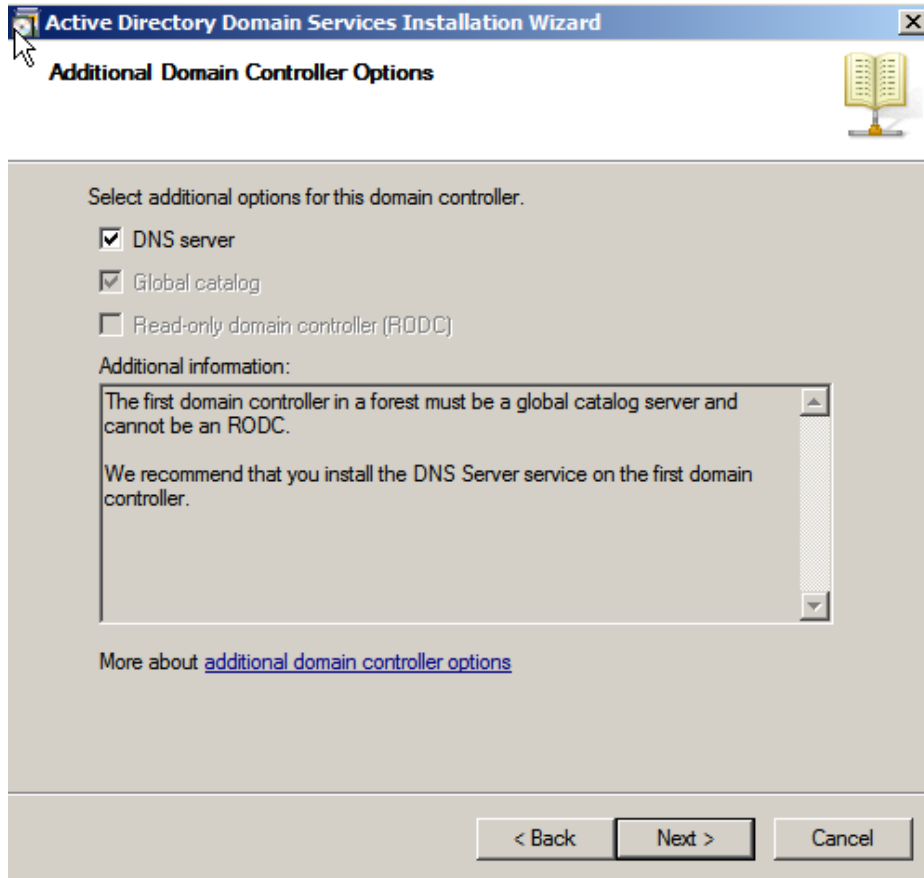
- Recycle Bin, which, when it is enabled, provides the ability to restore deleted objects in their entirety while Active Directory Domain Services is running.

Any new domains that are created in this forest will operate by default at the Windows Server 2008 R2 domain functional level.

 You will be able to add only domain controllers that are running Windows Server 2008 R2 or later to this forest.

More about [domain and forest functional levels](#)

< Back   Next >   Cancel



**Active Directory Domain Services Installation Wizard**

**Additional Domain Controller Options**

Select additional options for this domain controller.

- ☒ DNS server
- ☒ Global catalog
- ☐ Read-only domain controller (RODC)

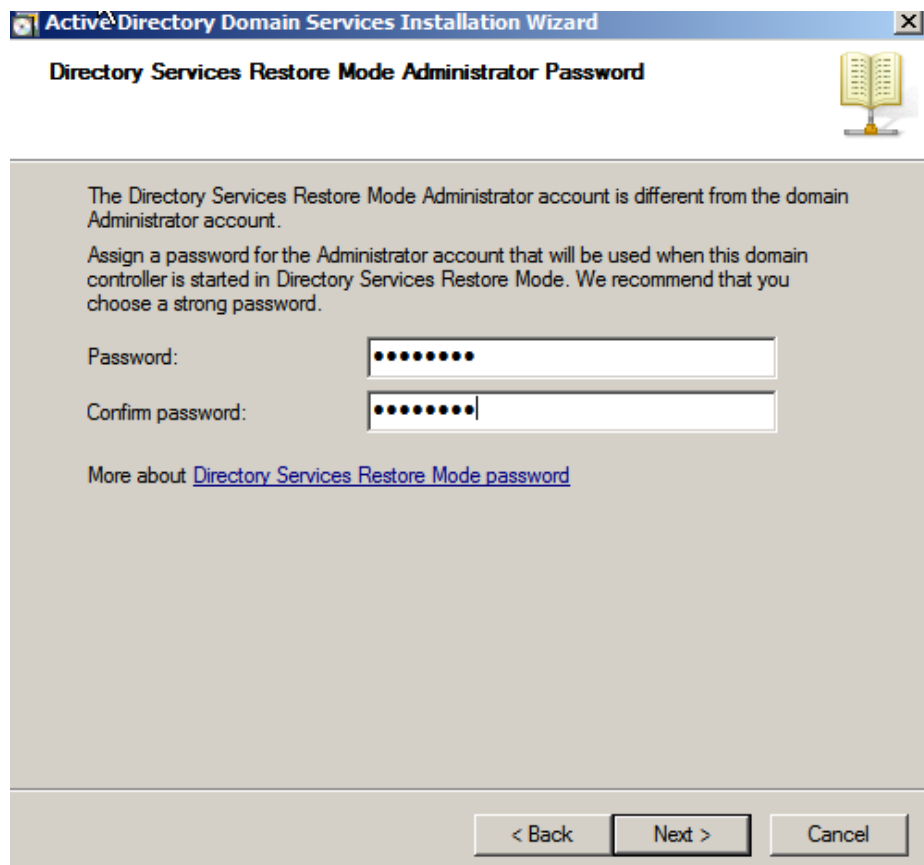
Additional information:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

We recommend that you install the DNS Server service on the first domain controller.

[More about additional domain controller options](#)

< Back   Next >   Cancel



**Active Directory Domain Services Installation Wizard**

**Directory Services Restore Mode Administrator Password**

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

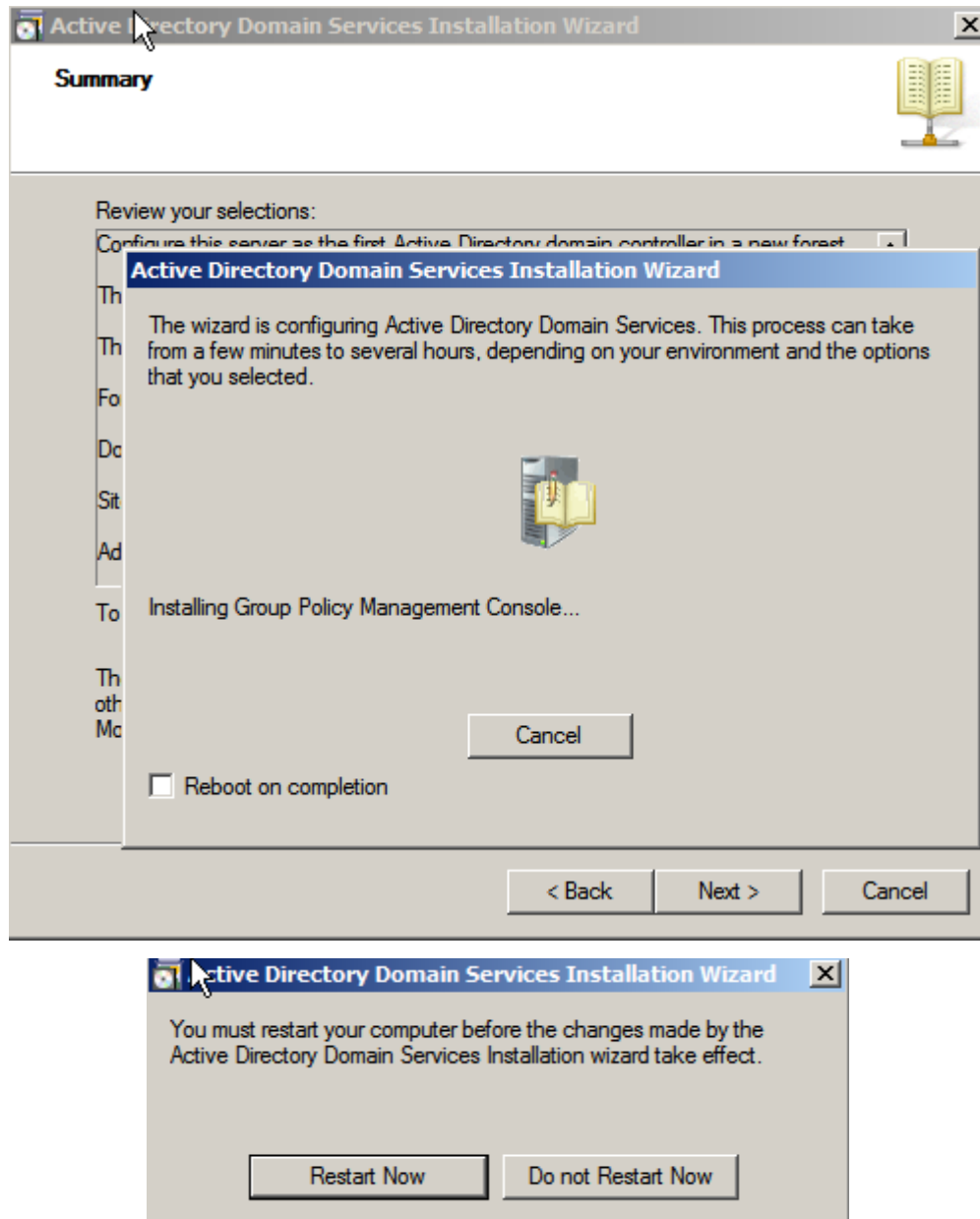
Password:

Confirm password:

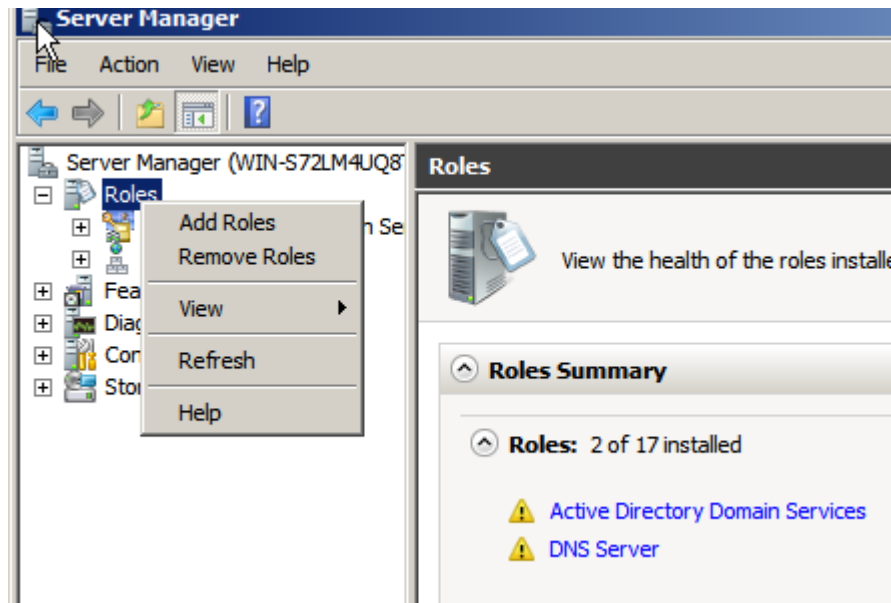
[More about Directory Services Restore Mode password](#)

< Back   Next >   Cancel

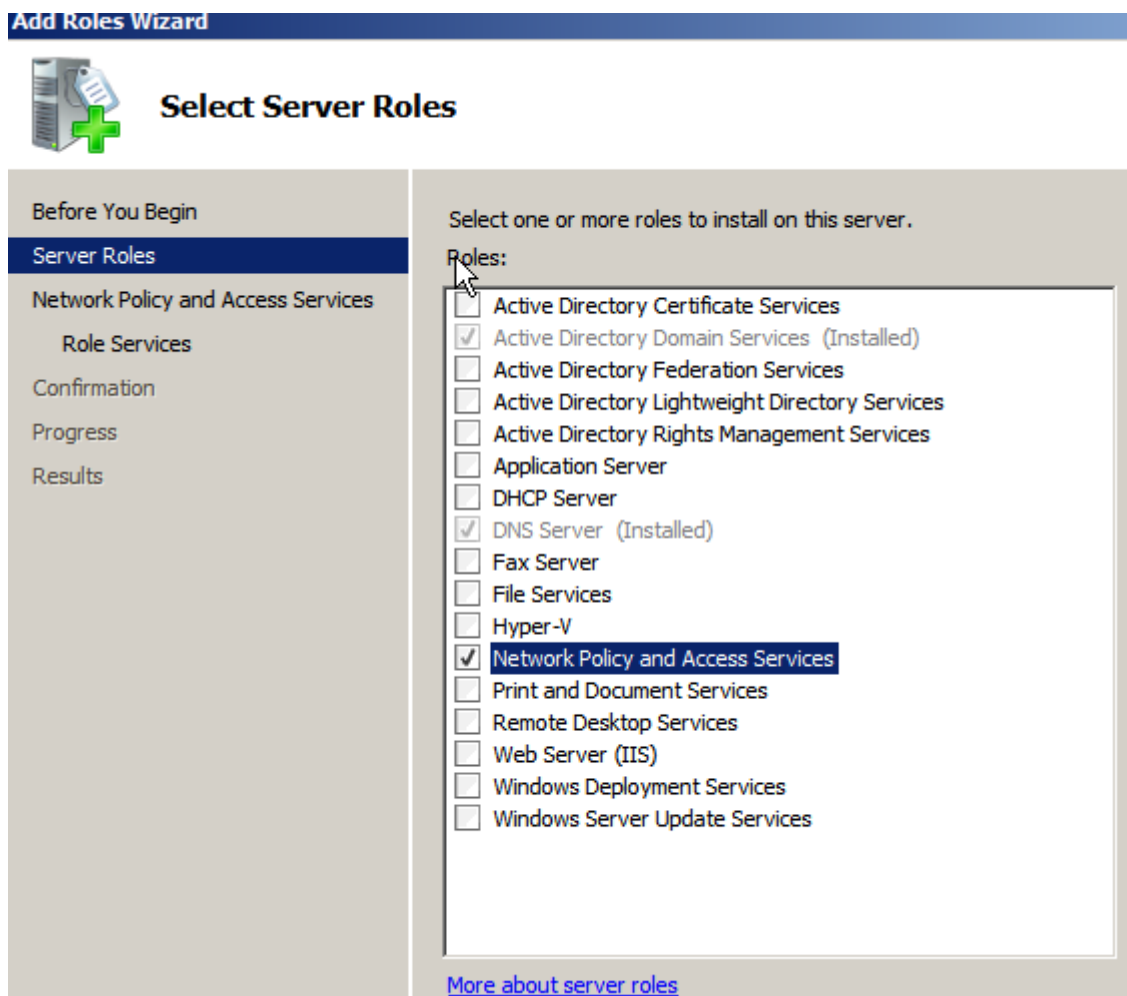
Khi hoàn thành cài đặt domain và hiện bảng yêu cầu restart máy, ta chọn restart.

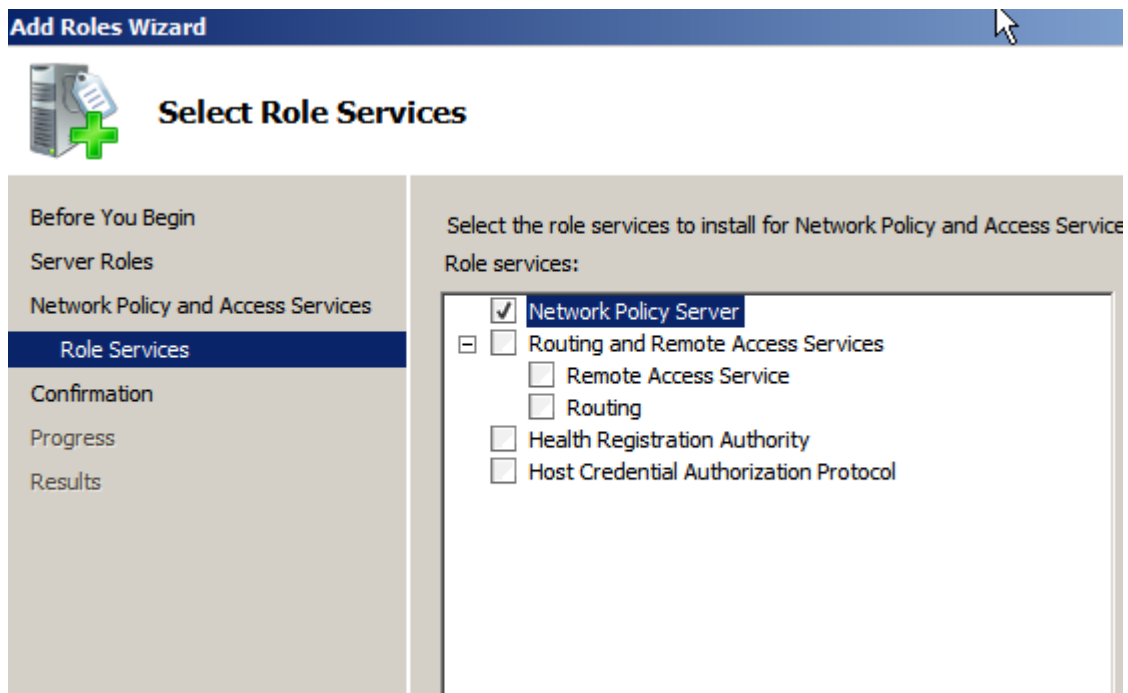


Sau khi khởi động xong ta vào Start -> Administrative Tools -> Server Manager, chọn Rules -> Add Rules.



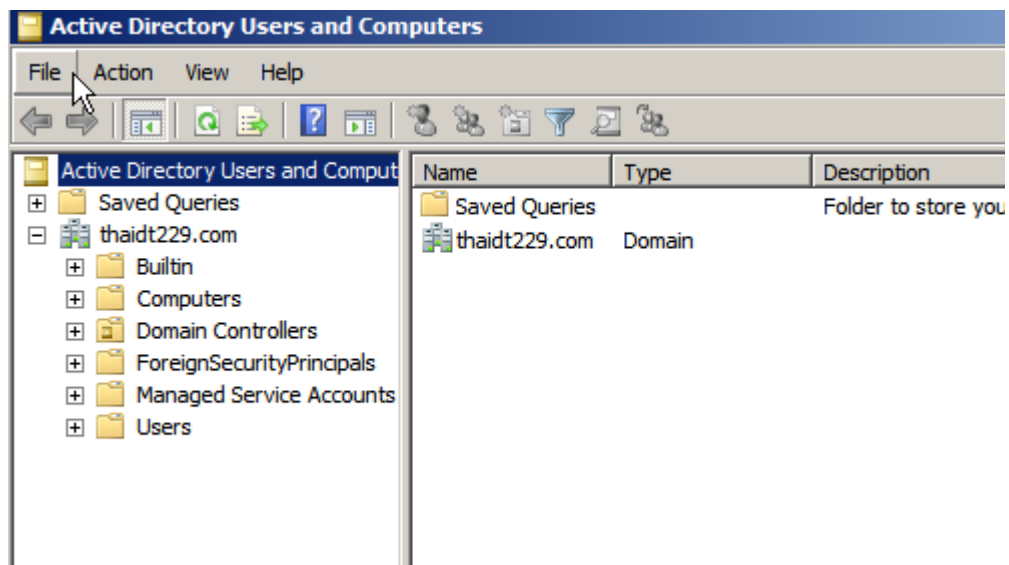
Chọn Network Policy and Access Services -> Network policy server(Radius)



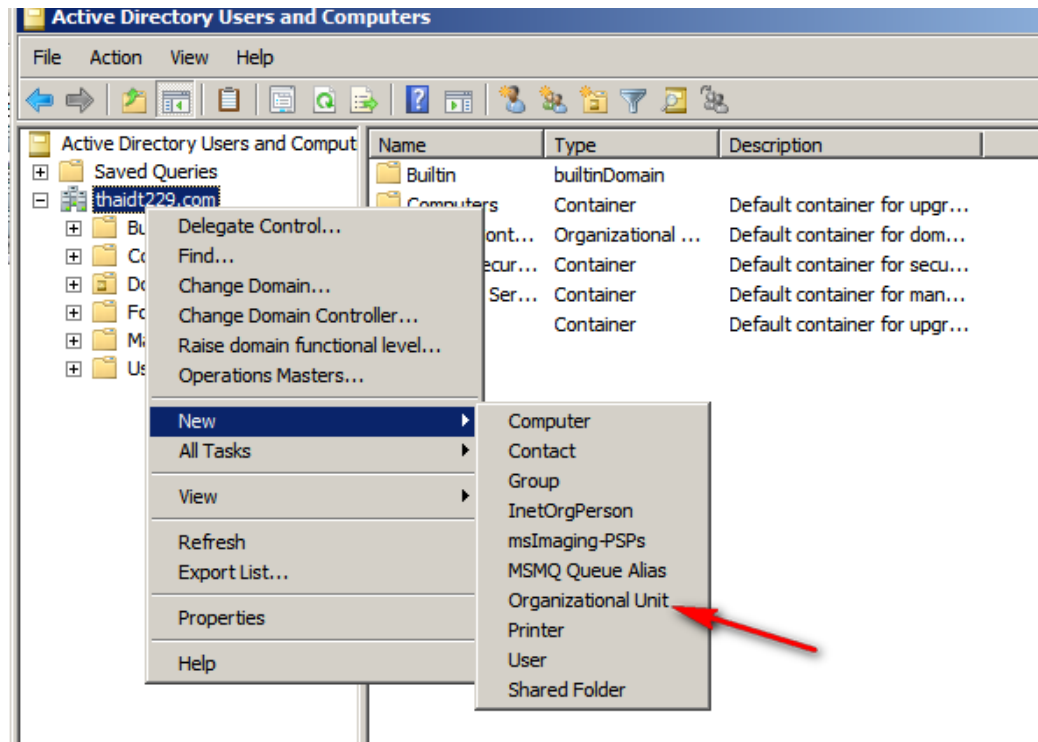


Và chờ đến khi hoàn thành.

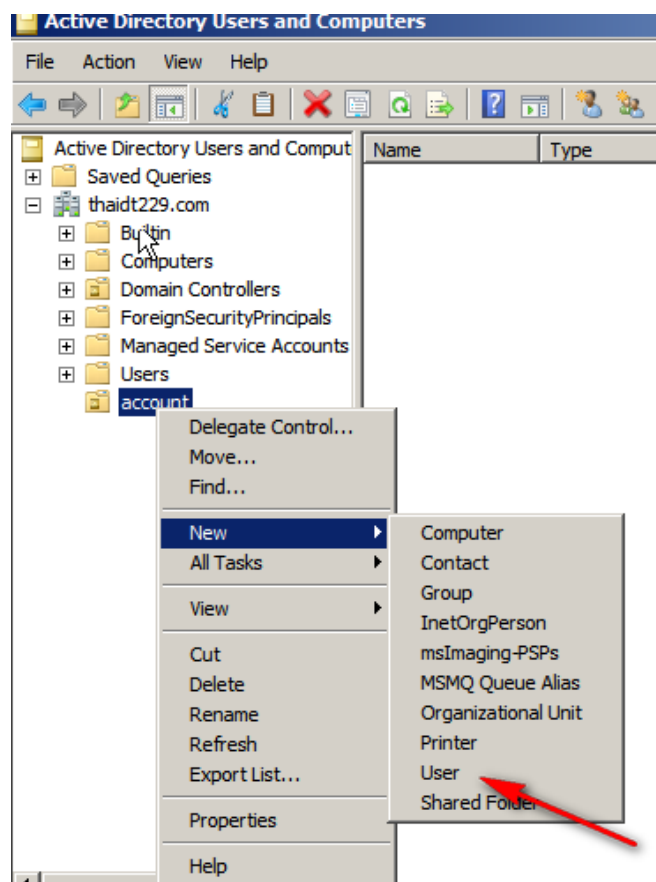
Tiếp theo, ta sẽ tạo Account cho Client bằng cách vào: Start -> Administrative tool -> Active Directory User and Computer



Tạo OU :



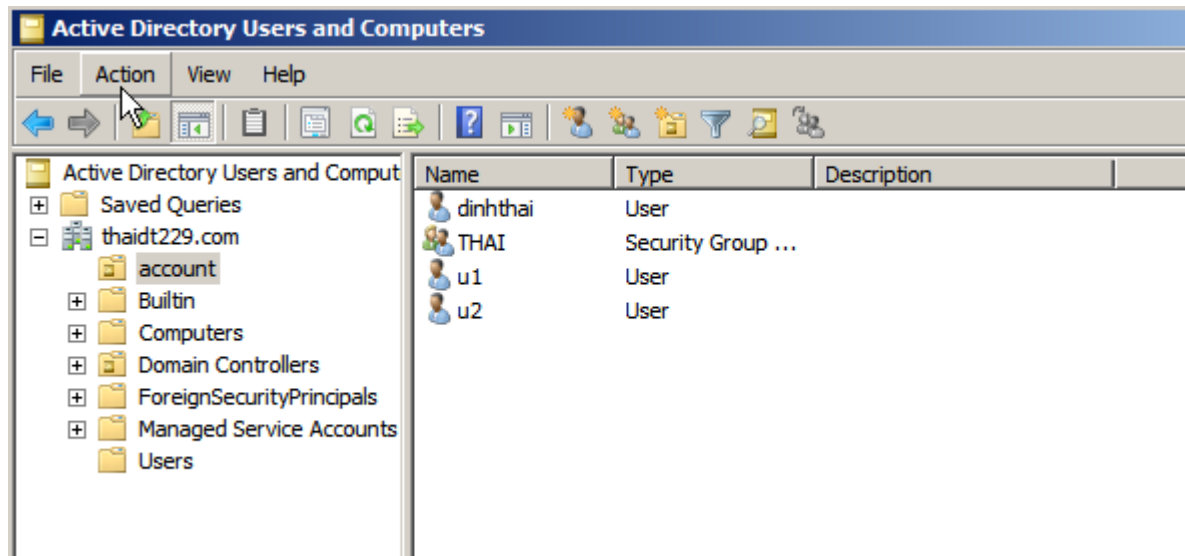
Thêm User vào OU vừa tạo :



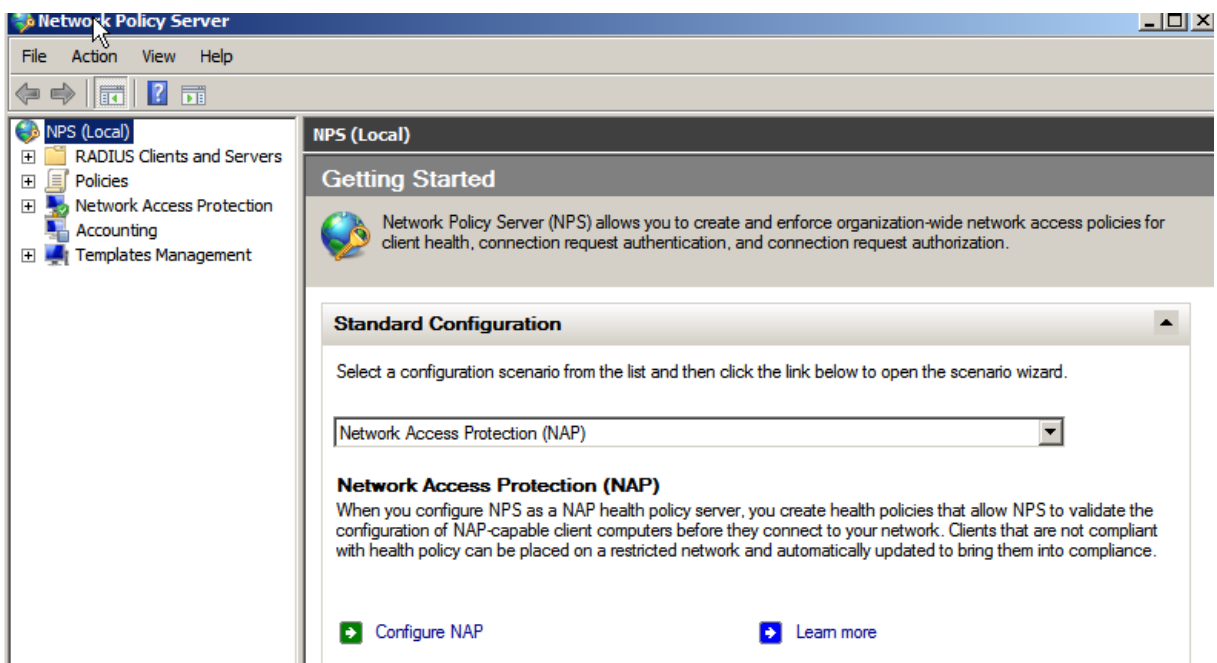


Các User vừa tạo xong :

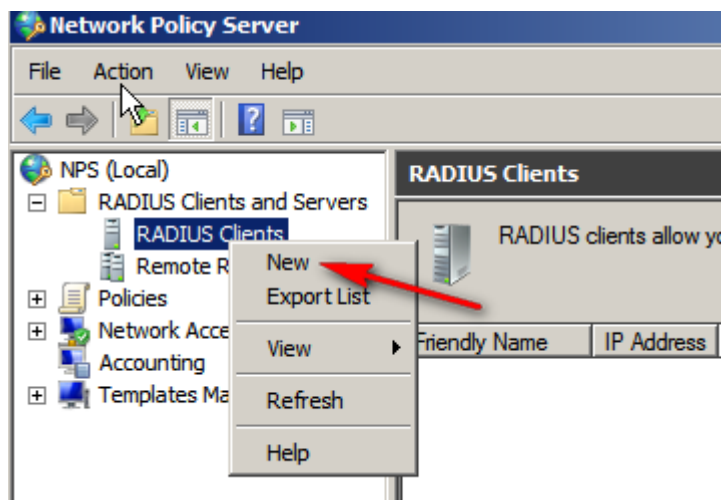
Tạo Group chứa User :



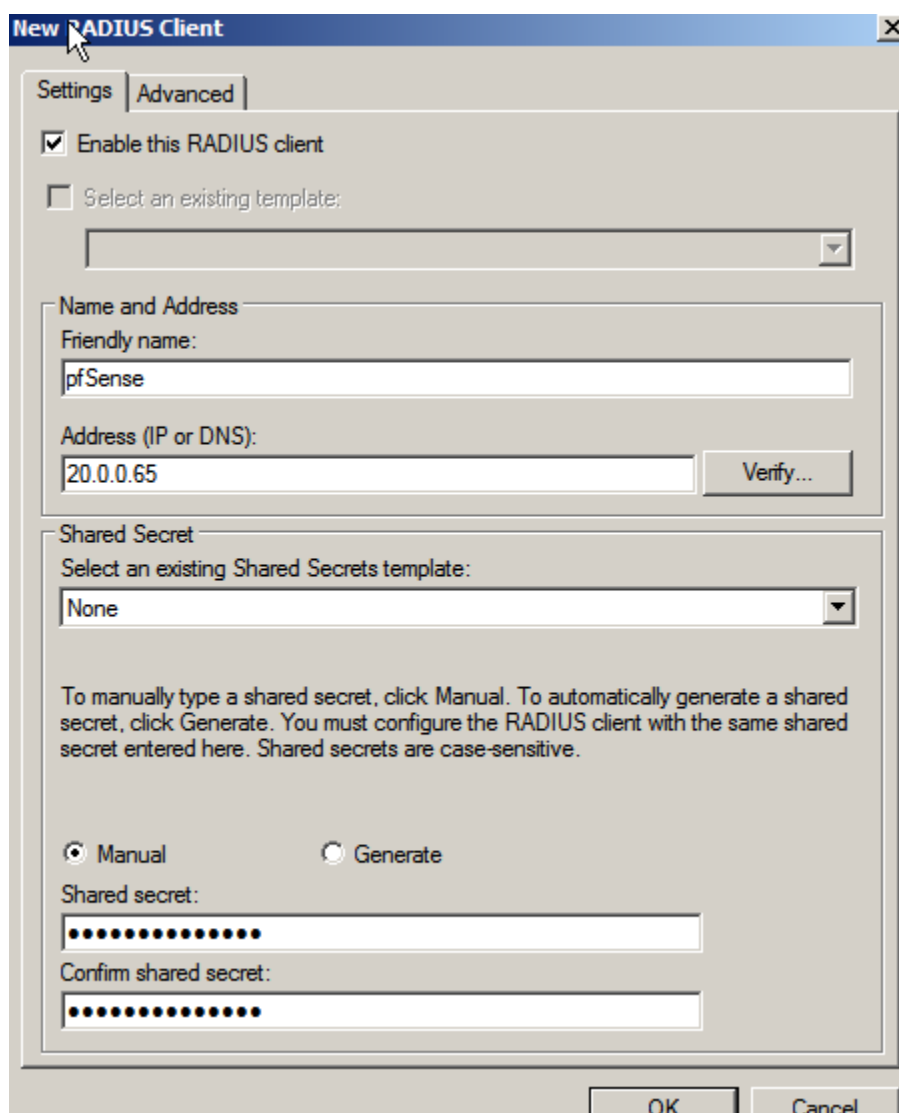
Tiếp theo ta sẽ cấu hình Radius: Start -> Administrative tool -> Network Policy Server.



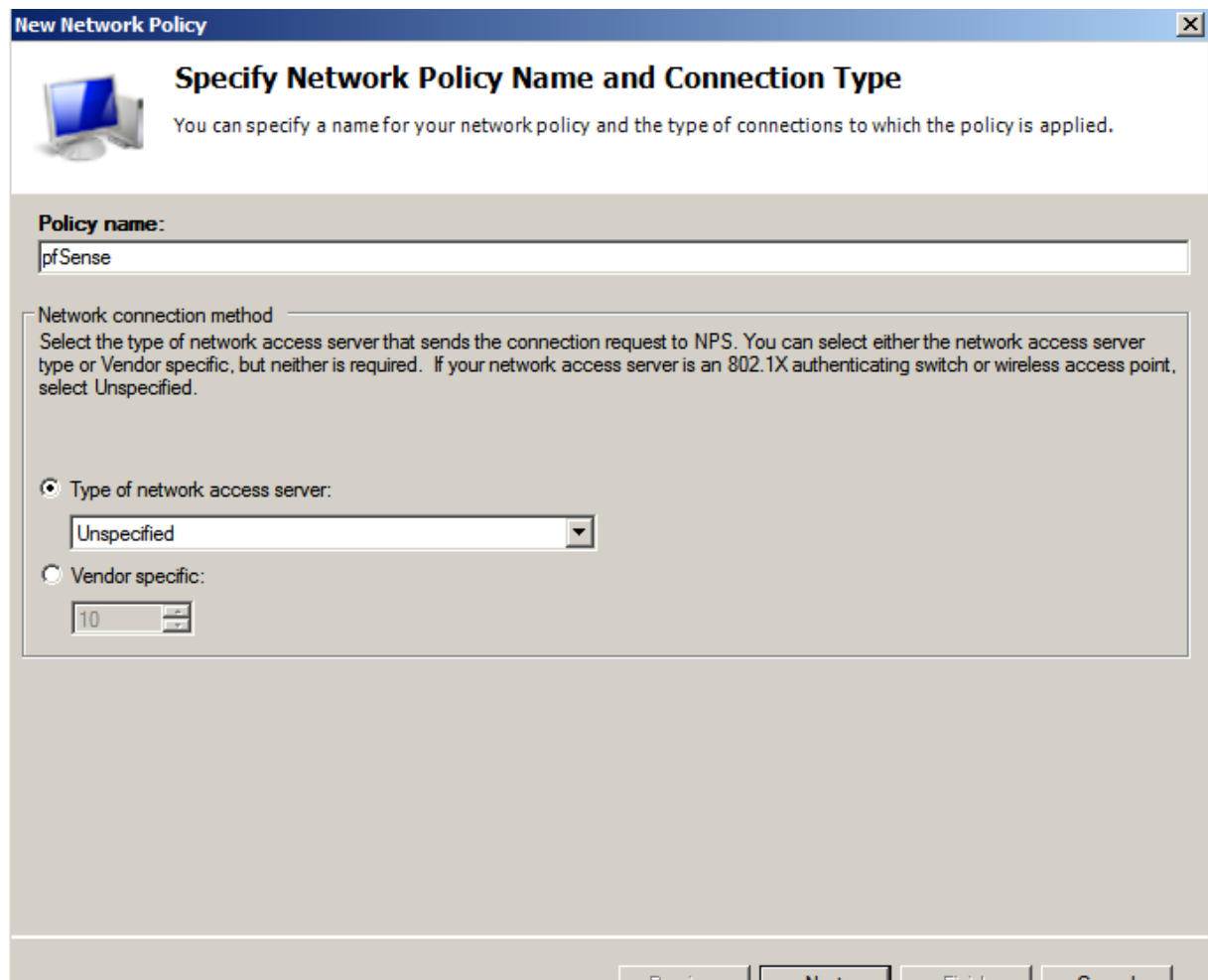
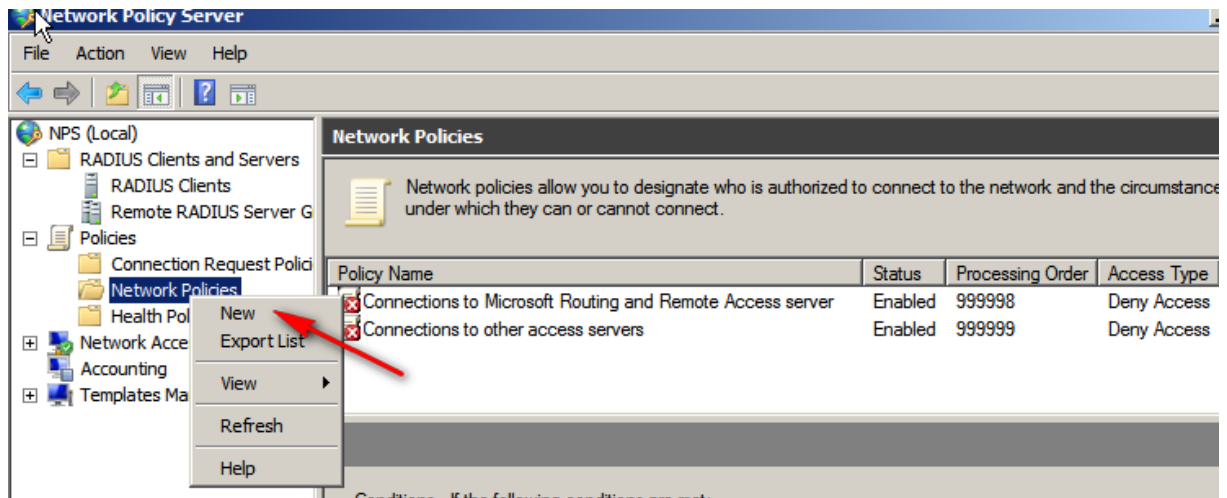
Tạo Radius Client mới :

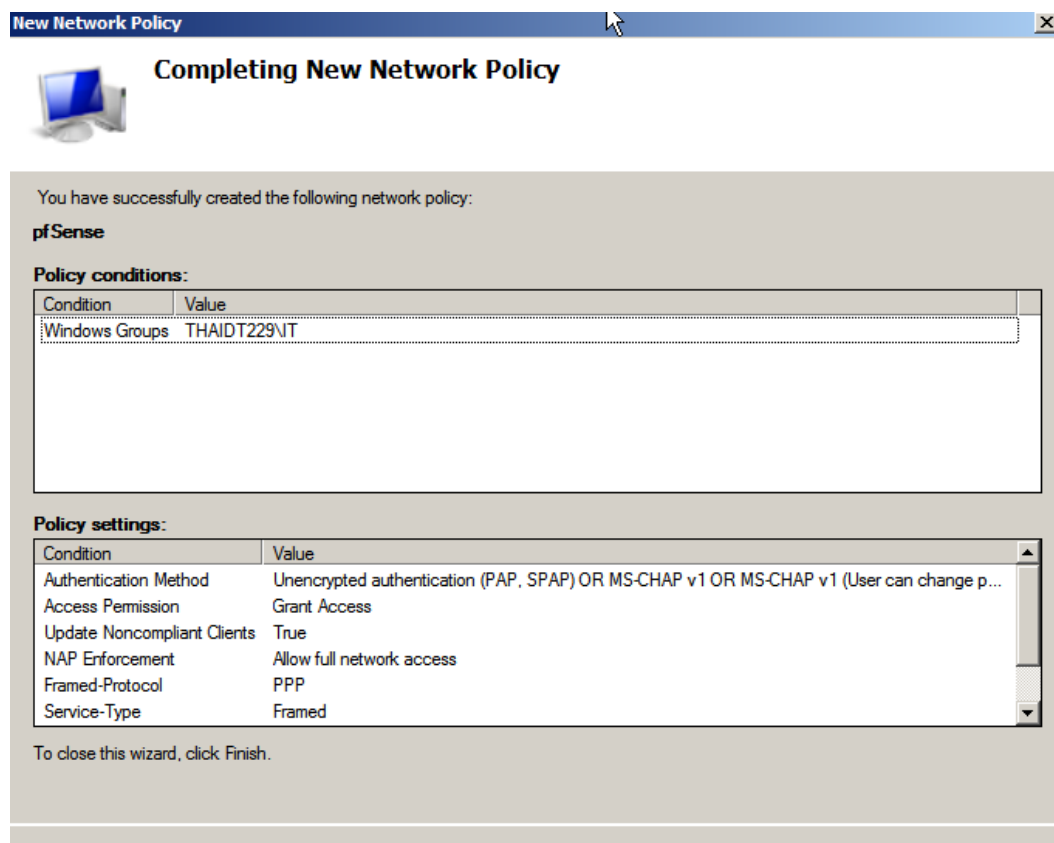
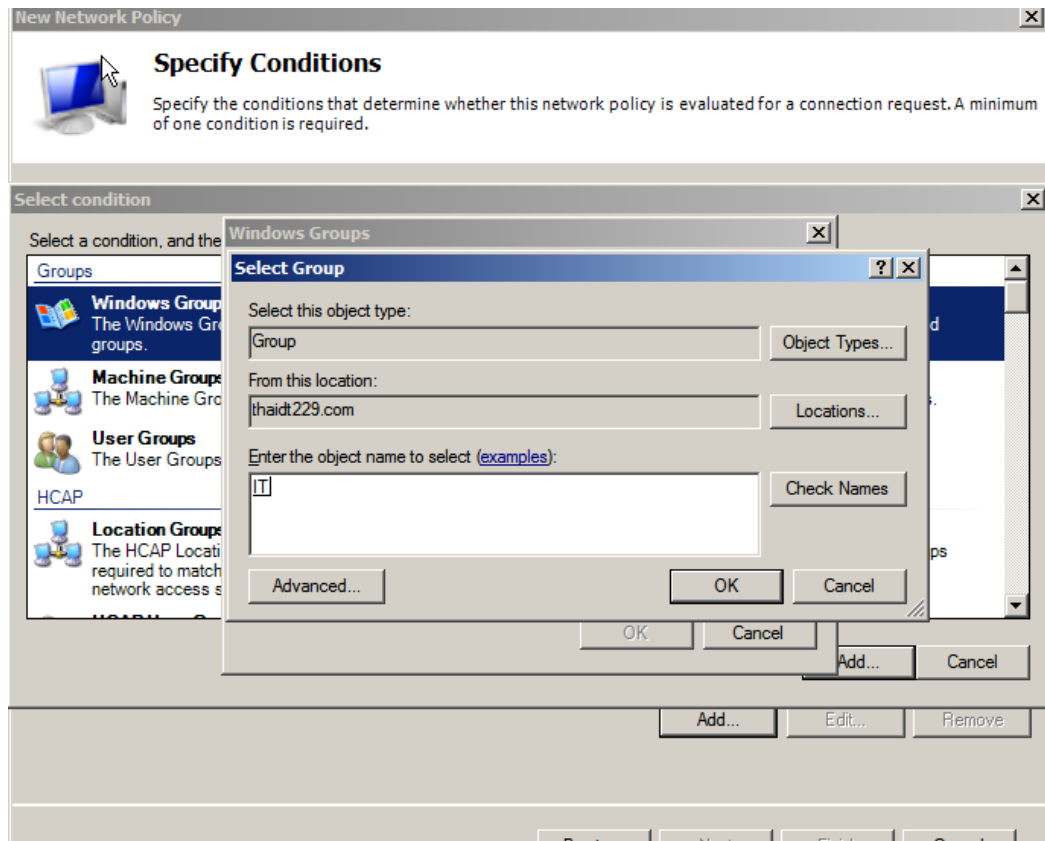


Nhập tên, IP gateway, và password



Tạo mới 1 chính sách :





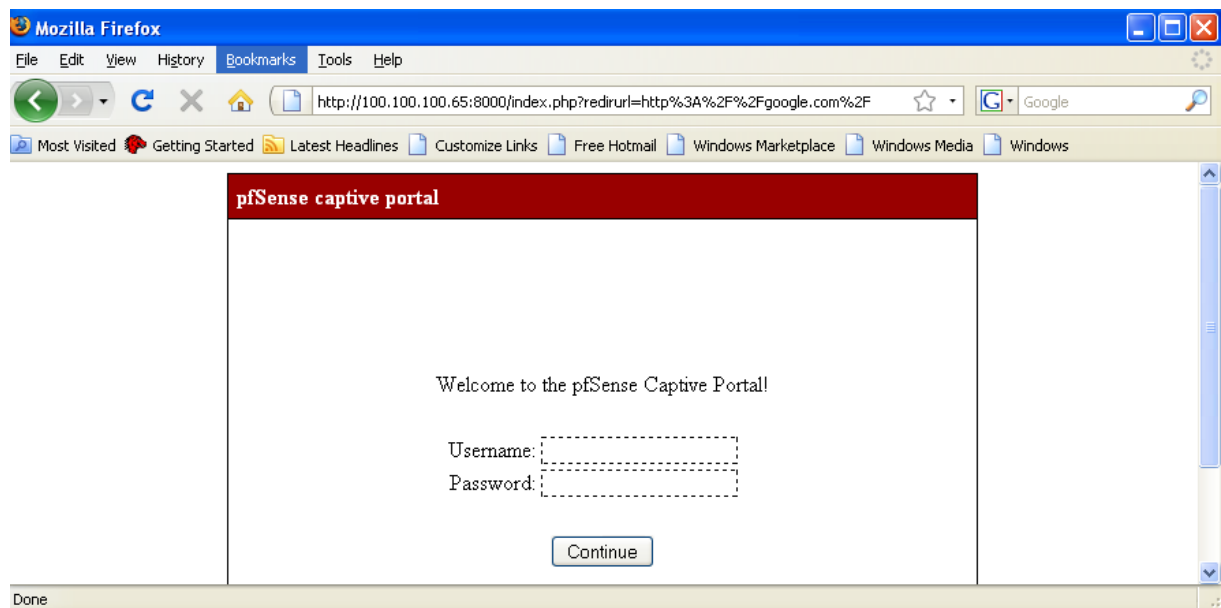
Như vậy là ta đã cấu hình hoàn thành Radius server, kế tiếp ta trở lại mục Captive portal bên pfsense để cấu hình Radius vào :

The screenshot shows the pfSense captive portal configuration interface. The browser address bar indicates the URL is 192.168.0.65/services\_captiveportal.php. The navigation menu includes System, Interfaces, Firewall, Services, VPN, and Status. The main content area is titled 'Authentication' and contains the following settings:

- Authentication:** Three radio buttons are present: 'No Authentication', 'Local User Manager / Vouchers', and 'RADIUS Authentication' (which is selected).
- Primary RADIUS server:**
  - IP address:** A text field containing '20.0.0.64'. Below it, a note states: 'Enter the IP address of the RADIUS server which users of the captive portal have access to.'
  - Port:** A text field containing '1812'. Below it, a note states: 'Leave this field blank to use the default port (1812).'
  - Shared secret:** A text field containing 'truongdinhthai'. Below it, a note states: 'Leave this field blank to not use a RADIUS shared secret (not recommended).'

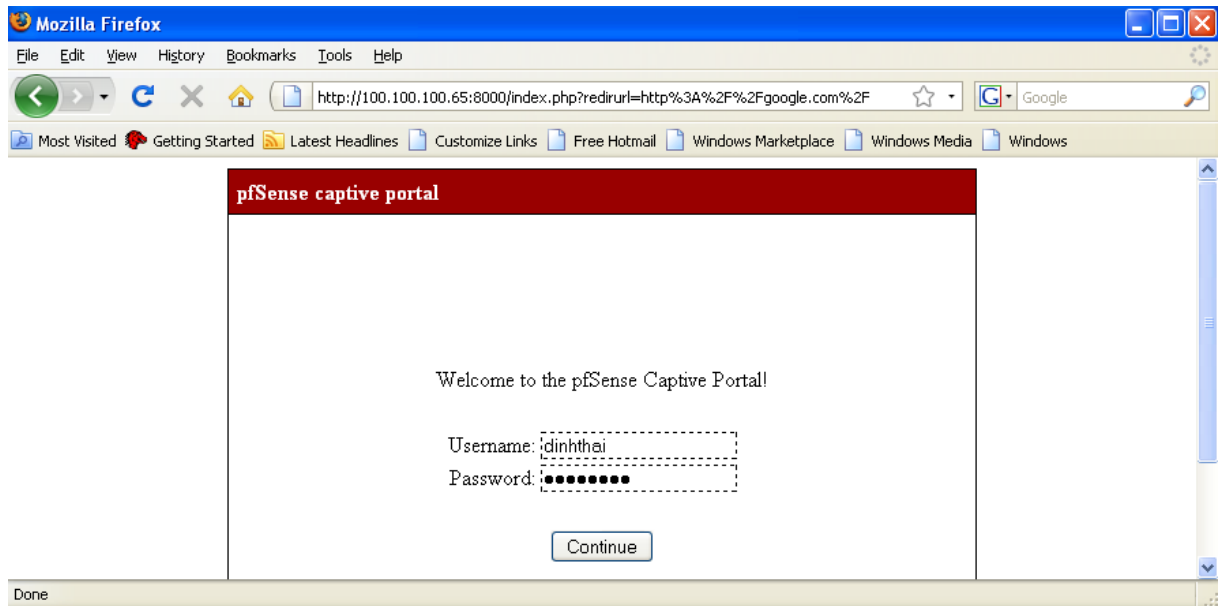
### 3.2.7. Kiểm tra hoạt động

Như ta đã cấu hình từ đầu. Bây giờ là phần kiểm tra hoạt động của Captive portal. Khi thực hiện, ta nên mở ứng dụng Wireshark lên để bắt các gói tin biểu hiện của tiến trình chuyển hướng. Ta sẽ sử dụng một máy laptop hoặc bất cứ 1 thiết bị di động nào có thể bắt wifi và có hỗ trợ trình duyệt web. Mở trình duyệt web lên gõ địa chỉ bất kì. Ta sẽ gõ vào username và password tương ứng với user khi này đã tạo trên máy chủ pfSense.

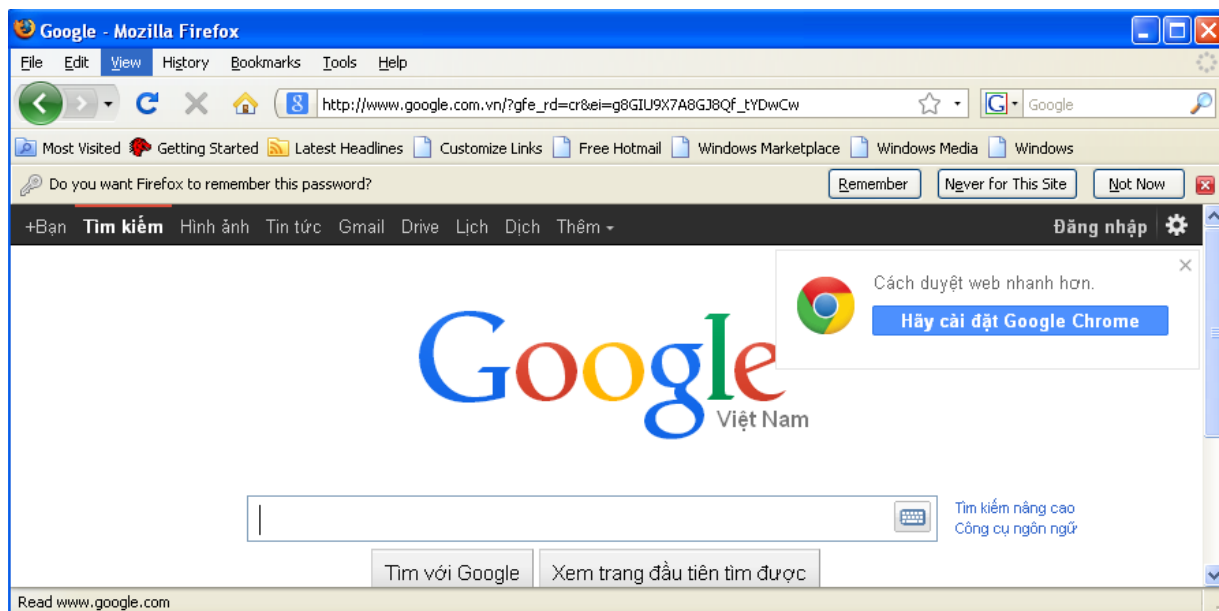


Tiếp đến, nếu cấu hình chính xác thì pfSense Captive portal sẽ tự động điều hướng ta đến trang web khi này mà ta đã truy cập đến.

Nhập user tạo bên Radius Server :



Đăng nhập thành công :



Kiểm tra file Log trên pfSense :

10.0.0.65/status\_captiveportal.php

Các tab mới đóng Facebook Tệp - OneDrive BongdaPlus ipSpace.net Hacking Cisco VIRTUALRACK CCIE TO BE CISCO Dreamer

pfSense System Interfaces Firewall Services VPN Status Diagnostics Help pfSense.localdomain

**Status: Captive portal (1)**

IP address	MAC address	Username	Session start
100.100.100.103	00:0c:29:44:f7:83	dinhthai	05/30/2014 17:36:03

Show last activity